LISBON
OCTOBER 10-13

ISMS 2022

Conference of the International Society of Military Sciences

Promoting Peace and Security in a new incomprehensible and non-linear world

INSTITUTO UNIVERSITÁRIO MILITAR
MILITARY UNIVERSITY INSTITUTE OF PORTUGAL

Book of Abstracts
(2nd Edition, revised)

Coordinators:
Lieutenant Colonel Cristina Fachada
Captain Coelho Gil
Commodore Ramalho Marreiros

MILITARY UNIVERSITY INSTITUTE OF PORTUGAL

Book of Abstracts
ISMS 2022 Conference of the
International Society of Military Sciences
(Lisbon, October 10-13)
(2nd edition, revised)

Coordinators
Lieutenant Colonel Cristina Fachada, PhD
Captain Coelho Gil, PhD
Commodore Ramalho Marreiros, PhD

Scientific Commission and Submission Reviewers
(Working Group [WG][1] Chairs)

WG1:   Marzena Żakowska, PhD (Poland), assisted by Marco Marsili, Dr. (Portugal)
WG2:   Art Johanson, MA (Estonia)
WG3:   Hannu Kari, PhD (Finland) and José Borges, PhD (Portugal)
WG4:   Peter Olsthoorn, PhD (Netherlands)
WG5:   Daniel Sommers, J.D. and Afton David, J.D. (Canada)
WG6:   Laurenz Furst, Dr. (Austria)
WG7:   Rene Moelker, Dr. (Netherlands)
WG8:   Markus Gauster, Dr. (Austria), assisted by Ugurhan Berkok, PhD (Canada)
WG9:   Nuno Loureiro, Mr./LCol. (Portugal)
WG10: Dirk Heinzmann, Mr./LCol. (Austria)

IUM Research and Development Center
August 2022

The publication ***IUM Actuality*** aims to publish electronically on the IUM website, essays or opinion articles on current security and defense topics, as well as works on relevant topics and of added value for the Institute's praxis, preferably authored by IUM professors. researchers from CIDIUM or other national or foreign researchers, at the invitation of the Director or on his own initiative.

Published numbers:

1. Intervenção Militar Francesa no Mali – Operação SERVAL (abril de 2014)

> Tenente-coronel de Infantaria Pedro Ribeiro
> Major de Infantaria António Costa
> Major de Infantaria Hugo Fernandes

2. A Aviação Estratégica Russa (dezembro de 2014)

> Coronel Técnico de Manutenção de Armamento e Equipamento José Mira

3. A Crise na Ucrânia (março de 2015)

> Tenente-coronel de Engenharia Leonel Martins (Coord.)
> Tenente-coronel Navegador António Eugénio (Coord.)

4. A Dissuasão Nuclear na Europa Central (outubro de 2015)

> Coronel Técnico de Manutenção de Armamento e Equipamento José Mira

5. Afeganistão treze anos depois (fevereiro de 2016)

> Tenente-coronel Técnico de Informática Rui Almeida

6. O Aviador do Futuro: evolução expectável e possíveis contributos da Internet das Coisas (IoT) (abril de 2016)

> Coronel Piloto Aviador António Moldão

7. (Versão Portuguesa)
Regras e Normas de Autor no CIDIUM: Transversais e Específicas das Várias Linhas Editoriais (julho de 2017)

> Coronel Tirocinado Lúcio Santos
> Major Psicóloga Cristina Fachada

7. (Versão Inglesa)
CIDIUM Publication Guidelines: General and Specific Guidelines of the IUM (novembro de 2017)

> Coronel Tirocinado Lúcio Santos
> Major Psicóloga Cristina Fachada

8. Capacidades balísticas no território de Kaliningrado (dezembro de 2017)

> Coronel Técnico de Manutenção de Armamento e Equipamento José Mira

9. O processo estratégico do poder financeiro internacional para a defesa do interesse nacional (junho de 2018)

> Professora Doutora Teodora de Castro

10. Armas "proibidas": O caso dos lasers cegantes (julho de 2018)

> Coronel (Res) José Carlos Cardoso Mira

11. A "nova" república da Macedónia do Norte: significado geopolítico e geoestratégico (agosto de 2018)

> Tenente-coronel (GNR) Marco António Ferreira da Cruz

12. Mobilidade no espaço da CPLP: Desafios securitários (setembro de 2018)

> Major de Artilharia Pedro Alexandre Bretes Ferro Amador

13. A crise dos migrantes e refugiados no espaço Europeu. Contributos do instrumento militar (novembro de 2018)

> Major de Engenharia João Manuel Pinto Correia

14. *NATO after the Brussels Summit. An optimistic perspective* (novembro de 2018)

> Tenente-coronel de Infantaria Francisco Proença Garcia

15. John McCain: o militar que serviu a América e deixou um exemplo ao mundo (dezembro de 2018)

> Major de Artilharia Nuno Miguel dos Santos Rosa Calhaço

7. (2.ª edição, revista e atualizada) Regras e Normas de Autor no IUM (janeiro de 2019)

> Major Psicóloga Cristina Paula de Almeida Fachada
> Capitão-de-fragata Nuno Miguel Brazuna Ranhola
> Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

Editor's Note:
The text / content of this publication is the sole responsibility of its authors.

Index

General introduction

The International Society of Military Sciences (ISMS) "is a free association of the highest level of military education institutions in small democratic countries. These are typically defence universities with a mandate for generating, curating, and disseminating knowledge of military sciences" (ISMS, 2022)[1]. The member organizations are the Austrian National Defence Academy, Baltic Defence College, Royal Military College of Canada, Royal Danish Defence College, Finnish National Defence University, Netherlands Defence Academy, Norwegian Defence University College, Swedish Defence University, War Studies University of Poland and Military University Institute of Portugal (ISMS, 2022).

Portugal, through its Military University Institute [Instituto Universitário Militar, IUM], has been part of this organization since 2019, having assumed the annual presidency in October 2021 (with Commodore João Marreiros as the President of the ISMS Council and Captain João Gil as the Conference Chair; both from the IUM). From October 10 to 13 of 2022, IUM will host, in its facilities, the 14th Annual Conference of the ISMS, as shown in Figure 1.

International Society of Military Sciences
Annual Conference 2022
"Promoting Peace and Security in a new incomprehensible and non-linear world"
A Hybrid Conference
10-13 October 2022
Military University Institute of Portugal
Lisbon, Portugal

President: Commodore Paulo Marreiros, Portuguese Military University Institute of Portugal

Past president: Dr. Harry Kowal, Royal Military College of Canada

President-elect: Dr. Niels Bo Poulsen, Royal Danish Defence College

Conference Chair: Captain Coelho Gil, Portuguese Military University Institute of Portugal

ISMS Secretary: David Last, Royal Military College of Canada, info(a)isofms.org

Council Members	Working Group Chairs
Austria: Wolfgang Peischel, Brigadier General, Doctor, Austrian National Defence Academy.	**WG1:** War Studies, Marzena Zakowska, War Studies University Poland, assisted by Marco Marsili, Military University Institute of Portugal.
Baltic Defence College: Zdzislaw Sliwa, Doctor, Baltic Defence College.	**WG2:** Military History, Art Johanson, Estonia.
Canada: Harry Kowal, Principal, Royal Military College of Canada.	**WG3:** Military Technology, Hannu Kari, Finland, and José Borges, Portugal.
Denmark: Niels Bo Poulsen, Professor, Doctor, Royal Danish Defence College.	**WG4:** Leadership, command, and basic competences, Peter Olsthoorn, Netherlands.
Finland: Hannu Kari, Director of Research, Finnish National Defence Academy.	**WG5:** Law and ethics, Daniel Sommers and Afton David, Canada.
Netherlands: Alexander Bon, Professor, Doctors, Netherlands National Defence Academy.	**WG6:** Security and defence policy, Laurenz Furst, Austria.
Norway: Anders McD Sookermany, Lieutenant-Colonel, Doctor, Norwegian Defence University College.	**WG7:** Armed Forces and Society, Rene Moelker, Netherlands.
Poland: Ryszard Szpyra, Dean, Professor, War Studies University.	**WG8:** Defence Management and Economics, Markus Gauster, Austria, assisted by Ugurhan Berkok, Canada.
Portugal: Paulo Marreiros, Commodore, Military University Institute of Portugal.	**WG9:** Military Education, Nuno Santos Loureiro, Military University Institute, Portugal.
Sweden: Stefan Silfverskiold, Commander, Chairman of Research and Education Board, Swedish Defence University.	**WG10:** Strategy, Dirk Heinzmann, Austria.

Figure 1 - ISMS Annual Conference 2022' members

---

[1] International Society of Military Sciences (ISMS) (2022). *Member Institutions*. Retrieved from https://www.isofms.org/member-organizations

In line with this, the present publication includes 162 *Extended Abstracts*[2], corresponding to 97% of the total amount (N=167) that were submitted to the ISMS 2022 and that will be presented in the Conference.

These *extended abstracts* – organized in the WG they related to – include, in addition to the text and the keywords, the author(s) name, affiliation, country and email address (as the author' indicated in the EasyChair platform), and, in most cases, the references used/suggested by the author(s). Also, in the upper left corner of the first page of each extended abstract, the submission number given automatically by the EasyChair platform is included.

Authors who wish to submit the article associated with the *extended abstracts* to the *Portuguese Journal of Military Sciences* – a double-blind peer-reviewed international journal, published in two versions (a digital version, bilingual, Portuguese and English, and a printed version) –, should comply with the *Call for Papers* and *IUM Author Guidelines,* both available at Call for papers – Portuguese Journal of Military Sciences (ium.pt) and IUM Author Guidelines_4th edition, revised and updated.pdf.

We wish you an enjoyable and interesting reading.

IUM, Portugal, 15 of August 2022

<div align="right">

The coordinators,

LCol. Cristina Fachada
Capt. Coelho Gil
Cdre. Ramalho Marreiros

</div>

---

[2] These *extended abstracts* are ordered by working groups and, in each of them, by their presentation order at the Conference.

WG1 – War Studies

Environment-disaster-conflict trinomial: a study of the concepts of resilience for peacebuilding in the *Anthropocene*

H. Júnior (1) and A. Rosinha (2)

(1) University of Vigo (Spain) and IUM/CIDIUM (Portugal), handradejunior@gmail.com
(2) IUM/CIDIUM, Portugal, rosinha.ajpe@ium.pt

Anthropocene has been considered a geological period of high risk due to the indiscriminate use of natural resources and the lifestyle taken by the world population, to the detriment of ecosystem conservation. The problem requires a transdisciplinary scientific approach due to its complexity. As a contribution to studies in the anthropocene, this article aims to add resilience to the peacebuilding and show its potential in the integrated response of the different systems or levels of analysis. This approach can find a favorable echo in the study on the levels of complexity of resilience, to mobilize and succeed in situations of disasters-conflicts. We discuss some aspects for integrative modeling and an holistic understanding of the individual, community or nation factors that can provide a more relevant and integrative perspective on resilience for peacebuilding in a disaster context. The contributions of resilience thinking to peacebuilding are in the possibility of navigating in holism, systemic theory and complexity theory (De Coning, 2016). Such theories consider people as inserted in complex relationships, with structures, causes and processes that are seen as non-linear. It also encompasses the view that societies are in a state of constant flux. A key implication of nonlinearity and complexity is that we cannot identify general laws and, therefore, the prediction of future events and patterns of transformation of the system becomes impossible. Another aspect is that the complex nature of contemporary conflicts requires a systemic understanding that goes "beyond past project-oriented approaches and silos" towards the transformation of entire systems or regimes. Resilience, therefore, encourages an integrated or comprehensive approach to the crisis: resilience means bridging short-term humanitarian intervention and long-term capacity building (Juncos & Joseph, 2020). Resilience has the potential to move the peacebuilding field from a series of one-off, technical and project-oriented interventions to a more systemic approach to address the root causes of conflict. Complexity and diversity are also relevant to the analysis and understanding of situations affected by conflicts, because they consider other perspectives and the perspective of the "other". Disasters that affect societies whether man-made or of natural origin create great difficulty and adversity for their populations. For a society to be well prepared for adverse situations, disasters or emergencies, it is important to mobilize populations and create the conditions to prepare them by disseminating information and raising awareness, and by providing training, resources, infrastructure or concrete leadership actions. Preparing for and anticipating the impact of disasters and conflict early on can minimize or even eliminate their costs and consequences. It is essential to help people return to normalcy as soon as possible or, if necessary, to help them rebuild their lives with as few scars as possible. Portugal has been hit by increasingly frequent serious natural phenomena. Thus, studies on resilience are urgently needed to educate the population and the country's authorities. The integration of the model by levels of resilience, from the most elementary to the most complex, invokes a set of disciplines to address the issues emerging from the problems of natural disasters as catastrophes and environmental crises, which influence the development and economic stability of the countries involved, the institutional, social, individual and material losses they suffer. The integration of knowledge and the parties involved also raises a transdisciplinary approach (Nicolescu, 2002; Klein, 2015) to the complex treatment of the related problems. The concept of resilience applied to peacebuilding, "resilient peacebuilding" is a construction based on holistic and systemic theories in the transdisciplinarization phase, with the potential for applicability as a "pacifying" transdisciplinary action. In addition, our *Integrative Model towards Resilient Peacebuilding in Disaster Context* (IMtRPinDC) proposed here encourages military educators, and others working to support the outcomes of individuals, to move their focus away from identifying levels of resilience for those individuals towards considering a range of environmental, relational and psychological factors which impact on individuals and groups of people in a dynamic way.

KEYWORDS

Peacebuilding; National resilience; Community resilience; Community mobilization; Complexity; Anthropocene.

Hobbesian Wars in the 21st Century: the Failure of the International Security Governance and Lessons Learned from the Russo – Ukrainian War

H. Mölder (1)

(1) Tallinn University of Technology, Estonia, hmolder62@gmail.com

The international system has become increasingly unstable after 9/11 terrorist attacks in New York and Washington, followed by the Iraqi intervention of 2003. Besides challenges to the status quo of the international system from revisionist powers, primarily from Russia and China, the present international political and security environment has been strongly influenced by various anti-establishment movements from alternative left to alternative right, which became more visible in the 2010s with the anti-migration movement in Europe, the Brexit process (UK) and Trumpism (US). The surprisingly powerful return from cooperative security trends to the concept nation-state as the major actor expected to be able to tackle such challenges have appeared in the United States (America first policy), Russia (military invasion against Ukraine), China (under the ambitious plans to become a major economic power). These revisionist challenges to the international system led to the abandonment of the principles Kantian political culture that the international system adapted in the 1990s, after the Cold War ended and instead of the Kantian principles of collective security and security community, the international system is moving further on towards Hobbesian enmity and Lockean rivalry (Wendt 1999; Frederking 2003; Mölder, & Sazonov 2018).

There appear new environments vaguely internationally regulated (cyber, space) which significantly extend the area of potential hostilities. Influence operations can effectively shape perceptions and misperceptions among public audiences, whose attitudes and preferences can in turn aggregate to elites and political processes, shaping political decision-making. The modern Hobbesian challenge is much about the Global Knowledge Warfare (GKW) (Mölder, Shiraev 2021) relies on intangible virtual weapons like strong emotions (e.g. fear, anger, and honor), myths, and beliefs able to manipulate with (dis)information.

The Hobbesian challenge based on strategic ambitions to follow national interests above all was strongly advocated by the President of Russian Federation Vladimir Putin, who on 10 February 2007 at the Munich Security Conference presented challenge to the United States and NATO, which allegedly did not take into account the security guarantees given to Russia (the Soviet Union) after the Cold War. Putin interpreted NATO in the Hobbesian terms as an expansionist alliance with aggressive strategic ambitions against the Russian Federation. In the following years Russia has vigorously strengthen the Hobbesian rhetoric in its strategic narratives against NATO, the European Union, the West and US. The war against Georgia in 2008 and against Ukraine since 2014 have pursued the strategic goals of the status conflict against the West (Renshon 2017; Murray 2019). On 24 February 2022 the conflict in Ukraine has been escalated into a full-scale war, which refers to Russia's ambition to restore warfare (called a special military operation in Ukraine) as a proper way how states interact each other, which is changing Kantian patterns to Hobbesian ones.

There are several issues that would characterize the Hobbesian wars of the 21st century. First is the failure of international security governance and international crisis management to efficiently prevent wars and initiate peace negotiations. The International organizations found to be in effective in holding crisis management process. OSCE failed to prevent war escalations in Ukraine and Nagorno-Karabakh. The United Nations was not able to take a lead in conflict resolution in Ukraine, which refers to the significant failure of international security governance to manage international security crises in a changing security environment. The goal of revisionist challengers is to change patterns of behavior by which the international system operates and, in this respect, challengers to the post-Cold War Kantian system met a certain success.

KEYWORDS

International conflict management; International system; Political cultures; War in Ukraine.

REFERENCES

Adler, J.M., & McAdams, D.P. (2007). Time, Culture, and Stories of the Self. *Psychology Inquiry, 18*(2), 97-128. Retrieved from https://www.sesp.northwestern.edu/docs/ publications/1394533777469664904db9f.pdf

Frederking, B. (2003) Constructing Post-Cold War Collective Security. *American Political Science Review, 97*(3), 363-378. doi:10.1017/S0003055403000741

Murray, M. (2019) *The Struggle for Recognition in International Relations. Status, Revisionism, and Rising Powers*. Oxford: Oxford University Press

Mölder, H., & Sazonov, V. (2018). Information Warfare as the Hobbesian concept of Modern Times – Principles, Techniques and Tools of Russian Information Operations in Donbass. *The Journal of Slavic Military Studies, 31*(3), 308−328. doi: 10.1080/13518046.2018.1487204.

Mölder, H., & Shiraev, E. (2021) Global Knowledge Warfare, Strategic Imagination, Uncertainty and Fear. In: Mölder; H., Sazonov, V., Chochia, A., & Kerikmäe, T. (Eds.) *The Russian Federation in Global Knowledge Warfare - Influence Operations in Europe and Its Neighbourhood*. Springer Nature.

Renshon, J. (2017) *Fighting for Status: Hierarchy and Conflict in World Politics*. Princeton University Press.

Wendt, A.(1999). *Social Theory in International Politics*. Cambridge: Cambridge University Press.

Space: The Final Frontier of War?

M. Marsili (1)

(1) CIDIUM/Instituto Universitário Militar, Portugal. info@marcomarsili.it

Iconic films such as *Star Wars* (1977) and *Starship Troopers* (1997) picture conflicts fought in outer space. *UFO* (1970) tells the story of a high-tech military organization established to defend Earth from space attack. *Space: 1999* (1975) and *Star Trek* (1966) are about travelling in deep space where no man has "bodly" gone before and imagine a technology that does not exist. Sometimes science fiction, inspired by science possibilities that one day can come true, simply imagines the future. Military applications of space technology, and considerations on space as a future theater of war when they would become technologically possible, were outlined in the *Introduction to Outer Space*, a pamphlet edited by the White House in 1958.

To avoid the militarization of space and celestial bodies, and to guarantee their exploration and use for peaceful purposes to all countries, in 1967 the US, the U.K. and the Soviet Union opened for signature the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, which has become customary international law (White, 2000). The Outer Space Treaty forbids from placing in Earth orbit weapons of mass destruction, including nuclear weapons, or otherwise stationing them in outer space, but does not prohibit the placement of conventional weapons, and thus some highly destructive attack strategies such as kinetic bombardment are still potentially allowable (Bourbonniere & Lee, 2007).

Since 1984, the Conference on Disarmament (CD), a body established by the UN General, has considered proposals, including draft treaties, aimed at preventing the placement of weapons in outer space. In 1998 Russia and China proposed a Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT). An amended text drafted in 2014 was rejected by the US because it failed to address a series of relevant issues: it did not provide a definition of "outer space" neither of what constitutes a "weapon in outer space", and it did not ban terrestrially-based ASAT systems launched from the ground (CD, 2014; UNGA GA/DIS/3591; Plath, 2018).

The US refused to negotiate a Proposed Prevention of an Arms Race in Space (PAROS) treaty as an international legally binding instrument in the CD, as Washington gathers that it simply mirrored the PPWT, including its failures. Therefore, the US voted against the Russian's No First Placement of Weapons in Outer Space (NFP) resolution (UNGA, A/C.1/72/L.53). So far, the international community failed to reach a solution to prevent an arms race in outer space. Space war is no more a science-fiction scenario; it's an emerging reality.

KEYWORDS

REFERENCES

Bourbonniere, M., & Lee, R.J. (2007). Legality of the Deployment of Conventional Weapons in Earth Orbit: Balancing Space Law and the Law of Armed Conflict. *European Journal of International Law 18*(5): 873901. doi: https://doi.org/10.1093/ejil/chm051.

Conference on Disarmament (2014, June 12). *PPWT Draft Treaty, CD 1985*.

Conference on Disarmament (2014, Sept. 3). *Analysis of the 2014 Russian-Chinese PPWT draft treaty (CD/1985)*. CD/1998.

Esper, M.T. (2019, Aug. 2). *The United States has withdrawn from the INF Treaty effective today*. U.S. Department

Plath, C. (2018, Dec. 5). *Explanation of Vote in the First Committee on Resolution: L.50, "No First Placement of Weapons in Outer Space"*. U.S. Department of State. Retrieved from https://www.state.gov/t/avc/rls/287137.htm.

Pompeo, M.R. (2020, May 22). *On the Treaty on Open Skies*. U.S. Department of State.

The White House (Ed.) (1958). *Introduction to Outer Space. An explanatory Statement Prepared by the President's Science Advisory Committee*. Washington, DC: Superintendent of Documents, U.S. Government Printing Office.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, opened for signature at London, Moscow and Washington on January 27, 1967, entered into force on October 10, 1967.

UN General Assembly, First Committee on Disarmament and International Security (2017. Oct. 12). *No first placement of weapons in outer space*, UN document A/C.1/72/L.53, 17-18074.

UN General Assembly (2017, Oct. 30). *First Committee Submits Six Drafts to General Assembly, One Calling for Immediate Start of Negotiations on Treaty Preventing Outer Space Arms Race*, GA/DIS/3591.

White, W. (2000). The Legal Regime in Private Activities in Outer Space. In: E.L. Hudgins, & D. Boaz. (Eds.), *Space: The Free-Market Frontier* (pp. 83-124). Washington, DC: Cato Institute.

The Challenge of Hybrid Warfare ³

J. Schmid (1)

(1) Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr(ZMSBw), Germany, schmid@ifsh.de

Empowered by globalization and new technologies and inspired by the "promise"/perception of unpretentious political success at supposedly manageable military risk and political cost, it can be expected, that the future of war to a large degree will be hybrid warfare.

As demonstrated on the Ukrainian battlefield, for example, or by the so-called Islamic State in Syria and Iraq in a different empirical manifestation, hybrid forms of warfare appear to offer unpretentious political success by smart recourse to a limited, deniable and supposedly manageable use of force. They are conducted on extended and interconnected multidomain battlefields: From the battlefield of ideas and ideologies and the fight for the "hearts and minds" of the people to the field of economic and financial pressure, from the diplomatic parquet to the military battlefield, not forgetting about the competitive spaces of information, law, technology, norms, values and psychological sentiment and many more. In this sense hybrid warfare creatively combines different battlefields on multiple domains through multi vector attacks and by the dynamic use of multi- and cross-domain operations. Therefore, hybrid warfare may appear as "mosaic warfare" on interconnected multidomain battlefields.

Hybrid warfare may go along with the assumption that the risk of military escalation and political damage could be kept within limits. This assumption may at the same time increase the likelihood of its offensive use. For this reason, it is more than likely that multidomain hybrid shadow-warfare in its various manifestations will shape the 'face of war' in the twenty-first century. It is particularly challenging that it clearly offers offensive options in particular. However, the assumption that the use of force and the risk of escalation could be kept limited, and political damage manageable, might be misplaced, as uncertain-ties, friction and the tendency to go to extremes are essential characteristics of the nature of war. In addition, hybrid methods of warfare are per se no guarantee for success, as the war in and regarding Ukraine shows.

In a different approach by adopting a silent, covert and indirect approach that fosters ambiguity and makes attribution difficult, hybrid warfare actors may achieve their political goals and change the status quo of a given political situation inconspicuously (salami tactics), or unexpectedly by surprise (fait accompli) before the victim even realizes they are under hybrid attack. The current COVID-19 crisis situation provides additional opportunities in this regard as it increases global insecurity on multiple domains, from public health to politics, from the economy to society and finally to global power politics and geostrategic confrontation.

With this in mind, it is high time that the EU, NATO and their member states improved their common and comprehensive understanding of hybrid warfare as a multidomain strategic challenge simultaneously employed on multiple interconnected battlefields. Connecting respective dots on different domains with each other is therefore essential to discover the hybrid strategies behind. Indeed, such an understanding is a precondition for joint and comprehensive action in defence and response, as well as for deterring, preventing and containing the offensive use of hybrid warfare in the first place. Building the respective analytical capabilities, and educating the judgement of political leaders and decision-makers accordingly, would naturally be the first step in countering hybrid warfare. To develop a comprehensive understanding of hybrid warfare as a creative combination and dynamic integration of different battlefields on multiple – military as well as non-military – domains with multiple and shifting centres of gravity would be a most promising starting point in this regard.

Comprehensive definition of hybrid warfare as a specific style of warfare and in contrast to 'militarycentric warfare' as its' counterpart:

Hybrid warfare is a creative act of force combining a broad spectrum of military and non-military instruments and vectors of power on an extended multi-domain battlespace – ranging from politics, diplomacy, information, economy, technology, military and society to dimensions like culture, psychology, legitimacy and morale – hile ambiguously

---

⁴ Compare: Schmid, J. (2021). Introduction to Hybrid Warfare – A Framework for comprehensive Analysis. In: *Ralph Thiele: Hybrid Warfare Future and Technologies*. Wiesbaden: Edition ZfAS, Springer VS, ix-xii, 11-32. Available at https://link.springer.com/book/10.1007%2F978-3-658-35109-0. Compare also: Schmid, J. (2019). Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence. *Sciendo: Journal on Baltic Security*, Tartu August, *5*(1), 5-15. Available at https://sciendo.com/article/10.2478/jobs-2019-0001

operating in the shadow/grey-zones of blurred interfaces – between war and peace, friend and foe, internal and external relations, civil and military as well as state and non-state actors and fields of responsibilities – with the ultimate goal to enable an own decision of the confrontation primarily on non-military centres of gravity while preventing being militarily overthrown or compelled by the enemy.

KEYWORDS

Hybrid Warfare; Multidomain Battlefields; Shadow Warfare.

The influence of private actors on the relationship between asymmetrical and symmetrical warfare

M. Häyhtiö (1)

(1) National Defense Training Association, Finland, markus.hayhtio@icloud.com

The nature of modern, contemporary conflicts involves the active involvement of private actors at different stages and in different roles of conflict. Private actors support, train, service and enable the operation of the public component of the conflict (Hammes, 2011). In this article, the author has explored how the performance of a private actor can be linked to public military service in an operating environment of asymmetric warfare In addition, it is explored what means or methods should be used as a development system for the desired performance. The purpose of this article is to show the reader that the production, development, and supply chain security of these services requires a system-wide approach.

The starting point of the study is that private actors are legal actors in a contractual relationship with the public component. The public component can be a multinational, non-profit organization, a military alliance, or a national military actor. The paper does not exclude any branch of defense or weapon type from the study. The perspective is to study, map and discuss the issues that improve the performance of private actors and the potential risks involved with their participation.

Public administration reports, open source intelligence reports and official documents have been used as sources for the study.

PRIVATE ACTORS IN CONFLICTS

Already in 2016, the annual turnover of private companies providing military services exceeded EUR 200 billion (Transparency.org, 2022). Estimated turnover by 2030 is $ 457 billion and the industry is expected to grow at an annual rate of more than 7% annually between 2020 and 2030 (asdnews.com, 2022). The figures also include non-high-risk operations and military services. These military service offerings previously include activities self-produced by military organizations, such as base support, construction, security, training and transportation services (Dunigan, 2014). In addition to activities that directly serve end-users, the role of private companies in subcontracting chains is also very important.

Reference frameworks and methods specifically in the context of asymmetric warfare that combine best practices in project management required for development and communication between the public and private parties do not exist, according to the author's observation. The situation arises, despite the fact that model of the Project Management Body of Knowledge (PMBOK) used in project management creates an operating environment that reduces the already recognized difficulties of performance development in a multi-stakeholder development environment.

The challenge in developing capabilities in an asymmetric warfare framework arises from the nature of private business together with the requirements definition processes required in operational conceptualization. In addition, coordinating different operating cultures and gathering the requirements for performance development adds challenges.

Private military and security companies operate as part of a global trading system. This global trade operates in an environment that is highly prone to disruptions and anomalies in all parts of the supply chain. Commitment to a private service provider requires a seamless service and IT infrastructure throughout the service supply chain. Although a network of different actors is a necessity for its members, it is at the same time prone to disruption and influence by means of asymmetric warfare. Yet the use of private actors is a lifeline for the modern military. Such disruptions have direct and indirect effects on all network participants.

When preparing for a possible hostile influence or considering one's own possibility to influence the goals of a hostile actor, the abilities in the following areas should be analyzed:
- Ability to generate baseline data that allows for the necessary vulnerability analysis
- The ability to store said adequate information in a manner that meets the protection requirements of all members of the supply chain
- the ability to manage a medium (human, information system) that uses valid data
- Ability to predict and create scenarios that require processed and stored data
- Ability to manage feedback information and, above all, to manage predefined activities based on scenarios (Häyhtiö, & Zaerens, 2017).

CONCLUSION

Although the development of asymmetrical and symmetrical warfare capabilities may even seem like the opposite of each other, the situation is not black and white. Continuous incremental development is essential, but at the same time broader, long-term development is needed. The use of demand-based development for symmetrical warfare needs is also possible in the development of capabilities related to asymmetric conflict.

If the above-mentioned objectives are described in the form of a requirement, it will be possible to increase the transparency of operations and provide an unambiguous method of communication between stakeholders. More precise but simple customer-centric requirements enable the development of operations without compromising the goals set in advance by each stakeholder. In addition, the utilization of requirements enables the development of leadership in areas that are essential to the end result, such as strategic management and organizational behavior.

KEYWORDS

Public Private Partnership, Private Military and Security Companies, Asymmetric Warfare, Requirements Management.

REFERENCES

ADSReports – Market Research (2020). *Private Military & Security Services Market to Total $457.3*. Retrieved from https://www.asdnews.com/news/defense/2020/02/19/private-military-security-services-market-total-4573-bn-2030

Dunigan, M. (2014). The future of US military contracting: Current trends and future implications. *Int. J., 69*(4), 510-524.

Hammes, T.X. (2011). *Private Contractors in Conflict Zones: The Good, the Bad, and the Strategic Impact*. Washington DC: National Defense Univ. Washington.

Häyhtiö, M., & Zaerens, K. (2017). A comprehensive assessment model for critical infrastructure protection. *Manag. Prod. Eng. Rev.*, 8.

Transparecy International (2016). *Private military and security companies: A call for better regulation*. Retrieved from https://www.transparency.org/en/press/private-military-and-security-companies-a-call-for-better-regulation

The impact of climate change on the threat of armed conflict

M. Palczewska (1)

(1) War Studies University, Poland, milena.palczewska@gmail.com

Climate change is having an increasingly noticeable impact on the social life of many countries. The dynamics of protests and conflicts in recent years may be proof of this. There is nothing new about it. But while droughts or floods used to be a kind of intervention of nature into the order created by man, today human intervention in nature has a feedback effect on societies.

In many places around the world, due to frequent heat and droughts devastating agriculture, increased exposure to overheating, the spread of tropical diseases or higher sea levels, it will simply be impossible to live. Due to climate change and increasingly frequent and stronger extreme weather phenomena, such as floods and hurricanes, many parts of the world will become unfriendly to life. The result will be human migrations. Such situations will repeat themselves, because people will always run to where they think it is safer and where they can lead a normal life.

Climate change can cause social conflicts and even wars, because when food and water are scarce, many of us are capable of the worst. Survival is what counts. Droughts and floods will destroy crops, so we can expect conflicts and wars in many parts of the world.

The risk of an armed conflict may be influenced by various factors: poverty, weakness of the ruling authority, large differences in income levels or competition for access to natural resources. Natural disasters caused by climate change should also be added to this list. The occurrence of a natural disaster related to climate change increases the risk of an armed conflict in ethnically diverse countries. The analysis of the convergence of wars and extreme weather phenomena over 30 years (1980-2010) showed that in 9% of cases, armed conflicts coincided with a natural disaster (SIPRI data - Stockholm International Peace Research Institute).

Summing up, it should be noted how much the ethnic diversity of countries stands out against the background of other factors, such as poverty, social inequalities or the history of armed conflicts. The related social tensions are exacerbated by weather phenomena (snowstorms, hailstorms, tornadoes, cyclones, storms), hydrological (avalanches, floods, long-term precipitation causing landslides) and climatic (severe frosts, heat waves, droughts, fires).

American research shows that in ethnically diverse countries, 23% of armed conflicts in the last 30 years took place in the same month as a natural disaster. As the average temperature on earth is likely to increase by 2-4C by 2050 compared to the 2000 average, there is the likelihood of significant modifications to patterns of interpersonal violence, group conflict and social destabilization in the future.

However, it cannot be clearly stated that climate change is increasing violence. In addition, it is worth remembering that ethnic or religious diversity alone is not a source of conflicts. Only using this diversity for political purposes and creating social divisions where they did not exist before can lead to bloodshed. The greatest ethnic diversity is found in the countries of Sub-Saharan Africa and South and Southeast Asia. They are also the regions most affected by the effects of climate change. With the increasing frequency of natural disasters, the risk increases that conflict moods in these parts of the globe will increase.

KEYWORDS

Climate; Armed conflict; Security.

Peacekeeping as a Balancing Act of Complexity

S. Paananen (1)

(1) National Defence University, Finland soili.paananen@mil.fi

The article examines how military leaders serving as peacekeepers navigate complexity and adapt to it. The theoretical underpinnings of the study are linked to adaptive peacebuilding and Complexity Leadership Theory (CLT), and specifically to how enabling leadership through adaptive space helps to work with the local conflict dynamics and change to sustain peace.

Complexity Leadership Theory is a meta-theory for adaptability (Uhl-Bien & Arena, 2018) that is needed to "meet complexity with complexity" (Ashby, 1962). Adaptability requires three leadership functions. *Operational leadership* encompasses formality, rules, standardization (Arena & Uhl-Bien, 2016) and efficiently managing routine challenges, as well as integrating innovation into formal systems (Uhl-Bien & Arena, 2017). *Entrepreneurial leadership* embraces innovation, learning, flexibility, and growth (Arena & Uhl-Bien, 2016) and creates novelty that helps adapt to pressure or capitalize on opportunities (Uhl-Bien & Arena 2017, p. 6). However, adaptability increases when both operational and entrepreneurial forms of leadership are intertwined (Uhl-Bien & Arena, 2017). *Enabling leadership* helps in this process by creating conditions for adaptive process through adaptive space (Uhl-Bien & Arena, 2018, p. 96). Adaptive space is a relational and fluid construction defined as a "network and organizational context that allows people, ideas, information, and resources to flow across the organization and spur successful emergent innovation" (Arena, Cross, Sims, & Uhl-Bien, 2017, p. 40). The adaptive process happens when "individuals and systems engage tensions between pressures for change (e.g., innovation, novelty, learning, growth) and pressures for stability (e.g., current performance, short-term results, status quo) through conflicting and connecting to generate adaptive outcomes" (Uhl-Bien, 2021, p. 1403).

Adaptive peacebuilding also acknowledges the importance of adaptation to uncertainty while encouraging a shift in the focus from ends to means and working with, not against, change to sustain peace (de Coning, 2018). As in CLT, the adaptive space is central to the adaptive and self-organization processes. It is important to give local people space and agency to engage with local communities and stakeholders and learn and innovate together (Loode, 2011). Doing so requires promoting curiosity and innovation, valuing failure and learning from mistakes, anticipating surprises, and capitalizing on crises, through experimentation and collecting feedback (de Coning, 2018). In particular, the process calls for multiple parallel interventions. Continuous iterative processes and short-cycle feedback loops aim to ensure the most effective initiatives are sustained and refined. This coevolving adaptation to local social systems fosters and sustains self-organization (de Coning, 2020). In other words, leaders facilitate and stimulate the creation of space in which the members of a community or society can collectively develop resilient self-organized systems and capacities for self-organization.

The findings are based on 29 interviews with military leaders with command experience on peacekeeping operations. The findings introduce five dimensions that unpack complexity into structural, functional, security related, professional, and steering-related complexity and provide empirical evidence on balancing actions relating to complexity in a peacekeeping context. The article develops an analytical framework for peacekeeping. It also contributes to Complexity Leadership Theory by unpacking the complexity into dimensions, unpacking the actors into groups and communities with commitments, and by addressing power relations and the dark side of their emergence.

KEYWORDS

Complexity leadership; Adaptive space; Peacekeeping.

REFERENCES

Arena, M., Cross, R., Sims, J., & Uhl-Bien, M. (2017). How to catalyze innovation in your organization. *MIT Sloan Management Review, 58*(4), 38–47.

Arena, M., & Uhl-Bien, M. (2016). Complexity leadership theory: Shifting from human capital to social capital. *People + Strategy, 39*(2), 22–27.

Ashby, W. R. (1962). Principles of the self-organizing system. In: H. von Foerster, & G. W. Zopf (Eds.), *Principles of self-organization* (pp. 255–278). New York: Pergamon.

De Coning, C. (2018). Adaptive peacebuilding. *International Affairs 94*(2), 301–317.

De Coning, C. (2020). Adaptive peace operations: Navigating the complexity of influencing societal change without causing harm. *International Peacekeeping 27*(5), 836–858.

Loode, S. (2011). Peacebuilding in complex social systems. *Journal of Peace, Conflict and Development 18*, 68– 82.

Uhl-Bien, M. (2021). Complexity and COVID-19: Leadership and followership in a complex world. *Journal of Management Studies 58*(5), 1400–1404.

Uhl-Bien, M., & Arena, M. (2017). Complexity leadership: Enabling people and organizations for adaptability. *Organizational Dynamics 46*(1), 9–20.

Uhl-Bien, M., & Arena, M. (2018). Leadership for organizational adaptability: A theoretical synthesis and integrative framework. *The Leadership Quarterly 29*(1), 89–104.

The scientific foundation for operational art

E. Meyer (1)

(1) Norwegian Defence University College/Command and Staff College, emeyer@mil.no

I made this model (Figure 1) to try to explain the reason for some of the tension between linearity and non-linearity in operational art. The model is – as for all models and theory about the real world – a simplification or reduction of reality and requires some explanation.

Figure 1 _ The scientific foundation for operational art

First, notice the model itself with shapes that integrates into each other, so both are present at the top and the bottom, but only one is dominant at each end. Those shapes represent theories of science, where the top shape represent social sciences and the bottom represent natural sciences.

Second, at the left side of the model I have added levels of command with strategic level then predominantly relying on social sciences, and the tactical level predominantly relying on natural sciences. This harmonizes also with the Clausewitzian logic of war: The logic of tactics is to gain battlefield victory, and the logic of strategy is to use those victories for the purpose of the war (Friedman 2021).

Third, as shown on the right side, the tactical logic is linear and focused on influencing, like destroying or controlling, a closed system with physical force, and clearly predominantly relying on the natural sciences to calculate the use of force. The logic of strategy operates in a different environment that is an open system, with non-linear attributes like emergence, causal uncertainty, and effectively non-predictability. At the strategic level we know what we have, but we cannot be sure what we get if we intervene.

There is general agreement that laws allow us to explain, predict, and successfully intervene in the world (Mitchell 2009). The laws of natural sciences, the so-called hard sciences, predict effects of interventions. Within the social sciences there is an enduring debate whether or not to talk about laws at all. And there are no laws of war, only principles that we put different emphasis on pending the situation. We only know after if we got a satisfying balance between the principles or not in relation to the opponent or opponents.

Therefore, this model also explains why a different skillset is required from a strategic leader than from a tactical leader, and that success at one level does not predict success at another.

However, this model does not place operational art in a clear space like strategy and tactics, but if it is a link, or the translation of strategy to tactics, it clearly involves the application of both social and natural sciences. The dynamic character of war and conflicts decides - or should decide - the balancing of social and natural sciences in the execution of operational art. And therefore, the operational level of command, that execute operational art in its purest form,

sometimes have a predominantly tactical focus, like a US JTF reinforcing the defence of Northern Europe, and sometimes a predominantly strategic focus, like ISAF HQ had in Afghanistan.

Operational art, therefore, needs a method that encapsulates both linear and non-linear sciences, processes, concepts and tools, adapting to the situation.

KEYWORDS

War studies; Operational art; Strategy; Tactics; Linearity; Non-linearity.

REFERENCES

Friedman, B. A. (2021). *On Operations: Operational Art and Military Disciplines*. Annapolis, Maryland: Naval Institute Press.

Mitchell, S. (2009). Complexity and Explanation in the Social Sciences. *Philosophy of the Social Sciences: Philosophical Theory and Scientific Practice*. Cambridge University Press.

The security vacuum in the post-conflict zone: lessons from Kosovo

M. Żakowska (1)

(1) War Studies University, Poland, m.zakowska@gmail.com

The withdrawal of Yugoslav military forces from Kosovo after the end of the armed conflict (1999) under the Military-Technical Agreement and UN Security Council Resolution 1244 created a security vacuum in which the Kosovo Liberation Army and KFOR "competed" to take administrative control of Kosovo. In the face of the administrative chaos and slowly evolving public order, numerous acts of retaliation were carried out by returning Albanians against Serbs and ethnic minorities remaining in Kosovo accused of cooperating with the Serbian government and armed forces during the war. Moreover, other forms of crime were proliferating, e.g., ethnic and politicly motivated murders, rapidly expanding destruction of religious buildings and smuggling. The security vacuum resulted in the emergence of new conflict and extremely challenging conditions for KFOR and UNMIKs efforts to restore security and a sustainable peace.

This article examines the security vacuum in post-conflict Kosovo as one of the main challenges to the peacebuilding process. The time frame encompasses the period of the withdrawal of Yugoslav forces from Kosovo and the deployment of KFOR. The study focuses on exploring socio-political factors caused by the security vacuum, namely (i) seizure of power by local political/armed groups; (ii) retaliation; (iii) criminal activities development; (iv) forced migrations. The research is based on implementing a few approaches, including human security, security dilemmas, and retaliation, which lead to understanding the motives of human behaviours behind the acts of revenge. The findings allowed us to answer the question: What mechanics should be used to decrease the security vacuum in the post-conflict zone and the emergence of socio-political factors caused by this security chaos?

Furthermore, the study showed the necessity for developing an agreed comprehensive strategy to enable the synchronization of the withdrawal of hostile armed forces from the conflict zone with the deployment of international forces (including police units) and the establishment of local administration.

KEYWORDS

Security vacuum; Kosovo; Retaliation; Criminal activities; Forced migration.

Withdrawal of the United States and NATO military forces from Afghanistan: implications for the international security

J. Krzyżanowski (1)

(1) War Study University, Poland, jakub.krzyzanowski@hotmail.com

In 2021 the United States and NATO decided to leave Afghanistan after 20 years of military presence. While leaving Afghanistan, The United States left behind nearly 300,000 trained armed forces of the Afghan National Security Force, being sure that the country would not be overrun by the Taliban, the Sunni Islamist extremist group. In his speech to the nation, the President of the US – Joe Biden, announced that the main objectives of the intervention in Afghanistan were achieved by assassinating Osama bin Laden and preventing the creation of a „safe haven" for terrorist organizations in the Central and Eastern Asia region. However, after the withdrawal of US and NATO military forces, the Taliban announced the formation of a new government dominated by Taliban loyalists.

The article aims to examine the consequences of the withdrawal of US and NATO military forces from Afghanistan for international security. The research focuses on analyzing the challenges for global security which were the consequence of the withdrawal: (i) the security vacuum in Afghanistan; (ii) new approaches to understanding the concept of "American pragmatism"; (iii) undermining by great power as Russia and Chain the leadership position of US and NATO in maintaining global security. The framework for this study is the theory of the challenge of inference developed by Maryann Barakso, Daniel M. Sabet and Brian F. Schaffner, and the primary method used is desk research.

The findings show that the withdrawal of USA and NATO forces from Afghanistan challenged the credibility and position of those actors in the international environment. Moreover, that situation was broadly used by Russia and China to undermine the engagement US and NATO in support of the territorial claim of Taiwan and Ukraine in ongoing conflicts.

KEYWORDS

United States of America; Afghanistan; NATO; International security; Withdrawal.

REFERENCES

'Only losses, tragedies': Putin blasts US for imposing 'norms' on Afghanistan for 20 years. (2021). Tass. Retrieved from https://tass.com/world/1332485

Afghan abandonment a lesson for Taiwan's, DPP: Global Times editorial. (2021). Global Times. Retrieved from https://www.globaltimes.cn/page/202108/1231636.shtml.

Barakso, M., Sabet, D. M., & Schaffner B. (2014). *Understanding Political Science Research Methods, The Challenge of Inference*. New York and London: Routledge.

Barnes, J. E., (2022). *Why the U.S. Was Wrong About Ukraine and the Afghan War*, Retrieved from https://www.nytimes.com/2022/03/24/us/politics/intelligence-agencies-ukraine-afghanistan.html

Byrd, W., (2022). *Why Have the Wars in Afghanistan and Ukraine Played Out So Differently*, United States Institute of Peace. Retrieved from https://www.usip.org/publications/2022/06/why-have-wars-afghanistan-andukraine-played-out-so-differently

Haass, R., (2021). *America's Withdrawal of Choice*, Project-Syndicate. Retrieved from https://www.projectsyndicate.org/commentary/americas-withdrawal-of-choice-by-richard-haass-2021-08

United States of America, Bureau of Political-Military Affairs. (2022). *U.S. Security Cooperation with Ukraine*, Retrieved from https://www.state.gov/u-s-security-cooperation-with-ukraine/

United States of America, Special Inspector General for Afghanistan Reconstruction. (2021). *Quarterly Report to the United States Congress*, Retrieved from https://www.sigar.mil/pdf/quarterlyreports/2021-10-30qr.pdf

United States of America, White House. (2012). *Remarks by President Biden on the Drawdown of U.S. Forces in Afghanistan*. Retrieved from https://www.whitehouse.gov/briefing-room/speechesremarks/2021/07/08/ remarks-by-president-biden-on-the-drawdown-of-u-s-forces-in-afghanistan/

United States of America, White House. (2021). *Remarks by President Biden on the End of the War in Afghanistan*. Retrieved from https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-presidentbiden-on-the-end-of-the-war-in-afghanistan/.

US leadership was aware of real situation in Afghanistan, says Russia's intel chief. (2021). Tass. Retrieved from https://tass.com/politics/1342025

Russian Peacekeeping Missions: Uses and Abuses

P. Jolicoeur (1)

(1) Royal Military College of Canada, pierre.jolicoeur@rmc.ca

On 21 February 2022, President Vladimir Putin announced that Russian forces would enter Ukraine to "perform peacekeeping functions". Peacekeeping has become central to Russia's policy of pursuing a continued interest in the "near abroad", a designation for territories consisting of former Soviet republics that are now independent states. However, Russia's use of the term "peacekeeping" seems to go against the established concept of "peacekeeping" developed under the remit of the United Nations (UN) and the principles associated with it. This paper examines the reasons why the use of this term by Russia is highly divergent from the "traditional" concept of peacekeeping. In the first part, we examine various Russian peacekeeping operations over the past thirty years to provide a general definition of what constitutes a genuinely "Russian" peacekeeping operation. In contrast to this, we retrace, in the second part of the paper, the constitutive principles of UN peacekeeping operations that have been for the near past seven decades the flagship of such operations. This comparison allows us to expose, in the third part of this paper, the fundamental differences between the Russian and the UN concept of peacekeeping. Based on these findings, we explore the consequences of the Russian way of peacekeeping for International Law, peace and security in the former Soviet Union territories and the World.

Part I - Russia's typical "peacekeeping operations" in the near abroad

Russia has a long history of framing its military interventions as "peacekeeping" operations which stems from Russian policy in the early 1990s aiming at protecting vital interests in the "near abroad". The wars in former Yugoslavia put peacekeeping on the Russian foreign policy agenda when Russia made substantial troop contributions to the UN Protection Force (UNPROFOR) in Bosnia. However, Russia uses the term "peacekeeping" to describe a multitude of different military operations. For example, Russia conducted military operations in Georgia and Moldova in the 1990s that were also labeled as peacekeeping. In both cases, Russia intervened after protests against legislation changing the official language of those countries had led to armed conflict. Russia's long-term engagement in Georgia, especially in South Ossetia and Abkhazia, culminated into a war in 2008 and Russian forces have remained present in Moldova for almost thirty years in the form of the Operational Group of Russian Forces (OGRF) in Transnistria.

More recently, Russia has been involved in "peacekeeping" efforts in Nagorno-Karabakh after the conflict in the Fall of 2020. Russian forces have been credited with providing a "sense of security" and it has been claimed that Azerbaijanis could return to the area under Russian protection.

In all these cases "peacekeeping" efforts serve primarily the Russian interest to maintain a military presence in the independent countries of the Near abroad. In some instances, this military presence could be exploited to reinforce the dependency of the host state on Russia.

Part II - UN peacekeeping principles

While many international organizations and coalitions undertake military operations that can fall under the general umbrella of peacekeeping, it is the UN that has led the way in the development of principles that distinguish peacekeeping from any other military action. In fact, the UN has led over 70 peacekeeping operations, more than any other actor. As a result, peace operations involving the UN constitute the standard in peacekeeping operations.A UN peacekeeping operation follows three general principles. First, it will only be deployed with the consent of the host state in respect for state sovereignty and territorial integrity. Second, impartiality, prevents a UN peacekeeping mission from being used to force a political settlement in the interest of one party to the conflict or influence the balance of power. The third principle of UN peacekeeping is that force must only be used for defensive purposes, where Chapter VII authorization is absent.

Part III - "Peacekeeping" in Ukraine compared to UN standard and to Russian practice

This paper analyses Russian military operations in Ukraine in the light of those UN guiding principles. We consider that Russian aggression of Ukraine is anything but a peacekeeping operation. It does not meet the UN accepted principles of peacekeeping operations, nor does it meet the standards of a typical Russian peacekeeping operation in the near abroad. The confusion seems to come from the fact that Russia label as "peacekeeping" almost every military operation in the near abroad. This lack of variation in the vocabulary employed by the Russian authorities leads to problems for the international Law and for the peace and security in the former Soviet Union territories and the World.

KEYWORDS

Typology of operational environment and its practical implications on military planning

R. Rosa (1)

(1) War Studies University, Warsaw, r.rosa@akademia.mil.pl

The increase in the number of elements in a given environment, as well as their features, may affect the degree of ordering of relations between these elements. Therefore, one should ask the question: Is it possible to speak of different types of operational environments due to the degree of ordering of relations in a given environment? In the author's opinion, finding the answer to this question was crucial from the point of view of the design approach. The research question formulated in this way determined the content of the working hypothesis, which was as follows: along with the increase in the number of actors and domains within which negative cooperation is conducted between specific parties of the conflict, the nonlinearity of relations between the elements shaping a given operating environment increases. Due to that operational environment may take following forms: simple, complicated, complex and chaotic. The issue of the typology of the environment in terms of the degree of order was the subject of research by David Snowden and Mary Boone. In their opinion, due to the degree of order, the environment may take a simple, complicated, complex and chaotic form.

The conducted research checks the relationship between the increase in the number of participants and the manner of acting in the framework of negative cooperation, and the presence of various operational environments. The researcher problem defined in this way and the working hypothesis determined the goals of the research. The cognitive goal was to identify the operating environments. The utilitarian goal was to propose the scope of application of specific operational concepts within defined environments.

During the research, theoretical methods were used, such as analysis, synthesis, abstraction, inference, comparison, generalization and analogy.

The research results confirm the validity of the research question posed. The adopted research hypothesis was confirmed. It should be noted that new challenges in the scope of the increasing complexity of the operational environment entail the necessity to redefine the modus operandi, the scope of problems and goals, the extent of involvement of the armed forces, and the identification of opportunities, opportunities and risks. It is reasonable to adopt a typology of the operating environment: simple, complicated, complex and chaotic.

With the references of the research author proposed following definitions of given operational environments. A simple environment is an environment with its elements, characterized by the possibility of a wide application of procedures and techniques. Achieving the set goals in a simple environment is associated with following strictly defined procedures. A complex environment is characterized by the presence of more material elements than a simple environment. These include morale or the level of discipline. Achieving the goals is based on the results of the planning process and on sufficiently good and acceptable ways of carrying out tasks. A complex environment is an environment with its elements characterized by limited possibilities of planning an action aimed at achieving a fully adopted goal. The activities and processes included in the design of the desired future in connection with the hitherto existing methods of operation.

At the same time, the adopted typology of the operating environment determines the scope of application of specific operating concepts. A simple environment requires the implementation of procedures, instructions, decisions, etc. In a complex environment, it is possible to effectively apply concepts such as the concept of the five rings or deep surgery. In a complex environment, it is reasonable to use a variety of concepts from the scope of the design approach.

KEYWORDS

Operational environment; Operational conception; Monlinearity; Planning; military design.

REFERENCES

Apanowicz J., (2002). *Metodologia ogólna.* Gdynia: Wydawnictwo Bernardinum.
Apanowicz J. (2000). *Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania.* Gdynia: WSAiB.
Balcerowicz B. (2002). *Pokój i Nie-Pokój. Na progu XXI wieku.* Warszawa: Dom Wydawniczy Bellona.
Beaulieu-Brossard P., & Dufort P. (2017a). Conclusion: Researching the Reflexive Turn in Military Affairs and Strategic Studies. *Journal of Military and Strategic Studies, 17*(4).

Beaulieu-Brossard P., & Dufort P. (2017b). Introduction: Revolution in Military Epistemology. *Journal of Military and Strategic Studies*, *17*(4).

Colin J. (1920). *Przeobrażenia wojny.* Warszawa: Główna Księgarnia Wojskowa.

Czupryński A (2006). *Myślenie operacyjne w sztuce wojennej*, Warszawa: AON.

Czupryński A. (2009). *Współczesna sztuka operacyjna*. Warszawa: AON.

Eikmeier D.C. (2016). Let's Fix or Kill the Center of Gravity Concept. *Joint Force Quarterly*, *4*(83), 111.

Feret S. (1960). *Zarys wojen i sztuki wojennej na przełomie XIX i XX wieku*. Warszawa: ASG WP.

Herman H. (1992). *Operacja w sztuce wojennej.* Warszawa: AON.

Jomini H. (1966). *Zarys sztuki wojennej.* Warszawa: Wydawnictwo MON.

Kośmider T., & Ślipiec J. (2008). *Operacje wojsk lądowych w poglądach przedstawicieli europejskiej myśli wojskowej od XVIII wieku do wybuchu drugiej wojny światowej*. Warszawa: AON.

Łobocki M. (2009). *Metody i techniki badań pedagogicznych*. Kraków: Oficyna Wydawnicza Impuls.

Łoś R., & Reginia-Zaharski J. (2010). *Współczesne konflikty zbrojne*. Warszawa: Wydawnictwo Naukowe PWN.

Macaulay D.A. (2008). *Campaign Design: One Framework for a Volatile, Uncertain, Chaotic and Ambiguous Environment?* Kingston: Canadian Forces College.

Münkler H. (2004). *Wojny naszych czasów*. Kraków: Wydawnictwo WAM.

Reid C. (1987). *Reflexive Control in Soviet Military Plannin.* Toronto.

Pinter W. (1986). Russian Military Thought: The Western Model and the Shadow of Suvorov. In P. Paret, G.A. Craig, & F. Gilbert, *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Princeton, NJ: Princeton University Press.

Rittel H.W.J., & Webber M.M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, *4*(2). doi: https://doi.org/10.1007/BF01405730

Sheehan M. (2007). *The Changing Character of War.* wyd. 4. Oxford: Oxford University Press.

Smith R. (2007). *Przydatność siły militarnej. Sztuka wojenna we współczesnym świecie*. Warszawa: PISM.

Vego M. (2007). *Joint Operational Warfare.* II-25–II-39.

Snowden D.J., & Boone M.E. (2007). A leader's framework for decision making. *Harvard Business Review*. Retrieved from https://hbr.org/2007/11/a-leaders-framework-for-decision-making

Sołkiewicz H. (2014). *Myślenie operacyjne na kanwie poglądów Milana Vego.* Rocznik XCVI (VIII). Warszawa: Bellona 4/2014 (679).

Toffler A. H. (2006). *Wojna i antywojna. Jak przetrwać na progu XXI wieku?* Poznań: Wydawnictwo Kurpisz.

Vego M. (2009). Systems versus Classical Approach to Warfare. *Joint Force Quarterly*, *52***.**

Warden J.A. (1995). The enemy as a system. *Airpower Journal*, *9*(1).

Wass de Czege H. (2009). Systemic Operational Design: Learning and Adapting in Complex Missions. *Military Reviev*, 1.

Wyszczelski L. (2000). *Historia myśli wojskowej.* Warszawa: Wydawnictwo Bellona.

Transition from Planning to Execution at the Operational Level

B. Ravn (1)

(1) Norwegian Defense University College, bravn@mil.no

In his essay On Strategy from 1871, Field Marshall Moltke wrote that no operation plan extends with any certainty beyond the first encounter with the main enemy forces. Moltke considered that only the beginning of a military campaign could be planned because it was impossible to foresee all eventualities that could unfold during the fighting between the different parties in a war (Moltke, 1871) There are numerous reasons why his concept is still valid. Modern conflicts tend to be more complex than the wars Moltke based his writings on. New technology, the modern media landscape, the growth of cyberspace, hybrid threats and the types and number of actors involved nowadays to mention a few, give even greater challenges than in Moltke's time when it comes to understand and determine an adversary's behavior in advance. The latest example to underscore the old saying is the Russian lessons learned during the beginning of the Ukrainian invasion in February 2022. How things were unfolding during the first days and weeks of the operation supports the notion that Russia had planned for a swift and quick occupation of Ukraine. As evidence suggest, the Russian plan did not survive the first encounter with the Ukrainian forces, and Russia had to adapt to the real situation on the ground and follow another path than originally planned for.

Operational art is the conceptual framework underpinning planning and conduct of operations in NATO. It includes two concepts. Operations design frames the problem and operational environment and expresses vision through plans, while Operations management translates the operations design into executable orders and directions by coordinating, synchronizing and prioritizing capabilities across the joint functions (NATO, 2017). Within this context, this article focuses on the interaction between the operations assessment and the joint synchronization processes as part of the operations management concept during execution of an operation plan. During multiple instances as a staff member, evaluator and trainer at different operational headquarters, both in Norway, the Middle East and in NATO, I have repeatedly observed challenges and shortcomings in the transition process during operations and exercises. Even though most of the observed shortcomings have been identified by the stakeholders, some of them seem hard to overcome and can be observed across the different headquarters year after year. There could be a number of reasons for this lack of improvement, and the article tries to shed some light on one part of the problem by answering the following question:

What are the challenges in the linkages between the operations assessment and joint synchronization processes at the operational level?

The article points out that lack of functional experience and scientific competence among the staff as a possible reason for the lack of improvement within the field. But as in most cases in hierarchical organizations, the responsibility for correcting flaws and shortcomings in the organization and in its processes is vested in the leadership. Unfortunately, lack of understanding of the fundamentals of both the assessment process and the joint synchronization process and the linkage between them also exist among the leadership. Generals and admirals also need education in these complicated processes in order to support their staff in their effort. Of particular interest related to the topic discussed is to get the leadership to understand the important linkage between the two processes and be able to identify the existing shortcomings in the operational assessment process, particularly concerning validity challenges in the delivered conclusions and recommendations during the assessment board. Further on, transition from an operation plan to executable orders takes places continually during conduct of operations as situation changes and events in the operational environment unfold. Synchronizing future tactical activities in a joint force across time, space, forces and information is complicated and time consuming. The article describes how the outcome of the joint synchronization process depends on the quality of the operational assessment process as an input. There are persisting shortcomings among the joint headquarters nationally and in NATO when it comes to understanding of and the ability to improve the linkage between operational assessment and joint synchronization.

KEYWORDS

Joint synchronization; Operational assessment; NATO.

REFERENCES

Moltke, H. von. (1871). *In Über Strategie. Militärische werke, series II: Die tätigkeit als Chef des Generalstab der Armee im Frieden* (Vol 2). Berlin: Mittler & Sohn

NATO. (2017). *Allied Joint Doctrine AJP-1 (E)*. Brussel: NATO Standardization Agency.

Revaluation of air superiority in a major war

P. Mroz (1)

(1) War Studies University, Poland, p.mroz@akademia.mil.pl

Until a war in Ukraine last decades witnessed military operations characterised by asymmetry in air capabilities. They were conducted against opponents of choice, who did not force mighty air powers to constantly fight for gaining and maintaining air superiority (Haun, 2021, passim). This period was relatively long and spanned more or less the whole career of an airman or strategist having an impact on mindsets, theories and training. The war in Ukraine of 2022 should be a quick awakening of traditional air power approaches to remind that fighting for control of the air is a very serious, dangerous, but also principal challenge without which nothing more might happen in a conflict with a potent enemy.

However, the situation today, as we see it while the war in Ukraine is unfolding, looks different from the one that early theorists knew (Meilinger, 1997, passim). New technologies, like ballistic and cruise missiles along with UAVs and hypersonic weapons, pose air threats of new types of unimaginative range, precision, speed and agility

(Ciaston, 2022, p. 1-6). Opponent's advanced and layered air defences along with great saturation of lethal active defence assets of A2/AD are to increase costs of air warfare to unacceptable level. Air forces of the West are technologically advanced but also have important dependencies like cyber, space, and surface infrastructure. Fighting for command of the air might be anyway very costly and arduous. In some scenario it should be noted that no one will be able to gain air superiority but only air denial (Bronk, 2021). It however carries a risk of being not able to utilise the paramount ability of air power namely offensive strike. Air power is inherently offensive and striking deep and hard directly into the heart of the enemy is the best option to achieve strategic effect avoiding tactical quagmire.

The article argues that the war in Ukraine calls for invigorating the discussion about air superiority. Its fundamentals and importance for the conduct of a major war will be shown in the paper. New conditions of gaining and maintaining air superiority will be presented through the prism of contemporary air threats and weapons employed, defensive measures, and dependencies and limitations of air power. Frames of concepts for gaining air superiority in a major war of tomorrow will also be proposed.

KEYWORDS

Air Power; Air Superiority; Air Warfare; War in Ukraine.

REFERENCES

Bronk, J. (2021). *Stratgem. An Unstoppable Force meets an Immovable Object: Air Superiority vs Airspace Denial Strategies*. Retrieved from https://www.stratagem.no/an-unstoppable-force-meets-an-immovableobject-air-superiority-vs-airspace-denial-strategies

Ciaston, R. (2022). *Russian Federation's use of ballistic and cruise missiles in the Ukrainian conflict*. The Casimir Pulaski Fundation.

Haun, P.M., Jackson, C., & Schiltz, T. (2021). *Air Power in the Age of Primacy*. Cambridge University Press.

Meilinger, P.S. (1997). *The Paths of Heaven. The Evolution of Airpower Theory*. Air University Press.

Technical and fundamental knowledge of stock as a open source Intelligence used for security purposes. Data gathering and intel verification alternative - approach

M. Słomka (1) and P. Kowal (2)

(1) 8 Air Defense Regiment, Poland, mariasylwiaslomka@gmail.com
(2) Military Uni. Forces Gen. T. Kościuszko/Andrzej F.M.Krakow Uni., Poland, Pawel.Andrzej.Kowal@gmail.com

Carl von Clausewitz defines an act of war as "*an act of violence intended to compel our opponent to fulfill our will*" (Kaldor, 2010). From the management and military science perspective, conflict is understood as a "*competitive or opposing action of incompatibles antagonistic state or action (as of divergent ideas, interests, or persons) a conflict of principles*" (van de Vliert, 1998). For decades, the security and intelligence community tries to find the best methods to establish perfect security strategy (Betts, 2009). A crucial factor for this is intelligence knowledge and its use for state security It is well known and widely understood that effective and efficient intelligence performed for security purposes can decrease one's own losses or gain the advantage over the enemy, even before any kinetic action takes place. Based on these findings, the source of data and techniques to verify possible benefits and fundamental correctness is crucial.

After having analyzed of theoretical factors of conflict, the stock market can be somehow understand as a sub-battlespace, which is coordinated by state and nonstate actors. As an example, the elements of combat power can be comparable to stock market factors. Dominance is not achieved with the firepower but mainly by correct capital use. The maneuver in this case can be seen as a stock trend. For decision making in military conflict as well as with stock trading environment, information is a main factor for anticipating the outcome of conducted action and risk management.

The main hypothesis of the paper regarding information gathering and intelligence processes is that **if market can be seen as a space of conflict with wide variety of actors, and elements of combat factors can be observed in the market game, the real-time analysis of market quotes can be source of data which may be useful to improve strategic intelligence.**

In order to confirm or deny presented hypothesis it needs to be assumed that the international market(understand here as an enormous amount of active traders with the same or opposite goal) take advantage of data reception and use it in order to bet the price direction (Livermore, 1940). The presented assumption is created with the following idea that the market duel due to its decentralization, can use information effectively, quickly and the trend is a direct result of traders use of knowledge, anticipations, and analysis. It also needs to be seen that the price of different stock instrument is linked to real economic situations, but is used in the stock game with human psychology and behavior (Arrow, 1981).

This paper proposes an approach to market analysis as an augmentation for intelligence process used for security reasons. Authors of this abstract mainly focused on the similarity between the way traders gather, analyse, use and trade due to retained data and military view of information management. Whole market mechanism is based on the speculative trading as a result of observed reality and directly used in order to receive income from the price change. From the historical perspective it can be observed that some market instruments appear to act prior to release of published news (Baruch, 1921).

KEYWORDS

Intelligence; Data; Gathering; Risk; Management; Information; OSINT; Stock market.

REFERENCES

Arrow, K. J. (1981). *Risk perception in psychology and economics*. Stanford Univ CA Inst for mathematical studies in the social sciences.
Baruch, B. M., et al. (1921). *American industry in the war*.
Betts, R. K. (2009). *Enemies of intelligence: Knowledge and power in American national security*. Columbia University Press.
Kaldor, M. (2010. Inconclusive wars: is Clausewitz still relevant in these global times?. *Global Policy*, *1*(3), 271-281.
Livermore, J. L. (1940). *How to trade in stocks: The livermore formula for combining time element and price*. Laurus-Lexecon Kft..
van de Vliert, E. (1998). *Conflict and conflict management*. Handbook of work and organizational psychology, 3, 351-376.

What do we talk about when we talk about Military Operations? Building a framework for future research

A. Sookermany (1)

(1) Norwegian Command and Staff College/Norwegian Defence University College, asookermany@mil.no

Work on the ***Handbook of Military Sciences*** (Høiback, 2021; Sookermany, 2020) has revealed that Military Operations as a research field is a rather diverse field of more or less random contributions from an eclectic group of authors with little paradigmatic awareness. Research on military operations seems to be both unsystematic (not very well connected) and those engaged in it have little academic awareness, training and experience from doing research (which partly is due to the fact that the majority of them are military professionals with limited academic training). Consequently, there is no agreed upon definition of what military operation is as a concept nor what it can be or develop into:

> It is under-researched, lacks rigorous intellectual investigation and an established academic literature to support the conceptual growth of this highly influential idea in military circles. (Finlan, Danielsson, & Lundqvist, 2021, p. 368)

This is problematic for at least three reasons. **Firstly**, while there exists a large body of knowledge and publications on military operations, little scientific attention has been given to the academic field of military operations itself. What are its constitutive elements, on what philosophical foundations are they built and where do they originate from? The scarcity of such insights, run the risk of establishing research programs that are not well grounded in relevant theory nor sufficiently situated in practical challenges. More so, the lack of such a field overview will be most damaging for those attempting to conduct academic inquiries into military operations with little prior academic training, as they presumably are the once with the weakest skills in conducting this type of work. The worrying part is that this group are hugely overrepresented among those faculty members who are recruited from the officer corps – hence, those who have an **insider** understanding of what military operations are. Accordingly, **establishing a scientific overview** of what military operations is and can be interpreted as, is of considerable significance for the further development of any research in this era, however, it is of fundamental importance if we are to facilitate a research culture on military operations where we want the insider experience and voice to be recognized as a qualified contributor to the scientifically qualified body of knowledge.

Secondly, there is a noteworthy concern that the lack of a systematic academic overview related to military operations as a research field will continue to diminish its true potential in providing concentrated research efforts able of making substantial progress in specific areas of the field. Contemporary military operations research lacks a clear sub-field categorization. Hence, what research efforts belong to the same school of thought, discourse, tradition, or even debate? The absence of such overview has a tendency to manifest itself in scattered research efforts where elaborations on a topic is deemed redundant due to the fact that it has overseen crucial findings from other relevant studies or is misplaced into a seemingly related research area. Accordingly, there is a need for **a categorization of research sub-fields of military operations**. From a researcher point of view, this is necessary for several reasons. Foremost, it is paramount to know your field of inquiry. If your field is 'military operations' it will be enormously large, and impossible to know it well. Hence, a researcher needs to carve out the part most relevant for her or his own research development and be able to follow the continued development in this field over time. But where do you begin? Putting together a **categorized research bibliography** (Block & Fisch, 2020) will facilitate a more directed and qualified research effort on both individual and institute level.

Thirdly, there is a genuine worry that even if we have an overview and we have been able to carve out a distinct part of the military operations field, we still do not know what is to be considered to be the research front of the field. Thus, if we as a research community in the field of military operations are to develop military operations into a serious academic endeavor, we need to bring clarity and rigor to what counts as knowledge and not. In academic terms this implies systematic critique and elaboration of propositions and findings within an area of *International Society of Military Sciences ISMS 2022 Conference Lisboa, 10-13 October 2022.*

inquiry. An important part of this process is **literature reviews**, essentially, they are systematic summaries and synopsis of published research on a limited topic displaying commonalities and diversities, strengths and weaknesses, resources, and barriers in similar research. In essence, they provide the reader with an overview and guide into the research front of a specific topic (Snyder, 2019). Accordingly, if we are to make sense of military operations, we need to make sure we are building our concepts on the best available research there are. Putting together literature reviews in areas we intend to field our own research is a meaningful step in that direction.

In consequence, this presentation aims at exhibiting some foundational assumptions and preliminary ideas of the newly started research program "Making Sense of Military Operations – What I Talk of when I Talk of Military Operations" so as to open our minds and doing for insight from a wider military academic community. In essence, the Making Sense of … program is launched to explore the scientific foundation of ***Military Operations*** as an academic field for the purpose of further research in the field. with, might we add, a particular interest in how we may bring the insiders perspective to the playing field. Thus, **theoretically**, this project will provide insight into what military operations is and can be as an academic field(s). Practically, it will foster a better suited military-academic research culture ready to identify, engage and tackle future challenges in the military operations field.

KEYWORDS

Military Operations; Research Field; Sub-Field Categorization; Body of Knowledge.

REFERENCES

Block, J. H., & Fisch, C. (2020). Eight tips and questions for your bibliographic study in business and management research. *Management Review Quarterly, 70*(3), 307-312. doi:10.1007/s11301020-00188-4

Finlan, A., Danielsson, A., & Lundqvist, S. (2021). Critically engaging the concept of joint operations: origins, reflexivity and the case of Sweden. *Defence Studies, 21*(3), 356-374. doi:10.1080/14702436.2021.1932476

Høiback, H. (2021). Military Operations. In: A. M. Sookermany (Ed.), *Handbook of Military Sciences* (pp. 1-20). Cham: Springer.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333-339. doi:10.1016/j.jbusres.2019.07.039

Sookermany, A. M. (Ed.) (2020). *Handbook of Military Sciences*. Cham: Springer Nature.

The evolution of intelligence activity in peacekeeping operations

C. Justo (1)

(1) Brazilian School of Command and General Staff of the Army, cmonte2005@gmail.com

This scientific article analyzes the evolution of intelligence activity in peacekeeping operations and its impacts on Latin American countries that contribute troops to the United Nations (UN). The United Nations has historically been marked by a deficiency in the field of intelligence, whether in terms of personnel, material or technology. After the Cold War, the blue helmets opted for a reduced intelligence activity, as there was a fear that the exercise of the intelligence activity would be confused with clandestine actions to obtain information, which would impact on the loss of the impartiality of the United Nations in the resolution of conflicts. However, peace operations had to evolve in the face of their new challenges, the evolution of armed conflicts and the complex and asymmetric threats made the UN finally accept intelligence activity as a central actor in its peace missions. Currently, in the United Nations Multidimensional Integrated Mission for the stabilization of MALI (MINUSMA) the intelligence has more than 400 men dedicated exclusively to this activity, in complex structures for obtaining information and with a large technological apparatus, all furnished only by the countries of the NATO system. Since 1990, Latin American countries have increased their participation in peace operations as a strategy of international insertion, in order to continue this expansion it is vital that Latinos understand the evolution of intelligence activity and have the necessary capabilities to mobilize these new UN structures. As for the methodology, this scientific investigation followed a qualitative approach, with a descriptive objective, in which a bibliographic research was carried out on the new UN regulation in the field of intelligence activity, especially in the Cruz Report and in the Agenda Action for Peacekeeping, which identified flaws in the UN intelligence process and made proposals for its improvement. Finally, the objective of this scientific article was to analyze the intelligence activity of the United Nations, presenting the characteristics of its current scenario, the new capabilities employed by the UN and its impacts for Latin American countries.

The objective of this scientific article was to analyze the intelligence activity of the United Nations, presenting the characteristics of its current scenario, the new capabilities employed by the UN and its impacts for Latin American countries.

It was observed that after the Cruz Report and the Action for Peacekeeping Agenda, UN peacekeeping missions evolved into what the author calls 5th Generation, with tactical missions guided by intelligence and the wide use of new capabilities and technological sources. In this sense, opportunities for improvement were identified in Latin American countries, to participate in this new scenario in Peace Operations.

KEYWORDS

Intelligence; United Nations, Peacekeeping Operations.

REFERENCES

Abdnur, A. et al. (2017). *O Brasil e a MINUSTAH: lições a partir da literatura acadêmica*. Instituto Igarapé, Centro Conjunto de Operações de Paz do Brasil, Edição Especial – Coletânea de artigos, Rio de Janeiro, 101-112. Retrieved from http://www.ccopab.eb.mil.br/phocadownload/revista-igarapeminustah/Participao%20do %20Brasil%20na%20MINUSTA-2004-2017-BR.pdf

Abdenur, A. E. & Call, C. T. A (2017). Brazilian Way?. Brazil's Approach to Peace building Rising Powers and Peacebuilding.

Dorn, W. A. (2009). Intelligence-led peacekeeping: The United Nations stabilization mission in Haiti (MINUSTAH), 2006–07. *Intelligence and National Security*, *24*(6).

Dorn, W. A. (n.d.). United Nations Peacekeeping Intelligence. In: Johnson, L. K. (Ed.), *The Oxford Handbook of National Security Intelligence*, 275–295.

Rietjens, S., & Dorn, W. A. (2017). Perspectives on Military Intelligence from the First World War to Mali. In: *Perspectives on Military Intelligence from the First World War to Mali*. [s.l.] Asser Press, 196–219.

Rodrigues, A. D. O., & Migon, E. X. F. G. (2017). *O papel do Brasil na evolução das Operações de Paz*. Carta Internacional, *12*(3), 77.

United Nations. (2017, November). *Improving security of united nations: we need to change the way we are doing business* (Cruz report).

Medical Intelligence

S. Sousa (1)

(1) Divisão de Saúde Militar do Ministério da Defesa Nacional, Portugal, silvia.sousa@defesa.pt

The capacity resulting from the interface between health and military intelligence, under the concept of Medical Intelligence (MedIntel), proves to be essential in the identification, assessment, mitigation and/or response to medical-sanitary risks and threats with impact on the Deployed National Forces and, consequently, on the operational capacity of the Armed Forces.

Throughout history, the outcome of military operations has often been affected by the lack of medical information and/or "medical intelligence" regarding risks and threats of a medical-sanitary nature, allowing, today, to say that mortality and morbidity rates of military personnel could have been reduced with the existence of a military MedIntel capability (NATO, AJMedP-3).

In this sense, and bearing in mind the possibility that the greater number of casualties resulting from armed conflicts probably had acquired diseases and not injuries resulting from the confrontation with the enemy, the MedIntel military capacity at the various decision-making levels is crucial (vertically) and in the various stages (horizontally) of planning and conducting military operations.

However, and without prejudice to the due recognition of the numerous activities carried out in the field of health and military information that contribute directly and/or indirectly to the identification, assessment, mitigation and/or response to risks and threats of a medical-sanitary nature with an impact in the health of the troops and, consequently, with an impact on the level of readiness of the military forces, Portugal has not yet built an effective MedIntel military capacity.

Once this gap is recognized, it is essential to carry out research studies in the field of military sciences, particularly in the area of human behaviour and health in a military context, in order to understand the importance of MedIntel, namely: at the operational level in the planning and conduct of military operations; at the strategic-military level in the identification, assessment, mitigation and/or response to risks and threats of a medical-sanitary nature with an impact on the operational capacity of the Armed Forces; and at the political-strategic level in contributing to goals that contribute to national security and defence strategy, considering is relevance in the field of strategic partnerships regarding the multisectoral approach in the broad context of global health security.

Having this in mind, the aim of the present investigation was to address the issue of Medical Intelligence, as a military capability, in the Portuguese Armed Forces, based on an inductive methodological approach, using qualitative methods and techniques, namely, the analysis of national legislation, doctrinal publications of the North Atlantic Treaty Organization and interviews with specialists in the field of health and military intelligence of the National Defence structure.

The results of this research show, from a holistic and transdisciplinary perspective, the benefits of having a military Medical Intelligence capability, as well as allow for a better understanding of its functional elements and knowledge of the internal and external factors influencing its development within the Portuguese Armed Forces.

KEYWORDS

Armed Forces capabilities for the new war(s)

A. Moldão (1) and C. Fachada (2)

(1) Portuguese Air Force, ammoldão@gmail.com
(2) Military University Institute, Portugal , fachada.cpa@ium.pt

Almost twenty years ago, Telo (2002, p. 222) stated that wars in the first decades of the 21st century have become a state of permanent asymmetric violence, with military interventions understood as a way of defending the essential values of a democratic society, such as those in the West, as well as their way of life and their security.

A permanent transformation of war it´s something expected considering the withdrawal of Afghanistan, as well as the growth of the international relevance of China and Russia, and the progressive departure from the media focus of the ongoing regional asymmetric conflicts, namely in Syria, Yemen, Libya and the countries of Sub-Saharan Africa (Bartholomees, 2012, pp. 234-235). This can mean a return to the past, a new Cold War, with new actors and on new stages, whether with Russia as the main actor in Cold War 2.0, as defended by Kanet (2019, pp. 190206), or with China, according to Goldstein (2021).

Being Portugal and its Armed Forces (FFAA) naturally subject to the aforementioned challenges, it´s urgent to identify contributions to the construction of a strategy for capability development at the FFAA in light of the challenges arising from the new (s) war(s). A construction purpose that should meet two major references, interconnected but also inter-independent.

On the one hand, the fact that the development of these military capabilities should take into account the possibility of accompanying multinational efforts within the scope of the North Atlantic Treaty Organization (NATO) and the European Union (EU), which contribute to the modernization and interoperability of national capabilities" (Despacho [Order] No. 2536/2020, of 24 February, p. 39). Interoperability defined as "[…] the ability to operate together using harmonized standards, doctrines, procedures and equipment" (NATO, s.d.), whose desired level does not necessarily require the use of common equipment, but rather its ability to "[…] share common facilities, [being] able to interact, connect and communicate, exchange data and services with other equipment" (NATO, 2022). As an example of the preponderance of interoperability in the strategic guidance, Silva and Freitas (2019, p. 40) identified as essential requirements for the replacement of weapons systems, associated with the F16MLU, the Low Observable (LO) and Sensor Fusion (FS), in order to survive the threat posed by the anti-air defense systems Sistem Anti-Access/Area-Denial (SA2AD), associated to the future possibility of territorial projection by the Russian Federation on European territory.

On the other hand, the imperative of this strategic guidance be aligned with the geopolitical and geostrategic context in which Portugal is inserted, as well as with the interests defined in the Constitution of the Portuguese Republic (CRP) and the guiding principles of National Defense (mirrored in the legislative edifice associated with this matter, including the definition of the military component of defense and the missions assigned to the FFAA).

Thus, the following question of research were formulated *How to optimize the strategy for capability development in the FFAA in light of the new war(s)?*.

For this purpose, data was collected through: literature review; semi-structured interviews to 12 experts in these subjects; and the study, although exploratory – because it refers to an ongoing situation, but which, given its centrality in the current world conjuncture and in the subject of this investigation, could not fail to be referenced – of the (new) war between Russia (East) and Ukraine (West).

The results lead to the conclusion optimizing the strategy for capability development in the FFAA in light of the new war(s), requires a bipartite intervention. On one side, in the stability in the generation of capabilities, and on the other, in the concurrent and combined employment of the IoP. Reflected, concretely and respectively, in the implementation of 2 + 2 measures – *Optimize the approximation between political leadership and military strategic planning* and *Stimulate the national Defense industry*, plus *Optimize the IoP employment process* and *Maximize the strategic potential of military capabilities* – and 16 associated actions.

KEYWORDS

Armed Forces Capabilities; Instruments of National Power; New war; Narrative.

REFERENCES

Bartholomees, B. J. (2012). A Theory of Victory. In B. J. Bartholomees, *Theory of War and Strategy* (Vol. I) (pp. 91-106). Carlisle, PA: U.S. Army War College.

Despacho [Order] n.º 2536/2020, de 24 de fevereiro (2020). *Diretiva Ministerial de Planeamento de Defesa Militar* [Ministerial Directive on Military Defense Planning]. Diário da República, 2.ª Série, 38, 36-41. Retirado de https://files.dre.pt/2s/2020/02/038000000/0003600041.pdf

Goldstein, P. (2021). *A 'Cold War 2.0' Between the US and China*. Retirado de https://rusi.org/explore-ourresearch/publications/commentary/cold-war-20-between-us-and-china

Kanet, R. (2019). *Routledge, European Politics And Society. Russian strategic culture, domestic politics and Cold War 2.0* 20(2), 190-206.

North Atlantic Treaty Organization (NATO). (2022, 22 de fevereiro). *Interoperability: connecting force*s [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_84112.htm

North Atlantic Treaty Organization (NATO). (s.d). *Partnership Interoperability Initiative* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_132726.htm

Silva, R. J., & Freitas, D. N. (2019). Substituição do F16MLU e Entrada na 5.ª Geração [Replacement of the F16MLU and Entry into the 5th Generation]. In: R.M. Martins (Coord.), *Novas Guerras: Da 5.ª Geração e do Outsourcing ao Espaço* [New Wars: From the 5th Generation and Outsourcing to Space] (pp. 7-47). Coleção ARES, 32. Lisboa: IUM

Telo, A. J. (2002). Reflexões sobre a Revolução Militar em Curso [Reflections on the Ongoing Military Revolution]. *Nação e Defesa*, 103, 211-249.

The challenges that a Multi-Domain Operational Environment poses to military infrastructures

A. Ferreira (1)

(1) IUM, Portugal, ferreira.acs@ium.pt

Military infrastructures are an essential element in military operations, always has been and will continue to be. Although in the last century the military infrastructures have not had a tactical use, being just a safe place to assure the readiness, regeneration and support of the military force, in a Multi-Domain Operational Environment (MDOE) the military infrastructures will be a manoeuvre platform from which protect, project and sustain the combat power against adversaries on military parity in the five domains.

But, in a theatre of operations marked by a volatile, uncertain, complex and ambiguous environment, where military operations take place in a multidimensional spectrum, military infrastructures acquire an even more fundamental role in the protection, projection and support of the combat power, as well as in the ability to command and control its use.

Therefore, which challenges does a Multi-Domain Operational Environment poses to military infrastructure?

This is the question that we intend to answer throughout this research, which main goal is to determine those challenges in order to develop methodologies to assess and increase the resilience of the military infrastructures.

To achieve this goal, we started by conceptualizing military infrastructures and the MDOE, by their dimensions: the applicability, the elements and the resilience of military infrastructures and the MDOE's domains and their influencing factors. Then we combined these dimensions, through space, time and effects and using a SWOT analysis, we identify the weaknesses and strengths of military infrastructures and the threats and opportunities resulting from an MDOE.

From this relationship, between military infrastructures' and MDOE's dimensions, eight strategies were determined in order to maximise their strengths and minimise their weaknesses.

The implementation of these strategies brings, in a MDOE, challenges for the future of military infrastructure and for its planning and projection.

As the final result of this investigation, an MDOE will challenge military infrastructures to be more "intelligent" as a result of new technologies integration, to be "cheaper" by reducing their logistical footprint and to be more "tactical", creating and exploit windows of opportunity, in order to seize advantage over the adversary and reseize superiority in the land, maritime, air, space and cyberspace domains.

KEYWORDS

Multi-Domain Operational Environment; Military infrastructures; Challenges; Resilience.

A comparison between the Soviet-Finnish Winter War and the present situation in Ukraine

D. Haitas (1)

(1) Faculty of Law, University of Debrecen, Hungary, danielhaitas@gmail.com

The present conflict in Ukraine and the broader context surrounding it may justifiably elicit a certain comparison with the Soviet-Finnish Winter War of 1939-1940. This presentation shall compare the two events, exploring certain similarities and differences. Firstly, we see here two sovereign European states, both having been part of the Russian Empire and in the case of Ukraine, also the Soviet Union. In both cases it can be observed that the Soviet and present Russian state claimed that the neighbouring smaller states in some way represented a potential threat (Sorainen, 2022; Mearsheimer, 2022) and also included failed negotiations leading up to both conflicts (Spring, 1986, p. 209; Prokip, 2022). Though an independent Finnish state survived the attack, as the war dragged on and the Soviets brought in reinforcements and changed tactics, significant territories were lost to Finland by the end of the hostilities, with a formal peace agreement having been reached between the warring parties (Limas-Villers, 2022; Sorainen, 2022). It could be argued that a similar phenomenon may possibly be observed in Ukraine, which survived the attack on Kyiv but has so far also lost significant territories in the southern and eastern parts of the country (Institute for the Study of War & CT Critical Threats, 2022). However, in the case of Ukraine the conflict is still raging there without a clear end in sight regarding its final outcome and ultimate contours. Furthermore, it should be noted that in the wake of recent events in Ukraine Finland, after a long period of neutrality, has now applied for NATO membership (Ministry for Foreign Affairs of Finland). It is also worth recalling that certain commentators in the past had spoken of the Finnish model as a possible example for Ukraine to follow, that is, integration with European Union whilst not joining NATO, that is, the maintenance of a position of military neutrality (Brzezinski, 2014). It is hoped that by employing a historical and comparative approach here, the present situation may be better understood and illuminated, as well as providing certain hypothetical possibilities regarding any final outcomes or settlements.

KEYWORDS

Finland; Russia; Soviet Union; Ukraine; Winter War.

REFERENCES

Brzezinski, Z. (2014). Russia needs a 'Finland option' for Ukraine. *Financial Times*, 23 February 014. Retrieved from https://um.fi/finland-is-applying-for-nato-membership.

Institute for the Study of War & CT Critical Threats (2022). Interactive Map: Russia's Invasion of Ukraine. Accessed Control of Terrain in Ukraine as of July 13, 2022, 3:00 PM ET. Retrieved from https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375

Limas-Villers, H. (2022). The Spring War: How Finland's Winter War Compares to Ukraine. *American Security Project* Retrieved from https://www.americansecurityproject.org/the-spring-war-how-finlands-winter-warcompares-to-ukraine/.

Mearsheimer, J.J. (2022). The Causes and Consequences of the Ukraine War. *Russia Matters*, 23 June. Retrieved from https://www.russiamatters.org/analysis/causes-and-consequences-ukraine-war.

Ministry for Foreign Affairs of Finland. Finland's application for NATO membership. Retrieved from https://um.fi/finland-is-applying-for-nato-membership.

Prokip, A. (2022). Ukraine Quarterly Digest: January-March 2022. *Focus Ukraine*, 6 April. Retrieved from https://www.wilsoncenter.org/blog-post/ukraine-quarterly-digest-january-march-2022.

Sorainen, A. (2022). Why Finland wants NATO: 20 similarities between Ukraine-Russia war and Winter War. *Sorainen*, 18 May. Retrieved from https://www.sorainen.com/publications/why-finland-wants-nato-20similarities-between-ukraine-russia-war-and-winter-war/.

Spring, D.W. (1986) The Soviet Decision for War against Finland, 30 November 1939. *Soviet Studies*, *38*(2), April, 207-226. Retrieved from https://www.jstor.org/stable/151203#metadata_info_tab_contents.

The organization of Ukraine's territorial defence in face of Russia's hybrid war

V. Frolov (1), V. Semenenko (2) and J. Bērziņš (3)

(1) National Defence University of Ukraine named after Ivan Cherniakhovskyi, frol_1@ukr.net
(2) National Defence Univ. of Ukraine named after Ivan Cherniakhovskyi, semenenko17viacheslav@gmail.com
(3) National Defence Academy of Latvia and BA Business School, Janis.Berzins01@mil.lv

In the face of Russia's war against Ukraine, the question of the Ukrainian territorial defense against hybrid threats remains acute. The aggressive essence of Russia's contemporary strategic objectives manifested by hybrid tactics poses a challenge expressed by four main vectors threatening Ukraine's security and strategic interests. First, the use of soft power measures to discriminate against Ukraine in areas of international cooperation such as economics, logistics, and energy supplies. Second, deploying and conducting aggressive information and cyber warfare, since fronts of information warfare can run anywhere.[1] Third, interfering in the internal affairs of state bodies by actively employing asymmetric means destabilizing the domestic political situation of rival states. Fourth, direct military aggression is usually employed when the previous three vectors do not achieve the strategic goals.

The planning, organization, support, and management of Russia's military can also be divided into four levels. First, by establishing a plan of attack, determining the political objectives to be achieved, the operational plan and its methods and implementation, and the organization of comprehensive support. It is managed by the political leadership of the Russian Federation together with the FSB and other security and defense structures. Second, the political platform. It includes establishing the occupation authorities, organizing the administrative management of occupied territories, persecuting anyone engaging in resistance under the guise of bringing order, information and psychological operations against Ukraine, and organizing rallies supporting Russia's occupation. The main actors are pro-Russian elements within the local population. They include pensioners and people nostalgic for the Soviet Union, criminal authorities, and deserters of the Ukrainian security services and the armed forces. The third component is the military. Its function is to seize and take control of local government and law enforcement agencies. This is done by capturing critical infrastructure objects, the blockade of military structures, establishing border control between Ukraine and the occupied territories, and regular troops blocking the action and fighting the Ukrainian armed forces and national guard. The main actors are the GRU, the FSB, military units of the Southern District and the Black Sea Fleet, and the "division" of the Kuban Cossacks. Fourth, the spontaneous actions of criminal elements by destroying the archives of law enforcement agencies, marauding and robbing banks and private property, taking part in hostilities with other gangs frighten ordinary people and increase societal instability, and seizing weapons and narcotics.

To deal with the threat, Ukraine developed a system of territorial defense based on four pillars. First, the intensification of defense reform measures to accelerate NATO membership and increase the cooperation with its member states. Second, the organization of active and large-scale counteraction to Russian information and cyber operations directed against Ukraine. Third, the creation of modern armed forces based on NATO principles, as part of highly mobile, joint, operational, and tactical units. They are to form an inter-specific strategic group of forces organized under a single command and control comprehensive system. They must successfully resist the offensive operations of groups of troops (forces) of the Armed Forces of the Russian Federation. Fourth, the formation of a modern territorial defense system integrated into the state's general defense system under the leadership of the General Staff of the Armed Forces. These should be able to successfully maintain martial law while organizing the protection and defense of critical infrastructure, especially the military.

This article critically evaluates Ukraine's territorial defense system's implementation and organization, comparing it with the foreign experience. It also identifies and suggests areas for improvement and proposes a better organizational structure to increase the effectiveness of the system of territorial defense.

KEYWORDS

Ukraine; Territorial Defence; Russia; Hybrid Warfare; Defence Planning.

Military Technology and Doctrine and the Current War in Ukraine: Historical Parallels

A. Dizboni (1) and R. Addinall (2)

(1) Royal Military College of Canada and Queen's University, dizboni-a@rmc.ca
(2) Royal Military College of Canada, Robert-Addinall@kingston.net

For approximately the last century (1919-2021) theories of war focused around new possibilities opened up by technological change have tended to dominate much of the discourse surrounding military doctrine, tactics, operations, and strategy. In the immediate aftermath of the First World War air power theorists such as Douhet and William Mitchell advanced ideas about how the use of aircraft would upend old ways of conducting war. Also during the 1920s and 1930s the German army developed by basis for what later came to be called manoeuvre warfare, while the Soviet armed forces developed, and then abandoned, Deep Battle theory, only to effectively re-instate it during the Second World War. After World War Two further changes took place, including what was at times in the mid-twentieth century called the advent of "push button warfare", the emergence of nuclear deterrence theory, and American airmobile operations during the Vietnam war. Manoeuvre warfare concepts underwent a renaissance during the late 20th century, perhaps best embodied by the 1980s American concept of Air and Battle, and were then superseded by the idea of an information technology driven, high-tech "revolution in military affairs" by the late 1990s. During the first two decades of the 21st century many theoretical approaches to warfare in the West, and to an extent other regions of the world, continued to emphasize some combination of manoeuvrist doctrinal and organizational ideas and attempts to leverage the latest technologies to gain a combat edge.

This enthusiasm for technological advancement has tended to be interspersed with bursts of pessimism about some of the major technological innovations of the twentieth century. For example, the death of the tank has been announced repeatedly since the mid-twentieth century, each time that a new generation of anti-tank weapons, including handheld rocket propelled grenades (RPGs) and, more recently, handheld anti-tank guided munitions (ATGMs) cause heavy losses amongst armoured vehicle fleets. Yet, typically, new and improved generations of armoured vehicles appear, and eventually the tank and other similar types of armoured fighting vehicle (AFV) are declared relevant again.

This sort of cycle of enthusiasm for new technology juxtaposed by pessimism about the ongoing relevance of various advanced technological weapons platforms that have come into service over the last several decades has been unfolding at a rapid pace over the past few months of the 2022 Russian invasion of Ukraine. In February and March, Ukrainian military use of drones for intelligence, surveillance and reconnaissance (ISR), combined with use of advanced ATGMs such as the NLAW and Javelin, led again to some questioning of the continued relevance of large AFV fleets. Then, during May and June, combat reverted to conditions resembling in some respects those of the First World War, with the Russian offensive in the Donbas making slow advances based on overwhelming opposing forces with artillery and missile fires. Nonetheless, as of summer 2022 various analysts also seem to believe that introduction of additional technologically complex weapons systems into the conflict, such as American-made MLRS and HIMARs, might disrupt this First World War type stalemate. The argument made in this paper is that the war in Ukraine has something to teach both sides of the century-old debate on military technology and doctrine; "high-tech" systems always have vulnerabilities that can negate much of their "revolutionary" impact on warfare, but reversions to old "tried and true" methods of warfare are also likely to be short-lived. Keeping both of these lessons in mind, although they may sometimes seem to be contradictory, is likely to be important in developing effective analysis of unfolding events.

KEYWORDS

War in Ukraine; First World War; Doctrine and technology; High tech systems.

The annexation of Crimea in 2014: a critical analysis

H. Gouveia (1) and J. Borges (2)

(1) CINAMIL, IUM, gouveia.hmr@exercito.pt
(2) CINAMIL, IUM, jose.borges@academiamilitar.pt

The conflict between Russia and Ukraine is undoubtedly the one that most compromises European security since the end of the Second World War. Russia adopted a rogue posture and challenged the world with a bold operation, unilaterally (re)starting a conflict with Ukraine in late February 2022. The objective of this work is to return to 2014 and analyse another relevant iteration of this conflict: Russia's annexation of Crimea. The political instability that Ukraine experienced in 2014 was the trigger Russia needed to invade and annex Crimea. However, the reasons that led Putin to take such a decision are not explicit.

This work aims to analyse Crimea's conflict by identifying motivations and consequences for all parties, especially Russia and Ukraine, and others responsible for ensuring regional security, namely Europe and NATO. It also intends to identify the reasons that led Putin to invade Ukraine and assess their legitimacy under international law.

Ukraine is the largest country on the European continent. Situated in Eastern Europe, it is bordered by Russia to the east and north-east, Belarus to the north-west, Poland, Slovakia and Hungary to the west, Romania and Moldova to the south-west and the Black Sea and Sea of Azov to the south and south-east respectively. The country had a population of about 45 million inhabitants[4] in 2014, characterised by different ethnicities, languages, religions, historical identities and cultural aspects.

The Crimean Peninsula occupies a strategically important location on the Black Sea and, throughout its history, has been of geostrategic interest to various external forces. In 1783, Crimea became part of the Russian Empire. With the end of the Russian Empire in 1917, it was a sovereign state until 1921, when it became part of the Soviet Union as the Autonomous Soviet Socialist Republic of Crimea. In 1945, following liberation by the Red Army from German occupation during World War II, Crimea became an administrative region of Russia. In 1954, the Soviet Union handed Crimea to the Soviet Socialist Republic of Ukraine (Gillich, 2015).

Ukraine gained sovereignty with the formal dissolution of the Soviet Union in 1991. Crimea remained part of Ukrainian territory, with significant autonomy, an independent constitution and legislation. In 1999 Ukraine and Russia signed the Black Sea Fleet agreement, which was located on the Crimean peninsula, divided between Russia (81.7%) and Ukraine (18.3%), with Russia retaining the right to use the port of Sebastopol in Ukraine until 2017. The treaty also granted Russia rights to station forces and means at its bases in Crimea (Gillich, 2015).

O'Loughlin and Toal (2020) identified the roots of the Crimea conflict in November 2013, when Viktor Yanukovych, Ukraine's president at the time, chose to deepen economic relations with Russia. Ukraine was on the brink of a severe financial crisis; President Yanukovych accepted a loan of around $15 billion from Russia, signalling a move to form the Eurasian Union that unleashed a wave of protests. The government's efforts to suppress these protests eventually strengthened them; president Yanukovych succumbed and left Kyiv on February 21, 2014 (O'Loughlin & Toal, 2020). An interim, pro-Western government resulted in the aftermath.

Vladimir Putin criticised the new government and considered it illegitimate for not observing the Ukrainian constitution. Russia also contested the new government for being made up of extremists who endangered the security of Russians in Ukraine and of Ukrainians themselves. Arguing a moral mission, Putin ordered the invasion of Crimea on February 24, 2014 (Cunha, 2017). Putin further claimed that the Russian government views Ukraine's situation through repeated Western betrayals, the invasion of NATO and disregard for its security concerns. Western countries attribute the tensions between Ukraine and Russia to Russia's reluctance to undertake liberal reforms and cooperate with Western powers, a reluctance they see as being based on historical phobias and yearnings for a return to past greatness (Wolff, 2015). The control over human and industrial resources in Eastern Ukraine, the geostrategic military advantages that this region offers, and the possibility of securing long-term control over the Crimean naval base may have underpinned Putin's decision (Marxsen, 2015).

According to Bukkvoll (2016), Putin has a particularly risk-prone personality. His decision may have been in response to the loss of the seemingly significant geopolitical triumph, i.e. halting Ukraine's westward drift before the overthrow of President Yanukovych. Additionally, Bukkvoll claims that reversing the internal downward trend of Putin's popular approval rating triggered his decision to invade Crimea.

---

[4] https://worldpopulationreview.com/countries/ukraine-population

The 2014 conflict between Russia and Ukraine started on February 24, eight years before Russia launched the 2022 military invasion of Ukraine. The 2014 conflict brought intense combats between the opposing forces, which resulted in immense financial damage, the loss of thousands of human lives[5], mainly Ukrainian, and compromised the international order since then (Cunha, 2017). In the aftermath, pro-Russian movements started several skirmishes in other Ukrainian cities to have these taken as well. Still, without much success except for the Donbas region: pro-Russian fighters became successful in the Donetsk and Luhansk provinces. It led the government in Kyiv to launch a military operation against the group, resulting in intense fighting for possession of the region and thousands of deaths resulting from the clashes (O'Loughlin & Toal, 2020). These provinces remained under the control of the forces of the self-proclaimed Donetsk People's Republic (DPR) and the Russian-backed Luhansk People's Republic (LPR).

The crash of the Malaysia Airlines aeroplane on July 17, 2014, in Donetsk, Ukraine, was a dramatic event that startled the globe in the aftermath of the invasion. A Russian surface-to-air missile fired from a position located in a territory in eastern Ukraine controlled by pro-Russian forces shot down an aeroplane carrying 283 passengers and 15 crew members of various nationalities (Dinis, 2015).

The conflict was not immune to the coronavirus pandemic. An intensified fighting in the Donbas in March 2019 resulted in hundreds of cases of Covid-19 in early May among DPR and LPR forces. These movements received aid from international humanitarian organisations, although they hoped for more significant support from Russia.

Arguably, the annexation of Crimea was advantageous to Russia. While it allowed Russia to control this region's geostrategic and economic potential, it also inflicted a number of setbacks in its strategic pretensions and partnerships. From a military point of view, it is clear that the New Generation Warfare[6] surprised the world and asserted Russia's position in the international community, increasing the security concerns of Europe and NATO. For Ukraine, the consequences were devastating, with the loss of territorial integrity and major economic consequences. For Europe, the conflict brought significant exposure to its weaknesses, e.g. the energy dependence, the lack of Europe's hard power and internal cohesion in defence matters, or the economic crisis's consequences.

The bibliographic research allowed us to conclude that the reasons that led to the annexation of Crimea are rooted in geostrategic issues and those related to President Putin's personality. From a military point of view, Russia surprised the world, raising the security concerns of Europe and NATO. The consequences for Ukraine were devastating, with a loss of territorial integrity and significant economic effects. The conflict has brought awareness and more substantial exposure to its weaknesses for Europe and NATO. The invasion of Ukraine by Russia on February 24, 2022, is the most tragic follow-up of this conflict.

KEYWORDS

Annexation of Crimea; Russian Federation; Ukraine; Europe; NATO.

REFERENCES

Bukkvoll, T. (2016). Why Putin went to war: ideology, interests and decision-making in the Russian use of force in Crimea and Donbas. *Contemporary Politics, 22*(3), 267-282. doi: 10.1080/13569775.2016.1201310

Cunha, G. A. (2017). O conflito Russo-Ucraniano, o gás natural e a segurança energética na europa. *Revista Militar*, 2587-2588, 715-736. Retrieved from http://www.revistamilitar.pt/artigo/1264

Dinis, R. (2015). *Observador*. Retrieved from https://observador.pt/2015/07/16/primeira-versao-relatorio-final-domh17-diz-missil-disparado-rebeldes-pro-russos/

Gillich, I. (2015). Illegally Evading Attribution? Russia's Use of Unmarked Troops in Crimea and International Humanitarian Law. *Vanderbilt Journal of Transnational Law, 48*(5), 1191-1223.

Marxsen, C. (2015). International Law in Crisis: Russia's Struggle for Recognition. *German Yearbook of International Law, 58*. 11-48.

O'Loughlin, J. & Toal, G. (2020). Does War Change Geopolitical Attitudes? A Comparative Analysis of 2014 Surveys in Southeast Ukraine. *Problems of Post-Communism, 67*(3), 303-318.

Wolff, A. T. (2015). The future of NATO enlargement after the Ukraine crisis. *International Affairs, 91*(5), 1103-1121. doi: 10.1111/1468-2346.12400

---

[5] https://www.polgeonow.com/2020/09/ukraine-war-2020-map.html
[6] It combines political subversion with the use of unidentified forces and information warfare.

Comparative analysis of the armed aggression of the Russian Federation against Ukraine in 2014 and 2022

S. Seheda (1)

(1) National Defence University of Ukraine named after Ivan Cherniakhovskyi, voyen_ist@ukr.net

Differences. In February 2014, Russian President Vladimir Putin claimed that the Russian troops in Crimea were in places of their permanent deployment. According to the Russian statements, the streets and villages were patrolled by the Crimean self-defense forces. There were no identification marks on the military men who tried to avoid contacts with local people. There was no armed resistance to the invaders in Crimea. Ukrainian troops did not receive a relevant order from the Command. At the same time, there were peaceful pro-Ukrainian demonstrations of local people.

Russian troops occupied Crimea using weapons for terror. There were isolated cases of murder of Ukrainian servicemen. There was no looting and mass deportation of the population. Special military units of the Russian Federation took part in the seizure of the Verkhovna Rada (parliament) of Crimea. During the occupation of Donetsk and Luhansk regions, Russian servicemen disguised themselves as locals and volunteers. The Russian authorities denied participation of their troops and the supply of weapons.

On February 24, 2022, at 05.40 A.M., the President of the Russian Federation Vladimir Putin openly announced a special military operation to "denazify and demilitarize" Ukraine. Ballistic missiles were fired to the entire territory of Ukraine. Battalion tactical groups of the Russian armed forces, which were concentrated near the Ukrainian borders, including Belarus, invaded the Ukrainian territory. Russian servicemen had identification marks and killed many civilians, destroyed civilian buildings and cars, kept hostages in basements, lived in local private houses without any permission. There were numerous cases of looting, bullying, torturing of civilians, and abduction of Ukrainian officials.

Similarities. The aggression of 2014 and the full-scale invasion of 2022 began in February. The claims of the invaders were similar about "liberation and protection" of the Russian-speaking population. The actions were also similar: the armed occupation of the territories of independent Ukraine, the terror of the population, the abduction of Ukrainian citizens and the large number of displaced persons. There was a similar legend of captured Russian servicemen as if they participated in military drill and no one used their weapons.

There was international support for Ukraine, which became more practical in 2022. The leaders of the European Union acted as mediators between Ukraine and the Russian Federation for a peaceful settlement. In 2014, there were talks on a special status for the temporarily occupied territories of Donbass as a part of Ukraine. The temporarily occupied territory of Crimea, which was claimed by the Russian Federation as its' part, was not mentioned during the talks. In 2022, there were also statements of leaders of certain states about the surrendering of part of the territory of Ukraine in exchange for peace.

However, the successful armed resistance of Ukrainians demonstrated to the international community another solution - a victory of Ukraine and the restoration of the rule of international law through the weakening of the Russian Federation. That's how the war between democratic and autocratic civilizations didn't switch into a simple territorial misunderstanding.

KEYWORDS

Russian aggression; Ukraine; Crimea; Temporary occupation.

Russia's strategic interests and way of warfare: implications for NATO

J. Bērziņš (1)

(1) National Defence Academy of Latvia and 2BA Business School, Janis.Berzins01@mil.lv

Russia's operations in Crimea and Eastern Ukraine, the operation in Syria, the immigrant crisis in the Poland and the Baltic States' borders, and most recently, the build-up near Ukrainian borders in what has been considered preparations for kinetic conflict surprised many Westerners as they innovatively employed well-known warfare methods with new technologies. Since 2014, Western analysts applied a wide range of new epithets to aggressive Russian actions short of open war, including hybrid warfare and hybrid threat, nonlinear warfare, fourth generation warfare, Gerasimov Doctrine, and most recently "gray zone" conflict. This has created a serious methodological problem since it projects strategic objectives and military instruments on Russia.

Though such analysis can be useful for Westerners determining how to train in response, it cripples understanding of official Russian sources as Western analysts search them in vain for references to the concepts they have been taught. In other words, it ignores the current Russian strategic culture and operational code influenced by both Soviet operational art and Western – mainly American – doctrine[7].

These Western inventions have perverted understanding of Russian strategy and operational art, misinforming officers and policymakers alike. It is fundamental to understand how the Russian Armed Forces define and practice its operational doctrine and how future warfare concepts are modeled in operations and exercises. In other words, to understand the Russian way of warfare as defined by the Russians rather than Westerners. A second issue is that compartmentalizing the Russian strategy within the boundaries of Western concepts limits our understanding of its flexibility.

The Russian military strategy and operational art are rarely valid beyond a single region. It is necessary to evaluate Russia's geopolitical interests in each geographical area to predict its posture and determine a strategic policy to deter 'below the threshold' and across all operational domains.

One of the main challenges is national resilience. It has two main aspects. First, the question of Russia interfering in Western democracy, for example, influencing election outcomes. Another, and no less critical, is influencing public opinion to make Western and allied countries' populations support Russia's interests. In other words, two fair questions are "what is NATO's role in political warfare, if any?" and "do the military have a role in increasing societal resilience, considering that one of the main issues exploited by the Russian is the disconnection between the State and society?" Answering these questions is fundamental for developing proper tools to deter this kind of "hybrid" operations.

This article aims to present a preliminary evaluation of the issues discussed above, providing a base for formulating the Russian threat within the NATO Strategic Concept and avenues for further discussions and research.

---

[7] See Berzins, J. (2020). The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *Journal of Slavic Military Studies, 33*(03). doi: 10.1080/13518046.2020.1824109.

Russian information war against Ukraine during Russian invasion in Ukraine: Russian strategic narratives against Ukrainian state, government, army and society

V. Sazonov (1)

(1) Estonian Military Academy, sazonov@ut.ee

The goal of this paper is to study Russian information war in the context of the war of Russia against Ukraine. I will focus on Russian strategic narratives which were disseminated by Russia against Ukrainian state, government, Ukrainian armed forces, and Ukrainian society since 2022.

Influencing activities can be considered a type of military activity in the modern security environment, which Russian Federation has used extensively in the escalation of the crisis and then war in Ukraine to support the Kremlin's military actions since 2014 (Ramsay, & Robertshaw, 2019). The war launched against the Ukraine on 24th February 2022 is a consequence of the gradual escalation of long-term Russian influence. To justify the war and war crimes against Ukraine, Russia continues to use various propaganda narratives in its influence activity. Russian information war narratives are largely based on Russia's opposition to Ukraine and more broadly the Western world and its institutions (Mölder, 2021; Mölder, Sazonov, 2020;Ventsel et al., 2021).

One of the important tools of this information influence are strategic narratives. Roselle et al. (2021) have argued that the soft power of the 21st century are strategic narratives. Strategic narratives are stories disseminated to the public that are used by political actors (various organizations, states, etc.) as a means of shaping the common past, present and future of international politics to shape the perceptions and behavior of domestic and international actors. Antoniades et al. (2010, p. 5) have argued that strategic narratives are representations of a sequence of events and identities, communicative means by which the political elite seeks to give purposeful meaning to the past, present, and future in order to achieve political goals. Miskimmon, O'Loughlin and Roselle (2013) accentuate that strategic narratives can affect following dimensions:

- the international system, expressing how a political actor (state or international organization(s), interest group) shapes perceptions of the organization of international relations;
- policies (e.g., the desire of political actors to influence international arms control negotiations or for example to interfere in the parties' disputes over the management of armed conflicts);
- identity, ie how political actors want to project their identity in international relations.

The strategic narratives created and disseminated by Russia are aimed at various target groups, including anti-US, anti-EU groups and other movements, groups, etc. By spreading this kind of strategic narratives, several populist political movements and politicians in the Western world (from both the left and right wing) are also exploited. As revisionist and imperialist power Russia is trying to influence not only the post-Soviet space, but it is also trying to shape opinions outside the post-Soviet space (Mölder, & Sazonov 2020).

During war in Ukraine Kremlin has not changed its strategy and is continuing to try influence Western world and to harm Euro-Atlantic security architecture. For this purpose, various strategic narratives were created by Kremlin and pro-Kremlin forces that would amplify or shape perceptions of the world and political preferences in accordance with the foreign policy goals of Russia.

KEYWORDS

Russia: Ukraine; Information war; Strategic narratives.

REFERENCES

Antoniades, A. et al. (2010). *Great Power Politics and Strategic Narratives.* Global Political Economy Center, University of Sussex.

Hinck, R. S., Kluver, R., & Cooley, S. (2018). Russia re-envisions the world: strategic narratives in Russian broadcast and news media during 2015. *Russian Journal of Communication, 10(1),* 21-37.

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic Narratives: Communication Power and the New World Order.* Routledge.

Mölder, H. (2021). Culture of Fear: the Decline of Europe in Russian political imagination. In: A. Krouwel, & A. Önnerfors (Eds.), *A Continent of Conspiracies: Conspiracy Theories in and about Europe. Abingdon-onThames*, England (pp. 231-252). UK: Routledge.

Mölder, H., & Sazonov, V. (2020). Kremlin Information Campaign in the Baltic States During the COVID-19 Pandemic Escalation of Spring 2020. *Modern Management Revue XXV*, *27*(4), 83-97.

Mölder, H., & Sazonov, V. (2018). Information Warfare as the Hobbesian concept of Modern Times – Principles, Techniques and Tools of Russian Information Operations in Donbass. *The Journal of Slavic Military Studies*, *31*(3), 308-328.

Mölder, H., & Shiraev, E. (2021). Global Knowledge Warfare, Strategic Imagination, Uncertainty and Fear. In: H. Mölder et al. (Eds.), *The Russian Federation in the Global Information Warfare* (pp. 13-32). Springer.

Ramsay, G., & Robertshaw, S. (2019). *Weaponising News: RT, Sputnik and Targeted Disinformation*. London: King's College London.

Roselle, L., Miskimmon, A., & O'Loughlin, B. (2014). Strategic narrative: A new means to understand soft power. Media. *War & Conflict*, *7*(1), 70-84.

Roselle, L., Miskimmon, A., & O'Loughlin, B. (2021). Strateegiline narratiiv: pehme jõu uus käsitlus. *Sõjateadlane,* 17, 13-32.

Ventsel, A. et al. (2021). Discourse of fear in strategic narratives: The case of Russia's Zapad war games. *Media War & Conflict, 14*(1), 21-39.

How Russia's Hybrid Warfare is Changing?

L. Goodson (1) and M. Żakowska (2)

(1) U.S. Army War College, larry.goodson@armywarcollege.edu
(2) War Studies University, Poland, m.zakowska@akademia.mil.pl

Russia's invasion of Georgia in 2008, followed by the invasions of Ukraine (2014, 2022) changed the previous understanding of war and its conduct. Russia's actions against these independent states, described as hybrid warfare, challenges their choice of democracy, and European and Euro-Atlantic values and the West's collective resolve to defend these principles and the rules-based international order. The article aims to examine Russia's hybrid tactics below the threshold of conventional war used against Georgia and Ukraine to secure the sphere of influence by destabilizing those states' internal security and territorial integrity. The research focuses on analyzing the hybrid methods used by Russia, including: (i) "borderization" policy; (ii) use of separatist movements and local unrest and (iii) disinformation campaigns. The study's methodological framework is based on the clash of interests approach and Gerasimov's doctrine of non-linear warfare. Evidence suggests that the Georgia War of 2008 and Ukraine War of 2014-2021 clearly demonstrate the reality of Russia's approach to hybrid war. However, comparison with the Ukraine War since February 2022 suggest that some hybrid war measures may be evolving. The earlier wars suggest that Russia's hybrid tactics are the first step to "opening the door" to implement a military operation in another state's territory. Russia undermines the sovereignty of the targeted states through election meddling to establish pro-Russian local government and induces widespread disinformation to build pro-Russian sentiments in the targeted society. Gerasimov's doctrine of non-linear warfare accepts the reality of conventional means of war being used, but the war since February 2022 suggests that hybrid war approaches as used in the earlier wars did not achieve Russian ends, thus leading to the use of traditional conventional means that call into question the utility of hybrid war. This allows for identifying determinants that show how Russia's hybrid war is changing.

KEYWORDS

Joint operations in the European Arctic

A. Lundesgaard (1)

(1) Norwegian Defence Command and Staff College, amlundesgaard@mil.no

Although the correlation of forces between Russia and NATO is more favourable than it was during the Cold War, Russia still presents a challenges to NATO in the European Arctic, and maintaining the ability to conduct joint operations in the region is arguably vital to the alliance. The aim of the paper is to present a broad picture of the strategic circumstances and challenges of conducting joint operations in the European Arctic. To do this, the paper addresses the challenge that Russia poses to NATO in the region, and the availability of select NATO allies' forces for operations in the region. The paper argues that NATO is not fully prepared for operations in the European Arctic, in large part due to uncertainty regarding the availability of forces to address the Russian challenge in the region.

In his speech at the 2019 meeting of the Russian Academy of Military Sciences, General Valery Gerasimov, Russia's Chief of the General Staff, presented what he termed a "strategy of active defence".

(Gerasimov, 2019). Arguably, this strategy is strategically defensive and operationally offensive (Bredesen & Friis, 2020; Gerasimov, 2019; Kofman, 2020, p. 4; Kvam, 2020, pp. 27-28, 39-43). Russian forces have significant disadvantages in a drawn-out war with NATO, and Moscow emphasises the initial phases of a conflict. This approach to warfare failed in Ukraine, however, operations in the European Arctic have a much stronger maritime component, and it is thus an open question to what degree the lessons from Ukraine apply to the European Arctic. Nevertheless, the initial phase of a potential war remains Moscow's emphasis, necessitating a rapid response from NATO. Russia also presents a challenge below the threshold of war in the region, such as the potential use of Russian crewed and owned commercial vessels as part of grey zone operations. A significant issue for the Arctic nations and their allies is what mandates allied assistance, and although it is difficult to have a pre-defined red line, awareness of the challenge and its complexities is vital.

The likely accession to NATO of Sweden and Finland will strengthen the air and land components of the defence of the region; however, the maritime defence will likely not benefit as much from the alliance expansion. The region has been, and will likely continue to be, reliant on swift reinforcements from allies, particularly in the maritime domain. Providing such a rapid response to the European Arctic is arguably NATO's most significant challenge in the region. The US practises what the author has termed a high-profile, lowavailability (HIPLA) approach to the region (Lundesgaard, Forthcoming). The availability of Washington's maritime forces for reinforcing the region in the event of a war are generally low, and the US compensates for this shortcoming by keeping a high profile on its intermittent presence in the European Arctic. US aircraft are likely the fastest responders, but Washington must maintain its strategic interests in other regions as well, limiting the number of aircraft that it can surge to the European Arctic.

The immediate defence of the European Arctic thus falls to the Nordic countries and their European allies. Principal among these European allies are the UK and the Netherlands. Both countries are heavily involved in the defence of the region through UK and Dutch Royal Marines, are members of the Joint Expeditionary Force (JEF), and have a significant naval presence in the region. These two countries are geographically close to the European Arctic and therefore well situated to reinforce the region in the event of an armed conflict. However, their availability for operations in the region is also uncertain due to, among other things, commitments elsewhere and reduced force structures.

Thus, NATO is not fully prepared for operations in the European Arctic, and a significant factor in the lack of preparedness is uncertainty regarding the availability of forces for operations in the region.

KEYWORDS

Military operations; European Arctic; military strategy; NATO; Russia.

REFERENCES

Bredesen, M. G., & Friis, K. (2020). Missiles, Vessels and Active Defence. *The RUSI Journal, 165*(5-6), 68-78. doi: https://doi.org/10.1080/03071847.2020.1829991

Gerasimov, V. (2019, 2 March) *Speech given at the Annual Meeting of the Academy of Military Science*. Moscow.

Kofman, M. (2020). Russian A2/AD: It is not overrated, just poorly understood. Retrieved from https://www.stratagem.no/russian-a2-ad-misunderstood/

Kvam, I. H.-P. (2020). Nordflåtens evne til kystnær maktprojeksjon. Implikasjoner for Bastionsforsvaret (The Northern Fleet's Capacity for Littoral Power Projection. Implications for the Bastion Defence). In: R. Espevik & B. Terjesen (Eds.), *Sjømilitær utvikling i Russland og Kina. Grunnlag for bekymring?* (pp. 22-58). Haakonsvern: The Norwegian Defence University College.

Lundesgaard, A. (Forthcoming). High Profile, Low Availability: The Emerging US Maritime-Strategic Approach to NATO's Northern Flank. *Scandinavian Journal of Military Studies*.

China's presence in the Arctic: A game theoretic perspective

A. Sokri (1)

(1) DRDC CORA, Canada, Sokriab@gmail.com

BACKGROUND

The Arctic is one of the world's purest and richest regions (Ekerhovd, 2013; Fata, 2009). As shown in Figure 1, the Arctic region is surrounded by the northern coasts of Europe, Asia, and North America (Boring, 2014). The area covers more than 30 million square kilometres representing about one-sixth of the planet's landmass. The region is the site of approximately 30 % of the world's undiscovered natural gas, 13 % of the world's estimated oil reserves, and 10 % of the world fish stocks. The Arctic also holds the sea passage between Asia and Europe (Berg, 2014; Borgerson, 2009; Ghanmi, & Sokri, 2010; Robertson, & Pierce; 2008;). As the ice melts due to transformations from climate change, the Arctic region is expected to become more accessible creating a real treasure hunt with many geopolitical interactions.

Figure 1 - The Arctic coastal nations

CHINA'S STRATEGY

China is a non-Arctic state that plans to become one of the main geopolitical actors in the region. It describes itself as a "near-Arctic state" and follows three main objectives in the Arctic:
- To get a share of the region's natural resources;
- To secure shorter shipping routes from the Pacific to the Atlantic; and
- To bolster its position as an emerging superpower (Virtanen, 2013).

To reach these objectives, China uses three different means:
- By conducting research in the region on environment, economy, and security to inform its decisions;
- By building political and economic relationships with some Arctic countries such as Norway and Iceland, and
- By cooperating with other Arctic and non-Arctic nations such as the United States and India to state that the sea passage is an international route and should be open to all nations.

AIM

The aim of this paper is to discuss China's strategy in the Arctic using game theory. This discipline uses proven mathematics to understand the strategic interactions between two or more players (Sokri, & Ghanmi, 2021). Its reasoning is well-suited to many problems in the Arctic (Cole, 2014). It can particularly translate the interactions between the Arctic and non-Arctic nations into graphs and clear mathematical models. The paper also offers a comprehensive review of literature on the application of game theory in the main international issues in the region.

KEYWORDS

The Arctic; Strategy; China; Game theory.

REFERENCES

Berg, S. (2014). Arctic states' strategies-how to defend the arctic market.

Boring, K. T. (2014). *Operational Arctic: The Potential for Crisis or Conflict in the Arctic Region and Application of Operational Art*. Army Command and General Staff College Fort Leavenworth KS School of Advanced Military Studies.

Cole, S., Izmalkov, S., & Sjöberg, E. (2014). Games in the Arctic: applying game theory insights to Arctic challenges. *Polar research, 33*(1), 23357.

Ekerhovd, N. A. (2013). Climate change and the benefits of cooperation in harvesting North-East Arctic cod. *Strategic Behavior and the Environment, 3*(1-2), 7-30.

Fata, D. P. (2009). *Arctic security: the new great game?. Policy Brief.* Washington: The German Marshall Fund of the United States.

Ghanmi, A., & Sokri, A. (2010). Airships for military logistics heavy lift: A performance assessment for Northern operation applications. DRDC-CORA, *Technical Memorandum, 63*.

Ghanmi, A. & Sokri, A. (2021). *How game theory can enhance wargames*. DRDC Scientific Report, DRDCRDDC-2021-R112.

Konyshev V.N. (2020). Is the arctic on the brink of a hybrid war? *Arktika i Sever* [Arctic and North], 40, 165–182.

Lagutina, M., & Leksyutina, Y. (2019). BRICS Countries' Strategies in the Arctic and the Prospects for Consolidated BRICS Agenda in the Arctic. *The Polar Journal, 9*(1), 45-63.

Robertson, J., & Pierce, B. (2008). *90 Billion Barrels of Oil and 1,670 Trillion Cubic Feet of Natural Gas Assessed in the Arctic*, *USGS, 2014*.

Rudd, D. (2021). *State-based challenges to peace and stability in the Arctic: Possible implications for Canada*. DRDC Scientific Report, DRDC-RDDC-2021-R157.

Virtanen, V. (2013). *The Arctic in world politics. The United States, Russia, and China in the Arctic— implications for Finland*. Weatherhead Center for International Affairs, Harvard University, 56.

Leveraging cultural differences in the High North

J. Kibsgaard (1)

(1) Norwegian Defence University College/Norwegian Military Academy, jkibsgaard@mil.no

A military campaign in the High North involving Norway would by default be both a joint and a multinational venture.

A set of multinational military organizations operating together can be very powerful. However, achieving synergies between air forces, armies and navies from different countries comes with its own inherent set of challenges. The friction generated by cultural differences is one of the major challenges to generating the full power potential of a multinational joint force (Andersen, 2016, p. 26). Cultural differences can for instance challenge concepts such as unity of command and unity of effort (Gundersen, 2016, p. 235; Norwegian Defence Staff, 2019, p. 88). The bottom line is that culture influences military organizations and their ability to fight wars significantly (Mansoor & Murray, 2019). Rather than being a liability, knowing and exploiting its cultural differences could provide a multinational force with an advantage when facing a culturally uniform opponent such as Russia (Berger, 2021, p. 5).

The research project Impact on Teamwork and Leadership in Combined Joint Operations in the High North will develop knowledge facilitating leveraging the potential benefits of cultural diversity within the alliance. The point of departure for the project will be the leadership philosophy mission command (MC). MC is a key concept for warfighting; moreover, it is also important for conducting multi-domain operations short of armed conflict (Balboni et al., 2020, p. 43). The project will approach MC from both a leader and a follower perspective, building on e.g. theory on implicit leadership and followership (ILT, IFT) (Lord et al., 2020) and Project GLOBE's research on culturally contingent ILT (CILT) (House et al., n.d.).

The project consists of three studies. The first study will investigate how cultural preferences of officers from different countries impact MC-based ILTs. The second study will look at how interaction and team efficiency vary and is moderated in multinational teams conducting/training for military planning and operations on a dayto-day basis through the lens of different leadership theories (e.g. Full Range of Leadership model, empowerment-based leadership). The third study will include a training intervention. The study will first aim at enhancing the ability of multinational military teams to be effective and subsequently measure the effects of the intervention. The High North signature of the research project is maintained through sampling officers and teams that have a similar multinational composition to what is expected in a High North campaign/operation. In light of the likely prospect of inclusion of Finland and Sweden into NATO (Alberque, & Schreer, 2022, p. 67), special effort will be made in order to integrate these cultures in the samples.

KEYWORDS

Mission command; High North; Multi-domain operations; Multinational teams.

ACKNOWLEDGMENTS

REFERENCES

Alberque, W., & Schreer, B. (2022). Finland, Sweden and NATO Membership. *Survival*, *64*(3), 67–72. Retrieved from https://doi.org/10.1080/00396338.2022.2078046

Andersen, M. (2016). Hva er fellesoperasjoner? In: M. Andersen & G. Ødegaard (Eds.), *Militære fellesoperasjoner— En innføring* (pp. 21–28). Abstrakt.

Balboni, M., Bonin, J. A., Mundell, R., Orsi, D., Bondra, C., Dunmyer, A., Marks, L. "Fran," & Miller, D. (2020). *Analyzing Mission Command Principles in Support of Multi-Domain Operations Short of Armed Conflict* (Mission Command of Multi-Domain Operations, pp. 33–44). Strategic Studies Institute, US Army War College. Retrieved from https://www.jstor.org/stable/resrep26552.9

Berger, D. H. (2021). *Talent Management 2030*. Headquarters Marine Corps. Retrieved from https://www.hqmc.marines.mil/Portals/142/Users/183/35/4535/Talent%20Management%202030_Nove mber%202021.pdf?ver=E88HXGUdUQoiB-edNPKOaA%3D%3D

Gundersen, P. C. (2016). Kommando og kontroll. In: M. Andersen & G. Ødegaard (Eds.), *Militære fellesoperasjoner— En innføring* (pp. 231–242). Abstrakt.

House, R. J., Dorfman, P. W., Javidan, M., Hanges, P. J., & de Luque, M. S. (n.d.). *Strategic Leadership Across Cultures: The GLOBE Study of CEO Leadership Behavior and Effectiveness in 24 Countries*.

Lord, R. G., Epitropaki, O., Foti, R. J., & Hansbrough, T. K. (2020). Implicit Leadership Theories, Implicit Followership Theories, and Dynamic Processing of Leadership Information. *Annual Review of Organizational Psychology and Organizational Behavior*, *7*(1), 49–74. doi: https://doi.org/10.1146/annurevorgpsych-012119-045434

Mansoor, P. R., & Murray, W. (Eds.). (2019). *The culture of military organizations*. Cambridge University Press.

Norwegian Defence Staff. (2019). Forsvarets fellesoperative doktrine. *272*. Forsvarsstaben. Retrieved from https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2631948

Future Dutch Navy contributions to operations in the High North

H. Warnar (1)

(1) Netherlands Defence Academy, h.warnar.01@mindef.nl

Reacting to the changing security situation, in June 2022 the Dutch Government has launched a new Defence Whitepaper that sketches the outlines for a 40% rise of its budget (MOD, 2022). In the maritime domain these plans consist of four pillars: amphibious warfare, submarines, ASW and Air Defence frigates and a land strike capability. Military innovation in small states such as the Netherlands often follows patterns of emulation in which doctrine and concepts are copied from abroad (de Wijk & Osinga, 2010; Farrell, Rynning, & Terriff 2013; Farrell & Terriff, 2002). Also, innovation is too often driven by cultural or technical factors rather than strategy and particularly small navies are challenged to define strategy (McCabe, Sanders, & Speller, 2019). A strategy to counter Russian threats in the High North should address asymmetric, grey zone naval operations, deter and defend against Russian aggression and methods to respond to crisis. This should be resolute and credible but also prevent undesirable escalation. Broad questions that undoubtedly qualify for this conference's subject of the incomprehensible and non-linear world but also imply the risk of strategy failure. To explore these risks in the Dutch choices, its four pillars will be evaluated through a strategy lens and for each of these capabilities the following questions will be addressed:

–   To what allied objective or end will it specifically contribute?
–   How will this be done?
–   Can the means be sustainably provided for?

It will be argued that the first three pillars appear strategically sound but that implementation of a land attack capability needs further research.

The Dutch amphibious force will be invigorated by more enablers such as precision strike weapons and the four ocean-going patrol vessels and two large Landing Platforms Docks will be replaced by six relatively small amphibious warfare vessels (LPX). These warships will conduct both amphibious warfighting and constabulary tasks. Replacing large with more and smaller amphibious warships makes sense in the context of Distributed Maritime Operations aiming to reduce vulnerability to A2/AD threat. Smaller vessels also fit the expected more limited style of amphibious and crisis response operations. Institutional arrangements consist of the UK/NL Amphib cooperation at brigade level and in the previous years detailed doctrine (FLITOC) has been developed and is further aligned with US and British counterparts within the NATO Amphibious Leaders Expeditionary Symposium (NALES) working group (Germanovich et al., 2019). So far these means seem to involve recruitable numbers of marines and affordable financial costs.

The Dutch MOD is replacing its Walrus class submarines with modern submarines of comparable but updated capabilities. These boats will be able to conduct intelligence and denial operations under A2/AD threat conditions and support Specials Forces. Dutch submarine operations build on more than hundred years of experience, largely in cooperation with British and US partners. In size the submarine service will maintain its existing size and history indicates that despite huge investments costs, exploitation has been reasonably affordable.

ASW and Air Defence frigates have always been the core of the Dutch fleet and both capabilities will be replaced by state-of-the-art versions. Although currently in the High North a balance of forces exists, both sides heavily tilt towards the offence (Kaushal, 2022). In the Netherlands such a tilt has been encouraged by thinktank HCSS that recommended to invest in land strike attack (Bekkers, 2019). This paper argues that defensive frigates provide denial capabilities that provide initiative and escalatory flexibility required in crisis response operations. Institutional connections with the Royal Navy and the Dutch industrial base ensure that Dutch Task Group participation is well integrated and sustainable.

The Dutch government announced to invest in land attack missiles. Although these are required within the alliance at sufficient numbers to conduct pre-emptive or coercive strikes the question is whether the Dutch Navy is the most efficient agent to deliver it. It is technically relatively easy to install strike weapons on Dutch Frigates. However, implementation of this entirely new capability, requires informed participation in intelligence and targeting processes by a country that is not a 5-eyes member. It will require new education, training and doctrine development. More research is needed to explore feasibility and sustainability.

KEYWORDS

High North; Small Navy; Strategy; NATO; Innovation.

REFERENCES

Bekkers, F. (2019). *Geopolitics and Maritime Security, a Broad Perspective on the Future Capability Portfolio of the Royal Netherlands Navy.* HCSS.

de Wijk, R., & Osinga, F (2010). 6 Innovating on a Shrinking Playing Field: Military Change in the Netherlands Armed Forces. In: *A Transformation Gap?*, 108-43. Stanford University Press.

Farrell, T., & Terriff, T. (2002). *The Sources of Military Change: Culture, Politics, Technology.* Lynne Rienner Publishers.

Farrell, T., Rynning, S., & Terriff, T. (2013). *Transforming Military Power since the Cold War: Britain, France, and the United States, 1991–2012.* Cambridge University Press.

Germanovich, G., Williams, J. D., Pettyjohn, S. L., Shlapak, D.A., Atler, A. & Martin, B. (2019). *Nato's Amphibious Forces: Command and Control of a Multibrigade Alliance Task Force.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR2928.html

Kaushal, S. (2022). The Balance of Power between Russia and NATO in the Arctic and High North. *Whitehall Papers* 100, 1, 96-98. doi: https://doi.org/10.1080/02681307.2022.2030971

McCabe, R., Sanders, D. & Speller, I. (2019). *Europe, Small Navies and Maritime Security: Balancing Traditional Roles and Emergent Threats in the 21st Century.* Routledge.

MOD, NL. (2022). *A Stronger Netherlands, a Safer Europe, Investing Ina Robust Nato Amnd Eu, Defence White Paper 2022 (Summary).*

The European Arctic – an undervalued and inadequately understood strategic hotspot

T. Strømmen (1)

(1) Royal Norwegian Naval Academy, tstromme@mil.no

In a geostrategic sense, the European Arctic is almost exclusively a maritime theatre. In all other geographical areas where Russia and NATO could fight each other by armed force, land power will be the most important whilst the maritime component will first and foremost be an enabler. Not only is the European Arctic a predominately maritime theatre of war, but in addition, the outcome of naval warfighting here could have an overall war-decisive effect on a great power conflict. It is thus of vital interest for the Alliance to understand this theatre and what Russia would like to achieve in and from it, and what they would like to prevent.

The foremost driver for the strategical importance of the European Arctic is nuclear deterrence. Russian strategic submarines (SSBNs) operate here and constitutes Russia's most viable 2nd strike and hence escalation control means. That fact also means that the region is a hotspot for Allied strategic anti-submarine operations and thereto strike warfare against key shore-based infrastructure. Furthermore, Russia is unlikely to be content with fending of NATO-attacks, it could be expected that Russia would mount their own strategic ASW against US, UK, and French SSBNs operating in the deep Atlantic to gain an advantageous nuclear force correlation.

The Nordic countries form a strategic island in NATO and hence depends on the maritime domain for any substantial allied support. Moreover, transatlantic, and interregional seaborne communications are of vital strategic importance for the Alliance. Any substantial threats against these communications would likely originate from the Arctic. Finally, Carrier strike groups, submarines, and long-range strategic bombers represent the most potent and readily available US counterforce if a conflict rapidly escalates into great power warfare. Although impressive tools, those assets still depend on access to sufficiently high value targets if they are to provide effective strategic leverage. The Arctic, due to both geography and the important strategic targets it contains, would be the obvious region to employ such means in.

There are no bilateral conflicts of interests between Russia and here European Arctic neighbours that are of huge strategic significance for Russia. In addition, the Nordic Countries are NATO members (or soon to be). Hence, the likelihood of bilateral war or warlike situations between Russia and any Nordic country remains low. However, for geostrategic reasons, the very same region would unquestionably experience spill-over from any other region or conflict where NATO and Russia clashes by arms. Key aspects of a great power war would by reasons of geography alone play out in the European Arctic, and those aspects would be so predominately maritime that land warfare in the region would only be important to the extent it influences developments at or from the sea.

Thus, it is of the outmost importance for the Alliance to understand Russian aims and operational approaches in this maritime region. Unfortunately, it seems like the Western understanding largely adheres to a rather dated and much misunderstood concept called the Bastion Defence. A concept that has been around since 1973 (Breemer, 1985; Dismukes, 2020). The Bastion Defence concept was an operational approach to ensure that Soviet SSBNs maintained operational freedom and turned them into guarantors for the survival of the state. In much Western literature it is claimed that Russian aim to maintain sea control east of North Cape and sea denial north of the Greenland-Iceland-United Kingdom line (Cantrill & Meyer, 2019, pp. 253-254; Forsvarsdepartementet, 2015; Olsen, 2017, pp. 4, 23-24; Skjelland et al., 2019). That is a dangerous and very dogmatic view of Russian capabilities, aims, and operational approaches. First of all, neither the Soviets nor Russia has ever used the term "Bastion Defence". For them it was only a geographic area were geography allowed them to effectively limit the threat and improve operational security through concentration and utilisation of defensive and joint capabilities (Kuzin & Chernyavskii, 2005). These ideas of control and denial are also not supported by current naval thinking, history, seapower theory, or unclassified Russian doctrine papers. I would suggest that our understanding of Russian operational art in and from this region rather should be approached using a multifarious analysis of naval and other military resources, technological developments, ship-building, and likely operational and strategic aims. I therefore claim that although we understand what Russia would like to achieve, and what she needs to achieve, we do not understand how she would like to achieve it, what tools and means she would employ, nor how she would employ them.

My paper will hence focus on alternative views of how Russia could go forth to secure her strategic objectives in and from this region. Views that collectively would offer much better understanding of both grand strategic objectives as well as naval operational art, and hence both what we potentially are up against and how we could or should act to effectively defeat them or rather their operational approaches.

KEYWORDS

A maritime theatre; Bastion defence; Strategic understanding; Russian operational approach; Strategic submarines; Nuclear correlation.

REFERENCES

Breemer, J. S. (1985). The Soviet navy's SSBN bastions: Evidence, inference, and alternative scenarios. *The RUSI Journal*, *130*(1), 18-26.

Cantrill, R., & Meyer, E. L. (2019). The JEF as a Force Multiplier: The Example of Joint Amphibious Response in the Nordic-Baltic Theatre. I *The United Kingdom's Defence After Brexit* (s. 245261). Springer.

Dismukes, B. (2020). The Return of Great-Power Competition—Cold War Lessons about Strategic Antisubmarine Warfare and Defense of Sea Lines of Communication. *Naval War College Review*, *73*(3), 6.

Forsvarsdepartementet. (2015). *Et felles løft: Ekspertgruppen for forsvaret av Norge*. Forsvarsdepartementet.

Kuzin, V., & Chernyavskii, S. (2005). Russian Reactions to Reagan's 'Maritime Strategy'. *Journal of Strategic Studies*, *28*(2), 429-439.

Olsen, J. A. (2017). *NATO and the North Atlantic: Revitalising Collective Defence*. Routledge.

Skjelland., E., Glærum, S., Beadle, A. W., Endregard, M., Guttelvik, M. S., Hennum, A. C., Kvalvik, S. N., Køber, P. K., Mørkved, T., & Olsen, K. E. (2019). *Hvordan styrke forsvaret av Norge?-Et innspill til ny langtidsplan (2021–2024)* (8246431536). FFI.

The Royal Navy and the Evolving Balance of Power in the Arctic and High North

S. Kaushal (1)

(1) Royal United Services Institute, United Kingdom, sidharthk@rusi.org

The purpose of the presented research will be to examine trends in the Arctic and High North which will shape the role of the Royal Navy in the region. The authors core hypothesis is that the evolution of the capabilities of the Russian Northern Fleet and Northern Joint Strategic Command (OSK Sever) will make a reactive maritime posture in the region increasingly difficult to sustain in conflict and will necessitate an adaptation in NATO's regional approach. This, in turn, will play a significant role in shaping the Royal Navy's missions and capability requirements going forward.

The revitalization of the Northern Fleet's capabilities, underscored by the establishment and reestablishment of a number of facilities along the Russian Arctic seaboard, poses prospective challenges to western freedom of action in both competition and conflict. The fleet has received a number of new assets, including the Yasen and Yasen-M submarines, which will substantially complicate the task of ASW, while ground and air based precision strike capabilities such as the P-800M and the air launched Kinzhal can pose a substantial threat to surface vessels well into the Barents Sea. Crucially, the near ubiquitous presence of long range precisions strike assets such as the 3M-14 Kalibr and the 3M22 Zircon on both surface and subsurface assets means that a barrier strategy of holding Russian submarines at the GIUK gap may well become inoperable. Moreover, equipped with these capabilities, the Russian surface and subsurface fleet may well be able to hold large swathes of Europe at risk from positions at or close to its maritime bastions.

As a result, then, NATO will likely have to defend forward in a conflict. As detailed by the author (Kaushal et al 2022) in a recent publication, this will substantially strain both the readiness and operating concepts of the UK and its partners within NATO. However, gaps in the defensive architecture of the Russian northern fleet- especially in the area of ASW- will also provide certain operational opportunities for a front footed approach in the high north- making it NATO's most viable option. The purpose of this presentation will be to lay out the rationale for a forward posture and its implications for the Royal Navy with respect to force design and operational requirements.

KEYWORDS

Military Sciences; Arctic; Navy.

REFERENCES

Kaushal, S. et al. (2022). *The Balance of Power Between Russia and NATO in the Arctic and High North*. London: Taylor and Francis.

Norwegian Problems of Confidence Building: Geopolitical Exposure and Military Vulnerabilities in the High North

T. Heiner (1)

(1) Norwegian Defence Command and Staff College, theier@mil.no

Russia's European neighbours are often forced to balance between deterrence and reassurance. Deterrence, by inviting US- and other NATO-forces closer to its' border for security reasons; reassurance, by keeping the same American forces at an arm's length to avoid unnecessary tension with Russia. However, as Russia went to war against Ukraine in February 2022, what are the prospects for confidence building in the High North, as seen from a Norwegian perspective?

The analysis starts by presenting a theoretical model of explanation. Thereafter, prospect for Norwegian non-antagonist behaviour vis-à-vis Russia is described; partly within the context of geopolitical exposure to US-Russian rivalry, and partly within the context of military vulnerabilities inside Norway's force structure. The chapter thereafter analyses Norwegian prospects for confidence building measures towards Russia with reference to the two variables.

The main finding is as follows: The two variables Geostrategic exposure and Military vulnerability seems to have a strong sense of covariance; increased US-Russian rivalry in the Arctic coincided with grave operative deficiencies inside Norway's force structure. As Russia annexed Crimea in 2014 and invaded Ukraine in 2022, Norwegian confidence building efforts became exposed to a dual pressure: Externally, from two assertive powers characterizing each other as strategic rivals in the High North. Internally, from military vulnerabilities inside a small force unable to sustain a credible presence outside Norway's coast.

A militarily irrelevant force that, according to the former Chief of Defence, Admiral Haakon Bruun-Hanssen, only can execute peace-time operations, therefore has made Norway more exposed to a growing security dilemma after the Ukrainian War. Lack of navy vessels, air crafts, manning and logistics in the vast air and sea space outside Norway has increased US-dependency. Following the Ukrainian War, this dependency makes it difficult to forge a consistent non-antagonist strategy towards Russia because US-forces must compensate for Norwegian operative deficiencies.

This is not to say that non-antagonist behaviour towards Russia is impossible. On the contrary, Norway's Centre-Left government is still keeping US forces at an arm's length west of the 24th longitude in order to avoid unnecessary provocations towards the Northern Fleet. The same government also urges US and other allied forces to perform better coordination with Norwegian defence officials in the North "to reduce tension" vis-à-vis Russia. The previous Centre-Right Government's 2019-decision not to integrate own frigates into the US Missile Defence also sends a signal of benevolence towards Russia; a different choice could easily have degraded the Northern Fleet's survivability in a crisis, thereby causing less rather than more stability in the region.

KEYWORDS

Arctic; High North; Norway.

WG2 – Military History

0385

Mutually beneficial cooperation should not turn into slipknot

S. Seheda (1)

(1) National Defence University of Ukraine named after Ivan Cherniakhovskyi, voyen_ist@ukr.net

The progress of the Russian Federation in the conquest of new lands depends and has always depended on the technical support of developed countries. A retrospective analysis of Russia's conquest of the peoples of the North confirms this idea. The colonization of the Ural and Siberia began in the second half of the 16th century and was supported by the construction and settlement of cities and bases by military personnel. The established settlements became bases for military campaigns in the Polar Urals, Eastern and Western Siberia, and Central Asia.

Russia tried to advance to the West, but military defeats forced it to give up such plans. Lithuania, Sweden and Turkey successfully defended themselves. In addition, the mentioned states were also conquerors, attacking Moscovia. The Russian tsars turned their attention to the North, where there were no state formations that could give adequate resistance.

Everyone knows Ermak's military campaigns, a well-organized and equipped army that conquered the peoples of Siberia. The natural tax in the form of fur, whalebone, walrus tusks became like a currency to pay in Europe, including for purchasing weapons. Army of Moscovia used firearms (pistols, muskets, fuselages), and the indigenous peoples of Siberia had bows, spears, knives. The confrontation was unequal.

The next step was the Russia's colonization of the North in the 18th century. Military-scientific expeditions were carried out for the purpose of conquest. One of these expeditions was led by Vitus Jonasen Bering. A native of Denmark, who received an excellent naval education in the Netherlands, was recruited for military service in Russia. He discovered the sea strait between Asia and America, explored Kamchatka, the Pacific coast of Russia, the western shores of North America. He brought fame not to his homeland, he was called a great Russian navigator.

The colonization of the North in Soviet times was carried out with the help of European technical equipment. In 1924, Junkers-20 seaplanes were used to discover the ice situation and to provide sea crossings for transport vessels in the Arctic. In 1929, Junkers W-33 transport aircraft were used to service shipping in the Kara Sea.

In the second half of the 20th century, the Soviet Union actively built an icebreaker fleet and Norway sold the most developed icebreaker vessels at that time. To extract oil and gas in the North, the Soviet Union purchased drilling rigs in Japan and Norway.

The Russian Federation still needs new technologies for mining in the Arctic. These technologies can be provided by developed foreign states. Is the World ready to strengthen the role of the Russian Federation in the Arctic? It leads to an increase in its military presence. The West can raise a monster with its own hands. Then we should expect that Russia will dictate its own rules in the region.

KEYWORDS

War; Moscovia; Arctic; technologies; Northern Sea Route.

REFERENCES

Bering, Vitus Jonassen (2022). In *Wikipedia, the free encyclopedia.* Retrieved from https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D1%80%D0%B8%D0%BD%D0%B3,_%D0%92D0%B8%D1%82%D1%83%D1%81_%D0%98%D0%BE%D0%BD%D0%B0%D1%81%D1%81%D0%B5%D0%BD

Bolosov, A.N. (2014). *Polyarnaya aviaciya Rossii 1946-2014. Kniga vtoraya* [Russian polar aviation. Book two]. Moscow: Paulsen.

Boevye dejstviya Sovetskoj Armii v Velikoj Otechestvennoj vojne (iyun 1941 g. – dekabr 1943 g.). T.1. [Military operations of the Soviet Army in the Great Patriotic War (June 1941 – December 1943). Vol.1. (1958). Moscow: Voenizdat.

Burkov, G. (1988). *Prolozhit okonchatelno... Polyarnyj krug* [Finally paving the way... The Arctic Circle]. Moscow: Mysl.

Burkov, G. (1989). *Vozdushnyj "povodyr" Arktiki. Polyarnyj krug – 1989* [Air "guide" of the Arctic. Polar circle – 1989]. Moscow: Mysl.

Ciporukha, M.I. (2004). *Pokorenie Sibiri. Ot Yermaka do Beringa* [Conquering Siberia. From Yermak to Bering]. Moscow: Veche.

Danilevskij, N.Ya. (1991). Rossiya i Evropa [Russia and Europe]. Moscow: Kniga.

Drobizhev, V.V., Kovalchenko, I.D., & Muravyev, A.V. (1973). *Istoricheskaya geografiya SSSR. Uchebnoe posobie* [Historical geography of the USSR. Textbook]. Moscow: Vysshaya shkola.

Elert, A.H. (2007). *Po sledam akademicheskogo otryada Velikoj Severnoj ehkspedicii* [In the footsteps of the academic detachment of the Great Northern Expedition]. Retrieved from https://cyberleninka.ru/article/n/po-sledamakademicheskogo-otryada-velikoy-severnoy-ekspeditsii

Hutsalo, Ye. (1996). *Mentalnist ordy: Statti.* [Horde mentality. Articles]. Kyiv: Vydavnychyi tsentr "Prosvita".

Laktinonov, A.F. (1955). *Severnyj polyus. Ocherk istorii putishestvij k centru Arktiki* [The North Pole. A story of the history of travel to the center of the Arctic]. Moscow: Morskoj transport.

Makarov, S., Kuznetsov, N., & Dolgova S. (2010). *Ledokol "Yermak"* [Icebreaker "Yermak"]. Retrieved from http://militera.lib.ru/explo/sb_ledokolermak/sb_ledokol-ermak.html?fbclid=IwAR23IT8f6S-_ImbLQT0L9CjtRnDwZ31Jxibl7gYeSGuX4MyjxsFFS4fC1XI

Melino, M., & Conley, H. (2021). *The ice curtain. Russia's Arctic military presence*. Retrieved from https://www.csis.org/features/ice-curtain-russias-arcticmilitary-presence

Perehovornyk vid RF u Zhenevi zaiavyv, shcho NATO "treba zbyraty manatky" [Russia's negotiator in Geneva says NATO has to get away] (2022) in *Ukrainska Pravda*. Retrieved from https://www.pravda.com.ua/news/2022/01/9/7319822/

Pervaya Kamchatskaya ekspediciya [First Kamchatka expedition] (2022). In *Wikipedia, the free encyclopedia.* Retrieved from https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B2%D0%B0%D1%8F_%D0%9A%D0%B0%D0%BC%D1%87%D0%B0%D1%82%D1%81%D0%BA%D0%B0%D1%8F_%D1%8D%D0%BA%D1%81%D0%BF%D0%B5%D0%B4%D0%B8%D1%86%D0%B8%D1%8F

Povernennia Ukrainoiu terytorii, zakhoplenykh Rosiieiu z 2014 roku, ne ye realnoiu metoiu – New York Times [The return of Ukraine's territories occupied by Russia since 2014 is not a real goal – New York Times (2022). In *Ukrainska Pravda*. Retrieved from https://nv.ua/ukr/ukraine/events/nyt-nazvav-nerealnimpovernennya-ukrajinoyu-teritoriy-zahoplenih-rf-z-2014-roku-novini-ukrajini50243772.html

Saltykov, Fedor Stepanovich (2022). In *Wikipedia, the free encyclopedia*. Retrieved from https://ru.wikipedia.org/wiki/%D0%A1%D0%B0%D0%BB%D1%82%D1%8B%D0%BA%D0%BE%D0%B2,_%D0%A4%D1%91%D0%B4%D0%BE%D1%80_%D0%A1%D1%82%D0%B5%D0%BF%D0%B0%D0%BD%D0%BE%D0%B2%D0%B8%D1%87

Sherl, D. (1988). *Most muzhetva i druzhby. Polyarnyj krug* [The bridge of courage and friendship. The Arctic Circle]. Moscow: Mysl.

Solovyev, S.M. (1989). *Sochinenie. Kniga 3. T. 5-6. Istoriya Rossii ot drevnikh vremen* [Work. Book 3. Volumes 5-6. History of Russia from ancient times]. Moscow: Mysl.

Sovetskaya Sibir [Soviet Siberia] (1945). № 209, October 23.

Territorialnye pretenzii SSSR k Turcii [Territorial claims of the USSR to Turkey] (2022). In *Wikipedia, the free encyclopedia*. Retrieved from https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D1%80%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%BF%D1%80%D0%B5%D1%82%D0%B5%D0%BD%D0%B7%D0%B8%D0%B8_%D0%A1%D0%A1%D0%A1%D0%A0_%D0%BA_%D0%A2%D1%83%D1%80%D1%86%D0%B8%D0%B8

The white book of the anti-terrorist operation in the east of Ukraine in 2014-2016 (2017). Retrieved from https://nuou.org.ua/assets/journals/bila_knyga/whitebook-ato.pdf

Yermak (ledokol, 1898) [Yermak (icebreaker, 1898) (2022). In *Wikipedia, the free encyclopedia.* Retrieved from https://ru.wikipedia.org/wiki/%D0%95%D1%80%D0%BC%D0%B0%D0%BA_(%D0%BB%D0%B5%D0%B4%D0%BE%D0%BA%D0%BE%D0%BB,_1898)

Polish 1939 campaign – project

M. Deszczyński (1), D. Miszewski (2), Ł. Przybyło (3), D. Rogut (4), J. Tym (5), P. Więckowski (6) and G. Wnetrzak (7)

(1) War Studies Academy, Poland, m.deszczynski@akademia.mil.pl
(2) War Studies Academy, Poland, d.miszewski@akademia.mil.pl
(3) War Studies Academy, Poland, przybylo@akademia.mil.pl
(4) War Studies Academy, Poland, d.rogut@akademia.mil.pl
(5) War Studies Academy, Poland, j.tym@akademia.mil.pl
(6) War Studies Academy, Poland, p[.wieckowski@akademia.mil.pl
(7) War Studies Academy, Poland, g.wnetrzak@akademia.mil.pl

ABSTRACT

The main objective of project is to present a new extensive assessment of the Polish 1939 Campaign. Its events have not been comprehensively and thoroughly examined by the modern historiography. Regrettably, despite so many years, there is still a lack of a systematic and detailed synthesis of this element of the European history. References to the II Polish Republic present in the public space, important role of the Polish 1939 Campaign in historical memories of generations, greater access to archives in all countries and new publications – all generate the need to revise and reconsider research results to date and launch a complex, objective and fair review of the first campaign of World War II.

BASIC INFORMATION ON THE "POLISH 1939 CAMPAIGN" PROJECT

Project name – *Polish 1939 Campaign— the Synthesis*

Project lifespan – 1st January 2022–30th November 2026

MAIN AND SPECIFIC OBJECTIVES

1. Status of research to date and identification of knowledge gaps and differences in historiography on the subject in question in countries fighting in WWII. Defining the starting point for identification and elaboration of research questions required to specify direction for research areas of the project.

2. Evaluation of international relations before WWII and in first six weeks of the war, with special focus on actions taken by countries involved in the conflict. Assessment of strategic cultures and factors impelling political and military decision-making processes as well as elements necessary to understand actual national interests and concrete objectives of all parts to the conflict as well as positions and roles of specific countries/actors on the political arena.

3. Estimation of economic potentials of all parts to the conflict, with special focus on war preparations in the context of specific political, legal and economic solutions, including armament programmes, infrastructure

4. development, administrative changes and information warfare. Such an approach is necessary to illustrate precisely factual potentials of all parts to the conflict. In addition, analysis of technology development and growth

5. of industry should indicate main trends of that time as well as elements that had been critical to maintain and increase combat potentials of all countries involved in this armed conflict.

6. Assessment of military potential of all parties to the conflict, with special focus on military preparations — analysed in the context of strategy, military doctrine, *Ordre de Bataille*, military education and training system, mobilisation capabilities, combat potential, options for operational deployments, logistics, support provided by other arms and services, intelligence capabilities — to define actual capabilities necessary to successfully launch military operations.

7. Evaluation of military operations, with the special focus on exploitation of archive material on all parties to the conflict (warning orders, initiating directives, corrective and supplementary orders, operational reporting). Comparison of military operations with tactical level regulations and instructions of that time, established rules of warfare, norms and principles. Assessment of military plans and their factual implementation. Comprehensive and

objective evaluation of military actions during the campaign. Assessment of intelligence operations before and during that WWII episode.

8. Evaluation of Lessons Identified and Lessons Learned from the Polish Campaign 1939. Their impact on art of war and other dimensions of armed forces activities. Processes and procedures for collection of Lessons Identified and Lessons Learned, their implementation to everyday practice of armed forces of all parties and other countries. Short- and mid-term assessment of impact of the Polish 1939 Campaign on art of war in Allied states and Axis countries.

9. Assessment of effectiveness of efforts to build public support for political decisions and military operations within the context of political and ethnic issues (position of ethnic minorities) — quantifying actual morale of the society, national spirit, determination to fight for the country and efficiency of defence preparations.

10. Evaluation of effectiveness of civilian authorities, civil defence system, public, economic and general safety elements, mobilisation of the economy and status of healthcare system, planned and unprompted evacuation schemes — all presented within the framework of operation of local authorities and national governments, including the issues of ethnic minorities, and preparation of the country for the armed conflict.

11. Strategic communication in parties to the conflict, propaganda campaigns directed at own societies and world's public opinion, carried out by states, political parties and private media, information operations.

12. Assessment of Polish losses in the 1939 Campaign vs. losses of other parties to the conflict during the period 1st September 1939–6th October 1939, including war crimes and crimes against humanity.

PLANNED OUTCOME

The planned output of the project is a new synthesis of the Polish 1939 Campaign, covering wide spectrum of geopolitical and diplomatic problems as well as behind-the-scenes elements, before and in the course of the campaign. It will also present II Polish Republic defence preparations and military operations during the conflict, within the context of foreign policy, economy, social and military issues.

The results of work of the international research team will be presented in the form of three volumes on foreign policy, economy, military and social issues — published in four languages: Polish, English, French and German. Such an approach will allow gaining publicity for the products and wide distribution of publications to recognized scientific and research centres. The participation of representatives from foreign academic communities will allow top positioning of project's elements in the world historiography and exalt the importance and status of this undertaking.

The project's schedule also envisages a number of publications in top ranking scientific journals, both in Poland and abroad. This will bring many evaluation points for researchers and their universities. It will also promote the project among academia.

International conferences will sum up subsequent stages of the project, publicise the project within the academic community.

KEYWORDS

II World War; Poland; Polish Campaign 1939; Polish Army; Military.

Human factor as a principle of the art of war – study of the examples form the Polish military history

M. Przybylak (1)

(1) War Studies University, Poland, m.przybylak@akademia.mil.pl

From ancient times theoreticians and practicians have tried to create a universal way to gain victory on the battlefields and beyond. Those attempts have been articulated as a principles of war, which can be defined as rules and guidelines that represent truths in the practice of war and military operations. Many examples of varying sets of principles of war can be found in military history. For example, British Defense Doctrine lists nine of them: selection and maintenance of the aim, maintenance of morale, offensive action, security, surprise, concentration of force, economy of effort, flexibility, cooperation and sustainability (Joint Doctrine Publication 0-01, British Defence Doctrine, 2014, p. 29-31). Polish military doctrine lists seven principles of war: maintenance of the aims, activity, optimal use of force, maneuverability, surprise, maintenance of combat capability and human factor (Regulamin Działań Wojsk Lądowych, 2009, pp. 19-20). The last one of them – human factor – is not very common in other military doctrines. In the Polish regulations, the human factor is a composition of leadership, morale, initiative, creativity and resilience. For numerous armies the human factor is restricted only to the morale. Unarguably, morale constitutes a very complicated element composed of multiple variables (van Creveld, 1982, p. 17-26). Hovewer, Lasota (2020, p. 487-490) suggests that morale is not the most important principle. This raises a question: why is human factor so significant in the Polish approach to the art of war? The author assumes that the answer is hidden in the military history. Throughout the Polish history, human factor has often been a key factor to gain advantage over the opponent on the battlefield and, consequently, to achieve victory.

The author of the paper attempts to illustrate the role of the human factor as a principle of the art of war, referring to two examples from Polish military history. The first one is the defense of the castle in Lanckorona in 1771. This skirmish (one of the few victories of the Polish military during the Bar Confederation of 1768-1772) is a perfect example of the fact that the weaker party, both quantitatively and qualitatively, can win by creating an advantage in the field of the human factor, especially morale (Przybylak, 2021, p. 91-108). The author analyzes the human factor and its components as the principles of the art of war. Furthermore, with the use of historical methods, the course of the short battle of Lanckorona on 20 February 1771 is described. Finally, the author indicates the moments when the human factor played a decisive role. The second discussed example is the Polish-Bolshevik War of 1919-1921. During this conflict both parties were right at the beginning of the army formation process. Frequently, soldiers on both sides had no uniforms, shoes, or even proper weapons (Davies, 2003, p. 140-153) . Since a big portion of military equipment was lacking, only the human factor could be utilized to gain significant advantage on the battlefield. The results of the analysis of both examples allowed the author to conclude that it was precisely the factors such as leadership, morale, initiative, creativity and endurance that enabled the weaker Polish defenders to build an advantage, and thus to achieve victory over the opponent. From today's perspective – especially keeping in mind the ongoing war in Ukraine – the final part of this paper also attempts to evaluate the role of the human factor in the art of war, particularly on the tactical level.

KEYWORDS

REFERENCES

Przybylak M. (2021). Czynnik ludzki jako zasada sztuki wojennej na przykładzie obrony Lanckorony w 1771 roku [The human factor as a principle of the art of war on the example of the defense of the Lanckorona Castle in 1771]. *Bellona, 707*(4), 91-108.

Creveld, M. (1982). *Fighting Power: German and U.S. Army Performance, 1939-1945*. Santa-Barbara: ABC-CLIO.

Davies N. (2003). *White Eagle, Red Star: The Polish-Soviet War 1919-20: The Polish-Soviet War 1919-20 and 'The Miracle on the Vistula'*. Warsaw: Vintage Publishing.

Lasota J. (2020). *Zasady sztuki wojennej [Principles of Art of War]*. Warszawa: Bookmark.

Joint Doctrine Publication 0-01, British Defence Doctrine. (2014). London: British Ministry of Defence. Regulamin Działań Wojsk Lądowych [Regulations Of The Activities Of Land Forces]. (2008). Warszawa: Dowództwo Wojsk Lądowych.

Slaves to history? How Russian history is at play in the current war in Ukraine

N. Poulsen (1)

(1) Royal Danish Defence College, nipo@fak.dk

The current war in Ukraine is highly conditioned by Russian history: The conflict have deep roots in the legacy of Soviet totalitarianism. It furthermore reflects an ongoing challenge of the current Russian regime to come to terms with the colonial legacy of the former tsarist / Soviet empires. In addition, the Russian past is deliberately used as a strategic tool by Putin's government – both as means to legitimize the aggression against Ukraine, but also as a means to create a Russian identity that underpins and strengthen the Kremlin's authoritarian politics. Especially the Second World War (in Russian parlance: the Great Patriotic War) have become the centerpiece of what some have termed a secular religion. The Great Patriotic War does, however, not stand alone in Russian memory politics. This time-period is fused with other (primarily war-related) historical events to create a state and war centered approach to Russian history (Carleton, 2017). Thereby the authorities convey the image of Russia as a besieged country. A country, which thanks to its natural resources and size, is subject to envy and plots for dismemberment and exploitation by its (western) neighbors. According to same narrative, only a Russia ruled by a strong state and free of inner tensions (and dissent) can stand against the perpetual threat from the outside world (Snyder, 2018). The cult of the Great Patriotic War also have other ramifications. The military culture and operational thinking of the Russian armed forces is still influenced by what are claimed to be eternal lessons of this conflict (Golts, 2019). As illustrated in the examples above, studying the invasion of Ukraine in the context of Russia's past and the Kremlin's instrumentalization of that very past not only offers insight in the causes of the war. It also helps understanding the Russian way of war in general and the operational and tactical pattern of its forces. Although looking to the past is far from a bullet proof guide to forecasting the future, it furthermore enables us to consider how the war may evolve and to consider possible scenarios about what we are heading for, in this extremely costly and dangerous conflict.

In my paper, I initially address the problem of seeking patterns in history, and of using them as a guide to inform the present and speculate about the future. Secondly, I address a number of aspects of the war, which in my opinion gains considerably from being contextualized and analyzed in historical terms. These will be the following topics: The world-view of the Russian regime; the operational mode of the Russian armed forces; the population's reaction to the war; Russian atrocities; and the long term perspectives for ending the war. Overall, the thesis, thus argued in my paper is that the lackluster, yet highly brutal performance by the Russian armed forces in the war in Ukraine is due to the evolution of Soviet security institutions in to Russian institutions without thoroughly democratizing them or subjecting them to true democratic-civilian control.

While there is a considerable scholarly literature on Russian history politics in general, how the Russian past influences and structures Russia's conduct of war in Ukraine is a topic, which still lacks in-depth studies. My research thus contributes to a matter still void of substantial scholarly research.

KEYWORDS

Military History; Russia; Russia-Ukraine War.

REFERENCES

Carleton, G. (2016). *Russia. The History of War*. Cambridge MA: The Belknap Pres.

Golts, A. (2019). *Military Reform and Militarism in Russia.* Washington D.C.: The Jamestown Foundation.

Kurilla, I. (2016). *The "Return of Stalin". Understanding the Surge of Historical Politics in Russia*. Ponars Eurasia Policy Memo, 429.

Poulsen, N.B. (2016). *Skæbnekamp*. Copenhagen: Gyldendal.

Poulsen, N.B,. & Staun, J. (2021). *Russia's Military Might. A Portrait of its armed forces*. Copenhagen: Royal Danish Defense College.

Snyder, T. (2018). *The Road to Unfreedom*. US: Random House.

Weiss-Wendt, A. (2022). *Putin's Russia and the falsification of history: reasserting control over the past*. London: Bloomsbury Academic.

A 19th century method to determine the ship's position at sea

A. Queirós (1), A. Canas (2) and T. Sousa (3)

(1) Escola Naval, Portugal, ana.filipa.queiros@marinha.pt
(2) Escola Naval, Portugal, costa.canas@marinha.pt
(3) Escola Naval, Portugal, teresa.maria.sousa@marinha.pt

Until the 19th century, to determine the Latitude the navigators used a method based on the observation of the Sun at the meridian passage, i.e., at its maximum height. In the 18th century, the appearance of the chronometer allowed the pilots to determine the Longitude at any time of the day outside the meridian passage using the hour angle method. Therefore, until the 19th century, to determine the ship's position the pilots used two different times of the day: the Latitude was obtained at the meridian passage while the Longitude was obtained outside the meridian passage.

Nonetheless, due to weather conditions or overcast sky at the meridian passage it could be hard or even impossible for the pilots to make the required observations to determine the Latitude. In order to solve this problem several authors have developed methods to determine the Latitude using two altitudes of the Sun at two different times of the day. With these new methods the pilots would determine the Latitude and Longitude outside the meridian passage. However in all the manuscripts that we have studied both Latitude and Longitude were determined at different times of the day.

In view of what has been said before, the following question arises: If there were methods to determine the Latitude by two altitudes of the Sun, and if Longitude was calculated outside the meridian passage, why there were no records of a method that determined both the Latitude and Longitude at the same time of the day?

In this context and in order to answer this question, we have studied two important methods to determine the ship's Latitude by two altitudes of the Sun, namely the method of Cornelis Douwes and the method of João Peregrino Leitão. The latter is based on a method originally developed by James Ivory in 1821 and improved by Edward Riddle in 1822. Having the ship's Latitude the Longitude is then calculated for the same time using the hour angle method thus obtaining the ship's position for that time of the day.

In 2021, during a short navigation from Lisbon to Azores, real observations were carried out and the data obtained was later used to determine the ship´s Latitude using Douwes' method and Leitão's method. At the same time, the hour angle method was used to determine the ship's Longitude for the same instant that the Latitude was determined, obtaining the ship's position. The results obtained were then compared with the real GPS (Global Positioning System) positions in order to assess the reliability of these 19th century methods.

KEYWORDS

Latitude; Latitude by two altitudes of the Sun; Cornelis Douwes; João Peregrino Leitão.

WG3 – Military Technology

Automation bias and anthropomorphism of technology: implications for the military

A. Viidalepp (1)

(1) University of Tartu, Estonia, auli@viidalepp.org

In human-machine interaction, people sometimes tend to exhibit automation bias, meaning that machine decisions and recommendations are attributed greater authority than those of human decision-makers (Cave & Dihal, 2020, p. 700; de Visser et al., 2016, p. 332). Also called 'android fallacy' (Chesterman, 2021; Richards & Smart, 2016), the problem is well researched in the field of healthcare (Goddard et al., 2012). Automation bias can be constituted as part of a larger problem area – that of the anthropomorphism of technology in general, and especially of intelligent systems with a degree of autonomy. Anthropomorphism can be the result of misplaced empathy or an individual's "misidentification with machine intelligence," leading to "false ethical evaluations of AI's potentials and threats" (Bryson and Kime 2011, 1642). Superficial similarities such as a human-like appearance, purposeful behaviour or even natural language use by robotic systems tend to trigger increased levels of anthropomorphism (Bryson & Kime, 2011, 2011; Harbers et al., 2017). The problem is further aggravated by the field of social robotics that sees anthropomorphism as a positive design choice for better usability (de Visser et al., 2016), and the general tendency in the public discourse to anthropomorphise anything called "artificial intelligence" (Viidalepp, 2022, forthcoming).

In the military context, however, automation bias is rather seen as a problem with potentially severe consequences (Johnson, 2022). The mistaken friendly fire by AEGIS, 1988 and Patriot, 2003 are often cited examples of misappropriated authority in military decision support systems. At the same time, critical scholarship on the shortcomings of automated 'intelligent' systems is rare (Raji et al., 2022). Therefore, it is necessary to review the functional problematics of automated systems and suggest ways to mitigate the excessive trust in machine decisions.

Legal scholars stress the importance of choosing appropriate metaphors and avoiding human-specific vocabulary when describing robotic systems (Richards & Smart, 2016). The impact of the public discourse on militaryspecialist one is severe enough that it is occasionally deemed necessary to explicitly stress that "autonomous weapon systems remain weapons and […] they do not become humans, although we use human-like characteristics to describe them" (Johansen, 2018, p. 90). Automation bias can be mitigated by "making AI visible and understood where it already exists" (Bryson & Kime, 2011, p. 1645). Partly, this comes down to the metalanguage used in the discourse on technology. While it is not possible to avoid anthropomorphism entirely, examples from public and specialist discourses show that when people gain experience and better understanding of the functions of the machines they are working with, anthropomorphism in their descriptive language decreases significantly.

KEYWORDS

Automation bias; artificial intelligence; automated decision support systems; anthropomorphism.

REFERENCES

Bryson, J. J., & Kime, P. P. (2011). Just an artifact: Why machines are perceived as moral agents. *Twenty-Second International Joint Conference on Artificial Intelligence*.

Cave, S., & Dihal, K. (2020). The Whiteness of AI. *Philosophy & Technology*, *33*(4), 685–703. doi: https://doi.org/10.1007/s13347-020-00415-6

Chesterman, S. (2021). *We, the robots? Regulating artificial intelligence and the limits of the law*. Cambridge University Press. de Visser.

Monfort, E. J., McKendrick, S. S., Smith, R., McKnight, M. A. B., Krueger, P. E., & Parasuraman, R. (2016). Almost human: Anthropomorphism increases trust resilience in cognitive agents. *Journal of Experimental Psychology: Applied*, *22*(3), 331–349. APA PsycArticles. doi: https://doi.org/10.1037/xap0000092

de Waal, F. B. M. (1999). Anthropomorphism and Anthropodenial: Consistency in Our Thinking about Humans and Other Animals. *Philosophical Topics*, *27*(1), 255–280. doi: https://doi.org/10.5840/philtopics199927122

Goddard, K., Roudsari, A., & Wyatt, J. C. (2012). Automation bias: A systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*, *19*(1), 121–127. doi: https://doi.org/10.1136/amiajnl-2011-000089

Harbers, M., Peeters, M. M. M., & Neerincx, M. A. (2017). Perceived Autonomy of Robots: Effects of Appearance and Context. In M. I. Aldinhas Ferreira, J. Silva Sequeira, M. O. Tokhi, E. E. Kadar, & G. S. Virk (Eds.), *A World with Robots: International Conference on Robot Ethics: ICRE 2015* (pp. 19–33). Springer International Publishing. doi: https://doi.org/10.1007/978-3-319-46667-5_2

Johansen, S. R. (2018). So Man Created Robot in His Own Image: The Anthropomorphism of Autonomous Weapon Systems and the Law of Armed Conflict. *Oslo Law Review*, *5*(2), 89–102. doi: https://doi.org/10.18261/issn.2387-3299-2018-02-03

Johnson, J. (2022). Delegating strategic decision-making to machines: Dr. Strangelove Redux? *Journal of Strategic Studies*, *45*(3), 439–477. doi: https://doi.org/10.1080/01402390.2020.1759038

Raji, I. D., Kumar, I. E., Horowitz, A., & Selbst, A. (2022). The Fallacy of AI Functionality. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 959–972. doi: https://doi.org/10.1145/3531146.3533158

Richards, N. M., & Smart, W. D. (2016). How should the law think about robots? In M. R. Calo, M. Froomkin, & I. Kerr (Eds.), *Robot law* (pp. 3–22). Edward Elgar Publishing.

Viidalepp, A. (2022). Sociocommunicative functions of a generative text: The case of GPT-3. *Lexia. Rivista Di Semiotica*, *40*. (forthcoming)

Viidalepp, A. (forthcoming). The semiotic functioning of synthetic media. *Információs Társadalom*.

Cyber Domain of the Future: Could Techno-Economic Coalitions challenge Military Alliances?

M. Ristolainen (1)

(1) Finnish Defence Research Agency, mari.ristolainen@mil.fi

This paper discusses the role of techno-economic coalitions in the contested cyber domain of the future. The objective is to consider if emerging techno-economic coalitions could challenge traditional military alliances some day. This paper belongs to the field of strategic foresight that explores scenarios and identifies trends and emerging issues when estimating changes in the cyber domain in the distant future (ca. 2035-2040).

Firstly, as a background, the different views and contemporary developments of the cyberspace governance are explained. Secondly, the concept of 'techno-economic coalition' is defined and the potential emerging technoeconomic coalitions are explicated. Thirdly, the forming of cyber defence inside a techno-economic coalition is described. And finally, the potentially changing role of traditional military alliances in future cyber domain is discussed.

The governance of global cyberspace is changing and that affects the development of cyber domain and the planning of future cyber defence as well. The idealistic notion of cyberspace as a 'free' and 'open' global infrastructure providing security together is progressively challenged by projecting territoriality and conveying traditional nation-state models of governance and independent safekeeping into cyberspace (cf. Demchak & Dombrowski, 2011; Muller, 2017; Kukkola & Ristolainen, 2018). The 2013 and 2015 Group of Governmental Experts (GGE) consensus reports stated that sovereignty as a fundamental principle of international law applies in cyberspace (GGE, 2013 & 2015). Moreover, in recent years, different countries have published statements that declare an aim for 'sovereignty in cyberspace' (e.g. Doktrina, 2016; Ulkoministeriö, 2020). However, these statements pose certain problems because the so-called 'national cyberspace' does not necessarily follow the physical borders of a nation-state, nor is there an internationally unified understanding of what sovereignty means in cyberspace (e.g. Pohle & Thorsten, 2020; Braud et al., 2021; Efremov, 2017). Moreover, it is almost impossible for a single country to achieve 'self-sufficiency' in cyberspace. In order to remain competitive and protected, one must either join or strengthen emerging techno-economic coalitions, which serves as an emerging issue or trend for strategic foresight.

In the distant future, techno-economic coalitions could be based on competing national technical standards and solutions (MGIMO, 2019). Furthermore, techno-economic coalitions could develop new technologies at a national (or coalition) level and build services based on national (coalition) technology. Potential techno-economic coalitions could emerge around the 'Anglosphere' led by the USA; around China; around Russia; around the EU; around Islamic countries; around criminal and anarchical groups, and (possibly) around a so-called 'joker' country (cf. original listing (1-4) MGIMO, 2019; additions (5-7) author). Techno-economic coalitions would share certain values and ideology and distinguish themselves from other coalitions by different attitudes towards (personal) data usage and protection. Where other coalitions would, for instance, use data freely for commercial purposes, others for political and/or religious control, there other coalitions would protect (personal) data profoundly. Divergent techno-economic coalitions would significantly influence and complicate the international cyber law development and application in practice. And thus, cyber defence in the future would be based on the different values and technical standards and solutions of the future techno-economic coalitions. Consequently, the role of traditional military alliances in future cyber domain would diminish substantially, which should be considered when doing strategic planning.

KEYWORDS

Strategic foresight; Cyber domain; Cyberspace governance; Techno-economic coalitions; Military alliances; Strategic planning.

REFERENCES

Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Network*, 35(2), 4-5.

Demchak, C. & Dombrowski, P. (2011). Rise of the Cybered Westphalian Age. *Strategic Studies Quarterly*, 5(1), 32-61.

Doktrina (2016). *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii,* 5.12.2016. Retrieved from http://static.kremlin.ru/media/acts/files/0001201612060002.pdf.

Efremov, A.A. (2017). Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva. *Pravo. Zhurnal Vysshchei ekonomiki*, 1, 201-215.

GGE (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General*, 24.6.2013. Retrieved from https://digitallibrary.un.org/record/753055.

GGE (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General*, 22.7.2015. Retrieved from https://digitallibrary.un.org/record/799853?ln=en.

Kukkola, J. & Ristolainen, M. (2018). Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', *Journal of Information Warfare*, *17*(2), 83-100.

MGIMO (2019). *Mezhdunarodnye ugrozy 2020: Kazhdyi za sebia*. Laboratoriia analiza mezhdunarodnykh protsessov MGIMO MID Rossii. Retrieved from https://mgimo.ru/upload/iblock/2ac/int-threats-2020.pdf.

Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Polity Press, Cambridge.

Pohle, J. & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, *9*(4), 1-19.

Radu, R. (2019). *Negotiating Internet Governance*. Oxford University Press, Oxford.

Ulkoministeriö (2020). *Kansainvälinen oikeus kyberympäristössä: Suomen kansallisia kantoja (online)*. Retrieved from https://um.fi/documents/35732/0/KyberkannatPDF-FI.pdf/c69fce1e-5753-3731-0b46356b8216df51?t=1603097434415.

Artificial Intelligence Cyber Operations

J. Martins(1) and J. Borges(2)

(1) Centro de Inv. Desenvolvimento e Inovação da Academia Militar, Portugal, martins.jts@ium.pt
(2) Centro de Inv. Desenvolvimento e Inovação da Academia Militar, Portugal, jose.borges@academiamilitar.pt

Cyberspace Operations (CO) encompasses and support several typologies of military operations: security actions; Intelligence, Surveillance and Recognition (ISR); operational environment preparation; Defensive CO (DCO) response actions and internal defensive measures; Offensive CO (OCO). These operations intend to protect (vertical and lateral) manoeuvre in the operational domains of land, air, maritime, space, and cyberspace (Hoehn, 2020).

Offensive CO targets adversaries in cyberspace, providing strategic support to deep fire areas across contested spaces through offensive actions. They intend to deny, degrade, disrupt, destroy and manipulate adversarial forces contributing to achieving superiority, anti-access area denial and strategic, operational and tactical manoeuvring advantages. A review of CO according to the current doctrine, mission, CONOPS and capabilities for the Joint All Domain Command and Control concept will allow identifying required capabilities and connecting sensors from military forces into a single network. (Hoehn, 2020) Aggregating these vectors into (cohesive, progressive and interactive) Multi-Domain Operations (MDO) has the potential to provide a digital cloud-like environment with supporting capabilities, e.g., intelligence and data, to sustain military decision-making.

Artificial Intelligence (AI) and Machine Learning (ML) have the potential to transform modern warfare. The capabilities leveraged by such technologies have proven helpful in civilian applications, such as autonomous vehicles, data processing, intelligence, decision-making processes, logistics and simulation technologies; CO is another area that may benefit from those capabilities. Several states have announced a considerable investment in AI for defence purposes, with AI-related research and development funding extending into billions of dollars annually and new AI centres (CCDCOE, 2021).

AI, expectedly, is nearing operational deployment in some applications in the military environment; nevertheless, it remains unproven in the hard testing ground of combat operations' engagement. Even so, it has become a technology that military forces cannot ignore, considering their future. The potential use of AI in the military domain has several flavours. For specific tasks inside a given field, narrow AI equals or exceeds human intelligence. In this type of AI, a learning algorithm is designed to execute a single task, and any information acquired from executing that job won't immediately be extended to other tasks. Nevertheless, its utility is context-dependent (Layton, 2021).

Another possible use results from applying unsupervised machine learning algorithms to find structure in large data sets, which is essential to developing effective AI systems. Although the process will begin with a known dataset for the initial training of the model, the AI algorithm will eventually identify and select its discriminators. This type of AI still demands validation, explicability, and assurance.

ML represents a new frontier and presents distinct challenges and opportunities, requiring new approaches, validation, test and explicability capabilities. Validating these systems will require expanding existing skills and developing new ones, particularly in mathematical modelling and simulation. The validation and assurance of algorithms and machine learning code is an emerging field that relies heavily on advanced scientific and mathematical knowledge bases. These developments in AI still require further efforts to help develop and provide ongoing assurance of AI systems, and new projects, such as the COLREGS, are already emerging to assess the potential for using AI to enhance compliance with regulatory standards and protocols (RAN, 2020).

While the improvements, accessibility, and use of these new developments represent a mindset change and a turnover in data-focused applications, they also imply understanding and dealing with the decisions and results obtained by models, which is a complex and challenging task. A starting point in this direction aims at creating human understandable AI models through a set of design options considering the explainability-performance tradeoff. This research line has already captured the interest of the academic community and practitioners, even if a theory for eXplainable AI (XAI) and universally agreed definitions are still lacking (Maathuis, 2022).

XAI aims to create a suite of machine learning techniques capable of delivering more intelligent, autonomous, and symbiotic systems. These systems are likely to produce explainable models, maintain a high level of learning performance in prediction and accuracy, and override current limitations by the machine's inability to explain their decisions and actions to human users. XAI, especially explainable machine learning, is essential for future

warfighters to understand, appropriately trust, and effectively manage an emerging generation of prospective machine partners with AI/ML capabilities.

Such systems, armed with enhanced capabilities, must be able to explain their rationale, characterize their strengths and weaknesses, and convey an understanding of their future behaviours. A strategy for achieving such goals may result from developing AI/ML for producing explainable models and usable human-machine interfaces capable of providing actionable information to support the commanders' actions. The Generative Adversarial Networks (GAN) of figure 1 give an example of such a strategy. GANs comprise two competing neural networks, operating unsupervised and learning through cooperative zero-sum games (Goodfellow et al., 2014).

Figure 1 – Adversarial explainable and deployable GANs

Two challenging problems, and their intersection, have emerged when defining events of interest in heterogeneous multimedia data and constructing decision policies for an autonomous system to perform a variety of simulated missions: classification and reinforcement learning. Together with these, Ridley (2022) also identified intelligence analysis and autonomous systems as critical challenges to be addressed.

Despite the efforts of academia, industry, and government, COs are rising at an unprecedented rate indicating that AI can play a critical role in providing valuable insights for supporting these operations. Areas, e.g., cyber threat intelligence, security operations, disinformation, information campaigns and propaganda, and security automation and response, are significant opportunities to develop techniques based on the heterogeneity and velocity of data available in cyberspace, providing deployable defence solutions (Samtani, Ahmadzadeh, & Chen, 2022).

It is also necessary to allow the model to learn, evolve and adapt continuously to the new environmental conditions and to redeploy it cyclically and continuously by implementing a continuous Machine Learning Operations Life Cycle (MLOPS). And in this area, some research also points to the development of sampling-based algorithms to enable fast and deployable AI and pre-processing steps that will be both computationally efficient and provably competitive with the results of the entire collection (Baykal, 2021).

KEYWORDS

Cyberspace Operations; Artificial Intelligence/Machine Learning; Explainable Artificial Intelligence; Deployable Artificial Intelligence; Machine Learning Operations Life Cycle.

REFERENCES

Baykal, C. (2021). *Sampling-based Algorithms for Fast and Deployable AI*. (Doctoral thesis). Available from MIT DSpace database. URI: 1721.1/139924

CCDCOE. (2021). *Recent Cyber Events and Possible Implications for Armed Forces*. The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. & Bengio, Y. (2014). *Generative Adversarial Nets. Advances in Neural Information Processing Systems, 27*. Curran Associates, Inc.

Hoehn, J. (2020). *Joint All-Domain Command and Control (JADC2)*. Report nr. IF11493 – Congressional Research Service, Washington, DC, US.

Layton, P. (2021). *Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-enabled Wars*. The Centre for Defence Research, Australian Defence College, Canberra, Australia. doi: 10.51174/JPS.004

Maathuis, C. (2022). *On Explainable AI Solutions for Targeting in Cyber Military Operations*. International Conference on Cyber Warfare and Security, 17(1), 166–175. doi: 10.34190/iccws.17.1.38

RAN (2020). *RAS-AI Strategy 2040: Warfare Innovation Navy*. Royal Australian Navy, Canberra, Australia.

Ridley, M. (2022). Explainable Artificial Intelligence (XAI). *Information Technology and Libraries, 41*(2). doi: 10.6017/ital.v41i2.14683

Samtani, S., Wang, G., Ahmadzadeh, A. & Yang, S. (2022). *ACM KDD AI4Cyber/MLHat*. Workshop on AI-enabled Cybersecurity Analytics and Deployable Defense.

Cyber resilient warfare

I. Tikanmäki (1) and H. Ruoslahti (2)

(1) Finnish National Defence University, ilkka.tikanmaki@laurea.fi
(2) Laurea University of Applied Sciences, Finland, harri.ruoslahti@laurea.fi

In recent decades, technologies that can be considered separate domains, such as cybersecurity, have been introduced into warfare (Cocron & Aronhime, 2022). As many of today's innovations are related to cyber systems this technological innovation has brought changes in how wars are waged. Non-physical areas of cyber warfare lead to multi-dimensional battle spaces. There are ongoing activities in the information environment and cyberspace, thus, activities need to be continuously developed and coordinated (Dempsey, 2012; Tammen, 2021). Conventional warfare can be preceded by hybrid influence and warfare. One of the most common methods of hybrid influence is the dissemination of disinformation. The initiator of the disinformation campaign has the advantage, so the dissemination of disinformation must be detected in time to enable countermeasures and retaliation. (Goksu & Cavus, 2020; Ozbay & Alatas, 2020).

The line between traditional military conflicts and cyberattacks is blurring. Attacks by actors, whether backed by the state or carried out by independent groups, can undermine the confidentiality, integrity, and availability of critical parties. Such threats must be prepared for, detected, and defended. Asymmetric and proxy wars have been in various forms for millennia and have become increasingly the norm in wars. (Salomon, 2022). Today, battles take place not only on the conventional battlefields but also in the cyber environment. In this environment, governmental and nongovernmental actors develop skills to achieve their goals.

We need to move from describing threats to combating them. Collaboration and exchange of information are needed to build common situation understanding. Training and practices, both in the form of tabletop and scenario-based exercises, should be increased to develop situation awareness and problem-solving. Participants in training and exercises need to trust and support each other in identifying vulnerabilities and building resilience. Building trust is a key prerequisite for protection against threats. (Bilal, 2021; Hagelstam & Narinen, 2018). Combining conventional and unconventional methods in modern warfare using special forces, armed actors, disinformation, and social polarization will help to achieve the desired outcome. There is no generally accepted definition of hybrid warfare, but the concept provides insights into security and defence challenges. (Bilal, 2021).

Combating hybrid threats is difficult in practice, but developing prevention and response, and combining military and non-military instruments, can improve capabilities to combat threats. By combining the most appropriate civilian and military means of action, it is possible to accelerate decision-making and counter-threats. (Rühle & Roberts, 2021) Artificial intelligence and big data analysis can be used to detect and combat, for example, fake news campaigns, but on the other hand, they can provide an attacker with support in carrying out a hybrid campaign. Citizens need awareness and personal resilience. Building organizational resilience against cyber threats and warfare is needed not only in the military but also in critical infrastructure and other business organizations. Combining personal and organizational resilience builds a resilient society.

KEYWORDS

Warfare; Hybrid threats; Hybrid warfare; Cyber environment; Training; Exercises.

REFERENCES

Bilal, A. (2021, November 30). Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review*. Retrieved from https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-andtrust-as-the-antidote/index.html

Cocron, A., & Aronhime, L. (2022, April 14). Risk, Uncertainty and Innovation. *NATO Review*. Retrieved from https://www.nato.int/docu/review/articles/2022/04/14/risk-uncertainty-and-innovation/index .html

Dempsey, M. E. (2012). *Capstone Concept for Joint Operations: Joint Force 2020*. Joint Chiefs of Staff. Retrieved from https://www.ndu.edu/Portals/59/Documents/Incoming/ccjo_2012.pdf

Goksu, M., & Cavus, N. (2020). Fake News Detection on Social Networks with Artificial Intelligence Tools: Systematic Literature Review. In: R. A. Aliev, J. Kacprzyk, W. Pedrycz, M. Jamshidi, M. B. Babanli, & F. M. Sadikoglu (Eds.), *10th International Conference on Theory and Application of Soft Computing, Computing with*

Words and Perceptions—ICSCCW-2019 (pp. 47–53). Springer International Publishing. doi: https://doi.org/10.1007/978-3-030-35249-3_5

Hagelstam, A., & Narinen, K. (2018, November 23). Cooperating to counter hybrid threats. *NATO Review*. Retrieved from https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Ozbay, F. A., & Alatas, B. (2020). Fake news detection within online social media using supervised artificial intelligence algorithms. *Physica A: Statistical Mechanics and Its Applications*, *540*, 123174. doi: https://doi.org/10.1016/j.physa.2019.123174

Rühle, M., & Roberts, C. (2021, March 19). Enlarging NATO's toolbox to counter hybrid threats. *NATO Review*, 10. Salomon, J. M. (2022). Public-Private Partnerships and Collective Cyber Defence. *14th International Conference on Cyber Conflict Keep Moving*, 45–64.

Tammen, J. W. (2021, July 9). NATO's Warfighting Capstone Concept: Anticipating the changing character of war. *NATO Review*. Retrieved from https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-conceptanticipating-the-changing-character-of-war/index.html

Latvia and the European Strategic Autonomy – capabilities first, institutions later

T. Rostoks (1)

(1) National Defence Academy of Latvia, toms.rostoks@mil.lv

Defence integration has become one of the key features of European integration over the past years, and it has largely been discussed in the context of the European Strategic Autonomy (ESA), the concept introduced by France. Much attention has been paid to positions of France, Germany, and Italy, and there has been extensive discussion on defining this initiative and its implications for European security. Unfortunately, there is still a dearth of studies that address positions of small states on ESA. This study looks at Latvia's views on the ESA. Latvia's approach to ESA has been cautious. It was seen as a proposal that could have either positive or negative impact on Latvia's security, depending on what form this proposal would take once it would transform into a policy with specific aims, plans, and budgetary allocations. Latvia's cautious engagement with ESA has been shaped by systemic and country-specific influences, and it came at a time when Latvia's reliance on NATO security guarantees increased. Although a greater focus on strengthening the European pillar of NATO was regarded as a welcome development, there were lingering questions about the overall direction of European defence integration efforts and the actual ability of the ESA to have a positive contribution to Latvia's security. Above all else, there were concerns that the vague notion of autonomy would take the form of a lesser involvement in European security by the US. Despite the extravagancies of Donald Trump's presidency, Latvia hoped that there would be continuity in the US approach towards Europe in the long term. This has been the case at least since early 2021, with Joe Biden's approach to NATO being more supportive. If ESA was a reaction to D.Trump's presidency, it became less relevant once J.Biden was sworn into office in early 2021.

EU defence integration efforts are not new, and neither is the realization of Europe's military weakness vis-à-vis its key ally – the US – and Russia as its key geopolitical competitor in Europe. For Latvia, the ESA proposal came at a time when its defence sector was undergoing profound change. Defence spending increased rapidly from 1.1 per cent of GDP in 2015 to 2 per cent in 2018. Since then, defence spending has increased further, and Latvia's defence spending is projected to reach 2,5 per cent in 2025 due to Russia's aggression towards Ukraine. In short, Latvia along with the other two Baltic neighbours has turned from a laggard into a frontrunner. This partially explains why ESA did not become the focal point of expert and public discussions on European security in Latvia. ESA has been scarcely mentioned in the annual reports by the Latvian Foreign minister since 2017 either. Also, there has been little academic and think tank interest in Latvia's approach to the ESA. The ESA proposal emerged against the backdrop of greater NATO military presence in Latvia. Measures such as rotational presence of NATO eFP battlegroups, prepositioning of military equipment, frequent military exercises with a specific focus on Russia, and rotation presence of the US troops that were almost unthinkable before 2014 were suddenly not only possible, but widely regarded as necessary. Thus, Latvia's prioritization of NATO deterrence posture in the Baltic region is key to understand its cautious approach to and limited engagement with European security and defence integration. However, Latvia also positions itself as a country that makes a positive contribution to international security and European integration. It does not intend to stay out of the European security and defence integration, as this process proceeds apace irrespective of how Latvian authorities feel about it. Thus, Latvia has been compelled to formulate its interests towards this area of European integration.

The analysis proceeds as follows. First, it addresses Latvia's position on the broad contours of ESA. Second, it looks at the variety of views about the relationship between the ESA proposal and NATO's (and the US) involvement in the security of Europe. Third, it looks at the issue of military and nonmilitary capabilities that ESA should eventually produce, as well as the potential institutional changes and innovations that the ESA might bring about. The final aim is to identify Latvia's aims regarding the ESA and the potential coalitions that it might use to accomplish those aims. The analysis concludes that Latvia's approach to ESA has been cautious at best. However, Latvia's has deemed it necessary to participate in European defence integration, and it has recently adopted a more optimistic outlook on ESA. The analysis of Latvia's involvement with ESA is largely based on annual foreign minister's reports, annual foreign policy debates in the Latvian Parliament, and semi-structured interviews with key Latvian political decision-makers and government officials.

U.S.' Allies' Offensive Cyber: Entrapment Risk or Entanglement Nuisance

M. Jensen (1)

(1) Royal Danish Defence College, msje@fak.dk

In NATO, the U.S. controls a major part of the alliance's conventional military capabilities and almost all its nuclear weapons. Snyder's 1984 analysis of dilemmas in military alliances argues that: "In general, entrapment is a more serious concern for the lesser allies than for the superpowers […] because the superpowers have a much greater capacity for taking initiatives (notably nuclear initiatives)" (Snyder, 1984, p. 484). Applying Snyder's analysis, U.S. possession of the majority of NATO's military means provides a dominant position and significant control over NATO's crisis management, which minimize the U.S.' risk of entrapment in conflicts.

Since Snyder wrote his analysis, cyberspace[8] has emerged as a new venue for military operations that changes the U.S.' strategic environment[9]. The U.S. were NATO's only declared actor in cyberspace during the first decades of the Internet, but is no longer alone. As of 2019, sixteen NATO members are developing military means for offensive cyber operations (OCO) (Smeets, 2019, p. 7). The U.S. has described her concerns over OCO proliferation amongst her foes (ODNI, 2021; Trump, 2018, pp. 2–3). Should she, based on Snyder's analysis, also be concerned over proliferation amongst friends and allies?

The purely theoretical answer would be "yes". Any increase in allies' potential for independent initiatives relatively decrease U.S. control over e.g. escalation, hence relatively increase the risk from entrapment. The real world answer depends on the degree to which OCO has potential for strategic impact. The counter-argument to OCO being an entrapment risk is that OCO's potential military impact is too insignificant, even in a crisis. If so, allies' independent or uncoordinated OCO constitutes a lesser risk, namely of nuisance due to involuntary U.S. entanglement.

Hence, the question is about the relative magnitude of the entrapment threat from allies' OCO: Does U.S. allies' new OCO capabilities constitute a credible risk for entrapment, or do they more likely only have the potential to be an entanglement nuisance?

Official U.S. statements do not provide a clear answer. Since 2018, they have increasingly signaled a more active role for national OCO as a deterrent both above and below the threshold of armed conflict, but have provided little insight into how allies' OCO capabilities fit this intent (Trump, 2018, pp. 20–21). Nor does the academic literature presently, a void that this manuscript aspires to begin filling.

The analysis establish that OCO's potential for destruction is not comparable to nuclear weapons but still convincingly capable of creating strategic effects, e.g. escalation, particularly during crisis. Thus, in Snyder's terms, OCO convincingly provide allies new means for "independent strategic initiatives" and constitute an entrapment risk to the U.S., particularly during a crisis, albeit less so than nuclear weapons. Furthermore, OCO-proliferation among U.S. allies will be harder to detect and assess than nuclear capabilities. Also, influencing allies' decisions on OCO development will require different efforts than countering allies' nuclear proliferation and some of the means used historically for that purpose will likely have less effect. Without aspiring to recommend whether or not counter proliferation of NATO allies' OCO capabilities should be a U.S. strategy, these findings suggests that the U.S.

should consider to incentivize allies by issuing clearer statements on how friends and allies could best develop OCO capabilities to support U.S. policy objectives.

KEYWORDS

Offensive cyber capabilities; Alliances; NATO; Entrapment.

REFERENCES

DOD. (2020). *DOD Dictionary of Military and Associated Terms*. Department of Defense.

---

[8] A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (DOD, 2020, p. 55).
[9] For a discussion of what constitutes the strategic environment, see Sokol (2021, pp. 13–23).

ODNI. (2021). *ODNI Annual Threat Assessment*. Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Smeets, M. (2019). NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis. *International Conference on Cyber Conflict, CYCON*, *May*, 1-15. doi: https://doi.org/10.23919/CYCON.2019.8756634

Snyder, G. H. (1984). The Security Dilemma in Alliance Politics. *World Politics*, *36*(4), 461-495. doi: https://doi.org/10.2307/2010183

Sokol, B. J. (Ed.) (2021). *The Marine Corps War College strategy primer*. Marine Corps University Press.

Trump. (2018). *National Cyber Strategy of the United States of America*. Retrieved from https://www.whitehouse.gov/wpcontent/uploads/2018/09/National-Cyber-Strategy.pdf

Ways to generate a military cyber capability – A review of three countries

J. Mattila (1)

(1) Aalto University, Finland, juha.mattila@aalto.fi

Past twenty years, some military powers have been in a race to build cyber force projecting capabilities as the emerging cyber environment has opened new vulnerabilities and ways to impact. (Mattila J. K., 2022) The paper reviews the USA, Russia, and Iran's ways of generating their cyber forces to identify lessons for countries that need to evolve their cyber-related capabilities. Success in the cyber domain requires a particular capability generation, especially in culture, processes, unique tool design, and competencies. Because the military has not been quick in adopting new capabilities (Mattila & Parkinson, 2017), the ways the sampled countries have used to accelerate their force generation may appear beneficial to other militaries striving to gain cyber capabilities.

Motivation for the review came from the researcher's need to create a cyber strategy for a smaller nation and accelerate its cyber force generation. Hence, the multidisciplinary research process had many sequenced spirals of analyses, implementation, and improvement spanning over 2014 to 2022. The original survey included several countries, but this publication samples only three based on their different competency sourcing approaches.

Building the cyber capability combined with its traditional information operations and control of the domestic information domain, Russia has fostered cyber criminals and other proxies to ramp up their financially motivated cadre of cyber warriors. (Bowen, 2022) Their military force generation seems challenged to maintain about 5000 strong cyber forces, possibly because of a cultural incompliance (Red Army vs young, urban ICT professionals). (Clark, 2020) Despite the evident challenges, Russia has been able to impact adversaries' behaviour through the cyber realm, e.g., 2016 hacking of U.S. political organisations, 2017 NotPetya disruption, and 2020 SolarWinds exploitation (Lilly & Cheravitch, 2020).

The U.S. has been building its capabilities with a narrow focus on the cyber domain gradually from information security, then cyber defence and finally, cyber offence. Starting from 2012, they generated over 6000 strong Cyber Mission Force in six years using a network of the defence industry, universities, and R&D organisations to provide the training. (USCYBERCOM, 2021) As a compliance-driven culture, the U.S. military struggles to keep its cyber warriors at expected competency levels, possibly because of the narrow population of recruits (GAO, 2019).

Iran's cyber capability builds on the need to control the domestic information sphere. After the 2010 Stuxnet attack, Iran accelerated its effort to build cyber defence and offensive capability. (Wood, 2021) Within twenty years, they have used many ideologically motivated people to gain a force (2400 + 1200) with low-level skills to exploit cyber vulnerabilities abroad. (Bastani, 2015) Iran has successfully used the global cyber-criminal society and open source to acquire tools and competency for its activists (KFCRIS, 2020).

All three countries have challenges recruiting, motivating, training and maintaining their cyber troops. Nevertheless, sourcing potential recruits is easier when there is a legacy field to combine the generation of new capabilities, i.e., control of domestic information space in Russia and Iran. These countries have used financial and ideological means to improve the motivation of their candidates. Subsequently, the competency has been gained either through hands-on training in small, entrepreneurial teams (Russia), industrial training programmes (USA), or acquiring tools and knowledge from open markets (Iran). However, all countries struggle to coordinate their cyber units in all-domain operations and improve their ability in a fast-evolving cyber environment.

KEYWORDS

Force generation; Cyber capability; National force projection, Cyber Strategy.

REFERENCES

Bastani, H. (2015). *Structure of Iran's Cyber Warfare*. Paris: Institut Francais D'analyse Strategique.
Bowen, A. S. (2022). *Russian Cyber Units*. Washington: The Congressional Research Service, USA.
Clark, M. (2020). *Russian hybrid warfare*. Washington D.C.: Institute for the Study of War.
GAO. (2019). *U.S. Cyber Command and Service should take action to maintain a trained cyber mission force*. Washington: United States Government Accountability Office. Retrieved from https://www.gao.gov/assets/gao-19-362.pdf

KFCRIS. (2020). *Iran's Cyberattacks Capabilities. Riyadh: King Faisal Center for Research and Islamic Studies*. Retrieved from http://www.kfcris.com/pdf/50781c86a6f571af0edb0189aa7594d75e2d6570cfa06.pdf

Lilly, B., & Cheravitch, J. (2020). *The past, present, and future of Russia's cyber strategy and forces*. Tallinn: NATO CCD COE. Retrieved from https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

Mattila, J. K. (2022). *A model for state cyber power - case study of Russian behaviour*. Proceedings of the 21st European Conference on Cyber Warfare and Security hosted in University of Chester 16-17 June 2022 (pp. 188-197). Reading, U.K.: Academic Conferences International Ltd.

Mattila, J., & Parkinson, S. (2017). *Evolution of military enterprise from architecture viewpoint*. International Society of Military Sciences 2017. Oslo, 16.November 2017.

USCYBERCOM. (2021, June 7). *A Command First: CNMF trains, certifies task force in full-spectrum operations*. Retrieved from https://www.cybercom.mil/Media/News/Article/2647621/a-command-first-cnmf-trains-certifies-taskforce-in-full-spectrum-operations/

Wood, F. (2021). *Iran's Cyber Capabilities. Kapolei: University of Hawai'i-West O'ahu*. Retrieved from https://westoahu.hawaii.edu/cyber/regional/world-news-middleeast/irans-cyber-capabilities/

Attended by a 'Bodyguard of Lies': understanding and navigating deception in today's operational environment

M. Fitzpatrick (1)

(1) Defence Research and Development Canada, Meghan.Fitzpatrick@forces.gc.ca

> "He who overcomes the enemy by fraud is as much to be praised as he who does so by force"
> Machiavelli (as quoted in Flaherty & Philips, 2016, p. 1).

Deception has played a role in warfare for centuries. From camouflage and concealment to ruses and feints, it can be employed at all levels of warfare from the tactical to the strategic (Bauer, 2016, p. 36; Whaley, 2007). What is more, deception has arguably been used to achieve some of the most significant military successes of the past hundred years, from the Normandy and Inchon landings to the Gulf War left hook (Bennett & Waltz, 2007, pp. 90-91; Daniel & Herbig, 1982, p. 155-177; Lemire, 2002, pp. 38-40). Over the last decade, nation-states like Russia have used deception to shape the battle space and to facilitate operations, including the 2008 war in Georgia, the 2014 annexation of Crimea and the present war in Ukraine (Blank, 2019, p. 444). In addition, both state and non-state actors regularly utilize deceptive techniques as a means to achieve their strategic goals. One need only point to the challenges posed by online disinformation as a salient example. This reality has prompted a reinvigoration of interest in the subject of military deception and related topics amongst Western armed forces. This is illustrated by an increasing emphasis in high-level guidance on the achievement of surprise and its offensive use in documents like the 2018 *US National Defense Strategy* and the recent revision of vital doctrine, including NATO's *Allied Joint Publication 3.10-2: Operational Security and Deception* (2020).

This paper will explore the role of deception in today's operational environment, where war is rarely declared officially and sub-threshold competition has become commonplace. Moreover, it will examine the curious impact that technology has had on shaping how deception is now conducted. On the one hand, technological advancement has made the battlefield significantly more transparent with the deployment of sensors and satellites. On the other, technology has also exponentially increased the means through which misleading and falsified information can be effectively transmitted to an adversary (Verrall, 2021, p. 77). Following this, the paper will then reflect on the implications for the West. It will conclude by considering the challenges that militaries in liberal-democratic states face in employing deception, from legality to possible reputational damage. Furthermore, it will explore how these factors are to be weighed against possible opportunities to be leveraged from gaining surprise to achieving economy of effort in a highly competitive environment (Heuer, 1981, p. 294; Headrick, 2008, p. 4).

KEYWORDS

Military Deception; Information Environment; Technology.

REFERENCES

Bauer, John W. (2016). *The Virtue of Truthfulness and the Military Profession: Reconciling Honesty and the Requirement to Deceive during War.* PhD Thesis, University of South Carolina.

Bennett, Michael, & Waltz, Edward. (2007). *Counterdeception Principles and Applications in National Security.* Boston; London: Artech House.

Blank, Stephen J. Ed. (2019). *The Russian Military in Contemporary Perspective* Carlisle, PA: US Army War College Press.

Daniel, Donald C, & Herbig, Katherine L. (1982). Propositions on military deception. *Journal of Strategic Studies 5(1),* 155-177.

Flaherty, Ryan Q, & Philips, Andrew R. (2016). *By Force or by Fraud: Optimizing US Information Strategy with Deception.* Monterey, CA: US Naval Postgraduate School.

Headrick, Deborah A. (2008). *Deception for the Operational Commander.* Newport, RI: Naval War College.

Heuer Jr., Richards J. (June 1981). Strategic Deception and Counterdeception: A Cognitive Process Approach. *International Studies Quarterly 25(2)*, 249-327.

Lemire, Guy A. (2002). *Employing Special Operations Forces to Conduct Deception in Support of Shaping and Decisive Operations.* Fort Leavenworth, KS: US Army School of Advanced Military Studies.

North Atlantic Treaty Organization. (6 March 2020). *AJP-3.10.2, Allied Joint Doctrine for Operational Security and Deception Edition A.* Brussels: NATO.

Whaley, Barton. (2007). *Stratagem: Deception and Surprise in War*. Boston: Artech House.

The Role of Regulatory Sandboxes for the Aviation Sector and Portuguese Approach to the Innovation Cycle

T. Cabral (1), D. Duarte (2) and J. Caetano (3)

(1) Portuguese Aeronautical Authority, tmcabral@emfa.pt,
(2) Portuguese Aeronautical Authority, dxduarte@emfa.pt
(3) Portuguese Air Force Academy Research Center, jvcaetano@academiafa.edu.pt

Defence Innovation initiatives, like the ones promoted by at a North-Atlantic Treaty Organization (NATO), the European Defence Agency (EDA), or European Union (EU) level are recognized as great enablers of development and synergies at a multi-national level. However, these require the definition of regulatory frameworks that allow for innovators to test new products, services and procedures in such an environment that boots safety and improves development cycles. One such framework is typically known as "regulatory sandbox", which stemmed from the Financial Industry, and is now mainstreamed throughout many areas of technology and development. Hence, the present article builds on the current status of the regulatory sandboxes, presents some of the most interesting approaches used so far, and delivers an essay on the advantages and challenges serving to the creation of aviation and automation sandboxes within the Portuguese Defence.

NATO Advisory Group on Emerging and Disruptive Technologies (EDT) was created in 2020, which developed the EDT policy and strategic plans to be implemented by the NATO Allies and the NATO Innovation Board, currently focusing on the following EDT (NATO, 2022). Subsequently, NATO AI Strategy was endorsed by the Ministers of Defence in 2021. In addition, NATO created two important mechanisms to foster and to promote its innovation strategy, viz., the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (Christie, 2022). Subsequently, NATO AI Strategy was endorsed by the Ministers of Defence in 2021. In addition, NATO created two important mechanisms to foster and to promote its innovation strategy, viz., the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (Christie, 2022).

In March 2022, the European Union, approved the Strategic Compass for Security and Defence and the EU Defence Innovation Hub (HEDI), where the investment in innovation is considered as one of its main pillars (EU External Action, 2022), boosting innovation initiatives at EU and EDA level, as well as to, to cooperate with the pMS, EU Commission and NATO in these matters (European Defence Agency, 2022).

Furthermore, the European Aviation Safety Agency (EASA) also devised the AI roadmap outlining its applications to aircraft at a large level; nevertheless, this roadmap lacks the regulatory tools for testing and experimentation of such applications in a safe and innovation friendly environment, where the regulator can follow up, learn, devise new regulation and guidance material (Orian Dheu, 2021).

Conversely, some nations have developed regulatory sandboxes and test centres, viz., the UK Civil Aviation Authority established a regulatory sandbox (UK CAA, 2021) and the Swiss Federal Office of Civil Aviation which established regulatory sandboxes to test UAS applications (Muhangi, 2020) on a case-by-case basis.

One of the challenges is to address this effort at international and national level, and to be prepared for the future battlefield with cutting-edge technology. The establishment of regulatory frameworks in Portugal, among digital innovation hubs, testbeds is a framework and governance model for the promotion of technologybased innovation via the creation of Technological Free Zones (TFZ) (Presidência do Conselho de Ministros, 2021) – TFZs consist of "a physical environment, geographically located […] for testing and experimenting with innovative technology-based technologies, products, services and processes, with direct and permanent monitoring by the competent authorities, namely in terms of carrying out tests, providing information, guidelines and recommendations, corresponding to the concept of a regulatory sandbox" (SEDMA, 2022).

In this initiative, Portugal, is stands as one of the countries that created a similar framework, amongst Australia, Singapore and United Kingdom (Everhart, 2020), Canada (Piri, 2019), India (SEDMA, 2022). Its goal is to take advantage of all the opportunities brought by new technologies. The main stakeholders of this framework are the Testing Authority, Regulatory Authorities, ZLT Management Organisation, testing promoters and participants.

In particular, the Testing Authority is deemed responsible for: i) managing the ZLT network, ii) taking the initiative for the creation of ZLTs, iii) endorsing proposals and regulations, iv) supporting, monitoring and supervising the tests in the innovation programmes, v) stimulating, supporting and accompanying the ZLT management

organisations in close coordination of with the Regulatory Authorities of the affected sectors (Presidência do Conselho de Ministros, 2021).

Regulatory Authorities are deemed responsible for: i) presenting to the Testing Authority the proposals for the creation of ZLT; ii) collaborating with the ZLT Management Organisations in launching the programmes for innovation, iii) providing the necessary technical support and iv) devising the regulations for innovations programmes, and to exercise supervision, by reference to the applicable sectorial legislation.

ZLT Management Organisation is responsible for: i) evaluating, selecting, authorising, supporting, monitoring, and supervising the tests in the ZLT, being the sole interlocutor of the Test Promoters.

Test promoters and participants are the ones that apply to carry out the experimentation activities in the ZLT, whereas the participants are the ones that collaborate with the promoters in such activities.

KEYWORDS

Regulatory Sandboxes; Technological Free Zones; Aviation; Automation; Portugal.

REFERENCES

Christie, E. H. (2022, March 31). Defence cooperation in artificial intelligence: Bridging the transatlantic gap for a stronger Europe. *European View*, 13-21. doi:https://doi.org/10.1177/17816858221089372

EU External Action. (2022, March 24). *A Strategic Compass for Security and Defence*. Retrieved from https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1en

European Defence Agency. (2022, May 17). *Hub for EU Defence Innovation (HEDI)*. Retrieved from https://eda.europa.eu/publications-and-data/factsheets/factsheet-hub-for-eu-defence-innovation-(hedi)

Everhart, J. R. (2020). The Fintech Sandbox: An Overview of Regulatory Sandbox Regimes. *Southern Journal of Business and Ethics, 12*, 64-73. Retrieved from https://www.proquest.com/scholarly-journals/fintechsandbox-overview-regulatory-regimes/docview/2485578619/se-2

Muhangi, M. K. (2020). The Journey to Gene Editing; A Case for Regulation. *International Journal of Technology and Management, 5*(2), 1-19. Retrieved June 15, 2022, from https://utamu.ac.ug/ijotm/index.php/ijotm/article/view/78

NATO. (2022, July 15). *NATO Emerging and disruptive technologies*. Retrieved from https://www.nato.int/cps/en/natohq/topics184303.htm

Orian Dheu, I. E. (2021). Flying High for AI? Perspectives on EASA's Roadmap for AI in Aviation. *Air & Space Law*, 1-28. doi:https://doi.org/10.54648/aila2021001

Piri, M. M. (2019). The Changing Landscapes of FinTech and RegTech: Why the United States Should Create a Federal Regulatory Sandbox. *Business & Finance Law Review, 2*(2), 223-255. Retrieved from https://gwbflr.org/wp-content/uploads/2019/04/Regulatory-Sandbox-Piri.pdf

Presidência do Conselho de Ministros. (2021, July 30). Decreto-Lei 67/2021.

Secretário de Estado da Digitalização e Modernização Administrativa. (2022, June 14). *Accelerating Digital Transition in Portugal*. Retrieved from https://portugaldigital.gov.pt/en/accelerating-digital-transitionin-portugal/testing-and-incorporating-new-technologies/technological-free-zones-zlt/

UK CAA. (2021). *CAP 2130 - Regulatory sandbox guidance for the Future Flight Challenge.* UK CAA. Retrieved from https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=10357

Advanced Phishing Detection Platform for Cyber Threat Intelligence, Cybersecurity & Cyber Defence Purposes

C. Pires(1) and J. Borges (2)

(1) CINAMIL/Academia Militar/IUM, Portugal, pires.cecv@academiamilitar.pt
(2) CINAMIL/Academia Militar/IUM, Portugal, jose.borges@academiamilitar.pt

This work proposes a novel platform for detecting, acquiring, processing, classifying and recording event data (defined as artefacts) from suspicious domains and websites (described as entities). The proposed platform aims to provide an analyst-friendly tool customised to specific end-user requirements, delivering state-of-the-art detection and classification methodologies and usability interfaces. Two use case scenarios are identified, internal and external, showcasing situations that would benefit from using such a platform in civilian and military Security Operations Centre (SOC) environments or in an external cyber threat monitoring context. The testing of the platform in these two scenarios will allow us to conclude its efficiency and efficacy in detecting and monitoring phishing entities and supporting the organisation's core activities related to cybersecurity and/or cyber defence.

Souppaya and Scarfone (2013) described phishing as "tricking individuals into disclosing sensitive personal information through deceptive computer-based means". In 2021, the European Union Agency for Cybersecurity – ENISA recognised phishing as a critical trend in cybercrime and information attacks. Indeed, "compromise through phishing e-mails and brute-forcing on Remote Desktop Services (RDP) remain the two most common ransomware infection vectors" and "phishing-as-a-Service (PhaaS) business model is gaining prevalence" (ENISA, 2021).

Figure 1 describes the platform's high-level architecture. The platform's core modules consist of: *sensors* (that detect and add entities to the platform's database through an API); *API* (that allows for entity ingestion and other external system integration); *collection and classification engine* (that extracts, processes and classifies specific artefacts from each entity); *user interface* (that presents the artefacts and allows for artefact correlation in a user friendly way); *reporting* (that sends out notifications when an entity is marked as malicious or as being active).

Figure 1 – Platform's high-level architecture description

The platform also supports several other relevant functionalities, tailored to the end-user specific requirements, such as: *proxy module* (which handles the platform's HTTP/HTTPS traffic, tunnelling it through non-corporate Internet access, thus simulating a regular user's behaviour, instead of relying on a public proxy system, for which the adversary may have some deception countermeasures in place); *export module* (which supports the extraction of an entity's artefacts using industry-standard protocols, such as the OASIS STIX (STIX™, n.d.) structured language for cyber threat intelligence and allows its exchange within trust groups).

On top of these functionalities, the engine also provides advanced functionalities using Artificial Intelligence methodologies such as data-driven *Artificial Neural Networks* (ANN) (Podder, 2021) and expert-driven *Fuzzy Logic* (Chauhan, 2021).

Artificial Intelligence and Machine Learning (AI/ML) methodologies are conquering a considerable space in cybersecurity (Apruzzese et al., 2018). In our work, we perform analysis and classification using data-driven ANN to support the model-based analysis of an entity's screenshot data (one of the acquired artefacts) and classify phishing websites. Expert *Fuzzy Logic* rules will enrich the analysis and classification processes by supporting the prioritisation of entities based on other artefacts, such as the IP address and its geolocation. Implementing these methodologies minimises the dwell time from detection to response, thus allowing for a faster Course of Action (COA) selection and deployment.

We propose two scenarios to test our platform concerning the efficiency and efficacy of cyber threat incident response in civilian and military SOC environments. The *Internal use case* focuses on the organisation's cybersecurity and cyber defence teams working in SOC environments. The *External use case* focuses on the organisation's anti-fraud and cyber threat surveillance teams. Both use cases also support the organisation's Cyber Threat Intelligence teams by acquiring, correlating and clustering artefacts.

In the first scenario, the *Internal use case*, the platform is leveraged to collect and classify data, in order to extract information on phishing entities that target an organisation and its users. The process runs alongside the COA selection and deployment. In the second scenario, the *External use case*, the platform is leveraged to identify, detect and classify entities that impersonate the organisation itself, and that target third-party (allied) organisations or persons within the same trust groups, such as customers or suppliers. These use cases aim to monitor confirmed (currently active) and potential (in case it is dormant, inactive, or is detected before being actively used on a campaign) fraud entities. They also aim to record artefacts on a timeline, from the time of detection, to the time of COA deployment (for active entities), or the time of dismissal (in case the entity is determined to be a false positive). It can also keep inactive and dormant entities under surveillance so they are acted upon in case they become active or update any of its artefacts.

Therefore, the main goals of our platform are to provide functionalities and automation to support the handling of large datasets, analyse them to detect cyber threats (in this work, mainly phishing) through complex data analytics and AI/ML, and support the risk assessment and decision-making of cybersecurity teams. This way, we expected to improve and positively impact the activities of civilian and military organisations and their departments, e.g., SOCs, anti-fraud, intelligence, military operations planning and conduct, and others relevant to accomplishing the organisation's core missions and goals.

KEYWORDS

Artificial Intelligence; Cyber Defence; Cyber Threat Intelligence; Cybersecurity; Machine Learning; Phishing

REFERENCES

Apruzzese, G., Ferretti, L., Marchetti, M., Colajanni, M. & Guido, A. (2018). *On the Effectiveness of Machine and Deep Learning for Cyber Security*. 10th International Conference on Cyber Conflict.
T. Minárik, R. Jakschis, & L. Lindström (Eds.). NATO CCD COE CyCon X: Maximising Effects. Tallinn, Estonia.
Chauhan, K. (2021). Fuzzy Approach for Designing Security Framework. In N. Bhargava, R. Bhargava, P.S. Rathore, & R. Agrawal (Eds.), *Artificial Intelligence and Data Mining Approaches in Security Frameworks*. Scrivener Publishing, Wiley. Hoboken, NJ, USA. doi: https://doi.org/10.1002/9781119760429.ch10
European Union Agency for Cybersecurity. (2021). *ENISA threat landscape 2021: April 2020 to mid-July 2021*.
Theocharidou, M., Malatras, A., Lella, I., Tsekmezoglou, E. (Eds.). *European Network and Information Security Agency*. Athens, Greece. Retrieved from https://data.europa.eu/doi/10.2824/324797
Podder, P., Bharati, S., Mondal, M., Paul, P., & Kose, U. (2021). Artificial Neural Network for Cybersecurity: A Comprehensive Review. *Journal of Information Assurance and Security, 16*, 10-23. doi: https://doi.org/10.48550/arXiv.2107.01185
Souppaya, M., & Scarfone, K. (2013). *NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. National Institute of Standards and Technology, US Department of Commerce. Gaithersburg, MD, USA. doi: https://doi.org/10.6028/NIST.SP.800-83r1
Structured Threat Information eXpression (STIX™). (n.d.). OASIS Cyber Threat Intelligence Technical Committee. Retrieved from https://oasis-open.github.io/cti-documentation/

Uncertainty as an aggregator of organizational responses in cyberspace

H. Jesus (1)

(1) IUM, Portugal, jesus.hmf@ium.pt

This article aims to present that the integration of different entities in Computer Security Incident Response Team (CSIRT) networks constitutes a measure of response to uncertainty to face malicious activities in cyberspace, with a tendency towards isomorphism, in light of the Institutional Theory.

The dependence of societies on the technological component has been increasing, which can be directly proportional to the growth of challenges and vulnerabilities in the area of security, keeping updated the VUCA (Volatile, Uncertain, Complex, Ambiguous) concept, presented in the last century. In turn, the more developed and more technologically dependent the countries are, the greater are their vulnerabilities to attacks in cyberspace. On the other hand, this situation has also exposed citizens, institutions and states to new threats that have had developed in cyberspace. We can thus infer that cybersecurity will be a real future challenge.

Given the characteristics of cyberspace, this development of digital technologies encourages the emergence of new actors and there has been a dramatic increase in malicious incidents in recent years. This growth, both in quantity, complexity and sophistication, makes the anticipation difficult, constituting a threat to society. Particularly at risk are critical infrastructures (CI) that rely heavily on information and communication technology to function, whose motivations can be categorized into three dimensions: Political, sociocultural and financial (Hedel et al., 2018). However, this characteristic of computerization of CIs and the connectivity of systems in the world has created fascinating challenges for computer science and control engineering (Veríssimo et al., 2008).

In the European Union (EU) context we can identify two important directives: (1) The identification and designation of European CIs and the assessment of the need to improve their protection is established in Directive 2008/114/EC . Its protection is a concern of society and cybersecurity regulatory bodies. Among these, and in the context of the European Union (EU), is the European Union Agency for Cybersecurity (ENISA) which has issued several regulations that are followed by national cybersecurity authorities. It has also published several studies, recommendations and good practices, published to support Member States, with a view to uniformity of procedures . And (2) Directive (EU) 2016/1148 aimed at ensuring a high common level of security of networks and information systems across the Union, with the goal to protect vital services to EU society and economy. This directive is intended to prepare Member States to deal with and react to cyber-attacks through the creation of CSIRTs in all type of great organizations, whether public, private, military, academic community or others. Cooperation between the various actors in cyberspace has been presented as a good practice in responding to threats in this domain, where CSIRTs have an important task, since it is difficult to respond autonomously. The CSIRT networks thus constitute an integrating pole of cyber awareness and a standardized security culture, with a view to prevention and collaborative responses in cyberspace.

Also of note is a United Nations survey on e-Government in 2018 that identifies Europe as the region in the world with the greatest presence of national, governmental and sectoral CSIRTs, showing the concern with CI in the EU. The study "Institutionalized Organizations: Formal Structure as Myth and Ceremony" (Meyer & Rowan, 1977) in the context of institutional theory, establishes that organizations would be led to incorporate the practices and procedures defined by the concepts that predominate in the organizational environment and institutionalized in society. Therefore, organizations are structured in accordance with the characteristics of their environments and tend to become isomorphic with them. One reason for Isomorphism is that organizations tend to become identical with the environment in which they operate due to technical interdependencies and the exchange of knowledge, a situation today enhanced by cyberspace. Subsequently, the concept of Isomorphism was deepened (Dimaggio & Powell, 1983) with the argument that changes in organizational structures are no longer driven by competition and the need for efficiency, resulting in processes where organizations become more similar, without necessarily be more efficient.

In terms of conclusion, we can say that CSIRT networks integrate different types of entities, with very different purposes and structures, which have in common the cyberspace and its threats to face. And these are increasingly in complexity and uncertainty, leading to a certain organizational isomorphism in these organizations.

KEYWORDS

Cybersecurity; Critical Infrastructures; CSIRT; Institutional Theory; Isomorphism.

REFERENCES

DiMaggio, P.J., & Powell W.W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48*(2), 147-160. doi: https://doi.org/10.2307/2095101

Hedel, R., Boustras, G., Gkotsis, I., & Rathke, P. (2018). Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector. *International Journal of Critical Infrastructures, 14*(4), 311-335. doi: https://doi.org/10.1504/IJCIS.2018.095616

Meyer, J. W. & Rowan, B. (1977). Institutionalised organisations: formal structures as myth and ceremony, *American Journal of Sociology, 83*(2), 340-363. doi: https://doi.org/10.1086/226550

Veríssimo, P., Neves, N.F., & Correia, M. (2008). The CRUTIAL reference critical information infrastructure architecture: a blueprint. *Int. J. System of Systems Engineering, 1*(1/2), 78-95. Retrieved from https://www.gsd.inesc-id.pt/~mpc/pubs/04_Verissimo.pdf

Use of plastic scintillators with silicon photomultipliers in mobile radiation detectors for the detection and localization of nuclear and radiological threats

Marques (1), A. Vale (2) and P. Vaz (3)

(1) Centro de Investigação da Academia da Força Aérea, Portugal, lumarques@academiafa.edu.pt
(2) Instituto de Plasmas e Fusão Nuclear, Portugal, avale@ipfn.tecnico.ulisboa.pt
(3) Centro de Ciências e Tecnologias Nucleares, Portugal, pedrovaz@ctn.tecnico.ulisboa.pt

Worldwide concern about the illicit traffic of special nuclear materials (SNM) and other radioactive sources led to the implementation of radiation portal monitors (RPMs) at international land borders and seaports to detect gamma-ray and in some cases neutron sources. While SNMs such as highly enriched uranium and plutonium can be used in improvised nuclear devices (with potential of causing large number of casualties), radioactive sources and materials with applications in industry, medicine and research areas can be used in the construction of radiological exposure devices (RED) or radiological dispersal devices (RDD). RDDs can become a weapon of massive disruption with huge social and economic consequences (Connolly & Martin, 2021; IAEA, 2007).

In order to detect weak sources, in particular SNMs, and/or shielded sources large and expensive RPMs with high operational and maintenance costs are used. Moreover, the radiation detection system has to present a high sensitivity and a very low rate of false positives to keep the normal flow of cargo (Downes, 2019). For that reasons, only 10% of the shipping containers, which pass by the seaports all over the Europe, are in fact screened by RPMs. The secondary inspections that are performed to shipping containers after an alarm is triggered are also very time consumption when handheld equipment are used. Therefore, it is necessary to find a high detection efficiency, low-cost, lightweight and compact mobile radiation detection system that can replace or complement RPMs (OECD, 2021).

In literature it is also referred the use of mobile radiation detection systems for use in security scenarios, with the capability to detect, identify and localize nuclear and radioactive sources in urban areas. However, due to large standoff distances and possible presence of weak or shielded sources, it is necessary to use large and heavy detection systems normally carried by cars, vans or trucks. Despite compact dual-mode (gamma-ray and neutron) detection systems can be coupled to multirotors (e.g. CLYM) the small volume available ($12,86$ cm^3) of the detector limits its detection efficiency. To identify the radionuclides (gamma-ray signature), normally inorganic scintillators such as CsI(Tl) and NaI(Tl) and semiconductors (e.g. CZT or HPGe) are used. While semiconductors can perform high-resolution spectroscopy, allowing distinguishing clearly the radionuclide (RN threat) from the naturally occurring radioactive materials (NORMs) or radioisotopes used in medicine, inorganic scintillators are limited by their medium resolution and by the crystal size, e.g. commercial SIGMA50 presents a $32,8$ cm^3 CsI(Tl). Despite their advantage in terms of energy resolution semiconductors are limited in crystal size (approximately 1 cm^3). The replacement of the traditional photomultiplier tubes (PMTs) by the silicon photomultipliers (SiPM) in some inorganic scintillators such as the CsI(Tl) and the LaBr3[Ce] allowed more compact, lightweight, low power consumption, and immune to magnetic field interference photosensors (Marques, 2021).

Plastic scintillators are a good alternative to the more heavy and expensive inorganic scintillators and semiconductors, for the gross counting of gamma-rays above 100 keV, due to their high detection efficiency (available in large sizes), fast response, low-cost, lightweight, and offers also a good beta particles detection efficiency. However, due to the low scintillation light yield of plastic scintillators they cannot perform gammaray spectroscopy.

In order to increase the overall detection efficiency and consequently the source localization, it is suggested an approach consisting in a two-stage process: 1) detection and localization of the RN threat using plastic scintillators with SiPM; and 2) use of a high energy resolution detection system for the identification of the radionuclide(s). The use of high detection efficiency and low cost detectors in the first step allows the fast detection and localization of radioactive sources and is an eager opportunity to reproduce multiple instances of detection systems able to be programmed aiming at autonomous operations of surveillance/inspection using unmanned vehicles.

In Figure 1 it is illustrated an example of the use of a compact, lightweight, low-cost and large cross sectional area plastic scintillator with silicon photomultiplier readout coupled to a multirotor for the screening of a shipping container cargo. The developed detection system is composed by an EJ-200 plastic scintillator (285 cm^3) for gamma-ray and beta detection and an EJ-426HD (with ^{6}Li content) plastic scintillator for neutron detection. The neutron

detector used is also an alternative to the ^{3}He gas (worldwide shortage) based detectors normally used in RPMs. A compact and modular high-density polyethylene (HDPE) moderator was also developed to increase the fast neutron component detection efficiency.

Figure 1 – Developed mobile radiation detection system coupled to a DJI Matrice 600 Pro multirotor for the inspection of a shipping container cargo. EJ-200 plastic detector (left side) and EJ-426HD detector with a HDPE moderator (right side).

The highly maneuverable multirotor allows reducing the source-detector distance increasing the overall detection efficiency. After the detection and localization of the radioactive source, a high-resolution semiconductor or inorganic scintillator can be used to identify the radionuclide.

KEYWORDS

Plastic scintillators; silicon photomultipliers; nuclear and radiological threats; gamma-ray detection; beta and neutron particles detection; radioactive sources localization.

ACKNOWLEDGMENTS

REFERENCES

Connolly E.L., & Martin P.G. (2021). Current and Prospective Radiation Detection Systems, Screening Infrastructure and Interpretive Algorithms for the Non-Intrusive Screening of Shipping Container Cargo: A Review. *Journal of Nuclear Engineering*, *2*(3), 246–280. doi:10.3390/jne2030023.

Downes, R., Hobbs, C., & Salisbury, D. (2019). Combating nuclear smuggling? Exploring drivers and challenges to detecting nuclear and radiological materials at maritime facilities. *The Nonproliferation Review*, *26*, 83–104. doi:10.1080/10736700.2019.1610256.

International Atomic Energy Agency (IAEA). (2007). Combating Illicit Trafficking in Nuclear and Other Radioactive Material, IAEA Nuclear Security Series No. 6, Vienna.

Marques L., Vale A., & Vaz P. (2021). State-of-the-Art Mobile Radiation Detection Systems for Different Scenarios. *Sensors*, *21*(4), 1051. doi:10.3390/s21041051.

OECD/European Union Intellectual Property Office. (2021). Misuse of Containerized Maritime Shipping in the Global Trade of Counterfeits, Illicit Trade. OECD Publishing, Paris.

Thermal management of CBRN equipment using microchannels based heat sinks

A. Moita (1), L. Quinto (2), R. Lucena (3), W. Antunes (4), L. Moreno (5), P. Pontes (6) and A. Moreira (7)

(1) CINAMIL/Academia Militar/IUM, Portugal, moita.asoh@exercito.pt
(2) CINAMIL/Academia Militar/IUM, Portugal, lquinto@academiamilitar.pt
(3) CINAMIL/Academia Militar/IUM, Portugal, rlucena@academiamilitar.pt
(4) CINAMIL/Academia Militar/IUM, Portugal, antunes@academiamilitar.pt
(5) CINAMIL/Academia Militar/IUM, Portugal, lmoreno@academiamilitar.pt
(6) IN+, Instituto Superior Técnico, Portugal, pedrodanielpontes@outlook.pt
(7) IN+, Instituto Superior Técnico, Portugal, aluismoreira@tecnico.ulsiboa.pt

INTRODUCTION

Chemical, biological, radiological and nuclear - CBRN equipment is used by military and civil staff in harsh environmental conditions, being frequently used in decontamination missions as those recently lived in pandemic situations. These suits intend to isolate the user from the surrounding environment. Consequently, heat and mass transfer processes are limited, thus turning humidity regulation and thermal management inside the suits very difficult to achieve in this kind of equipment (Tokizawa et al., 2020). This leads to thermal stress, hyperthermia, cardiac alterations and ultimately in the collapse of the user of the equipment (Tokizawa et al., 2020).

Despite of the research performed so far in this field, there is still no effective solution for this issue, so that the use of this kind of equipment is frequently limited to 45min to 1h. Recent solutions, inspired in airspace suits cooling (e.g. Bartkowiak et al., 2017; Tokizawa et al., 2020), address a complex tubes system for a liquid cooling system. However, the tubes have large dimensions, thus requiring a significant pumping power. Consequently, the systems are large and heavy, and may further increase the weight of the equipment up to 10kg.

In this context, the work introduced here addresses the development of a modular type cooling system to be adapted to the CNRN suits, based small microchannels heat sinks. The tests performed consider the use of various fluids and working conditions which balance the maximization of the heat transfer against the minimization of pressure losses and consequent pumping power.

MATERIALS AND METHODS

To perform the heat transfer tests, the microchannel heat sinks, with a global size of the order of 100x100cm are made from PDMS – Poly(dimethylsiloxane). The imposed heat was achieved by Joule effect, applying direct current, which is supplied by a HP 6274B DC power supply on a thin (20 $\Box$ m thick) stainless-steel foil (AISI 304), which is glued to the microchannel heat sink. Flow dynamics is described by visualization and image post-processing, using a high-speed camera (Phantom v4.2 high-speed camera). A small sapphire window allows for the optical access to a high-speed infrared thermographic camera (Onca MWIR-InSb-320, from Xenics). Temperature distribution is taken from the bottom of the stainless-steel foil, based on the post processing of the obtained thermal images. These data further allows to evaluate the heat transferred from the surface to the flowing fluid in the heat sink. Working fluids are water, HFE7100 and water based nanofluids, with alumina ($Al2O3$) nanoparticles, with particles concentration varying between 0.5wt% and 3wt%. Detailed description of the experimental setup and methodology can be found in Moita et al. (2022).

SAMPLE RESULTS AND CONCLUSIONS

Initial tests were performed at pool boiling conditions (quiescent fluid) and then on forced convection in the microchannel based heat sinks. Considering pool boiling tests, the setup used was the same as in Pontes et al. (2020).

The results obtained under these conditions with nanofluids show advantages of using nanoparticles (in this case alumina, Al_2O_3) to increase the heat transfer, as the obtained heat transfer coefficients are higher, as depicted in Figure 1.

Figure 1 - Effect of Al2O3 nanoparticles concentration in distilled water in pool boiling conditions: Heat transfer coefficient vs the dissipated heat flux.

However, when using liquids under phase change conditions in the heat sinks, the results are not so clear, given that despite of the increased heat fluxes achieved (of the order of 7000W/m^2), there is a penalty (which increases about 4 times when compared to single phase flows) on the pressure drop which consequently will increase the required pumping power, as shown in Figure 2. This is mainly due to the occurrence of instabilities, due to the formation of the bubbles, which lead to significant fluctuations in the pressure and also in the heat transfer coefficients. This problem may be overcome with the use of micro/nanostructured interfaces in the heat sinks. A detailed analysis of these results is given in the full paper.

Figure 2 - Effect of using liquid phase change in forced convection cooling in the microchannels based heat sink: a) Heat transfer coefficient; b) Pumping power.

KEYWORDS

CBRN; Microchannel heat sink; Time resolved thermography.

ACKNOWLEDGEMENTS

REFERENCES

Bartkowiak, G., Dabrowska, A., & Marszalek, A. (2017) *Assessment of an active liquid cooling garment intended for use in a hot environment*. *Appl Ergon*, *58*, 182–189.

Pontes, P., Cautela, R., Teodori, E., Moita, A.S., Liu, Y., Moreira, A.L.N., Nikulin, A., & Del Barrio, E. (2020) *Effect of pattern geometry on bubble dynamics and heat transfer on biphilic surfaces*. *Experimental Thermal and Fluid Science*, *115*(1), 110088.

Pontes, P., Martins, L., Coelho, M., Carvalho, O., Brito, F. B., & Moreira, A. L. N. (2022) *Complex fluid flow in microchannels and heat pipes with enhanced surfaces for advanced heat conversion and recovery systems*. *Energies*, *15*, 1478.

Tokizawa, K., Son, S.-Y., Oka, T., & Yasuda, A. (2020) *Effectiveness of a field-type liquid cooling vest for reducing heat strain while wearing protective clothing*. *Industrial Health*, *58*, 63-71.

Development of an ankle exoskeleton to reduce the metabolic costs during walking

L. Quinto (1), P. Pinheiro (2), A. Machado (3), S. Gonçalves (4), I. Roupa (5), E. Chambel (6), P. Simões (7), J. Martins (8), C. Quental (9), L. Reis (10) and M. Silva (11)

(1) Academia Militar, IUM, Portugal, luis.quinto@academiamilitar.pt
(2) CINAMIL, IUM, Portugal, pinheiro.pmb@exercito.pt
(3) CINAMIL, IUM, Portugal, machado.ajsc@exercito.pt
(4) Instituto Superior Técnico, Portugal, sergio.goncalves@tecnico.ulisboa.pt
(5) Instituto Superior Técnico, Portugal, iroupa@gmail.com
(6) Academia Militar, IUM, Portugal, enio.chambel@academiamilitar.pt
(7) Academia Militar, IUM, Portugal, paula.simoes@academiamilitar.pt
(8) Instituto Superior Técnico, Portugal, jorgemartins@tecnico.ulisboa.pt
(9) Instituto Superior Técnico, Portugal, carlos.quental@tecnico.ulisboa.pt
(10) Instituto Superior Técnico, Portugal, luis.g.reis@tecnico.ulisboa.pt
(11) Instituto Superior Técnico, Portugal, miguelsilva@tecnico.ulisboa.pt

The interest in human enhancement systems has grown significantly in the past few years, particularly in defence, industry, and rehabilitation. Military operations require a high energy expenditure, which could result in high exhaustion rates and increase soldiers' injury risk (Knapik et al., 2004; US Army Research Laboratory, 2018).

Exoskeletons have been pointed out as a viable solution to mitigate such issues, supporting soldiers during demanding tasks, and reducing the likelihood of injury as well as their level of fatigue (Mooney et al., 2014; Mudie et al., 2018; Orr et al., 2021; US Army Research Laboratory, 2018). They comprise three main components, a rigid structure, an actuation and a control system that together allow to support and enhance the performance of its user during specific tasks (Pons, 2008).

This work aims to develop and assess the effectiveness of a military ankle exoskeleton to reduce the metabolic costs during walking. State of the art was evaluated to identify the studies with significant outcomes and lessons learned from such publications (Quinto et al., 2017). The evaluation of the soldiers' load, most demanding activities, and the overall operational environment were also assessed (Santos et al., 2021) and the results were included in the concept development process (Ulrich et al., 2020).

The product development cycle application resulted in developing two different exoskeleton prototypes, both actuating the ankle. The first prototype was entirely passive, comprising a custom-developed exoskeleton structure designed for military purposes and integrating force elements and a control system similar to Collins et al. (2015). A qualitative and quantitative analysis of this prototype was performed by 15 subjects belonging to the Portuguese Armed Forces, being the results integrated into the development process. This prototype reduced the metabolic costs during walking with 10 of the 15 subjects while presenting significant outcomes regarding comfort and range of motion at the ankle (Quinto, Pinheiro, Gonçalves, Roupa, et al., 2022). Such results were achieved by using an external structure fixed to the footwear and the shin, a single support rod in the upper section of the exoskeleton, and a connector which enabled 3 degrees of freedom at the ankle (Quinto, Pinheiro, Gonçalves, Ferreira, et al., 2022). The outcomes of this phase were included in the development process, namely: the need for the control system to adjust to each user's specific needs and the demand for a custom force element designed to fit each user.

The development of the second prototype comprised a significant modification to the initial concept. In this solution, the actuation system was aligned with the ankle joint, enabling its application to different joints. Also, the control system encompassed an electronically controlled actuator, allowing for the adjustment of the system to each user's gait pattern. Additionally, the compact design, enables its easy integration in the current soldier systems architecture. Preliminary results show that the system can actuate the ankle according to each users' gait pattern. Comfort and range of motion are not significantly affected utilizing the system, with little interference in the users' gait when disconnected.

Future work will comprise the development of custom-fit force elements for each user, enabling laboratory trials with the second prototype. After laboratory validation, the exoskeleton will also be evaluated by resorting to field testing.

REFERENCES

Collins, S. H., Bruce Wiggin, M., & Sawicki, G. S. (2015). Reducing the energy cost of human walking using an unpowered exoskeleton. *Nature*, *522*(7555), 212–215.

Knapik, J. J., Reynolds, K. L., & Harman, E. (2004). Soldier Load Carriage: Historical, Physiological, Biomechanical, and Medical Aspects. *Military Medicine*, *169*(1), 45–56.

Mooney, L. M., Rouse, E. J., & Herr, H. M. (2014). Autonomous exoskeleton reduces metabolic cost of walking. *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC 2014*, 3065–3068.

Mudie, K. L., Boynton, A. C., Karakolis, T., O'Donovan, M. P., Kanagaki, G. B., Crowell, H. P., Begg, R. K., LaFiandra, M. E., & Billing, D. C. (2018). Consensus paper on testing and evaluation of military exoskeletons for the dismounted combatant. *Journal of Science and Medicine in Sport*, *21*(11), 1154–1161.

Orr, R., Pope, R., Lopes, T. J. A., Leyk, D., Blacker, S., Bustillo-Aguirre, B. S., & Knapik, J. J. (2021). Soldier load carriage, injuries, rehabilitation and physical conditioning: An international approach. *International Journal of Environmental Research and Public Health*, *18*(8). Retrieved from https://doi.org/10.3390/IJERPH18084010

Pons, J. L. (2008). Wearable Robots: Biomechatronic Exoskeletons. In: José L Pons (Ed.), *Wearable Robots: Biomechatronic Exoskeletons*. Wiley.

Quinto, L., Gonçalves, S. B., & Tavares da Silva, M. (2017). Systematic review of lower limb exoskeletons (in Portuguese). In P. Flores et al. (Ed.), *Proceedings of the 7th Portuguese Congress on Biomechanics* (pp. 111–112). Guimarães, Portugal. Retrieved from https://doi.org/978-989-20-7304-0

Quinto, L., Pinheiro, P., Gonçalves, S. B., Ferreira, R., Roupa, I., & Tavares da Silva, M. (2022). Development and Functional Evaluation of a Passive Ankle Exoskeleton to Support Military Locomotion. *Advances in Military Technology*, *17*(1) (accepted).

Quinto, L., Pinheiro, P., Gonçalves, S. B., Roupa, I. F., & Tavares da Silva, M. (2022). Analysis of a Passive Ankle Exoskeleton for the Reduction of the Metabolic Costs During walking—A Preliminary Study. *Biosystems and Biorobotics*, *27*, 541–544. Retrieved from https://doi.org/10.1007/978-3-030-69547-7_87

Santos, J., Quinto, L., Gonçalves, S. B., Roupa, I. F., Tavares da Silva, M., & Simões, P. (2021). Identification of Requirements for the development of Exoskeletons for Infantry personnel (in portuguese). *XXV Congresso Da Sociedade Portuguesa de Estatística*.

Ulrich, K. T., Eppinger, S. D., & Yang, M. C. (2020). *Product Design and Development Seventh Edition*.

US Army Research Laboratory. (2018). Methodologies for Evaluating the Effects of Physical Augmentation Technologies on Soldier Performance. In *US Army Research Laboratory* (Issue May). Retrieved from https://apps.dtic.mil/sti/pdfs/AD1057611.pdf

Utilization of New Digital Technology for Command and Control in the Norwegian Armed Forces

B. Mobech-Hanssen (1)

(1) Norwegian Defence University College, bmobechhanssen@mil.no

New, disruptive, digital technology characterizes modern military organizations today, and enables new ways to interact, also within the realms of military command and control (C2) (Raska, 2021). Expectations of the possibilities that new technology provides are high, and the goal is increased operational capability through faster communication, a clearer common situational picture, and faster decision-making processes (Brose, 2019). New technology should, though, be followed-up by new routines and procedures to fully benefit from the possibilities within the technology, and new technology may claim new ways of thinking (Birkheim, 2020; Zysk, 2021). Questions arising from this are if new digital technology for C2 actually does contribute to enhancing military organizations' operational capability, or if new technology demands more procedural and organizational changes than military organizations are capable of (Osmundsen, Iden, & Bygstad, 2018; Ahmad, & Murray, 2019; Bowers, & Kirchberger, 2021). Also, as much-needed critical voices point out in a technology-positivist reality, is if this technology actually is revolutionary and disruptive, or just old wine in new bottles (Schousboe, 2019).

The Norwegian Armed Forces' Joint Headquarters (NJHQ) is an example of a military organization where C2 is central, operating in a country characterized by a high degree of digitalization. The headquarters has developed vastly over the past years, and still is continually changing. Even considering that no national armed forces are alike, and thus making direct comparisons difficult, the NJHQ may serve as a relevant and interesting case for studying the effect of the digital shift within C2 in contemporary military organizations in western small states. Organization theory may provide lenses to seeing different sides of and understanding this phenomenon (Christensen et.al., 2017; March, & Olsen, 1989; Smircich, 1985; Thompson, 2007). This makes the following research question interesting; What characterizes the NJHQ's utilization of new digital C2 technology for faster communication, a clearer common situational picture, and faster decision-making processes; and how may this ability to utilize the technology be explained through organization theory perspectives? Through the attempt to answer this question, this research project addresses an area that is still quite pristine in academic research and will provide new knowledge on the effects of the digital shift within the armed forces.

KEYWORDS

Digitalization; Command & Control; Operational Capability; Military Technology; Disruptive Technology.

REFERENCES

Ahmad, M., & Murray, J. (2019). Understanding the connect between digitalisation, sustainability and performance of an organisation. *IJBEX, 17*(1), 83–96.

Birkheim, L. H. (2020, July 8). *Teknologien er mer moden enn organisasjonen*. Stratagem. Retrieved from https://www.stratagem.no/teknologien-er-mer-moden-enn-organisasjonen/

Bowers, I., & Kirchberger, S. (2021). Not so disruptive after all: The 4IR, navies and the search for sea control. *Journal of Strategic Studies, 44*(4), 613-636. doi: 10.1080/01402390.2020.1848819.

Brose, C. (2019). The New Revolution in Military Affairs, War's Sci-Fi Future. *Foreign Affairs*, May/June. Retrieved from https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs

Christensen, T., Egeberg, M., Lægreid, P., Roness, P. G., & Røvik, K. A. (2017). Organisasjonsteori for offentlig sektor (3rd ed.). Oslo: Universitetsforlaget.

March, J. G., & Olsen, J. P. (1989). *Rediscovering institutions. The organizational basics of politics*. New York: The Free Press.

Osmundsen, K., Iden, J., & Bygstad, B. (2018). *Digital Transformation: Drivers, Success Factors, and Implications*. MCIS 2018 Proceedings. Retrieved from https://aisel.aisnet.org/mcis2018/37

Raska, M. (2021). The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies, 44*(4), 456-479. doi: 10.1080/01402390.2020.1848818.

Schousboe, L. (2019, July 15). The Pitfalls of Writing About Revolutionary Defense Technology. War on the Rocks. Retrieved from https://warontherocks.com/2019/07/the-pitfalls-of-writing-about-revolutionary-defensetechnology/

Smircich, L. (1985). Is the concept of culture a paradigm for understanding organizations and ourselves? In: P. N. Frost, L. F. Moore, M. R. Louis, C. C. Lundberg, & J. Martin (Eds.), *Organizational culture* (pp. 55–72). Thousand Oaks, CA: Sage.

Thompson, J. D. (2007). Organizations in action. Social science bases of administrative theory (5th ed.). Piscataway, NJ: Transaction Publishers.

Zysk, K. (2021). Defence innovation and the 4th industrial revolution in Russia. *Journal of Strategic Studies, 44*(4), 543-571. doi: 10.1080/01402390.2020.1856090

Risky or Rewarding? Navigating diversity in contemporary Intelligence, Surveillance, and Reconnaissance (ISR)

A. Svendsen (1)

(1) Bridgehead Institute (Research & Consulting), UK/DK, adam@asgonline.co.uk

Adopting an international focus, this paper evaluates contemporary understudied Intelligence, Surveillance, and Reconnaissance (ISR) trends, extending its analysis and assessment to more widespread-occurring Command, Control, Computers, Communications, as well as Cyber, or C4ISR/ C5ISR, considerations.

Concluding, the paper argues that substantially greater diversity in ISR is reflected overall. That situation is thanks, at least in part, to the increasing adoption of emerging technologies, such as automation and artificial intelligence (AI), which undeniably impact several changes influentially. There are many implications, for instance, including those as articulated by the main overarching theme of this conference, namely for 'promoting peace and security in a new incomprehensible and non-linear world.'

To summarise, many rewards figure from engaging in (C4/C5)ISR work, notably that of, first, acquiring, and, then subsequently, maintaining to sustaining 'information advantage' statuses. On the other hand, less desirably, multiple pressing challenges and persistent uncertainties remain in the form of attendant risks, hazards, and other vulnerabilities, particularly those that can be characterised as being of an ethical and cyber nature.

Continuing to be represented in a prominent manner, those last considerations are worthy of their continued future constant, close, and careful examination in overall (C4/C5)ISR enterprises. Related work efforts extend towards advancing further sustainable command-and-control-related management and addressing via 'safeguards' and similarly-guiding 'tools' to 'frameworks' during navigation, such as deploying and employing suitably calibrated 'guiderails', which all perform important 'containment' to 'rollback' functions in their overall configuration and impact.

Ultimately, developing concepts, such as 'Intelligence Engineering', increase. Both regionally to globally, many corresponding implications for operations to strategies prevail, as well as - as already suggested - for war to peace more broadly. That is as significant disruptors, even 'spoilers', continue nearby, again constantly and persistently encountered and experienced both now, immediately today, and wherever and however they might precisely range into futures anticipated ahead.[10]

KEYWORDS

---

[10] This paper is substantially based on: Svendsen, A.D.M. (2022, March). Risky or Rewarding? Navigating diversity in contemporary Intelligence, Surveillance, and Reconnaissance (ISR). *RSIS Policy Report*, Singapore. Retrieved from https://www.rsis.edu.sg/rsis-publication/ idss/risky-or-rewarding-navigating-diversity-in-contemporary-intelligence-surveillance-and-reconnaissance-isr-strategies/#.YjHQRbinzOS. See also: Svendsen, A.D.M. (2018). Intelligence, Surveillance and Reconnaissance (Chapter 22). In: D.J. Galbreath & J.R. Deni (Eds.), *Routledge Handbook of Defence Studies.* London: Routledge. Retrieved from https:// www.routledgehandbooks. com/doi/10.4324/9781315650463-23.

Efficient Information Distribution Method in a Hostile Wireless Environment

H. Kari (1)

(1) National Defence University, Finland, hannu.kari@mil.fi

Information integrity and confidentiality is traditionally ensured in end-to-end communication using digital signatures and encryption of entire messages. In wireless communication environments, especially in the military context, radio links may be disturbed and are not necessarily available all the time. This unreliable transmission environment easily leads into a large number of retransmission and higher probability of revealing our location. In this paper, we present an idea to combine two widely used communication protection methods at the untraditional levels of the protocol stack. Our approach utilizes efficiently sporadically available communication channel and storage capacity of the neighboring nodes in minimizing transmission needs and location disclosure.

Integrity of a message (or its fragments) can be protected with various methods depending on the protocol level. At the datalink level, cyclic redundancy check (CRC) can be used to detect transmission errors. Similarly, message authenticity code (MAC) is utilized at the session level to protect integrity of an entire message. CRC ensures that accidentally corrupted message is detected at the receiver side. However, it doesn't protect the message from an unsolicited alteration as CRC uses the same algorithm for generating and checking the integrity. Hence, an adversary may alter the message and recalculate the checksum without detection. To circumvent this problem, MAC is using digital signatures to protect checksums. Instead of sending the original checksum in plain text, the checksum is encrypted (i.e., digitally signed) by the original sender with its private key using for example RSA or ECDSA algorithms. Thus, only the sender that possesses the private key can sign the checksum but anyone can verify the integrity of the message with the respective public key. As the checksums and signatures are mathematically strong, it is computationally hard for an adversary to use brute force to guess encrypted right checksum for the altered message.

In many radio communication channel forward error correction codes (FEC) are used in coping with occasional transmission errors. For example in mobile phone networks, such as GSM, UMTS, 4G, and 5G, an adaptive FEC is utilized to adjust with the varying radio channel quality. Depending on the settings and coding, FEC is capable of correcting one or several missing or incorrect bits of one radio frame. Similar error correcting scheme is utilized also for example in fault tolerant storage systems in which failure of one or several hard drives can be recovered without data loss. In a hard drive, every storage fragment (i.e., sector) has its own strong integrity protection thus defining three clearly defined alternative states for every storage bit: zero, one or missing. This is very beneficial for error correction mechanisms over the radio level FEC protocols in which each bit can be zero, one, or erroneously zero or one.

We utilize these two above mentioned protection principles, but in a novel way, to distribute arbitrary sized messages. First, a user message is divided into fixed sized message blocks. Depending of the FEC coding settings, N such message blocks are protected with M same sized FEC blocks forming one FEC-row. These N+M blocks are called FEC-protected blocks. E.g., if M=1, FEC corresponds to a parity protection mechanism that is capable of recovering one missing block of that FEC-row. The larger the M is, the larger number of missing blocks can be recovered in that FEC-row. With larger messages, additional message recovery capacity can be obtained by using multi-dimensional FECs. Thus message recovery capability can be adjusted with parameters of N, M, and the level of FEC-dimensions.

Second, the integrity of each FEC-protected block is done utilizing digital signatures of the original sender. The FEC-protected block is put into an "envelope" that contains necessary information for any recipient to verify the integrity of that block using only the information that is available in that envelope (i.e., integrity-and-FECprotected block). Naturally, each envelop header contains also information that specifies to which user's message this FEC-protected block belongs, what is the structure of FEC-protection, and what is the right location of that block in the message.

This construction ensures that any recipient can verify integrity of that integrity-and-FEC-protected block. The receiver also learns into which user's message it belongs to and in what place. Once the recipient gets enough many FEC-protected blocks of one FEC-row, it can reconstruct locally any missing data blocks of that row. The benefits are twofold. First, the communication channel can be erroneous and there is no need for retransmissions of missing blocks. Thus this works perfectly with unicast, multicast, and broadcast transmission and even with one-directional

links. Second, integrity-and-FEC-protected blocks can be shared amongst neighbors without need to trust each other. This is very beneficial for example with the challenging radio condition of battlefield, when some of the nodes utilize hibernation to save energy, or in which some nodes may be compromised.

Trust management in ad-hoc high-security networks

K. Zaerens (1) and J. Vankka (2)

(1) National Defence University, Finland. Klaus.Zaerens@iki.fi
(2) National Defence University, Finland. Jouko.Vankka@mil.fi

Trust management has been a topic of keen interest in recent years. Security and privacy demands have increased at the same time as new solutions for ubiquitous computing such as edge and fog computing have evolved (Kumar et al., 2021). Research in ad-hoc networks has evolved to a level where new enhanced solutions provide sufficient applicability for highly dynamic environments as in transportation environments (Soleymani et al., 2021).

Increased amount of information in systems and utilizing novel sensor technology have enabled benefits for advanced situational awareness and decision-making systems in multiple fields, but also increased the necessity of sharing knowledge between organizations and stakeholders. Prerequisite for knowledge sharing is that the shared knowledge must be trustworthy (Zaerens, 2018). Trust management can be used to evaluate the accuracy of shared information or define the trustworthiness of information recipients.

This paper discusses the subject of trust management in a high-security ad-hoc network environment, where information is sensitive, environment is constantly evolving and requirements for data consistency, redundancy, reliability, and timeliness are high. Furthermore, in a high-security environment such as the military, malicious actors attempting to obstruct information transfer, corrupt data, or otherwise interfere for their own purposes is a perpetual threat.

We conduct a literary review on novel approaches in trust management field focusing on ad-hoc networks, and analyze applicability of solutions in high-security environment such as military environment. We address the most essential problems and obstacles to be considered before the benefits of trust management can be fully enabled therein.

As a solution to problems with the information transfer management in high-security ad-hoc network, we propose a novel conceptual approach which ensures sufficient security and privacy in relation of time for operative endeavors. We also present some intriguing areas for future research based on findings during this research. The discussion and views presented in this paper can be adopted in any field with doubts concerning the sensitive and classified contents of ad-hoc network-based systems.

KEYWORDS

Trust management; Ad-hoc networks; Internet of Things; Information Sharing; Military.

ACKNOWLEDGEMENTS

REFERENCES

Ali, A. K. S., & Kulkarni, U. (2015). Characteristics, applications and challenges in mobile Ad-Hoc networks (MANET): overview. *Wireless Networks, 3*(12), 6-12.

Kumar, M., Dubey, K., & Pandey, R. (2021). Evolution of Emerging Com-puting paradigm Cloud to Fog: Applications, Limitations and Research Challenges. In: 2021 11th International Conference on Cloud Computing, Data Science & Engineering.

Soleymani, S. A., Goudarzi, S., Anisi, M. H., Zareei, M., Abdullah, A. H., & Kama, N. (2021). A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Vehicular Communications, 29*.

Zaerens, K. (2018). Concept for Controlled Business Critical Information Sharing using Smart Contracts. 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 1-8.

Hydrogen Fuel Cell for Unmanned Aerial Systems: Operational Environment Contamination Response

J. Moura (1), J. Caetano (2) and P. Ribeirinha (3)

(1) Air Force Academy, Portugal, jgmoura@academiafa.edu.pt,
(2) Air Force Academy, Portugal, jvcaetano@academiafa.edu.pt
(3) Faculty of Engineering/University of Porto, Portugal, pauloribeirinha@gmail.pt

Air contaminations found in areas of operation of the Portuguese Air Force cause significant degradation in the aircraft that there operate. Moreover, durability is one of the extensive challenges in proton exchange membrane fuel cells, as chemical and physical degradation phenomena hinder the system's performance over time. This article aims to study the response of fuel cells to contaminations mimicking those found in military aircraft operating conditions.

After system optimisation and baseline testing, NaCl, CO, and NO contaminations were admitted into the fuel cell cathode. Firstly, in values similar to those found in wildfire and maritime environments, and then in higher concentrations. The NaCl and NO tests revealed that these contaminations have a minimal reversible effect on performance for the studied periods, conditions, and concentrations.

CO tests determined some irreversible losses, namely a 17 % drop in Electrochemical Surface Area, ECSA, suggesting significant blockage of catalytic sites. Hence, prolonged wildfire operation is unadvised. Lastly, ex situ analyses were undertaken to support the performance results.

KEYWORDS

Proton Exchange Membrane Fuel Cell (PEMFC); Degradation; Membrane Poisoning; Impedance Spectroscopy; Electrochemical Surface Area (ECSA).

INTRODUCTION

Green regulations and environmental concerns push the vehicle industry to study, invest and develop carbonneutral systems. Lithium battery technology, the most common application for tactical UAS, provides lower specific power and energy (Lapeña-Rey et al., 2017) than fossil fuel counterparts. On the other hand, hydrogen fuel cells offer rapid refuelling, higher specific power and specific energy, which translates to increased aerial system endurance., higher efficiency, low noise, low infrared signature and, since the only product of fuel cell propulsion systems is water, zero emissions (Pan et al., 2019).

The main objective of this work is to test a generic fuel cell in environments mirroring the ones faced by UAS in real areas of operation above 500 ft, to test the concept of a zero-emission hydrogen fuel cell system as a mean of electric propulsion for a tactical UAS, adapted for the Portuguese Air Force's operational needs.

RESULTS AND CONCLUSIONS

After the test bench assembly, the operating conditions were optimised for the highest and most stable performance. Quintech Nafion-212 membrane, Zahner PP240 load, Alicate controllers and water pumps were used in the test bench. Thales software controlled and recorded the characterisations. Two bubblers were connected before the cell to maintain humidification and insert the NaCl contamination. The contamination concentrations were chosen to resemble the desired environments, obtained from atmospheric observations (Blanchard et al., 1984; Miranda et al., 2005). NaCl to mimic oceanic operation and CO and NO to mimic wildfire operation were tested. Contamination periods vary from 30 to 60 hours.

Regarding NaCl contamination tests, the critical factor would be the adsorption of chloride ions in the catalyst layer and subsequent reduction of active sites, causing irreversible performance loss (Yan et al., 2011). There is no comprehensive evidence that salt particles crossed the GDL and reached the catalyst, as ICP results show significant concentration of Na^+ in no part of the MEA. Meaning all salt particles were removed during the recovery, and in situ tests show minimal irreversible losses, likely associated with the natural decay of the cell. This indicates that the concentration of NaCl used in the experiments for this thesis does not affect the PEMFC performance.

Carbon Monoxide was responsible for the biggest performance losses seen in this study. Data from performance tests, polarisation curves, EIS and CV point to irreversible performance decay caused by CO contaminations. The tests presented a deterioration varying from 0.3 to 0.5 mV h⁻¹. EIS results, shown a significant increase of mass transport resistance, in Figure 1. A drop in ECSA of 14 % after the test suggests a significant blockage of catalytic sites.

Figure 1 - EIS Nyquist plots performed before and after CO contaminations

Nitrate Oxide tests displayed the most stable performance and the lowest decay rate of all contaminations. These results were unexpected compared to the literature (Misz et al., 2016). The reasoning could be that in this work, the stoichiometry of the fed gases was significantly lower, the platinum loading of the cathode catalyst layer was higher, as well as the humidity levels.

The study shows that for the tested conditions, and only concerning the cathode contaminations, no significant permanent damage was recorded in the cell for an operation time range from 15 to 60 hours. At least for the first 60 hours, environmental causes will not produce significant and permanent degradation in actual drone operation. However, prolonged wildfire operation may cause damage to the fuel cell, reducing ECSA over time.

ACKNOWLEDGEMENTS

REFERENCES

Blanchard, D. C., Woodcock, A. H., & Cipriano, R. J. (1984). The vertical distribution of the concentration of sea salt in the marine atmosphere near Hawaii. *Tellus B*, *36B*(2), 118–125. doi: https://doi.org/10.1111/j.1600-0889.1984.tb00233.x

Lapeña-Rey, N., Blanco, J. A., Ferreyra, E., Lemus, J. L., Pereira, S., & Serrot, E. (2017). A fuel cell powered unmanned aerial vehicle for low altitude surveillance missions. *International Journal of Hydrogen Energy*, *42*(10), 6926-6940. doi: https://doi.org/10.1016/j.ijhydene.2017.01.137

Miranda, A. I., Ferreira, J., Valente, J., Santos, P., Amorim, J. H., & Borrego, C. (2005). Smoke measurements during Gestosa-2002 experimental field fires. *International Journal of Wildland Fire*, *14*(1), 107. doi: https://doi.org/10.1071/WF04069

Misz, U., Talke, A., Heinzel, A., & Konrad, G. (2016). Sensitivity Analyses on the Impact of Air Contaminants on Automotive Fuel Cells. *Fuel Cells*, *16*(4), 444-462. doi: https://doi.org/10.1002/fuce.201500159

Pan, Z. F., An, L., & Wen, C. Y. (2019). Recent advances in fuel cells based propulsion systems for unmanned aerial vehicles. *Applied Energy*, *240*, 473-485. doi: https://doi.org/10.1016/j.apenergy.2019.02.079

Yan, W.-M., Chu, H.-S., Liu, Y.-L., Chen, F., & Jang, J.-H. (2011). Effects of chlorides on the performance of proton exchange membrane fuel cells. *International Journal of Hydrogen Energy*, *36*(9), 5435-5441. doi: https://doi.org/10.1016/j.ijhydene.2011.01.158

The prospects of neuro-silica interfaces for military neuroenhancement

Ł. Kamieński (1)

(1) Jagiellonian University, Poland, lukasz.kamienski@uj.edu.pl

For centuries, militaries across the world have sought to boost men-at-arms and increase their resilience. Psychopharmacology was the primary means of performance enhancement throughout most of history (Kamieński, 2016), until in the 21st century biotechnology began to open up brand new opportunities (National Research Council, 2009; The Royal Society, 2012). Recently, the most promising developments for human augmentation have come from neuroscience and neurotechnology (neuro S/T) (Giordano, 2015; Cinel, Valeriani & Poli, 2019; Moreno & Schilkin, 2020, pp. 139–164). Research on their real-world applications for defence and national security has boomed over the past two decades, fostered in the United States by such projects as the US BRAIN Initiative and facilitated by one of its leading participants: the Defense Advanced Research Projects Agency (Moreno 2006; DARPA and the Brain Initiative). Lately, China has also shown an increasing interest in this field, placing it high on its national defence technology development agenda (Kania, 2020).

Military neuro S/T can take on four distinct functions: therapy, enhancement, offensive weapons, and countermeasures (Krishnam, 2017). The presentation looks into enhancement and explores perhaps its most transhumanist and consequential form: the brain-computer interface (BCI). Already widely tested in numerous laboratory experiments, the neural interface has great potential for combat applications (Cutter, 2015). The technology has already proved its ability to control external systems and devices, such as computer software, robotic arms, and prostheses. Thus, remote and thought-controlled operating swarms of unmanned automated platforms and other weapons systems will be the most functional future application of BCIs (Turner, 2018). Brainto-machine interfaces have also been intensively researched and developed for yet other purposes: to multiply human computational and cognitive powers, expand existing and grant new senses or types of perception, as well as optimize mental states (treat and even prevent disturbances, mood swings, etc.). In brief, neuro-silica interfaces for defense and national security purposes could advance the control of military hardware, increase situational awareness, improve threat recognition and target acquisition, augment sensory perception, and optimize cognitive and mental states (Emanuel et al., 2019; Turner 2018).

With the fields of neuro S/T and Artificial Intelligence (AI) rapidly converging and co-producing each other, the application of AI in neuroengineering promises to accelerate the progress in neural interface technology. The Holy Grail of BCI-based solutions is to produce a reliable and survivable bidirectional closed-loop braincomputer system that can provide sensory feedback directly to the cortex and 'write' into the brain (i.e. download information). If translated into successful innovations, these AI-supported intelligent neurotechnologies would mark a breakthrough in military human enhancement. However, attempts to merge the military brain with war machines and algorithms present numerous problems and pose challenging questions that need to be addressed.

KEYWORDS

Brain-computer interface (BCI); DARPA; Performance enhancement; Man-machine symbiosis; Neuro S/T.

REFERENCES

Cinel C., Valeriani D., Poli R. (2019). Neurotechnologies for Human Cognitive Augmentation: Current State of the Art and Future Prospects. *Frontiers in Human Neuroscience*, 13 (art. 13). doi: 10.3389/fnhum.2019.00013.

Cutter, P. A. (2015). *The Shape of Things to Come: The Military Benefits of the Brain-Computer Interface in 2040*. Maxwell Air Force Base, AL: Air Command and Staff College, Air University. Retrieved from https://apps.dtic.mil/sti/pdfs/AD1012768.pdf

DARPA and the Brain Initiative. Defense Advanced Research Projects Agency. Arlington, VA. Retrieved from https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative

Emanuel, P., Walper S., DiEuliis D., Klein N., Petro J. B., & Giordano J. (2019). *Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD*. Aberdeen Proving Ground, MD: U.S. Army Combat Capabilities Development Command.

Evans, N. G. (2021). *The Ethics of Neuroscience and National Security*. London: Routledge.

Giordano, J. (Ed.). 2015. *Neurotechnology in National Security and Defense. Practical Considerations, Neuroethical Concerns*, New York: CRC Press.

Kamieński, Ł. (2016). *Shooting Up. A Short History of Drugs and War*. New York: Oxford University Press.

Kania E.B. (2020). Minds at War. China's Pursuit of Military Advantage through Cognitive Science and Biotechnology. *PRISM*, 8(3), 83–101.

Krishnam, A. (2017). *Military Neuroscience and the Coming Age of Neurowarfare*. London: Routledge.

Moreno, J. D. (2006). *Mind Wars. Brain Research and National Defense*, New York: Dana Press.

National Research Council (US) Committee on Opportunities in Neuroscience for Future Army Applications. (2009). *Opportunities in Neuroscience for Future Army Applications*. Washington, DC: National Academy Press.

The Royal Society (2012). *Brain Waves Module 3. Neuroscience, Conflict, and Security*. London.

Turner, P. (2018). It's Now Possible To Telepathically Communicate with a Drone Swarm. *Defense One.* Retrieved from https://www.defenseone.com/technology/2018/09/its-now-possible-telepathicallycommunicate

Inert and Reusable Artillery Projectile for the Training Exercises of the Artillery Units' Military

M. Cláudia (1), G. Humberto (2), B. José (3), S. Ricardo (4), A. Brito (5) and L. Jorge (6)

(1) Centro de Investigação, Desenv. e Inovação da Academia Miliar, IUM, Portugal, id9230@alunos.uminho.pt
(2) Academia Militar, Portugal, gouveia.hmr@exercito.pt
(3) Centro de Invest., Desenv. e Inovação da Academia Miliar, IUM, Portugal, jose.borges@academiamilitar.pt
(4) Instituto Politécnico do Cavado e do Ave, Portugal, rsimoes@ipca.pt
(5) Universidade do Minho, Portugal, amb@dep.uminho.pt
(6) MOLDIT Industries, Portugal, jorge.laranjeira@molditindustries.com

Artillery field training exercises provide the means and processes of preserving and improving the military's technical proficiency and readiness to engage and perform military operations at both the individual and collective levels. Such exercises provide emulated scenarios that resemble fires and use force in operational contexts. (Fernandes, 2019; Sousa, 2020) In the context of the NATO Alliance, artillery units use conventional high explosive (HE) ammunition, such as the 155 mm or 105 mm rounds. Conventionally, the production process of these rounds consists of manufacturing hollow forged steel projectiles filled with high-explosive materials, such as TNT. (Baltazar & Fonseca, 2017; Nascimento, 2020; Silva, 2017) For instance, the usual 155 HE rounds contain 6.6 kg of TNT.

We can list some disadvantages and harmful environmental consequences of the artillery field training using conventional HE rounds: the ecological impact of the firing exercises due to the release of TNT and other energetic materials into the environment, which might add up to hundreds of kilograms of the high explosive chemical components released per training exercise on the proving ground and atmosphere; the degradation of the metal fragments and remaining chemicals released by the explosives left on the proving ground that infiltrate and contaminate the soils; the cost of each training exercise for the armed forces due to, mainly, the unit cost of conventional HE ammunitions.

In this work, we discuss shifting the artillery field training paradigm by proposing using inert and reusable artillery training projectiles for artillery units' training, readiness, and proficiency exercises. Thus, we propose innovative artillery training projectiles composed of two distinct parts: a plastic shell with a specific geometric shape that ensures aeroballistic performance; a metal core that constitutes the mass of the projectile, which is critical for aeroballistic stability. The projectile then results from assembling the plastic shell and the metal core. As mentioned before, the plastic shell provides the projectile's external geometry, with a shape similar to conventional ammunition, for the aeroballistics function. The materials used in the shell are standard commercial engineering polymers selected and designed according to each part's specific requirements, such as the ogive and bourrelet, the rotating band and the basis. These parts are produced by injection molding or through high-precision CNC machining. The metal core is the projectile's body and is a steel part manufactured by CNC machining. The metal core is the projectile's body, and its design ensures two critical physical characteristics: the total mass and the longitudinal mass distribution.

From a project's perspective, our first projectile is a 155 mm inert artillery round. The steel body represents 91.2 % of the projectile's weight and is fundamental for conserving the angular momentum that confers the trajectory's stability of the ammunition. The plastics part introduces the aerodynamic characteristics of the solution, contributing to the aerodynamic forces and moments acting on the symmetric projectile and, therefore, contributing to the aerodynamic stability of the projectile. Moreover, the plastic body defines the appearance of the 155 mm artillery projectile, matching the standard 155 mm artillery HE ammunitions. The artillery solution for a 155 mm howitzer will enable realistic training, from the battery levels to the forward observer functions, contributing to the training of all procedures in the artillery units.

We forecast that the cost of artillery ammunition in polymeric and metallic materials will be lower than that of the 155 mm conventional rounds. Such assertion is based on the costs of raw materials and for processing and manufacturing of the parts. The environmental impact of our artillery training solution is expectedly lower than that of conventional ammunition since metal and plastic parts can be collected from the training exercise area to be reintroduced in new projectiles or forwarded for recycling. The end-user, or a contractor, can collect the metal cores from the proving ground to be reused in new grenades after a quality control process. The plastic fragments can be collected and forwarded for recycling. Since the metal core accounts for 91,2 % of the projectile's mass, the approach indicates that the solution minimizes the metal waste disposed of during the artillery training exercise (mainly the metal material abandoned on the ground during the artillery exercise).

The proposed solution does not carry the high explosive payload of conventional rounds. Therefore, its inert nature will reduce the environmental footprint of artillery practice and the risk of accidents during hot months, allowing for executing training procedures throughout the year. The inert solution will also allow for less strengthened requirements regarding transport and storage. Our artillery training solution aims to contribute to the proficiency of the armed forces military with a focus on sustainability, environment and economic advantages.

KEYWORDS

Artillery Ammunition; Artillery Training Exercises; Inert Ammunition; Reuse; Recycle.

REFERENCES

Fernandes, L. (2019). Focos de desenvolvimento a considerar na artilharia de campanha. *Revista de Artilharia, 1127-1129*(5), 69-74.

Sousa, S. (2020). Perspetiva de futuro da artilharia portuguesa. *Revista de Artilharia, 1142-1144*(3), 43-54.

Nascimento, J. (2020). A proficiência técnica na formação da artilharia de campanha. *Revista de Artilharia, 1139-1141*(1), 7-20.

Silva, N. (2017). O processo de desenvolvimento de capacidades militares na união europeia. *Revista Militar, 25842584.* Retrieved from. https://www.revistamilitar.pt/artigo/1240

Baltazar, M., & Fonseca, D. (2017). As Forças Armadas, a Estratégia da presença Internacional e as informações Militares. *Revista Militar, 2583*. Retrieved from https://www.revistamilitar.pt/artigo/1235

Boot-integrated piezoelectric generator for armed ground forces

J. Vitorino (1), B. Damas (2) and V. Viegas (3)

(1) Portuguese Naval Academy, amaro.vitorino@marinha.pt
(2) CINAV/ Portuguese Naval Academy, bruno.damas@escolanaval.pt
(3) CINAV/ Portuguese Naval Academy, vitor.viegas@escolanaval.pt

Nowadays there is an increasing dependence on electronic devices, and military operations are no exception, employing navigation and communication devices. These devices need an electric power source and batteries are the most common solution, but they can only store certain amount of energy. In the general case, batteries with larger capacity are heavier, compromising military ground forces by reducing their agility (Swanner et al., 2017). Instead of using electrochemical batteries, electric energy can be produced by betavoltaic batteries (which use radioactive materials), fuel cells (powered by external elements, like oxygen and hydrogen) or by harvesting dissipated energy, like solar, or kinetic energy (Jon Harper, 2015), for example, by human walking. A piezoelectric generator (PEG) may be applied in footwear to harvest that energy. Energy from the wind, thermal or radiation from communication devices can also be harvested (Swanner et al., 2017).

Many works on PEG's have been developed, not only for harvesting energy from human walking but also for mechanical energy dissipated from heavy machinery. J. Rocha, Gonçalves, P. Rocha, Silva, & Lanceros-Méndez (2010) developed an energy harvester placed under a shoe composed by a piezoelectric and a triboelectric generators, which could produce a mean power of 15 μW from a person running at four paces per second. Zhao and You (2014) developed two prototypes of PEG's, installed inside of a shoe, and registered a mean power of 1 mW from a person walking at one pace per second, which can fully charge cell phone with a 3500 mA.h battery in approximately two years, after 63 million steps.

A simple PEG is composed by three main components (Figure 1): the piezoelectric material, the key component that converts mechanical energy in electric energy by the piezoelectric effect (B. Jaffe, Cook Jr., & H. Jaffe, 1971; Uchino, 2017; IEEE, 1987); the electronic circuit, responsible for processing the electric energy produced making it possible to be used by the load (once many electronic devices use DC power, a current rectifier is used, and the output voltage is regulated by a converter); and the load is any device powered by the electric energy produced (consumer or energy storage device).

Figure 1 – Block diagram of a PEG

To study the viability of using a PEG as an electric power supply for ground troops, we developed a prototype in two stages. In stage 1 a fixed structure was made to study the positions, beneath the foot, where the piezoelectric material generates more electric power (Figure 2). We used muRata's 7BB-20-6LO piezoelectric diaphragms as piezoelectric materials. Polylactic acid (PLA) structures were printed in 3D, and then glued to the diaphragms to raise the electrical power generated (Figure 3).

Figure 2 – Fixed structure used in stage 1

Figure 3 – Diaphragm with PLA structure

In this stage multiple tests were conducted registering the waveforms of the voltage produced by the materials using resistors as the load (without an electronic circuit). Figure 4 represents the voltage waveforms across a 1 MΩ resistor, generated by one step, using a single diaphragm placed on the heel area, with and without the PLA structure. With the structure, the diaphragm produced a mean power of 76.8 μW and a mean current of 8.8 μA. With multiple diaphragms connected in parallel it is possible to increase the generated electric power.

Figure 4 – Voltage waveforms generated by one step across a 1 MΩ resistor

In stage 2 a boot equipped with a PEG was developed and tested. In this stage we used multiple diaphragms and an electronic circuit, Sparkfun's "Energy Harvester Breakout - LTC3588", that already contains the components showed in figure 1. The work on stage 2 is still in progress.

KEYWORDS

Piezoelectricity; Piezoelectric generator; Energy harvesting.

REFERENCES

Harper, J. (2015, October). The Army Wants to Power Up Dismounted Soldiers. *National Defense, 100(743),* 42-45. Retrieved from https://www.jstor.org/stable/10.2307/27021024

IEEE std. 176-1987 (1987). *IEEE Standard on Piezoelectricity.* New York: IEEE.

Jaffe, B., Cook Jr., W. R., & Jaffe, H. (1971). *Piezoelectric ceramics.* London: Academic Press inc..

Rocha, J. G., Gonçalves, L. M., Rocha, P. F., Silva, M. P., & Lanceros-Méndez, S. (2010, March). Energy Harvesting From Piezoelectric Materials Fully Integrated in Footwear. *IEEE transactions on industrial electronics, 57(3),* 813-819.

Swanner, J., Bito, J., Nichols, G., He, X., Hewett, J., & Tentzeris (2017, October). *Integrating Multiple Energy Harvesting Systems for Department of Defense Applications*. Paper presented at the EESAT conference held by U.S. Department of Energy, San Diego.

Uchino, K. (2017). Advanced Piezoelectric Materials Science and Technology (2nd Ed.). Duxford: Woodhead Publishing.

Zhao, J., & You, Z. (2014, July 11). A Shoe-Embedded Piezoelectric Energy Harvester for Wearable Sensors. *Sensors, 14,* 12497-12510. doi:10.3390/s140712497

Software Architecture for Low-cost UAVs: an application considering automatic target tracking mission scenarios

J. Alves (1), T. Oliveira (2), G. Cruz (3) and D. Silva (4)

(1) Air Force Academy, Portugal, jfalves@academiafa.edu.pt
(2) Air Force Academy, Portugal, tmoliveira@emfa.pt
(3) Air Force Academy, Portugal, gccruz@emfa.pt
(4) Air Force Academy, Portugal, dasilva@emfa.pt

Since 2009, the Portuguese Air Force Academy Research Centre (CIAFA) has been involved in several research projects (e.g., PITVANT) using UAVs. Typically, Piccolo (Collins Aerospace, 2022) autopilots have been used by CIAFA for research purposes. However, this autopilot is relatively expensive and resorts to closed source software. Therefore, CIAFA is exploring new open-source hardware and software options that allow for rapid prototyping and flight testing of UAVs, such as the Pixhawk (Kortunov et al., 2015).

This work aims to implement an adequately validated and documented software architecture compliant with the low-cost hardware architecture previously proposed by Silva et al. (2020), by considering open-source software tools available in the scientific community. Once the software architecture is outlined, an autonomous ground target tracking mission is implemented using the proposed software tools, thus illustrating the effectiveness of the proposed solution.

The software architecture proposed in this research is presented in Figure 1. The architecture comprises four main blocks, PX4 autopilot (including a feature for Software in the Loop Testing - SILT), Gazebo (only used for SILT purposes), QGroundControl (QGC) and Robot Operating System (ROS). The PX4 block corresponds to the autopilot's software that enables the conversion of the thrust, pitch and bank reference-values provided by the guidance algorithms at the ROS environment (detailed in the sequel) to the deflection of the aircraft's flight surfaces and motor settings. The Gazebo simulator module provides the physical simulation environment, and the QGC corresponds to the software running at the Ground Station. Finally, the ROS environment contains a set of modular nodes, namely Guidance and Control, Video Acquisition, Target Detector, Target Geolocation and Target Estimate that allows a UAV equipped with a video camera to detect, extract target's features and compute a set of control references to autonomously follow that target.

Figure 1 – Proposed system software architecture

In the Guidance and Control node, the outer loop controller uses the PX4 Offboard mode to compute roll, pitch, yaw and thrust commands, which are then used by the PX4 autopilot's inner loop controller. The trajectory control for the UAV is separated into lateral and longitudinal control of the UAV. The lateral control was implemented based on Oliveira and Encarnação (2013) Moving Path Following (MPF) method, and the longitudinal control was based on Proportional Integral (PI) controllers.

The Video Acquisition node imports the camera video from the simulator and provides it to the Target Detector node, which uses a neural network, YOLOv3 (Redmon & Farhadi, 2018), to detect the vehicle. The Target Geolocation block implements a Geolocation algorithm from Barber et al. (2006) to compute the position of a ground

target through its location and motion streamed in the video sequence. Next, a Kalman Filter is used in the Target Estimate node to estimate and predict the other parameters required by the MPF.

In this work, a modular and incremental validation method was adopted, until the entire closed-loop system was successfully validated. Figure 2 shows the trajectory of a UAV following a ground vehicle in a simulated environment, using a video camera to detect and autonomously track a ground vehicle. This simulation demonstrates the effectiveness of the proposed architecture, considering both the selected software tools and the implemented control system.

Figure 2 – 2-Dimensional view of the UAV, target estimated position and target's true position.

KEYWORDS

Software architecture; Unmanned Aircraft Systems; YOLOv3, Moving Path Following; PX4 autopilot.

REFERENCES

Barber, D. B., Redding, J. D., McLain, T. W., Beard, R. W., & Taylor, C. N. (2006). Vision-based Target Geolocation using a Fixed-wing Miniature Air Vehicle. *Journal of Intelligent and Robotic Systems*, *47*(4), 361–382. doi: https://doi.org/10.1007/s10846-006-9088-7

Collins Aerospace. (2022). *Piccolo^{TM} Autopilots*. Collins Aerospace. Retrieved from https://www.cloudcaptech.com/products/piccolo-autopilots

Kortunov, V. I., Mazurenko, O. V., Gorbenko, A. V., Mohammed, W., & Hussein, A. (2015). Review and comparative analysis of mini- and micro-UAV autopilots. *2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, 284–289. doi: https://doi.org/10.1109/APUAVD.2015.7346622

Oliveira, T., & Encarnação, P. (2013). Ground Target Tracking Control System for Unmanned Aerial Vehicles. *Journal of Intelligent & Robotic Systems*, *69*(1–4), 373–387. doi: https://doi.org/10.1007/s10846-012-9719-0

Silva, R., Félix, L. & Oliveira. T. (2020). *Projeto Conceptual de uma Aeronave Pequena de Baixo Custo para Aplicações em Controlo Cooperativo*. Academia da Força Aérea Portuguesa.

Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. *ArXiv:1804.02767 [Cs]*. Retrived from http://arxiv.org/abs/1804.02767

Discrimination between vehicles and buildings in military aerial images

R. Amante (1), J. Silvestre Silva (2) and A. Neves (3)

(1) DETI/University of Aveiro, Portugal, rita.amante@ua.pt

(2) Portuguese Military Academy/ CINAMIL & LIBPhys-UC, jose.silva@academiamilitar.pt

(3) DETI/IEETA, University of Aveiro, Portugal, an@ua.pt

ABSTRACT

The advancement of technology has facilitated the detection of objects in aerial images, a task which must be performed quickly and accurately. This work analyzed the performance of object detection algorithms, Faster RCNN, YOLOv3 and YOLOv5l, for the detection of vehicles and buildings in aerial images obtained by UAV. The results showed that YOLOv5l had the best performance and the fastest detection time.

KEYWORDS

Deep Learning; Object Detection; Transfer Learning; UAV.

INTRODUCTION

The expansion of Unmanned Aerial Vehicles (UAV), remotely controlled aerial vehicles, made it possible to access hard-to-reach places and vast amounts of data, as well as enabled the improvement of object detection algorithms, a growing topic of great interest and applicability, in both civil and military contexts. UAVs capture images which can be used in traffic monitoring, road accidents, operations supporting government agencies, predicting enemy movements, locating areas occupied by enemy troops, disaster assistance, detecting illegal activities, planning offensive operations, among others.

This gave emphasis to the development of algorithms for the detection of vehicles and buildings in aerial images, namely in military scenario.

METHODOLOGY

The adopted methodology started with the choice of Faster R-CNN, YOLOv3 and YOLOv5l algorithms. A total of 11945 instances, 9500 vehicles and 2445 buildings, were used. The images were resized to 640×640 (pixels per inch), to which brightness and Gaussian blur transformations were applied, resulting in the Portuguese Military Academy with Data Augmentation (PMA-DA) dataset. Both sets were divided into three parts: training (80%), validation (10%) and testing (10%).

The following step consisted of inferring the pretrained algorithms using the Transfer Learning (TL) pretrained network as a classifier approach, to carry out qualitative (direct observation of detection results) and quantitative (observation of the detection times) evaluations. The TensorFlow 2 Object Detection API was used for Faster R-CNN and the open-source code developed by Ultralytics was used for YOLO, both pretrained with the Microsoft Common Objects in Context (MS COCO) dataset (Lin et al., 2015).

The training parameters of batch size, learning rate, Intersection Over Union (IoU) limit and confidence limit were configured with values of 2, 0.013, 0.5 and 0.3, respectively. The YOLOv3 and YOLOv5l were trained for 100 and 200 epochs with the PMA dataset and for 100 epochs with the PMA-DA dataset. The Faster R-CNN was trained for 14500 and 29000 steps with the PMA dataset, the equivalent to 100 and 200 epochs, respectively, and for 43500 steps with the PMA-DA dataset, the equivalent of 100 epochs with the augmented data. The training of the algorithms followed the pretrained network as a feature extractor approach of TL.

RESULTS AND DISCUSSION

The results show that Faster R-CNN has the lowest mean Average Precision (mAP) because, although it shows high Precision, Recall is low, which indicates that most objects were detected correctly, but the number of false negatives was high. The YOLO algorithms have a higher mAP since both Precision and Recall are high, which indicates that most objects were detected correctly, decreasing the number of false positives and false negatives. Figure 1 illustrates the YOLOv5l algorithm detection results, able of detecting all vehicles and buildings. However,

there were still some false positives.

Figure 1 – YOLOv5l algorithm detection results for two images from the PMA dataset, captured in a UEO of Portuguese Army

CONCLUSION

The performance of the algorithms show that the Precision for the building class was higher than that of the vehicle class, which indicates that the algorithms recognize larger objects more effectively; the Recall of the building class was lower than that of the vehicle class, due to the smaller number of instances of this class in the datasets; training with data augmentation did not improve the performance of the algorithms, probably because there was an increase in new difficulties, requiring more training time for the algorithms to learn. It was concluded that YOLOv5l was the most efficient for detecting vehicles and buildings in aerial images and useful for real-time applications, which is in line with the two studies mentioned.

In terms of future work, two approaches can be applied to the YOLOv5l algorithm: the expansion of the dataset with images from other locations and environments, and the adjustment of hyperparameters.

ACKNOWLEDGEMENTS

REFERENCES

Lin, T., Marie, M., Belongie, S.J., Bourdev, L. D., Girshick, R. B., Hays, J., … Zitnick, C. L. (2015, Feb). *Microsoft COCO: Common Objects in Context*. doi: 10.48550/ARXIV.1405.0312v.

Nepal, U. & Eslamiat, H. (2022, Jan). Comparing YOLOv3, YOLOv4 and YOLOv5 for Autonomous Landing Spot Detection in Faulty UAVs. *Sensors 22*(2). doi: 10.3390/s22020464.

Saetchnikov, I. V., Tcherniavskaia, E. A. & Skakun, V. V. (2021, Jun). Object Detection for Unmanned Aerial Vehicle Camera via Convolutional Neural Networks. *IEEE Journal on Miniaturization for Air and Space Systems, 2*(2). doi: 10.1109/JMASS.2020.3040976

Unmanned Ground Vehicles – Overview of technology

A. Machado (1), P. Pinheiro (2), L. Quinto (3), S. Moreira (4), E. Chambel (5) and A. Moutinho (6)

(1) UAGME and CINAMIL/IUM, Portugal. machado.ajsc@exercito.pt
(2) CINAMIL/IUM, and Regimento de Manutenção, Portugal, pinheiro.pmb@exercito.pt
(3) CINAMIL/IUM, Portugal, luis.quinto@academiamilitar.pt
(4) UAGME, Portugal, moreira.smm@exercito.pt
(5) CINAMIL/IUM, Portugal, chambel.erp@exercito.pt
(6) IDMEC/Instituto Superior Técnico, Portugal, alexandra.moutinho@tecnico.ulisboa.pt

In recent years society has witnessed an impressive race for emerging and disruptive technologies (EDP), such as advanced robotics, artificial intelligence (AI), computational power, networking, and engineering, among other technologies (European Defence Agency, 2022). These developments have enhanced the growth of several fields, such as unmanned platforms like Unmanned Ground Vehicles (UGV) (NATO S&T , 2022). The application of UGVs is highly desirable by the cities of the future but also in the military context. The North Atlantic Treaty Organization (NATO) and the European Defence Agency (EDA) have supported several projects in this field, generating synergies between Defence, Industry, and Academia to develop UGVs aiming to reduce human exposure to dangerous contexts while contributing to the increase of military capabilities (European UGS seminar, 2021).

UGVs are considered of particular interest in logistics, combat and Intelligence, Surveillance, and Reconnaissance (ISR) operations. These systems can be used, for example, in search and rescue operations, to reach challenging and dangerous situations, for instance, while extracting victims from dangerous environments such as during combat operations or natural catastrophes (Prišmantaitė, 2019).

UGVs are typically deployed in uncontrolled environments. For a UGV to be successful in an environment with so much information, it is essential that it has the following capabilities: (Hu, et al., 2020): 1) Collect data about the surrounding environment; 2) Detect objects of interest (e.g., people, vehicles and obstacles); 3) Move between waypoints with partial or no human assistance; 4) Operate without human intervention for an extended period; 5) Avoid situations which are harmful to people and assets, unless they are intended for that; 6) Scan and/or remove explosives. All these capabilities require applying a considerable number of key technologies, supporting the development of increasingly more complex and improved solutions. UGVs generally consist of a platform, sensors, AI system, a guidance interface and communication links (Zahradníček, Rak, Hrdinka, Nohel, & Rýznar, 2021).

Referring to the platform, defence-oriented solutions have converged towards implementing X-by-wire technology (drive-by-wire, brake-by-wire, and steer-by-wire). This technology replaces mechanical connections with electrical connections, which allows for considerable weight and volume reduction, and ensures greater flexibility to the system to meet rigorous military requirements (Ni, Hu, & Xiang, 2020).

As for sensors, radar and ultrasonic sensors can be used for navigation, to detect large objects or landmarks, and in well-controlled indoor environments or roads with pre-defined settings (Biagini, et al., 2020). However, in unknown and complex outdoor environments, the inherent variability in nature leads to reaching the limits of such sensors. Light Detection and Ranging (LIDAR) systems can also be used to produce a 2D or 3D rendering of the surrounding environment. LIDAR systems use a laser or combination of lasers and are not affected by low visibility conditions such as fog or darkness (Bonadies & Gadsden, 2019). In addition to these, sound navigation and ranging (SONAR), radio detection and ranging (RADAR), monocular cameras, thermal cameras, polarised cameras, and thermal infrared cameras are also commonly used (Hu, et al., 2020).

AI allows the system (e.g., UGV) to adjust its performance while performing a determined task depending on the context and surrounding environment. The control strategies are often based on computer vision, Kalman, fuzzy logic methods and reinforcement learning (Wang, et al., 2020). Generally, redundancy and complementarity of sensors are required, so it is necessary to cross-reference information from different sensors (Hu, et al., 2020). Asynchronous multi-sensor-based information fusion methods have attracted considerable attention for harsh environments, but results are still insufficient to deal with multiple asynchronous heterogeneous real-time sensors. Further improvements are needed for fast and reliable detection algorithms. Temporal fusion is another valuable and common way to increase the continuity and reliability of object detection because it takes advantage of temporal information (Hu, et al., 2020). AI would have the distinct advantage of learning or collecting specific data sets and rapidly transferring them to other systems (Hu, et al., 2020). Using AI, it is also possible to make predictions, based on large data sets, about how events will possibly unfold (NATO S&T Organization, 2018). Results show that,

although recent advances have enabled the development of low-cost high-efficiency sensors, there are still significant limitations when applied in real-life context, implying that further developments are needed in this field (Hu, et al., 2020). AI has been widely developed, presenting innovative and increasingly accurate techniques, and is reaching a mature stage, integrating machine learning, computer vision, navigation, manipulation, planning and reasoning, and language processing into a general framework (NATO S&T Organization, 2018). As a way ahead for the development of UGV systems, several vulnerabilities were also identified, namely interoperability with different platforms or cyberphysical Defence.

KEYWORDS

Unmanned Ground Vehicle; Sensor; Artificial Intelligence; Defence; Military Operations.

REFERENCES

Biagini, M., Pizzi, M., Koerner, B., De Mattia, S., Turi, M., & Picollo, M. (2020). *Synthetic Environment for Robotics and Autonomous Systems*.

Bonadies, S., & Gadsden, S. A. (2019). *Engineering in Agriculture, Environment and Food*. Elsevier.

European Defence Agency. (2022). *Combat Unmanned Ground System - CUGS*.

European UGS seminar. (2021, April). *European Unmanned Ground Systems Seminar 2021 April*.

Hu, J.-w., Zheng, B.-y., Wang, C., Zhao, C.-h., Hou, X.-l., Pan, Q., & Xu, Z. (2020). *A survey on multi-sensor fusion based obstacle detection for intelligent ground vehicles in off-road environments*. Frontiers of Information Technology & Electronic Engineering.

NATO S&T. (2022). 2022 *Collaborative programme of work*.

NATO S&T Organization. (2018). *Robots Underpinning Future NATO Operations*.

Ni, J., Hu, J., & Xiang, C. (2020). A review for design and dynamics A review for design and dynamics. *Journal of Automobile Engineering*.

Prišmantaitė, K. (2019). *Research and innovation in the development of unmanned ground vehicles: the european union and the baltic states*.

Wang, H., Yuan, S., Guo, M., Chan, C.-Y., Li, X., & Lan, W. (2020). Tactical driving decisions of unmanned ground vehicles in complex highway environments: A deep reinforcement learning approach. *Journal of Automobile Engineering*.

Zahradníček, P., Rak, L., Hrdinka, J., Nohel, J., & Rýznar, B. (2021). Combat unmanned ground vehicles: Perspectives for implementation into operational application. *International Scientific Journal "Security & Future"*.

Identification of people in the Wild

R. Menino (1), J. Silva (2) and A. Neves (3)

(1) University of Aveiro, Portugal, ruben.menino@ua.pt
(2) Military Academy & CINAMIL & LIBPhys-UC, Portugal, jose.silva@academiamilitar.pt
(3) University of Aveiro, Portugal, an@ua.pt

ABSTRACT

In recent years facial recognition has become increasingly important, with the main objective of identifying and recognizing a person. In this work, a study is carried out on several detection algorithms in various types of images, and recognition in visible spectrum images using various pre-processing methods. Experimental results on these algorithms are presented, as well as an improvement of about 30% in the detection of faces in thermal images

KEYWORDS

Face detection; Face recognition; Image processing; Deep learning; Algorithms; Image acquisition.

INTRODUCTION

Having an image of a person's face, it is possible to identify and recognize any person, who is in a set of images (Li et al., 2020). This theme is very important these days, due to the various places in which it can be used. It is a research area with a high growth due to the plurality that can be used, including the control of access to stadiums and important events and also increasing the security level in the access to military critical facilities. It is possible to recognize people previously flagged as terrorist groups, people who were aggressive and did not cooperate with security forces, and also recognize people who are considered a threat to national security. To achieve a facial recognition system, it is necessary to have a dataset, perform face detection, extraction and classification.

METHODOLOGY

The focus of this work is the exploration of algorithms for recognition in non-cooperative environments. Since there was no dataset that provided the best conditions in this work, we proposed the creation of a dataset that was carried out at the University of Aveiro.

Several methods are be used to perform face detection such as Haar Cascades, Gradient Histogram and Dlib CNN. The next step is to extract the main features of the face (mouth, eyebrows, nose, eyes) in the image. Through these characteristic points, facial frontalization is performed, where the face is rotated in the image to an angle of 0º (front face) and then the same image is resized with the detected frontalized face. Then a recognition method transforms the characteristics of a face from a training database into a certain data set and is then able to classify and obtain a prediction of that face according to the data acquired after processing of image

RESULTS

Several images were acquired at the University of Aveiro to use as training and testing of the algorithms. Three different cameras provided by the military academy were used, where facial images of people with different angles of rotation of the face, between -90º and 90º were captured. Images were acquired in various spectra (Visible, LWIR, SWIR, NIR). For the analysis of the detection methods, the created dataset and an online dataset were used. The detection was carried out with the 3 proposed algorithms, Haar Cascades, Hog and Dlib CNN for each of the datasets. After obtaining data from the two datasets, it was possible to observe that the same face angle was not always detected. Factors such as lighting at the time of capture, camera and face positioning are factors that change these results.

As for the recognition methods, the dataset made with images in the visible spectrum was used, and results from the Eigenfaces and Fisherfaces methods were acquired, with and without the frontalization of the face performed. The results show that the number of images in the training dataset is a key factor for the success rate of the algorithms. The larger the dataset, the greater the number of true positives and the corresponding hit rate.

CONCLUSION

The results allow us to conclude that there are several factors that change the performance of the algorithm. Factors such as brightness, image acquisition camera quality and pose substantially alter these results. Although the Dlib CNN neural network presented more hits than the other methods, there are more factors that can be considered, in this case the processing time, where the HOG algorithm achieved a relatively high hit rate, but with a shorter processing time. Making sudden changes to the image like frontalization makes the algorithms worse due to the altered pixels of the images.

REFERENCES

Álvarez, C.(2021, April 13). *Dlib-models*. Retrieved from https://github.com/davisking/dlib-models

Amos, B., Ludwiczuk, B., & Satyanarayanan, M. (2016). Openface: A general-purpose face recognition library with mobile applications. *CMU School of Computer Science*, *6*(2), 20.

Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. *IEEE access*, *8*, 139110-139120.

Souza, D. (2018, February 18). *Face Frontalization*. Retrieved from https://github.com/dougsouza/face-frontalization

3D Image Reconstruction of Road Accident

P. Valério (1), J. Silva (2) and A. Neves (3)

(1) DETI, University of Aveiro, Portugal, pedrovalerio@ua.pt
(2) Portuguese Military Academy/CINAMIL & LIBPhys-UC, jose.silva@academiamilitar.pt
(3) DETI & IEETA, University of Aveiro, Portugal, an@ua.pt

ABSTRACT

The reconstitution of a traffic accident scene is an important task which directly affects users of land transport, allowing military or civil entities to authorize the opening of roads to traffic. However, the process of information gathering must be both as quick and as thorough as possible. This work analyses the process of drone-based digital 3D reconstruction and how it is affected by different conditions, to quickly obtain a reliable digital representation of a road traffic accident.

KEYWORDS

Photogrammetry; Drone; Point cloud; 3D reconstruction; Traffic accident.

INTRODUCTION

Digital 3D reconstruction methods can be used, as opposed to traditional, manual techniques, to generate a reliable 3D digital representation of real-world data and has, in recent years, been applied to many fields, including road traffic accident investigation. The typical method is to capture spatial information and generate a point cloud. These point clouds can be transformed into other 3D products, such as triangular meshes or Digital Elevation Models. A recent technique employs the use of drones to capture photographic imagery of an area. Then, this set of images is processed to generate the point cloud. The process of measuring and interpreting photographic images is known as photogrammetry and, with the use of lightweight, affordable drones, provides a cheaper and flexible way of capturing many different physical scenarios. This work evaluates how the different stages of 3D reconstruction are affected by different strategies and algorithms, using existing established software tools.

METHODOLOGY

The program used to generate the point clouds was Agisoft Metashape 1.8.2 which provides a well-defined workflow for generating 3D products from images. In this stage, a SIFT approach was used to identify the features of the images and map them to a sparse point cloud, consisting of the feature points of all images, which is then processed into different dense point clouds. For the generation of the 3D triangular model, MeshLab 2022.02 was selected, to have a higher degree of control over the generation strategy as well as a series of post and pre-processing operations. To reduce the size of the cloud, down-sampling strategies were studied. For the reconstruction, two widely used algorithms were compared, namely the Poisson Reconstruction and Ball-Pivoting Algorithm. Finally, post-processing cleaning operations, namely Edge Collapse face reduction techniques to reduce the number of redundant faces of the final model and the application of a HC Laplacian Smoothing filter were analysed.

RESULTS AND DISCUSSION

For this work, two real traffic accidents were captured, resulting in two image dataset. It was found that the Poisson Reconstruction outperformed the Ball-Pivoting Algorithm. The former was able to correctly reproduce more complex features such as writing on the vehicles, while the latter rendered these illegible. Additionally, the Ball-Pivoting Algorithm had a much higher processing time and produced various gaps in the model, being heavily affected by the varying density of points in the point cloud. The use of prior down-sampling in the point cloud succeeded in reducing the processing time for the algorithms, however, in comparison with the unsampled reconstruction, produced a less well-defined surface and more blurred texture. The smoothing filter was found to not produce significant changes to the model. Figure 1 shows both a generated point cloud and reconstructed triangular mesh.

Figure 1 – Generated Point Cloud (left); Reconstructed Mesh (Right)

From the images, several elements in the scene are correctly and clearly distinguishable, such as the cars on the road and building. In some areas, such the walls of the house or the space under the cars, there are noticeable holes in the point cloud. This is a typical problem for photogrammetry, since the photos were taken from above, which means these areas were occluded. However, this still did not severely affect the mesh reconstruction.

CONCLUSIONS

It was found that factors like the volume or the complexity of the terrain influence the final quality, however, and thus, care should be taken when choosing the appropriate strategy and generation settings. It was concluded that the input point cloud had the biggest impact on the quality of the mesh, more than the mesh reconstruction itself, in particular, because the number of points and point density directly influence the amount of detail and features the cloud can represent.

ACKNOWLEDGEMENTS

REFERENCES

Almeshal, A.M., Alenezi, M.R., & Alshatti A.K. (2020), Accuracy Assessment of Small Unmanned Aerial Vehicle for Traffic Accident Photogrammetry in the Extrem. Operating Conditions of Kuwait. *Information*, *11*(9), 442. doi:10.3390/info11090442.

Jiménez-Jiménez, S.I., Ojeda-Bustamante, W., Marcial-Pablo, M.D.J., & Enciso, J. (2021). Digital Terrain Models Generated with Low-Cost UAV Photogrammetry: Methodology and Accuracy, *ISPRS International Journal of Geo-Information*, *10*(5). doi:10.3390/ijgi10050285

Maiti, A., & Chakravarty, D. (2016), Performance analysis of different surface reconstruction algorithms for 3D reconstruction of outdoor objects from their digital images, *SpringerPlus, 5*(1), 932. doi:10.1186/s40064016-2425-9.

Pérez, J.A., Gonçalves, G.R., Rangel, J.M., & Ortega, P.F. (2019). Accuracy and effectiveness of orthophotos obtained from low cost UASs video imagery for traffic accident scenes documentation. *Adv. Eng. Softw., 132*(1), 47-54. doi:10.1016/J.ADVENGSOFT.2019.03.010.

Takhirov, S.M., & Kayen, R.E. (2021). Point Clouds of Bridge Generated by Terrestrial Laser Scanner and Images via Structure from Motion Technique: Comparison Study. *3rd International Congress on Human- Computer Interaction, Optimization and Robotic Applications (HORA).* doi:10.1109/HORA52670.2021.9461365.

Application of artificial intelligence to the detection of foreign object debris at aerodromes' movement area

J. Almeida (1), G. Cruz (2) and T. Oliveira (3)

(1) Air Force Academy, Portugal, jmbalmeida@academiafa.edu.pt
(2) Air Force Academy, Portugal, gccruz@academiafa.edu.pt
(3) Air Force Academy, Portugal, tmoliveira@academiafa.edu.pt

ABSTRACT

This work describes a low-cost and passive system that detects Foreign Object Debris (FODs) at aerodromes, using neural networks. FODs pose safety risks and cause high costs . Existing FOD detection systems are based on radars, making them expensive.

We created a dataset of images to test this solution, using three different electro-optical sensors: visible, near-infrared plus visible and long-wave infrared. Our approach to this problem is based on image classification and object detection networks.

For classifier, we choose Xception, achieving a 98.86% accuracy. In the case of object detection, we opt for a single-stage detector – YOLOv3 –, achieving an AP of 91.08%. Finally, we evaluate the same models on completely new samples.

KEYWORDS

Foreign Object Debris; Computer Vision; Dataset; Image Classification; Object Detection.

INTRODUCTION

Safety plays a vital role in aviation, and prevention is the preferred method to ensure it. FODs pose a double threat, where the first has to do with safety and the second with the associated costs. In addition, the costs associated reach over $5 billion globally yearly (McCreary, 2010). The most well-known FOD strike occurred with Concorde, which reinforced the awareness to this problem.

Aerodromes perform daily visual inspections to the movement area to ensure aircraft's safe circulation. However, this traditional inspection method is meagre because of its periodicity and capability of human detection. Modern radar and electro optical-based systems installed at some major airports can accurately detect FODs in various weather conditions. Notwithstanding, their implementation and costs are significant downsides to smaller aerodromes.

In recent years, the advent of deep learning and computer vision allowed the implementation of solutions to tasks that before would require visual inspection by humans at lower costs and near-human accuracy. Works by (Cao et al., 2018) and (Han et al., 2015) reveal that the application of computer vision to this problem is viable.

SYSTEM ARCHITECTURE AND DATASET

Our approach to this problem is based on computer vision since it is passive, low-cost and does not require special authorisations as radar-based systems do. Additionally, we intend to have a fully embedded system on a mobile platform based on small but powerful computational boards, further reducing the need for third-party systems or infrastructures. Conversely, the main difficulty lies in building a dataset. We test the viability of this system with image classification with Xception (Chollet, 2017) and object detection with YOLOv3 (Redmon & Farhadi, 2018). To build the dataset, we opted for a system architecture installed on the top of a vehicle, resembling the intended deployment of the system and three different sensors operating in different wavelengths: from long-wave infrared to visible. The cameras were mounted at a height and angle that provided a good trade-off between field-of-view and no image contamination with background other than the ground.

Our dataset contains 9,260 images from the visible sensor (sensor01), 5,672 images from the visible plus near-infrared sensor (sensor02) and 10,388 images from the long-wave infrared sensor (sensor03). From sensor01, 336 images contain FODs, 256 from sensor02, and 102 from sensor03. The relative median average area of the objects

is below 0.180%, and, based on MS COCO dataset standard (Lin et al., 2015), we can consider our targets as small. The dataset is publicly available at Harvard Dataverse. Finally, we trained the neural networks on different subsets from sensors 01 and 02 and evaluated them.

CONCLUSION

The classification model with the best performance achieved a 98.86% accuracy at 90.9 fps (Table 1). This was trained in an imbalanced subset with a class proportion of 5:1 from 'no_fod' to 'fod'. However, its training curve, especially the validation loss in conjunction with the training accuracy, shows signs of overfitting. Secondly, we trained the detection network with a single label – 'fod'. The subset containing every image from both sensors achieved the best performance with an AP of 91.08% at 11.5 fps (Table 2). Despite the good results, we suspected that the detector was overfitting because of the insufficient number of images and excellent results in the testing set.

Table 1 – Summary of the results obtained during training for each classification model.

subset	# epochs	test set		learning rate	fps
		accuracy	loss		
1	23	0.9603	0.1310	1.00E-05	
2	34	0.9521	0.2522	1.00E-04	90.9
1+2	13	**0.9614**	**0.1291**	1.00E-05	
(1+2)*	32	0.9500	0.2259	1.00E-05	
1	11	0.9839	0.0642	1.00E-04	
2	15	0.9728	0.1366	1.00E-04	90.9
1+2	24	**0.9886**	**0.0338**	1.00E-04	

Table 2 – Summary of the results obtained on the test set.

subset	# epochs	initial learning rate	AP	fps
1	150	0.001	83.79	
2	153	0.001	83.91	
1+2	**166**	**0.001**	**91.08**	11.5
(1+2)*	170	0.001	76.34	

This led to a fourth image acquisition with sensors 01 and 02 that intended to test the neural networks on new objects. As expected, the accuracy and AP of the classifier and the detector dropped while retaining the fps. The classifier went from a 98.86% accuracy to 77.92%, while the detector dropped from an AP of 91.08% to 37.49%.

Figure 1 – False positive classification of plants as FOD (in red) and the true positive classification (in green)

REFERENCES

Cao, X., Wang, P., Meng, C., Bai, X., Gong, G., Liu, M., & Qi, J. (2018). Region Based CNN for Foreign Object Debris Detection on Airfield Pavement. *Sensors*, *18*(3), 1-14. doi: https://doi.org/10.3390/s18030737

Chollet, F. (2017). Xception: Deep Learning with Depthwise Separable Convolutions. *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1800-1807. doi: https://doi.org/10.1109/CVPR.2017.195

Han, Z., Fang, Y., & Xu, H. (2015). Fusion of low-level feature for FOD classification. *2015 10th International Conference on Communications and Networking in China (ChinaCom)*, 465-469. doi: https://doi.org/10.1109/CHINACOM.2015.7497985

Lin, T., Maire, M., Belongie, S., Bourdev, L., Girshick, R., Hays, J., Perona, P., Ramanan, D., Zitnick, C. L., & Dollár, P. (2015). Microsoft COCO: Common Objects in Context. *ArXiv:1405.0312 [Cs]*. Retrieved from http://arxiv.org/abs/1405.0312

McCreary, I. (2010). *FOD, Birds, and the Case for Automated Scanning* (1st ed.). Insight SRI Ltd.

Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. *ArXiv:1804.02767 [Cs]*. Retrieved from http://arxiv.org/abs/1804.02767

The Challenges of using Non-certified Military Unmanned Air Systems for the conduction of real Operations

D. Duarte (1), T. Cabral (2), J. Caetano (3) and R. Marques (4)

(1) Portuguese Aeronautical Authority, dxduarte@emfa.pt
(1) Portuguese Aeronautical Authority, tmcabral@emfa.pt
(3) Portuguese Air Force Academy Research Center, jvcaetano@academiafa.edu.pt
(4) Portuguese Air Force, IGFA, rhmarques@emfa.pt

The use of new technologies is of the utmost importance in military conflicts, as they strongly contribute to set the pace of war, though the increase of weapons´ accuracy, survivability of protection systems and performance and reliability of surveillance and communication systems. Since the beginning of the second world war, the military aircraft industry has been considered essential to achieve military advantage, and this drove a great investment in the development of aircraft technology during the second half of the 20th century, leading to the development of different aircraft with innovative designs and ground-breaking technologies that, for the purpose of shortly attaining that military advantage, were sometimes produced without adequate proofing and testing and ended up by being abandoned due to low reliability or inability to perform the intended missions (Duarte, 2019). In fact during, those years the number of accidents with military aircraft was substantial, and this was due not only to the risk of the missions performed, but also to the low Technology Readiness Level (TRL) in which the air systems were put to operate in those real war theatres and to the scarce training of the pilots operating them, in order to have them operationally flying as soon as possible to achieve and maintain the so seeked airpower advantage.

Nowadays, in modern societies, the evolution of war-culture has led to a significant reduction in the societies´ tolerance for loosing human lives in the battle fields, and today it is unthinkable to have aircraft operating real missions without the necessary proofing to ensure that they are safe to be flown by the pilots without the risk of having unintentional failures that could result in the loss of the aircraft and pilot´s life. For that purpose, nowadays all military aircraft undergo extensive testing, validation and certification campaigns before their use in the battle fields, and it is only when these new technologies reach a TRL of nine, that they are used in real military operations (GAO, 2020). Also, considering the investment put on the development of these cutting-edge aircraft, it is unthinkable, and economically unbearable, to accept the risk of having unsufficiently trained pilots operating them, for which nowadays nations substantially invest on the training of the pilots to enable them to fly those military assets with the lowest possible risk of loosing aircraft that cost millions to be developed and produced due to insufficient or inadequate training.

However, the use of unmanned aircraft in certain military operations has increased in the recent years and this strategy has steared the approach of nations strongly and almost blindly investing in the proofing of technologies and on the training of the pilots operating the air assets that perform those missions, as it eliminates the "*society´s intolerance to the loss of the pilot´s life*" from the equation and reduces it to the balance between the mission value and the risk of the material loss of the asset performing it.

Today, the use of small UAV to perform certain missions is growing worldwide, and their applications often surpass strictly military contexts, and if a manned aircraft is designed for service lives that often exceed 30 years (Duarte, 2016), these small systems tend to become obsolete in 5 to 10 years, which highlights the importance of reaching an adequate balance between the investment put in their development to increase the systems reliability, and the value of the mission that the system is designed to perform.

In fact, the consciousness that the conduction of formal certification process is economically and timely unbearable to be applied to small systems, designed to operate and perform missions of reduced scope, has driven nations to use these systems without undergoing a formal certification process, which although being extremely appealing from the cost and development times perspective bears an inherently nigher risk of losing the asset and of not completing the intended mission.

Nevertheless, in some cases, this may be the only possibility as an urgent need of performing a specific mission in a particular context , may require that this risk is accepted and, for those situations, one must be aware that the use of technologies at lower TRL combined with reduced training of the men operating and servicing the systems, will inherently bring challenges that must to be dealt with concurrently with the operation of the systems, requiring from the operator, the system manufacturer, and the Regulating Authority, a constant and active cooperation in investigating accidents and occurrences with those systems, to constantly solve the identified problems without

extensively compromising the mission. This paper uses real case studies of Portuguese UAV crash investigations to highlight the importance of this active cooperation between the operator, the system´s manufacturer and the regulating Authority to increase the systems reliability and to tune operational procedures, bringing the UAVs to higher levels of TRL, while they are used in real operational scenarios.

KEYWORDS

Risk-based certification; UAV TRL; Portuguese UAV crash investigations; Operator; Aircraft Manufacturer; Regulating Authority.

REFERENCES

Cabral, T. et al. (2018). *Unmanned Aircraft Systems Risk Assessment: Review of Existing Tools and New Results, STO-MP-IST-166.*

Caetano, J., Duarte, D., & Cabral, T. (2018), Unmanned aircraft Systems Risk Assessment – a new approach. *Military Sciences and future Security Challenges.*

Duarte, D. et al. (2016). An overview on how failure analysis contributes to flight safety in the Portuguese Air Force. *Engineering Failure Analysis*, *65*, 86-101.

Duarte, D. et al. (2019). Recent Studies and Developments made by the Portuguese Airforce for the enhancement and sustainability of its Military Air Power. In *International Society of Military Sciences*, Vienna.

GAO, US Government Accountability Office (2020, January). *Technology Readiness Assessment Guide, Level, GAO-20-48G.*

Formation Flight Control for Search Missions in a Maritime Environment using UAVs

L. Santos (1), T. Oliveira (2) and G. Cruz (3)

(1) Academia da Força Aérea, Portugal, lvsantos@academiafa.edu.pt
(2) Academia da Força Aérea, Portugal, tmoliveira@academiafa.edu.pt
(3) Academia da Força Aérea, Portugal, gccruz@academiafa.edu.pt

This work is part of the Portuguese Air Force Academy Research Centre (CIAFA) and aims to develop a control system for formation flight of Unmanned Aerial Vehicles (UAVs), with a leader-follower methodology, to be used in missions within the scope of maritime search.

Initially, the main references of UAV motion control and maritime search are studied. In particular, the planning of search and rescue missions is addressed. This planning stage is typically carried out by the local Rescue Coordination Centre (RCC), which, based on parameters that increase the probability of the mission's success, defines the search pattern and the means to be used. In this work, the commonly used search patterns are presented, and the most appropriate pattern for the search for castaways, considering that the mission should be carried out by a formation of 3 unmanned aircraft, is presented (see IAMSAR Manual, 2016).

Then, an adequate geometry of the flight formation (i.e., the relative positions between the UAVs) while performing the previously selected search pattern is proposed, considering that each of the 3 unmanned aircraft has a different camera on board (providing a greater range of collected data). The proposed geometry of the flight formation also takes into account the coverage area (footprint) of the cameras to be used and a pre-specified safety distance between each UAV in the formation.

The overall formation flight control system considers a hierarchical implementation of controllers. Namely, this hierarchy is composed of three modes: i) collision avoidance, ii) target tracking and iii) search mode. The collision avoidance mode defines the behavior of the aircraft's formation when safety distance limits between each UAV are breached. The target tracking mode is responsible for controlling the flight's formation when an object of interest is found during the search. Finally, the search mode, the main focus of this work, establishes the formation control during most of the flight. This control mode is supported by two types of motion control laws (Aguiar and Hespanha, 2007): path following and trajectory tracking. The first type is applied to the motion control of the lead aircraft and the second to the remaining (follower) UAVs. The implemented control laws were first deployed in a numerical simulation environment, using Simulink, a MATLAB software tool. From the analysis of the simulation results, it is possible to verify that both the lead and the follower UAVs present an adequate tracking of their flight references.

Finally, Software In The Loop (SITL) simulations are performed using the Simulink tool and an opensource toolchain to account for realistic physical behavior of aircraft dynamics, during all phases of flight. The SITL simulation architecture is based on the Robot Operating System tool (ROS – Quigley et. al. 2009). The obtained results allow for validation of the designed control system. Therefore, one can conclude that a preliminary version of a formation flight solution for application of UAVs in maritime search mission scenarios was successfully developed in this research work.

KEYWORDS

Flight formation; Unmanned Aerial Vehicle; Maritime search; Path following; Trajectory tracking.

BIBLIOGRAPHY

Aguiar, A. P., & Hespanha, J. P. (2007). Trajectory-tracking and path-following of underactuated autonomous vehicles with parametric modeling uncertainty. *IEEE transactions on automatic control, 52*(8), 1362-1379.

Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., ... , & Ng, A. Y. (2009, May). *ROS: an opensource Robot Operating System*. In ICRA workshop on open source software, *3*(3.2), 5.

Higham, D. J., & Higham, N. J. (2016). MATLAB guide. Society for Industrial and Applied Mathematics. In: IAMSAR Manual, *International aeronautical and maritime search and rescue manual*. London: International Maritime Organization, IMO Publishing.

Automatic 3D building reconstruction

A. Jin (1), J. Silva (2) and A. Bernardino (3)

(1) Portuguese Military Academy & Instituto Superior Técnico, jin.ay@exercito.pt
(2) Portuguese Military Academy & LIBPhys-UC, jose.silva@academiamilitar.pt
(3) Instituto Superior Técnico & Institute for Systems and Robotics, Portugal, alex@isr.tecnico.ulisboa.pt

Nowadays, it is common to use automatic or semi-automatic systems, such as computer programs, robotic arms, or autonomous vehicles, to assist man in the most diverse tasks, including military operations. The work presented is based on 3D reconstruction using Unmanned Aerial Vehicles (UAVs) multi-view photos, built on an incremental Structure from Motion (SfM) pipeline with a Convolutional Neural Network (CNN) architecture for feature extraction.

Unlike traditional methods of soft-copy photogrammetric, there is no need for a priori knowledge of the camera parameters and the site location since an SfM algorithm is based on an input set of 2D images with a high level of overlapping that aims to extract and match features, followed by the computing of the camera motion and pose estimation. A typical incremental SfM comprises two primary modules, the Correspondence Search responsible for the treatment of features, and Incremental Reconstruction, which aims to create the dense reconstruction based on the previous stage's output (Figure 1).

Figure 1 - Incremental SfM with a CNN implementation for feature extraction proposal workflow

The proposed methodology of our work, shown in Figure 1, is divided into three sections. In the first stage, the input images' features' detection and extraction are done with the auxiliary VGG-16 CNN architecture. The second stage consists of the matching process, which aims to find common features extracted on different images by searching for the nearest neighbors of each CNN descriptor in the upper max-pooling layer since it has a larger respective field giving more semantic information. The third step builds the dense point cloud based on the features found to be similar and adds the respective images to the reconstruction set in order to create de 3D model. The input set is a collection of images taken by a drone in a region outside the urban zone of Vila Real, Portugal, with about 10,000 m2 . A 3D view reconstruction using Agisoft PhotoScan and Pix4Dmapper is presented in Figure 2. With the aid of these two commercial softwares as a preliminary test, it is possible to have a preview of what is the desirable goal and to compare it with the output of the SfM pipeline proposed. From what is perceived from the reconstructions, most of the scene is surrounded by vegetation as the most noticeable objects are a roadway in the middle of the sample and three houses corresponding to the highest objects found. The most significant difference between the two models is in the structure of the center-left house. While the Pix4Dmapper left most of the front side of the house with empty black spots, the Agisoft Phototoscan efficiently reproduced its components, meaning that better feature extraction and reconstruction were made.

Figure 2 - 3D Aerial view of the study area from (1) Agisoft PhotoScan and (2) Pix4Dmapper

As is possible to observe from the preliminary test, 3D modeling reconstruction from aerial images can bring numerous advantages if implemented in the military field. As urban terrains operations come with the problems of situation awareness, the possibility of sending a UAV to do the work of surveillance and reconnaissance while having the ability to create a 3D model of the area of interest gives military commanders a multi-view perspective that allows them to the operation be built based on more robust pillars, improving the efficiency of management of human resources and the available means leading to the higher success of a mission.

KEYWORDS

Structure from Motion; Convolutional Neural Networks; Unmanned Aerial Vehicle; 3D Reconstruction.

ACKNOWLEDGEMENTS

REFERENCES

Bulatov, D., Häufel, G., Meidow, J., Pohl, M., Solbrig, P., & Wernerus, P. (2014). Context-based automatic reconstruction and texturing of 3D urban terrain for quick-response tasks. *ISPRS Journal of Photogrammetry and Remote Sensing*, *93*, 157–170. doi: https://doi.org/10.1016/j.isprsjprs.2014.02.016

Gross, H., Thoennessen, U., & Hansen, W. v. (2005). 3D-modeling of urban structures. *International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, *36*, 137–142. doi: https://doi.org/10.1016/j.isprsjprs.2014.02.016

Schonberger, J. L., & Frahm, J. M. (2016). Structure-from-Motion Revisited. *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 4104-4113. doi: https://doi.org/10.1109/cvpr.2016.445

Simone, K., & Zisserman, A. (2014). Very deep convolutional network for large-scale image recognition. *arXiv*. doi: https://doi.org/10.48550/arXiv.1409.1556

Westoby, M., Brasington, J., Glasser, N., Hambrey, M., & Reynolds, J. (2012). 'Structure-from-Motion' photogrammetry: A low-cost, effective tool for geoscience applications. *Geomorphology*, *179*, 300-314. doi: https://doi.org/10.1016/j.geomorph.2012.08.021

Widya, A. R., Torii, A., & Okutomi, M. (2018). Structure from motion using dense CNN features with keypoint relocalization. *IPSJ Transactions on Computer Vision and Applications*, *10*(1). doi: https://doi.org/10.1186/s41074-018-0042-y

Yu, D., Ji, S., Liu, J., & Wei, S. (2021). Automatic 3D building reconstruction from multi-view aerial images with deep learning. *ISPRS Journal of Photogrammetry and Remote Sensing*, *171*, 155–170. doi: https://doi.org/10.1016/j.isprsjprs.2020.11.011

WG4 – Leadership, Command and Control and Basic Competencies

Through The Lens of Cultural Schizophrenia in NATO Military Doctrines

A. Zotkeviciute (1)

(1) General Jonas Zemaitis Military Academy of Lithuania, agniete.zotkeviciute@lka.lt

Despite the perceived significance of the cultural element in warfare, there is still very limited academic research on the institutionalisation of the cultural element in military doctrines. The importance of the cultural element reflects the general increase in the significance of the soft power in the current definition of state and military power. This research intends to answer the question of how the cultural element – particularly cultural competences of military personnel – finds its way into the NATO military doctrines. Therefore, the object of the study is the cultural element in the NATO military doctrines. In this research, the application of document analysis method is used. This method is aimed at disclosing how cultural competences of military personnel are defined and in what primary documents of NATO military doctrines, without undertaking to assess the effectiveness of teaching cultural competences under research. The method of document analysis aims to systematically examine military doctrines (documents) and reveal how cultural competencies vary in different doctrines. Information analysis methods are: analysis of primary data; qualitative content analysis; and interpretative method. Qualitative analysis of NATO military doctrines is based on the following criteria: 1. To determine when cultural competencies were introduced into military doctrines after the Cold War. 2. To determine the types of military doctrines that emphasize the importance of the cultural element. 3. To reveal how cultural element are described in doctrinal documents. In the research, documents addressing the NATO involvement in the international operations after the Cold War from August 1990 to December 2021 are analysed. A total of 45 doctrines were selected which highlighting the importance of the cultural element. Documents used in NATO's case study are available on the official NATO website (www.nato.int).

Based on an analysis of NATO's military doctrines between August 1990 and December 2021, military doctrines which include the cultural element can be divided into four main groups: 1. Doctrines for functional professionals; 2. Doctrines for asymmetrical warfare; 3. Doctrines for the cultural environment; and 4. General military doctrines. Despite the increasing importance of the cultural element in warfare, NATO's military doctrines can be distinguished by cultural schizophrenia. First, given that cultural competencies are included but limited in standardization in NATO doctrinal documents, it can be debated that despite NATO's declarative rhetoric of the importance of the cultural element in warfare, it does not have a significant impact on the regulation of cultural competencies in the military doctrines of nation states. The absence of NATO-level standardization affects countries working in a coalition that have differing interpretations of the cultural competencies of soldiers and its need in international operations. The influence of the structural level (NATO) exerts on unit level (NATO states) and it is the fundamental reason why cultural competencies cannot remain only a declarative matter in NATO military doctrines. Second, the visible profusion of terminology describing the cultural element in NATO military doctrines promotes irresponsible and speculative use of it. Most of the terms used to describe cultural competencies in NATO doctrines causes confusion in trying to understand how cultural competencies should be perceived at NATO level. Lastly, even the importance of the cultural element in warfare is unquestionable, therefore, its exclusively declarative usage in NATO military doctrines forms a practice of considering a cultural element an important but, in a sense, unrealizable element in warfare. Such an example can be passed to NATO member countries, thus exacerbating flawed practices.

Intercultural Competence in the Lithuanian Armed Forces: A Pilot Study

D. Prakapienė (1)

(1) General Jonas Žemaitis Military Academy of Lithuania, dalia.prakapiene@lka.lt

Military intercultural competence is general knowledge, skills, abilities, and attributes of culture developed through education, training, and experience that provide the ability to operate effectively within a culturally complex environment (Mackenzie, Miller, 2019, p. 6). Therefore, to perform their duties effectively and efficiently soldiers often have to operate in a cultural environment that is unusual for them. The following components of intercultural competence are essential for the efficient and effective performance of duty: cultural understanding, flexibility, the ability to build sustainable intercultural relationships, tolerance of uncertainty, empathy, and openness (Portera, 2014; Miller and Tucker, 2015; Rodman, 2015; L. J. Rasmussen et al., 2016; Ibrahimov, 2017, Koziar et al., 2020; Abbe, 2021). This is achieved through the development of knowledge, skills, attitudes, and cultural awareness. All this opens the way to intercultural dialogue, and constructive communication and cooperation between people of different cultures.

Intercultural competence is not a given, but needs to be developed and refined throughout life at different levels: national, institutional, and personal. When developing and improving intercultural competence at a national level, it is important that strategic documents emphasise the importance of intercultural education, create conditions, and allocate funding for its implementation. At an institutional level, it is important for the institution to be involved in the internationalisation process, i.e., the development of internationalisation within the institution. At a personal level, intrinsic motivation, the desire to develop intercultural competence, and to actively participate in intercultural activities and exchanges are essential to the acculturation process. Therefore, the aim of this report is to identify the trends in manifestation and development of intercultural competence in the Lithuanian Armed Forces. For this purpose, two qualitative research methods were chosen: document analysis and in-depth interviews.

To assess the concept and importance of intercultural competence in official documents that regulate the activities of the Lithuanian Armed Forces, 6 documents were selected and analysed using keywords. The interviews were conducted with 8 officers. A purposive sampling of informants was used, where only officers serving in the Lithuanian Armed Forces with experience of working in an international environment were interviewed.

The study revealed that Lithuanian military documents define intercultural competence as the ability to operate in a multinational, multicultural, interinstitutional, interorganisational and transnational environment. However, it was noticed that the documents contain generalised phrases, but do not provide for specific activities or developments in this regard.

The results of the interviews with the officers show that intercultural competence is expressed in terms of language skills, knowledge of other cultures, the ability to communicate and integrate with other cultures, and the ability to quickly apply intercultural knowledge to real-life situations. However, the informants also pointed out that this alone is not enough. They indicated that experience and knowledge of general patterns of behaviour and thinking in certain critical situations is also very important. According to the informants, the Lithuanian Armed Forces lack systematic development in this area and advance preparation for future activities in intercultural environments. In their opinion, this should not be left to the personal responsibility of the officer/soldier but should be organised at institutional level. This can be achieved by combining the theoretical and practical levels, by providing guidelines for the development of intercultural competence in the strategic operational documents of the armed forces, through the organisation of courses or specialised training, the sharing of experiences, or the analysis of case studies of lessons learnt.

Based on the results of the study, the success of the development of intercultural competence in the Lithuanian Armed Forces must be based primarily on the ability of personnel to learn and develop cultural competence independently. In particular, this requires that both the organisation and its members realise that most cultural learning takes place not in the context of formal training, but through experiential activities and concrete situations, and that the development of intercultural competence must therefore focus on the development of a set of practical strategies and the possibility of making use of them in the course of learning.

KEYWORDS

Intercultural competence; Development of intercultural competence; Lithuanian Armed Forces.

REFERENCES

Abbe, A. (2021). Evaluating Military Cross-Cultural Training Programs. *Expeditions with MCUP*, 1-59.

Ibrahimov, M. (2017). The army's approach to culture and language applications. In *Cultural Perspectives, Geopolitics & Energy Security of Eurasia: Is the Next Global Conflict Imminent?* Kansas: The Army Press: Fort Leavenworth, 1, 183–200.

Kozyar, M. M., Nanivska, L. L., Romanyshyna, O. Y., Romanyshyn, A. M., & Yakimets, Y. M. (2020). Communicative Competence Formation of Future Officers in the Process of Foreign Language Training. *International Journal of Higher Education*, *9*(7), 153-165.

Mackenzie, L., & Miller, J.W. (2019). Intercultural Training in the United States Military. *The International Encyclopedia of Intercultural Communication, 1-10.* doi: 10.1002/9781118783665.ieicc0189

Miller, J., & Tucker, J. (2015). Addressing and assessing critical thinking in intercultural contexts: Investigating the distance learning outcomes of military leaders. *International Journal of Intercultural Relations*, 48, 120–136.

Portera, A. (2014). Intercultural competence in education, counselling and psychotherapy. *Intercultural Education*, *25(2)*, 157–174.

Rasmussen, L. J., Sieck, W. R., & Duran, J. L. (2016). *A model of culture-general competence for education and training: Validation across services and key specialties.* Yellow Springs, OH: Global Cognition. Final Report. H9821D-13-C-0025, 85 p.

Rodman, J. (2015). *Cross-cultural competence: Review of assessment methodology and available assessment tools.* Fort Leavenworth, KS: Mission Command – Capabilities Development and Integration Directorate (CDID). Retrieved from http://cgsc.contentd

Organising the innovation structure in military organisations

A. Nogueira (1) and P. Água (2)

(1) CINAV/Escola Naval, Portugal, pedroso.nogueira@marinha.pt
(2) CINAV/Escola Naval, Portugal, pedroagua@escolanaval.pt

Innovation is one of the most likely factors to boost the effectiveness, efficiency, and sustainability of an organisation, including military organisations (Hill, 2015). An innovative organization should design and implement a strategy aimed at obtaining results that allow it to scale in the value chain (Água & Correia, 2020). The objective of this study was the analysis of the state of the art and trends, with regard to organizational innovation. Extensive bibliographical research was used; case studies of organizations that have made innovation part of their DNA were studied; and different methods and tools were studied that aim to facilitate or pave the way for innovation in organizations with different characteristics. The results contribute to an updated overview of current trends with regard to three distinct concepts: the culture of innovation, the innovation process and the management of change motivated by innovation (Nogueira, Água & Correia, 2021).

Innovation thus emerges as a factor to be taken into account for the success of organisations nowadays, where the change of circumstances and reality is permanent. Therefore, the need arises for organisations to continuously adapt and, consequently, to be shaped to each conjuncture. As such, the structure of organisations has to be properly organised so as to support a more or less innovative strategy, but which allows the development of the trends matching reality on a daily basis (Skarzynski & Gibson, 2010). This question is even more prevalent in military organizations, where the conflict between a culture that does not easily accommodate attitudes and values more in line with the typical cultures of innovation, and a world in continuous change and uncertainty in terms of future scenarios. This study suggests some solutions to balance this conflict. These solutions will be based mainly on a more innovative culture, a properly implemented innovation process and a properly monitored change management process (Vilà, 2012) (Figure 1).

Figure 1 - Organising for innovation

A culture of innovation assumes that the members of the organisation often present innovative solutions to existing problems, through exploration, experimentation, and entrepreneurship, with an emphasis on learning, optimisation, knowledge sharing, risk taking and tolerance to failures that may occur in the innovation process (Whittinghill, Berkowitz, & Farrington, 2015). To achieve a culture of innovation the existence of a leadership willing to innovate is critical, and that happens with a strategy based on training, mainly concerning the next generation of leaders in an organization (Miller, & Brankovic, 2010). The innovation process consists of the set of actions aimed at promoting innovation within an organisation, under the leadership of the top leaders (Deschamps, 2008). The implementation of the innovation process is carried out in phases: (1) the collection of a portfolio of ideas; (2) the selection of suitable ideas according to criteria of added value for the organisation, risk involved in the development, and the success of prototyping and proof of concept; and (3) its implementation, safeguarding the barriers, internal or external to the organisation. The transformation of culture through change management has to occur for innovation to become a systemic capability within an organisation (Kotter, 2012).

KEYWORDS

Armed forces; Change; Culture of innovation; Organising for innovation; Process.

REFERENCES

Água, P. B., & Correia, A. (2020). Innovation governance in practice: A business policy approach. *Corporate Board: Role, Duties and Composition, 16*(2), 54-64.

Deschamps, J. P. (2008). *Innovation Leaders: How Senior Executives Stimulate, Steer and Sustain Innovation*. São Francisco, Estado Unidos da América: Jossey-Bass.

Hill, A. (2015). Military Innovation and Military Culture. *Parameters, 45*(1), 85-98.

Kotter, J. P. (2012). *Leading Change*. Boston: Harvard Business Review Press.

Miller, P., & Brankovic, A. (2010). *Building a "Creative Culture" for Sustainable Innovation*. Barcelona, Spain: IESE Business School.

Nogueira, A., Água, P. B., & Correia, A. (2021). Organização para a inovação: revisão sistemática de literatura. *Proelium, VIII*(8), 361-384.

Skarzynski, P., & Gibson, R. (2010). *Inovar no essencial. Transforme o modo como a sua empresa inova*. (C. Pedro, Trad.) Lisboa: Actual Editora.

Vilà, J. (2012). Normalize innovation to transform your firm. A customised road map. IESE insight. *Third quarter 2012, 14*, 36-43.

Whittinghill, C., Berkowitz, D., & Farrington, P. A. (2015). Does your Culture Encourage Innovation? *Defense Acquisition Review Journal, 22*(2), 26-239.

The spectre of leadership: from the individual to the collective

A. Rosinha (1) and H. Júnior (2)

(1) IUM/CIDIUM, Portugal, rosinha.ajpe@ium.pt
(2) IUM/CIDIUM, Portugal and University of Vigo, Spain, handradejunior@gmail.com

This paper addresses the spectrum of leadership as a complex and multifactorial phenomenon, one that is dynamic and interactive, involving multiple actors.

Volatility, uncertainty, complexity, and ambiguity (VUCA) foster a hazardous climate that places new demands on leadership and challenges leaders' ability to adapt. A prompt, timely and appropriate response that guarantees collective security requires fine cooperation between different stakeholders. The military must be prepared to transition rapidly from brutal combat situations to situations of close interaction with local populations (negotiations or psychological operations) and to maintain a high level of emotional self-control.

Traditional leadership models are too restrictive and too focused on the leader-subordinate dyad, therefore justifying a multilevel approach to leadership. Both research on leadership and a theoretical framework for leadership are still in early stages. Leadership should thus be understood as a complex and dynamic process where different organisational roles are performed by several individuals (Gronn, 2010) and where those roles can be switched among work teams (Day, Gronn, & Salas, 2004).

Leadership theories have been slow to incorporate into their conceptions the demands placed by irregular and counterinsurgency operations and the need for the Armed Forces to operate in a joint, combined, networked manner.

Research on leadership that focuses on the formal leader is reductionist in that it fails to address leadership development as an inherently multilevel, longitudinal social process. Leadership is a psychological group process that involves the principle of social identity and the reinforcement of 'doing it for us 'behaviours in order to build and actively rebuild the very meaning of 'us'. A strong collective identity is critical to the development of group-motivated and group-oriented leadership behaviours. Thus, individuals who identify more strongly with their organisation and team are more likely to view others as sources of leadership and to be seen as potential leaders, regardless of whether or not they are formal leaders. The development of the organisation's collective identity emerges as a process that will lead to more plural forms of leadership.

Thus, the evidence provided by neuroscience shows that coordinated activity (affective and cognitive) in the right frontal area of the brain is directly related to the inclusion of the 'we' in the process, which reinforces the social and collective genesis of leadership. The propensity for leadership occurs in individuals with a broad outlook of the whole as well as systemic thinking, who recognise and include others in the process of building the organisational vision, and who present high levels of emotional and cognitive coherence.

A study by Hannah, Jennings, and Nobel (2010) identified roles and meta-leadership factors that characterise the adaptive function of leaders. The authors combine the more traditional aspects of leader-focused leadership, such as the tactical and technical component, with other aspects more focused on the collective, which require flexibility and sharing awareness to build collaborative relationships, resolve conflicts, coordinate and manage processes of support to civilians, facilitate local governance, and develop a shared leadership system with both internal and external leaders.

Thus, we must understand that leading a military operation involves following pre-established tactical and technical procedures, according to the principle of subordination, as well as reacting in an adaptable and flexible manner, as any given individual may have to think and act alone in specific circumstances as well as act collectively. If, on the one hand, military leadership is embodied in the commander and in hierarchical organisational structures, on the other, its processes include the knowledge that these multiple stakeholders bring to the influence process, according to an interactive dynamic perspective.

Shared leadership prevents the collapse of traditional leadership because a single leader cannot be expected to deal with multiple factors that require diversified knowledge, something that can only be achieved through communication by the sharing of information and by the social interaction typical of formal and informal networks. This reflects the changes in the literature that now sees leadership as a relational property rather than an individual entity (Chrobot-Mason, Ruderman, & Nishii, 2014).

Ultimately, all leadership is about self-identity, self-leadership, and shared and collective leadership. Future commanders must manage themselves and become more aware of their thoughts, feelings, and actions in order to expand them to wider and more complex networks of contacts and relationships, fostering ongoing change at all levels of the organisation through collective leadership.

This paper outlines the assumptions of collective leadership and provides a framework for collective leadership in the organisational context, which can be defined as the selective use of expertise within a network, including the role of formal leaders. Finally, we suggest that the development of a leadership culture is a strategic imperative, and compare the concepts of leader development and leadership development. We also address the developmental and multilevel nature of leadership in the design of leadership development models.

KEYWORDS

Collective Leadership; Shared Leadership; Leadership Development.

REFERENCES

Chrobot-Mason, Ruderman, & Nishii (2014). Predicting leadership relationships: The importance of collective identity. *The Leadership Quarterly, 27* (2), 298-311.

Day, D., Gronn, P., & Salas, E. (2004). Leadership capacity in teams. *The Leadership Quarterly*,15, 857-880.

Gronn, P. (2010). Distributed Leadership. In: K. Leithwood, P. Hallinger, K. Seashore-Louis, G. Furman-Brown, P. Gronn, W. Goleman, D., Boyatzis, R., & McKee, A. (2002). *Primal leadership: Realizing the power of emotional intelligence*. Boston: Harvard Business School Press.

Hannah, S. T., Jennings, P. L., & Ben-Yoav Nobel, O. (2010). Tactical military leader requisite complexity: Toward a referent structure. *Military Psychology*, 22, 412-449.

Data-Informed Leadership: Using Measurement on Physiological and Psychological Stress Response during Mandatory Military Service

R. Smaliukiene (1), V.Giedraityte (2) and R. Vaicaitiene (3)

(1) General Jonas Zemaitis Military Academy of Lithuania, rasa.smaliukiene@lka.lt.
(2) General Jonas Zemaitis Military Academy of Lithuania, vidmante.giedraityte@lka.lt
(3) General Jonas Zemaitis Military Academy of Lithuania, ramute.vaicaitiene@lka.lt

Leadership in mandatory military service is challenging because, platoon and squad leaders must get to know their subordinates, train them, and achieve the desired results in a short period of time. Accurate and timely data on the physical and psychological condition of subordinates could help leaders make effective decisions without even knowing the subordinates well. With comprehensive and timely data on conscripts, platoon and squad leaders can make sound decisions and adopt their training toughness accordingly. In this context, the stress response data of the conscripts are critical, as physiological and psychological stress can significantly weaken performance (Weeks et al., 2010).

Recent advances in biomedical research make it possible to provide high-precision data to decision makers.

Knowing that the analysis of a 1 cm hair sample can indicate the level of hormones accumulated over one month (Groeneveld et al., 2013), which is a reliable biological marker of physiological stress levels, and knowing that standardized perceived stress tests provided accurate data on psychological stress response (Mazeikiene et al., 2021; Smaliukienė et al., 2022), we aimed to provide actual data for conscript leaders throughout the entire period of mandatory military service (9 months) and draw guidelines for stress management.

Research methodology
A longitudinal study was conducted in conscripts to monitor changes in the stress response data. Using hair samples, steroid hormones were analyzed throughout mandatory military service. A random sample of 185 conscripts was selected for the investigation in two Lithuanian military bases and their hair samples were analyzed to determine the variation in cortisol concentrations. To measure the psychological response to stress, the perceived stress scale (Cohen et al., 1983) was used. Furthermore, self-reported data on group cohesion as well as military service-related and nonrelated factors were assessed.

Results
Each conscript squad and platoon are different in terms of physiological and psychological stress response rate; therefore, actual data are of great relevance for leader decision making.

The aggregated data show that at the beginning of military service, the interpersonal cohesion of the conscripts has the greatest positive effect; therefore, the platoon and squad leaders must lead by example and promote interpersonal bonds among the conscripts during the first month of their service. Interpersonal cohesion greatly reduces the level of stress hormones and perceived stress. The middle of the service is critical in terms of physiological and psychological stress response, because the stress level tends to increase. The end of military service, when conscripts are heavily involved in final exercises and settlements, are associated with a higher stress response only in the groups with low group cohesion. Accordingly, leaders have to focus their attention and leadership on group cohesion building in conscripts' squads and platoons.

Conclusions
Data-informed leadership can decrease the level of physiological and psychological stress in conscript groups during mandatory military service. The data show that leadership by example is a good stress management technique at the beginning of mandatory military service, while leadership in supporting team spirit decreases the level of stress at the end of mandatory military service.

KEYWORDS

Data-informed leadership; Physiological stress level; Psychological stress level; Mandatory military service; Conscripts.

REFERENCES

Cohen, S., Kamarck, T., & Mermelstein, R. (1983). A global measure of perceived stress. *Journal of Health and Social Behavior*, *24*(4), 385–396. doi: https://doi.org/10.2307/2136404

Groeneveld, M. G., Vermeer, H. J., Linting, M., Noppe, G., van Rossum, E. F. C., & van IJzendoorn, M. H. (2013). Children's hair cortisol as a biomarker of stress at school entry. *Stress*, *16*(6), 711–715. doi: https://doi.org/10.3109/10253890.2013.817553

Mazeikiene, A., Bekesiene, S., Karčiauskaite, D., Mazgelytė E., Larsson, G., Petrėnas, T., Kaminskas, A., Songailienė, J., Vaičaitienė, R., Utkus, A., & Smaliukienė, R. (2021). he Association between Endogenous Hair Steroid Hormones and Military Environment-related Factors in a Group of Military Conscripts. *International Journal of Environmental Research and Public Health*, *18*(10).

Smaliukienė, R., Bekesiene, S., Mažeikienė, A., Larsson, G., Karčiauskaitė, D., Mazgelytė, E., & Vaičaitienė, R. (2022). Hair Cortisol, Perceived Stress, and the Effect of Group Dynamics: A Longitudinal Study of Young Men during Compulsory Military Training in Lithuania. *International Journal of Environmental Research and Public Health 2022, Vol. 19, Page 1663*, *19*(3), 1663. doi: https://doi.org/10.3390/IJERPH19031663

Weeks, S. R., McAuliffe, C. L., DuRussel, D., & Pasquina, P. F. (2010). Physiological and Psychological Fatigue in Extreme Conditions: The Military Example. *PM&R*, *2*(5), 438–441. doi: https://doi.org/10.1016/j.pmrj.2010.03.023

Food and Motivation in the Military – More than just receiving the right nutrients

S. De Rosa (1) and T. Tresch (2)

(1) Military Academy at the ETH Zurich, Switzerland, stefano.derosa@vtg.admin.ch
(2) Military Academy at the ETH Zurich, Switzerland, tibor.szvircsev@vtg.admin.ch

There is plenty of historical as well as anecdotal evidence of the importance which food has for the morale and motivation of the soldiers. For example, many World War I soldiers told very different and detailed stories about their relation to food, going further than just satisfy the hunger (Duffett, 2011; Stanley, 1944). Also today, the influence of food on the morale of military units is still recognized (Moody 2020). However, detailed scientific knowledge is missing. The question of why and how food is related to motivation in a military environment is insufficiently analyzed.

We know for instance that soldiers who feel unease or who report to experience distress in military life, eat less healthy food and show more often the habit of snacking sweet food (Jallinoja, 2011; Schei, 1995). This suggests that food may be seen as an essential part of emotional regulation of the soldiers, especially in an isolated and alien situation like the life in a barrack. However, first findings show other paths which link eating and morale in the armed forces.

This presentation is based on qualitative interviews and on results of a quantitative survey among conscripts in the Swiss Armed Forces. This setting is especially revealing for the analysis of morale and motivation, since conscripts show very different levels of motivation for service. Thus, the role which food plays in creating a positive and mission-oriented climate can be disentangled with more detail. The goal is to provide further scientific knowledge to understand the catchphrase "an army marches on its stomach".

First results show how the soldiers experience appreciation through the food they receive. Hard work should be rewarded with good food. This is the expectation during trainings. Another way motivation is increase by food is the camaraderie, which is created and fostered during the meals.

KEYWORDS

Military Food; Morale; Motivation; Conscription.

REFERENCES

Duffett, R. (2011). Beyond the Ration: Sharing and Scrounging on the Western Front. *Twentieth Century British History, 22*(4), 453-473.
Jallinoja, P, Tuorila, H, Ojajärvi, A., Bingham, C., Uutela, A.,& Absetz, P. (2011). Conscripts' attitudes towards health and eating. Changes during the military service and associations with eating. *Appetite, 57,* 718-721.
Moody, S. M. (2020). Feeding the US Military: The Development of Military Rations. In: H. L. Meiselman (Ed.), *Handbook of Eating and Drinking* (pp. 1055-1068). Cham: Springer.
Schei, E. (1995). Sweet comfort: Changes in food habits during military service. *European Journal of Public Health, 5*(2), 97-102.
Stanley, A.W. (1944). Food as a Factor in Public Moral and Military Strength. *Agriculture in the Transition From War to Peace*, *17*, 240-245.

Online addictive behaviors prevention in the Portuguese Armed Forces: the case study of the PoAF

D. Silva (1) and C. Fachada (2)

(1) Portuguese Air Force, dpfreixo@emfa.pt
(2) CIDIUM/IUM, Portugal, fachada.cpa@ium.pt

In today's western society, the Internet emerges as an omnipresent and inseparable dimension of everyday life, whose capabilities are beneficially and empoweringly applicable to almost all areas of life (Stepien, 2014).

The evolution of increasingly powerful and small platforms and, therefore, more portable (Musetti & Corsano, 2018), combined with the increasing ease of access to the Internet, at progressively more accessible costs, have increased the presence of this tool in daily life to the power of ubiquity. Additionally, the pandemic context experienced since the beginning of 2020 catalyzed the movement of people and digital resources closer, with an increase in time spent online and/or in front of screens playing games, during the confinement imposed for containment. of the COVID19 pandemic (Service for Intervention in Addictive Behaviors and Dependencies [Serviço de Intervenção nos Comportamentos Aditivos e Dependências, SICAD], n.d.).

In this context, and despite its undeniable advantages, the Internet presents a set of temptations and dangers to its users (Stepien, 2014), capable of contributing to the development of problematic usage patterns, with an adverse impact on routines, academic performance and/or work, family relationships and emotional state (Patrão & Sampaio, 2016).

These disruptive behavioral patterns, associated with the uncontrolled and harmful use of the Internet - and due to the similarities presented with the characteristic symptomatology of addictive diseases, related, or not, to the consumption of substances -, were called "Internet addiction" (Young, 2009).

An "addition to the Internet" that brings together a range of behaviors, characterized by already recognized patterns, such as excessive time spent with online activities, psychological disturbance, neglect of routines and duties motivated by exaggerated involvement in those activities, and/or disproportionate expenses associated with Internet use (Griffiths, Kuss, Billieux & Pontes, 2016; Sharma, Nagarajan, Bharadwaj, & Kattimani, 2021; Young, 1999, cit. by Griffiths, 2011; Young, 2009).

Recognizing the magnitude of the impact of this problem, at progressively earlier ages, the World Health Organization (2014, cit. by Jo et al., 2019) classified it as a public health problem, leading several authors to emphasize the importance of its prevention (King et al., 2018).

Since the military institution is not alien to this reality, there are already several studies carried out on the presence/evaluation and prevention of this problem in the military environment, as is the case of the United States of America (Miller, Martin, Yeung, Trujillo, & Timmer, 2014; Breslau, Aharoni, Pedersen & Miller, 2015; Schmidt et al., 2019). Particularly important studies in view of the particularities of this context, considering that the presence of addictive behaviors causes negative consequences in terms of discipline, operationality and military security, and can cause serious consequences both for the fulfillment of missions and for the image of the Armed Forces (Despacho [Order] No. 11921/2015, of October 23).

Alerted to this environment, the Portuguese Armed Forces (FFAA), with a view to preventing addictive behaviors and addictions in the military context, have this matter operationalized through the Program for the Prevention of Addictive Behaviors and Combating Dependencies in the Armed Forces (PPCACDFA; [Programa de Prevenção dos Comportamentos Aditivos e Combate às Dependências nas Forças Armadas]). Nevertheless, this program does not mention anything specific regarding the issue of addictive online behaviors (AOB [CAO; Comportamentos aditivos online), nor does it contemplate any mitigating actions or measures aimed at them.

The aforementioned considerations highlight the urgency of studying the expression of OAB in Portuguese FFAA, in general, and in the Portuguese Air Force (PoAF), in particular (branch of the FFAA to which the study will be spatially delimited). Thus, the following question of research were formulated Is it appropriate to extend the preventive methodology of addictive behaviors applied in the PoAF OAB?.

For this purpose, data was collected through literature review, semi-structured interviews to eight entities involved in the prevention of addictions in the military, and a questionnaire with measures pertaining to online behaviors and the assessment of internet addiction in a sample of 766 military personnel (12,97% of the universe).

The results lead to the conclusion that in PoAF there are occasional preventive actions of OAB. In addition, in the studied sample it was found a prevalence of 0.3% of severe addiction to the internet and 27% of light and moderate addiction, which leads to the conclusion that extension of the preventive methodology of addictive behaviors applied in the PoAF to OAB is not only adequate but also desirable, and ideally achieved as soon as possible, considering that although the severe addiction values found were residual, the fact is that some of them are at the level of mild and moderate severity, and it is important to avoid aggravation. Finally, it was also concluded that this expansion should be based on five structuring focuses, presented in a model. Namely, objectives, target population, stakeholders, measures/actions, thematic areas to be covered, and evaluation of effectiveness.

KEYWORDS

Online addictive behaviors; Armed Forces; Online addictive behaviors prevention

REFERENCES

Breslau, J., Aharoni, E., Pedersen, E., & Miller, L. (2015). *A Review of Research on Problematic Internet Use and Well-Being with Recommendations for the U.S. Air Force*. Santa Monica: RAND. Retrieved from https://www.rand.org/pubs/research_reports/RR849.html

Despacho n.º 11921/2015, de 23 de outubro (2015). *Programa para a Prevenção dos Comportamentos Aditivos e Combate às Dependências nas Forças Armadas (PPCACDFA)*. Diário da República, 2.ª Série, 208, 30680-30687. Lisboa: Gabinete da Secretária de Estado Adjunta e da Defesa Nacional.

Griffiths, M (2011). Gambling Addiction on the Internet. In K. Young, & C. Abreu (Eds.), *Internet Addiction. A Handbook and Guide to Evaluation and Treatment* (pp. 91-112). New Jersey: John Wiley & Sons.

Griffiths, M.D., Kuss, D.J., Billieux, J., & Pontes, H.M. (2016). The evolution of internet addiction: A global perspective. *Addictive Behaviors*, 53, 193-195. doi: 10.1016/j.addbeh.2015.11.001

Jo. Y, Bhang, S., Choi, J., Lee, H., Lee, S., & Kweon, Y (2019). Clinical characteristics of diagnosis for internet gaming disorder: comparison of DSM-5 IGD and ICD-11 GD diagnosis. *Journal of Clinical Medicine*, 8(7), 945-958. doi: 10.3390/jcm8070945

King, D., Delfabbro, P., Doh, Y., Wu, A., Kuss, D., Pallesen, S., … Sakuma, H. (2018). Policy and prevention approaches for disordered and hazardous gaming and internet use: An international perspective. *Prevention Science*, 19, 233-249. doi: 10.1007/s11121-017-0813-1

Miller, L., Martin, L., Yeung, D., Trujillo, M., & Timmer, M. (2014). *Information and communication technologies to promote social and psychological well-being in the Air Force: A 2012 survey of airmen*. Santa Monica: RAND. Retrieved from https://www.rand.org/pubs/research_reports/RR695.html

Patrão, I., & Sampaio, D. (2016). Introdução. In I. Patrão, & D. Sampaio (Coords.), *Dependências Online - O Poder das Tecnologia*s (pp. 97-116). Lisboa: PACTOR.

Schmidt, G., Valdez, M., Farrell, M., Bishop, F., Klam, W., & Doan, A. (2019). Behaviors Associated with Internet Use in Military Medical Students and Residents. *Military Medicine*, 184, 750-757. Retrieved from https://academic.oup.com/milmed/article/184/11-12/750/5425726

Serviço de Intervenção nos Comportamentos Aditivos e Dependências (SICAD) (s.d.). *Comportamentos Aditivos em tempos de COVID-19: Internet & Videojogos (Sumário Executivo)*. Retrieved from https://www.sicad.pt/BK/EstatisticaInvestigacao/EstudosConcluidos/Lists/SICAD_ESTUDOS/Attachments/210/Sum%C3%A1rio%20executivo_COVID19_Internet_e_videojogos.pdf

Sharma, B.N., Nagarajan, P., Bharadwaj, B., & Kattimani, S. (2021). Problematic use of the Internet and its correlates with psychological well-being among undergraduate dental students. *Indian Journal of Community Medicine*, 46(1), 167-169. doi: 10.4103/ijcm_188_20

Stepien, K. (2014). Internet addiction. The phenomenon of pathological internet use – Problems of interpretation in the definition and diagnosis. *Internal Security*, 6(2), 79-90. doi: 10.5604/20805268.1157164

Young, K. (2009). Internet Addiction: Diagnosis and Treatment Considerations. *Journal of Contemporary Psychotherapy*, 39, 241-246. doi: 10.1007/s10879-009-9120-x

Leadership in law enforcement work applied to dangerous contexts: an integrative review and scientific mapping using VOSviewer and Google Trends tools

L. Carvalho (1), A. Rodrigues (2) and M. Zappellini (3)

(1) Polícia Militar de Santa Catarina, Brazil, luciuscarvalho@gmail.com
(2) Universidade do Estado de Santa Catarina, Brazil, agrillorodrigues@gmail.com
(3) Universidade do Estado de Santa Catarina, Brazil, marcellozapelini@gmail.com

The purpose of the article is to identify the current scientific knowledge of the phenomenon of leadership applied to law enforcement work and in dangerous contexts.

The integrative review allowed a research of the quantity and quality of publications on the topic, in Scopus, Web of Science, Ebsco Host, ScienceDirect – Elsevier (The Leadership Quarterly journal), Core, SciELO and Pergamum databases, resulting in 69 files, according to the research strategy outlines. Of these, 15 publications fit correctly into the search strategy (query) Leadership AND ("law enforcement" OR police) AND (crisis OR incident OR "high risk" OR "dangerous context")), bringing a summary idea about the approaches and observations of the emphasis topic, showing the various concepts of leadership discussed, such as instrumental, transformational, charismatic, consultative, ethical, authentic, military, destructive or laissez-faire (Northouse, 2016).

The application of the VOSviewer software to the research corpus allowed the visualization of cluster with 6 prominent authors, out of a total of 129 analyzed, highlighting Evernham, Allen, Dongier, Hillmann, Khosh and Murgallis, in addition to linking the co-occurrence from leadership, as a central word, to the keywords law enforcement, police, management, crisis management, emergency management and decision making.

Scientific mapping is integrated using the Google Trends tool, which shows the interest of web searches on the topic of leadership in Brazil and in the world, in the science category, from 2004, initial data processing date provided by the tool, to the present day.

Considering the historical evolution and the trends presented, there are indications that the Brazilian scientific interest on the subject remains low. The little incidence of studies that examine leadership in police organizations and in crisis contexts denotes the necessary exploration of the theme, considering that the police profession is one of the most dangerous in the world and critical contexts are non-routine, confusing, and eventually chaotic, scenarios and adequate leadership ensures the search for solutions related to the preservation of life, the physical integrity of people and the safety of property.

KEYWORDS

Leadership; Law enforcement; Police; Crisis; Incident; Dangerous context.

REFERENCES

Google Trends (2022a). Explore *what the world is searching*. Retrieved from https://trends.google.com.br/trends/?geo=BR

Google Trends (2022b). *Understanding the data. How to interpret Trends results*. Google News Initiative.

Northouse, P. G. (2016). *Leadership: theory and practice* (17 Ed.) Thousand Oaks: Sage Publications.

Van Eck, N. J., & Waltman, L. (2021). *VOSviewer Manual. Manual for VOSviewer version 1.6.17*. Universiteit Leiden.

WG5 – Law and Ethics

The legal and ethical implications of autonomous drone warfare

T. Quadros (1)

(1) Royal Military College of Canada, teresaquadros@hotmail.com

Since the last century, states, and non-state actors, have moved away from traditional methods of warfare and towards the use of unmanned aerial vehicles (UAVs), commonly referred to as drones, in military combat operations. Since the dawn of the Industrial Revolution, the rate of technological innovation has advanced at an alarming rate, and has outpaced the political, legal, and ethical frameworks that govern interstate and intrastate armed conflicts, both in international and domestic situations. The onset of modern drone weapon systems has posed new challenges to the current legal interpretations and moral standards of war that are greater and more uncertain than those posed by any other technological advancement of warfare innovation. Within a decade, UAV usage in military operations have moved from counter-insurgency measures to full-scale conventional combat.

As technology continues to advance, a fully autonomous armed drone equipped with artificial intelligence (AI), will create new legal and ethical dilemmas under the law of armed conflict, as the weapon will no longer be under the control and decision-making restraints of any individual within a state's security apparatus. This raises questions of who will be held accountable for the consequences of the misuse, misconduct, or mishaps resulting from the decision of artificial intelligence, and also raises important ethical questions about the balance between promises of unparalleled operational advantages and the unpredictability and loss of accountability necessary to make the complex ethical choices in the dynamic, constantly evolving battlespace.

While current non-autonomous or semi-autonomous drone programmes abide within the provisions of conventional legal and ethical frameworks, analogous under the guidelines of International Humanitarian Law (IHL) that govern traditional manned aircraft systems, this paper considers the challenges that future fully autonomous drones will pose to the standards of armed conflict. Currently, there are no principles that directly regulate and govern the use of armed drones, nor does it consider the impact AI technology advancements will have on weapon platforms and weapon systems, and how this rapid modernization of warfare will heighten tensions already present in international security dilemmas.

However, through reconsideration and reanalysis of the laws of war (*jus ad bellum*) and the laws in war (*jus in bello*), the current interpretations of international legal and ethical frameworks can be adapted and adjusted to best reflect the technological changes of the modern security environment and oversee the just deployment of these new technologies on the battlefield, always complying with general humanitarian and environmental standards.

KEYWORDS

Drones; Law; Ethics; Armed conflict.

Self-defence in Outer Space: Legal aspects of space attacks

K. Metcalf (1) and A. Carlo (2)

(1) Tallinn University of Technology, Estonia, katrin.nyman-metcalf@taltech.ee
(2) Tallinn University of Technology, Estonia, ancarl@ttu.ee

The development of legal regimes for cyberspace and outer space have in common that in their respective early days, there were romantic notions about entering an entirely new era in which traditional law and jurisdiction would not play any role (Metcalf, 2018, p. 2). Instead, entirely new ways of cooperating would be found. However, reality did not match these aspirations. The regulation of these areas, where national borders have a different role than for "earth based" activities, instead came to focus on how to have rules while not preventing innovation and maintaining the positive aspects of the "borderless" nature. This common feature is one reason why cyberspace and outer space are discussed together. Another reason is that space technologies are essential for important cyber tasks. Regarding attacks and self-defence, this means that there are many instances when the distinction between a space attack and a cyberattack is not clear. It may not be possible or relevant to try to make the distinction. - disrupting a satellite may be an effective way to cause cyber mayhem (Carlo, 2021 p. 55-57). The distinction between civilian and military is equally difficult to uphold for reasons that differ between cyberspace and outer space but that amount to the same thing: dual-use and the impossibility to strictly categorise activities or objects. The same computer may be used to launch cyber war or to write poetry and the same space technology can show where enemy troops are or whether the farmer has grown the crops he got subsidies for.

The question of the extent of the right to self-defence in either outer space or cyberspace is not settled. The legal framework of self-defence has been stressed by modern weapons for some time already and has become increasingly urgent as space technologies, usually with a link to cyberspace, increase in relevance. The question of what amounts to peaceful uses of outer space has been discussed since the early space age. The term can be interpreted as only permitting civilian use or to mean that space use cannot be aggressive (which would anyway violate general international law, which applies in space). In practice, the response lies somewhere between these positions. Space has had important military uses since the beginning of the space age. Many space technologies used in civilian applications, like position-based services (GPS, etc.), are of military origin and it is the norm rather than the exception that things are dual-use (Klein, 2019: Marchiso, 2019). For cyberspace, the nature of activities and of the area itself is such that it is futile to make pre-determined definitions of permitted peaceful use. Instead, this depends on the circumstances.

Legislatively, outer space and cyberspace are quite different. Space activities were initially carried out by states. The key legal principles are set out in a number of international agreements (the main one is the 1967 Outer Space Treaty, with over 100 parties). States also have national space legislation, with systems to ensure control over private subjects engaged in space activities, adopted to a large extent in the past decade. Cyberspace instead developed mainly through private activities and various non-binding rules play an important role. Lately, it has been difficult to agree on binding international space law instruments while there have been attempts to codify cyberspace rules, so to some extent the distinction may lessen. When addressing questions on whether "space war" is allowed and under what conditions, there are existing rules to refer to, but in reality these rarely give clear answers. A common feature between cyberspace and outer space is that questions like attribution, nature of a specific activity, intent, or effective control by superiors will most likely increase in importance.

Against this background, our main question for discussion is the extent of the right to (national or collective) selfdefence against attacks on space objects, taking into consideration the link to cyberspace, as the domain where the effect of the attack is likely to be felt.

KEYWORDS

Outer space; cyberspace; international law; self-defence; dual-use.

REFERENCES

Carlo, A. (2021). Cyber threats to space communications: Space and Cyberspace policies. In: A. Froelich (Ed.) *Outer Space and Cyber Space* (pp. 55-66) Heidelberg: Springer.

Klein, J.J. (2019) *Understanding Space Strategy The Art of War in Space*. London/New York: Routledge.

Marchisio, S. (2019) *Lo Spazio Cyber e cosmico: risorse «dual use» per il sistema Italia in Europa.* Giappichelli Editori.

Metcalf, K. N. (2018) *A Legal View on Outer Space and Cyberspace: Similarities and Differences.* Tallinn: CDCOE.

War Crimes and International Law: A Critical Analysis of Gaps

D. Bajpai (1)

(1) Gujarat National Law University, India, dakshatabajpai@gmail.com

The report of Bucha massacre in March, 2022, during the course of Russia-Ukraine war has once again raised the question of efficacy of international law to prevent and address the challenge of war crimes. Bucha a suburban are of Ukraine's capital Kyiv was under the occupation of Russian invading forces. After a month long occupation, Russian forces left the city on 31 March, 2022. According to the reliable sources some 1000 people were shot dead at point blank range while their hand tied at the back. Many burnt and mutilated bodies along with mass graves were found after Russian left the town. Girls as young as 14 years of age have been raped. While international community has expressed shock and the International Criminal Court (ICC) has launched investigation into these crimes, bur Russia has denied committing any such crimes. Even Russia has accused Ukraine of displaying false and fabricated proofs in the form of photo and video to make a strong plea for more sanctions against Russia (Kinetz, 2022; Patel, 2022; Sarah, 2022). Even if the international agencies investigate and establish that war crimes have been committed by Russian forces, will it be possible to hold accountable and punish those responsible for such war crimes in Bucha? Perhaps it is not possible for many reasons. If judicial actions are taken by the International Court of Justice (ICJ), its decisions are implemented through the UN Security Council. But as a permanent member of UNSC, Russia will block any such move. On the other hand, if the ICC is handicapped by the fact that Russia is not a member of the ICC. Even if ICC on the proposal of UN takes action and issues arrest warrants against accused Russia authorities, who will implement those arrest warrants. Russia does not extradite its citizens to other countries for criminal trial. Finally the law on war crimes takes a back seat.

In this situation, this paper tries to address the two fundamental issues: First, what are the weaknesses of international law on war crimes? Second, what measures, if any, the global community can take to address the war crimes like the one committed in Bucha?

In the process the paper will critically analyze the nature and scope of international legal regime, related to war crimes and list its glaring gaps. The law on war crimes was evolved during late 19th century by the Hague Conventions of 1899 and 1907. In the aftermath heinous war crimes in the form of Holocaust, the war crimes tribunals were held by allied powers in Nuremburg and Tokyo for the war crimes committed by German and Japanese forces. The Four Geneva Conventions of 1949 and two Protocols of the Convention (1977) further codified the law on war crimes. The third attempt to codify and broaden the scope of war crimes law was made by the Rome Statute 1998, which led to establishment of ICC in 2002.

As per these legal provisions, 'War crimes are those violations of international humanitarian law (treaty or customary law) that incur individual criminal responsibility under international law' (UN, 2022). More recently, definitions of war crimes have been codified in Rome Statutes and the war crimes tribunals in Yugoslavia and Rwanda. In comparison to earlier definitions, modern definitions are more expansive and criminalize certain actions committed by civilians as well as by military personnel (Penrose, 2022). Broadly speaking war crimes falls into three categories: Crime against Peace (waging war without just cause); war crimes during war; and crimes against humanity. In all cases killing civilians and non-combatants or destroying civilian infrastructure are serious violation of law on war crimes.

While the law on war crimes is well elaborated but it suffers from certain limitations like widespread misuse of provision of amnesty (Naqvi:2003), lack of universal jurisdiction in war crimes; problems of enforcement of law and the anarchic nature of international order, politicization of war crimes acts and so on. The law on war crimes as it stands today fails to punish victor in the war or a powerful nation. This needs to be made balanced and effective by suitable legal and political measures to prevent another Bucha in future.

KEYWORDS

War crimes; Amnesty; Universal jurisdiction; Crimes against humanity.

REFERENCES

Kinetz, E. (2022, 4 April). War Crimes Watch: Hard Path to Justice in Bucha, Ukraine, Atrocities. *Frontline*. Retrieved from https://www.pbs.org/wgbh/frontline/article/bucha-ukraine-civilian-deaths-justice-tribunal-international-criminal-court/

Naqvi, Y. (2003, September). Amnesty for war crimes: Defining the limits of international recognition. *IRRC, 85*(851). Retrieved from https://www.corteidh.or.cr/tablas/r27221.pdf

Patel, M. (2022, 07 April). Explained: What happened in Ukraine's Bucha, and was it 'genocide'? *The Indian Express*. Retrieved from https://indianexpress.com/article/explained/explained-what-happened-in-bucha-ukraine-and-was-it-genocide-7854561/

Penrose, M. M. (2022, 22 May). *War Crimes, International Law. Britannica* (updated). Retrieved from https://www.britannica.com/topic/war-crime

Sarah, R. (2022, 16 May). *Ukraine: The children's camp that became an execution ground*. BBC. Retrieved from https://www.bbc.com/news/world-europe-61442387

UN (2022) *War Crimes. UN Office on Genocide Prevention and Responsibility to Protect*. Retrieved from https://www.un.org/en/genocideprevention/war-crimes.shtml#:~:text=War%20crimes%20are%20those%20violations,criminal%20responsibility%20under%20international%20law

0439

Medical confidentiality in military environment – Ethical and deontological implications in the Portuguese Armed Forces

A. Anão (1)

(1) Portuguese Navy, oliveira.anao@gmail.com

Professional confidentiality is a structuring element of medical deontology relating to ancestral principles of western medical practice originated from the Hippocratic tradition (Boléo-Tomé, 2000, pp. 136–138).

The practice of military-medicine has unique characteristics (Gross, 2006, pp. 1–2), that may, in specific situations, justify the appreciation and revaluation of the underlying principles of confidentiality, confronting values of personal-individual interest with supra-individual values related to personal and collective safety as well as operational effectiveness (Gibson & Coker, 2002, pp. 130–131).

From the specific characteristics of military medicine, we highlight the double ethical subordination that relates both with the deontological medical principles and the obligation to the military codes. As a matter of principle NATO AJP 4.10 Allied Joint Doctrine for Medical Support (NATO, 2019, pp. 1–14) states that "Medical support should always strive to achieve a standard of care equating to internationally accepted best medical practice", that "Medical support is to be provided in compliance with humanitarian, ethical and legal standards" but also in accordance "with the respective national regulations for both the military and the clinical profession" it also states that "Medical confidentiality is to be ensured" and that "sensitive clinical information is not to be communicated to any individual organization that does not have a medical need-to-know."

At the present there are not specific laws or regulations in Portugal that specify the subject of medical confidentiality in the military services. This lack of normative orientation as contributed to some subjectivity in the interpretation and management of medical cases that may pose conflicting ethical issues in the articulation of the right to medical secrecy and the superior interests of the armed forces. The present study aimed at proposing ethical contributes for the management of medical confidentiality in the Portuguese armed forces. For this purpose, according to a hypothetical-deductive strategy, a mixed study was carried out, with integration of quantitative data based on an ordinal scale survey, and qualitative information supported by document analysis and semi-structured interviews.

In the quantitative study 10 questions regarding the ethical perspective about medical confidentiality were posed to two groups: "Medical-group" – composed of military-doctors directing clinical services in the Portuguese Armed Forces Hospital and "Non-medical group" – composed of non-medical officers integrating the Portuguese Promotion Course to General Officers. Descriptive and inferential statistics was performed to both groups.

The qualitative study comprised a normative review about medical confidentiality in Portugal and the respective confrontation with military deontology, analyzing the points of articulation and potential conflict as well as the analysis of ethical elements recollect from the interviews given by specialists and decision makers both in military and civil medicine.

In conclusions, we found in the qualitative study significant differences in the ethical perspective between both groups in 3 questions of the survey. In the qualitative study we concluded for the lack of a clear normative framework that allows the resolution of ethical conflicts in the practice of military health care providers. In an ethical perspective, in accordance with the results, we propose that in exceptional cases, it is deontologically admissible to confront medical confidentiality with the defense of superior personal and collective interests. For this purpose, we recommend the creation of doctrine about these matters, as well as training on the subject within the Portuguese Armed Forces.

KEYWORDS

Medical confidentiality; Medical deontology; Military deontology; Military health.

REFERENCES

Boléo-Tomé, J. (2000, maio-junho). Juramentos Médicos e a Noção de Dignidade Humana. *Acta Médica Portuguesa, 13*(3), 129–142. Retrieved from https://actamedicaportuguesa.com/revista/index.php/amp/article/view/ 1769/1346

Gibson, T. M., & Coker W.J. (2002). Medical Confidentiality: The right of a commanding officer to know. *Journal of the Royal Army Medical Corps*, 148, 130–136. doi: http://dx.doi.org/10.1136/jramc-148-02-05

Gross, M. L. (2006). *Bioethics And Armed Conflit - Moral Dilemas of Medicine and War*. Cambridge: MIT Press.

NATO (2019). *AJP 4.1 Allied Joint Doctrine For Medical Support* (Ed. C Version 1) Brussels: NATO Standardization Office (NSO).

Ethical foundations of Rousseau's vision of the armed forces. Conclusions for contemporary thinking about military services

K. Majka (1)

(1) University of Warsaw, Poland, majka_konrad@o2.pl

Jan Jakub Rousseau (1712-1778) went down in history as one of the most influential philosophers of the West. It is enough to mention the influence that the thinker from Geneva had on, for example, Immanuel Kant or Maximilien Robespierre. It is also worth noting that it is in Rousseau's writings that many researchers look for the ideological sources of the concept of an army that began to materialize during the French Revolution.

In my speech I will focus on this aspect of his vision of the armed forces, the meaning of which goes beyond the context of the times in which he wrote. I mean ethical issues - the moral justification of military service.

The paper will consist of two main parts.

The first will be devoted to what provides the reasoning for the concept of armed forces he pushes for: the axioms and principles of moral thinking and certain notions of his philosophy of politics. At the beginning, I will focus on the general will (*volonté générale*), in which resonates his view on the relationship between the individual and the community, which is situated at the source of his thinking about morality. The next part of the speech will be devoted to his philosophical anthropology, especially his concept of the state of nature. This issue is important because in human nature - after its "social" foundation - Rousseau diagnoses the presence of egoism. The tendency to put self-interest over the interest of the community is destructive both from the perspective of the possibility of the existence of the state and the ability of citizens to sacrifice their lives for the sake of their homeland. Further part of speech will be focused on the methods proposed by Rousseau to counteract this tendency. In particular about the demand to create virtues among citizens of special value from the perspective of military service. As the philosopher teaches: also members of modern society should lead an existence in the spirit of ancient Sparta and their attitude should be characterized by passionate patriotism, combined with almost religious adoration of the motherland.

The second of the main parts of the speech will treat on the subject of those views of Rousseau which explicitly concern military issues. Three main points must be emphasized. The first one refers to his critique of financial incentive for military service. In this context, I will consider the topicality of the view on the non-moral nature of treating financial issues in the terms of motivation for military service. Analyzing these issues, one should be aware that Rousseau lived in times when professional armies were based on principles different from modern professional troops. After all, the idea of a national army was born as a result of the French Revolution. The second of the raised issues concerns the non-moral nature of the aggressive war. This view will considered from the viewpoint of question whether the philosopher would be against the treatment of human rights as a source of legitimization of actions against the state that violates them. The last part of speech will be devoted to the specificity of his understanding of the duty of all citizens to defend their homeland.

KEYWORDS

Rousseau; Ethics; Armed forces.

Economic Sanctions: An Ethical Perspective

J-M. Lehtonen (1) and A. Mutanen (2)

(1) National Defence University, Finland, juha-matti.lehtonen@mil.fi
(2) Naval Academy, Finland, arto.mutanen@mil.fi

There is a wealth of research on the effectiveness of economic sanctions from both the political science and economic perspectives. A benchmark study in the field by Hufbauer et al. (1990) concluded that economic sanctions would have a success rate of 34 %, based on empirical analysis of imposed sanctions. Pape (1997) has criticized their classification of successes and claimed that only 4 % were actually successful. For example, Hufbauer classify UK vs. Argentina dispute over Falkland Islands as a sanctions success because UK won and sanctions had some effect, while for Pape the issue was settled through war. Moreover, as Hufbauer. study was based on imposed sanctions, the possibility of successful threats was not included. Omitting threats render empirical studies of sanctions effectiveness invalid (Smith, 1995).

The ethics of economic sanctions is an issue that has been curiously neglected by philosophers and political theorists as there are only a handful of scientific publications discussing whether and when they are morally justified (Ellis, 2013). According to Pattison (2015), these few contributions view broad economic sanctions as highly objectionable. This was recognized by the UN General Secretary Ghali (1995): "Sanctions ...raise the ethical question of whether suffering inflicted on vulnerable groups in the target country is a legitimate means of exerting pressure on political leaders whose behaviour is unlikely to be affected by the plight of their subjects" In response to such ethical problems, targeted sanctions were developed. They are designed to hurt regime elite supporters while imposing minimal hardship on the public (Drezner, 2011). They clearly solve the political problem of ''*doing something*'' in the face of target state transgressions but they do not solve the policy problem of coercing the target state into changing its policies (Drezner, 2011)

Economic sanctions are a pluralistic tool that can have a wide variety of intentions, so the evaluation of them isn't easy task to do (Peksen 2019). For example, Marks (1999) considers economic sanctions as a tool to generate "*a norm of international behavior*" that could also be understood as a symbolic message sent to a wrongdoer. Ellis (2013) shows economic sanctions might have several other intentions, like intention to change the behavior of the target or intention to punish the target. Hence, besides the effectivity of sanctions, we have to study their ethical justification (Ellis 2013; Pattison 2015).

Marks (1999, 1511) shows that the ethical foundation of economic sanctions cannot be studied without detailed knowledge about the economic sanctions and their consequences as the observation that *"[t]here can be no doubt that the civilian populations in targeted countries are victims of human rights violations"* demonstrates. Drawing from Just War principles, Gordon (1999) reminds that morally defensible sanctions should also consider issues of proportionality and just cause that both vary from situation to situation. So, the ethics of economic sanctions cannot be studies in an ethicist's paradise in which acts and their consequences are clearly identified and can be ethically evaluated as right or wrong acts. The target of economic sanctions is not easy to specify, for example, if the intention is to punish, then who are those to be punished? To be ethical, punishment has to be relative to the act causing the punishment. In the case of economic sanctions, the punished individuals might be innocent ones (Ellis, 2013).

Economic sanctions are not sensitive to the moral responsibility of the people. Western ethical tradition is fundamentally individualistic. That is, moral agent is an individual who is responsible for his or her acts (and consequences of the acts). It is not clear how to distribute the moral responsibility to the members of a given group. Especially, in the case of broad economic sanctions, all the citizens of the state cannot be considered responsible for the actions of the state. (Mäkelä & Halki 2018.) Targeted sanctions, however, are more sensitive to the responsibility problem (Ellis 2021).

Sometimes it is obvious that the actions of a state are simply wrong, and it is not possible to allow this keep going. A good example is war of aggression. So-called better than war, better than doing nothing -argument is formulated to justify economic sanction is cases like these. Unfortunately, the argument is not a valid one; because there are several other things that might be done. One way to avoid the problem is to think "economic sanctions as a method of '*preserving clean hands*'" which makes the applicability of ethical sanctions more flexible. Moreover, clean hands argument reverses the justification conditions of ethicality: it becomes a moral duty not to participate morally blamable activities. (Ellis 2013.) While this may appear as a good argument, from the utilitarian perspective it suffers from a clear causal relationship between the trade with the target country and the morally blamable activities of

target country, such as waging of war of aggression. Economic sanctions, almost by definition reduce the well-being in both countries, so to offset this, there should be a causal link on how economic activity aids the objectionable activity, such as war of aggression. If the causal link is missing, the only thing that remains from the clean hands argument is guilt by association. From the utilitarian ethics perspective, that is not enough.

KEYWORDS

Economic sanctions; Ethics.

REFERENCES

Ellis, E. (2013), *The Ethics of Economic Sanctions*. PhD Philosophy, The University of Edinburgh.

Ellis, E. (2021) The Ethics of Economic Sanctions: Why Just War Theory is Not the Answer. *Res Publica, 27*(3). 409–426. doi: https://doi.org/10.1007/s11158-020-09483-z

Drezner, D. W. (2011). Sanctions sometimes smart: targeted sanctions in theory and practice. *International Studies Review*, *13*(1), 96-108.

Ghali, B-B. (1995). *Report of the Secretary-general on the work of the organization, supplement to an agenda for peace: position paper of the Secretary-general on the occasion of the fiftieth anniversary of the United Nations.* Retrieved from https://www.un.org/documents/ga/docs/50/plenary/a50-60.htm

Gordon J. (1999). Economic Sanctions, Just War Doctrine, and the "Fearful Spectacle of the Civilian Dead". *CrossCurrents, 49*(3), 387-400.

Hufbauer, G., Schott, J., & Kimberly A. E., (1990). *Economic sanctions reconsidered: History and current policy.* Washington: Institute for International Economics.

Marks, S. (1999). Economic Sanctions as Human Rights Violations: Reconciling Political and Public Health Imperatives. *American Journal of Public Health*, *89*(10), 1509-1513.

Mäkelä P., & Hakli R., (2018). Bad Arguments for Responsibility Sharing. In: M. Coeckelbergh et al. (Eds.), *Envisioning Robots in Society – Power, Politics, and Public Space.* doi:10.3233/978-1-61499-931-7-275

Pape, R. A. (1997). Why economic sanctions do not work. *International Security*, *22*(2), 90-136.

Pattison, J. (2015). The Morality of Sanctions. *Social Philosophy & Policy*, *32*(1), 192-215.

Peksen, D. (2019) When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature, *Defence and Peace Economics, 30*(6), 635-647. doi: 10.1080/10242694.2019.1625250

Smith, A. (1995). The success and use of economic sanctions. *International Interactions, 21*(3), 229-245.

Changes in the values of European society in the context of the COVID-19 pandemic

K. Kądzielski (1)

(1) University of Warsaw, Poland, .kadzielski@uw.edu.pl

The men kind who is in the center of the world and the processes taking place in it, adapted the surrounding environment to meet his own needs. For over 20 years, the people of Europe have been enjoying the values professed by the West, which are the basis for the functioning of most European countries. In the process of implementing the features of Western societies, a sense of security was also developed for the purpose of development, thanks to which it became possible to obtain material and spiritual goods. The level of advancement, both technical and scientific, has allowed European society to function in a relatively calm and controlled environment. However, it should be remembered that the level of this sense of security and the related procedures for the protection of values can be deceptive, especially in the case when a person does not feel a direct threat to his existence. This creates a state of incorrect perception of security, which Daniel Frei has already written about.

The aforementioned sense of security, as well as the system of protecting the social values of the inhabitants of Europe, collapsed with the COVID-19 pandemic. The peace and world order that had been binding so far were put into question. Uncertainty, panic, and fear of losing your own health and that of your loved ones have taken the place previously reserved by the feeling of freedom from threats. Due to the need for man to adapt to life in the new reality, as well as the need to develop effective procedures for the elimination and mitigation of the effects of the COVID-19 pandemic, it was necessary to update the law in force.

Therefore, the author will answer the problem question: Has the COVID-19 pandemic had negative effects (repercussions) on the fundamental values of European society? The occurrence of the SARS-CoV-2 virus forced the inhabitants of Western countries to reevaluate their views on the values professed in life. Until the prepandemic times (until the end of 2019), there were repeated patterns of action and values cultivation, which were the pillars of the functioning of the European Union countries. Since the turn of 2019/2020, there has been a change in the perception of Europeans so far, which resulted in the need for quick and, above all, effective measures to protect Western societies. The constant development of the pandemic situation and the related number of restrictions make it impossible to predict future events.

KEYWORDS

COVID-19; SARS-CoV-2; Social security; European values; International society.

REFERENCES

Armin, b. (2019). *Fundamentals on Defending European Values, VerfBlog,* Retrieved from https://verfassungsblog.de/fundamentals-on-defending-european-values/ . doi: 10.17176/20191112-153757-0.

Bilbeny N. (2020, January). The transformation of European values. *History and Values*.

Bor A., Jørgensen F., & Bang Petersen M. (2021, December). *The COVID-19 Pandemic Eroded System Support But Not Social Solidarity*, Department of Political Science, Aarhus University. DOI: 10.31234/osf.io/qjmct

Darrida J., & Habermas J., *Europa, jaka śni się filozofom*, trans. Andrzej Kopacki, *Gazeta Wyborcza*, 134, 2003.

European Commission (2022, March). *A New Era of Europe. How the European Union Can Make the Most of its Pandemic Recovery, Persue Sustainable Growth, and Promote Global Stability*, 48-78.

Habermas J. (1993). *Obywatelstwo a tożsamość narodowa. Rozważania nad przeszłością Europy*, Warsaw: IFiS PAN.

Habermas J. (2001). Why Europe Needs a Constitution. *New Left Review*, September-October. Retrieved from https://revistaidees.cat/en/la-transformacio-dels-valors-europeus/ and https://european-union.europa.eu/principles-countries-history/history-eu_en

Pacces A. M., & Weimer M (n.d.). *From Diversity to Coordination: A European Approach to COVID-19*, Cambridge.

Pietrzyk-Reeves D. (2003). Democracy or Civil Society?. *Politics*, *23*(1), 38-45.

Pietrzyk-Reeves D. (Ed.) (2007), *Tożsamość Starego Kontynentu i przyszłość projektu europejskiego*, Warsaw: Biblioteka Jedności Europejskiej.

Pietrzyk-Reeves, D., & Kułakowska, M. (EdS.) (2010). *Studia nad wielokulturowością*. Cracov: Księgarnia Akademicka,152-171.

Policy Department for Structural and Cohesion Policies (2022, January). *The impacts of the COVID-19 pandemic on EU cohesion and EU cohesion policy*.

Riedel. R. (Ed.) (2010). *Central Europe two decades after*. Warsaw: Centre of Europe Warsaw University, 141-154.

University Pres (2020, June). *11*(2), pp. 283-296. doi: https://doi.org/10.1017/err.2020.36

World Health Organization (n.d.). *World Health Statistics 2021. Monitoring Health for the SDGs*, 1-16.

Pacifism as a proposal for creating international security. Peter Brock's concept

B. Bado (1)

(1) University of Warsaw, Poland, blazej.bado@onet.pl

Peter de Beauvoir Brock (1920-2006) is the best-known contemporary scholar on the history of pacifism. He is the author of numerous scientific publications, many of which have been published in various languages. Brock's research covered a period stretching from early Christianity to the 20th century. To sum up his work, Martin Ceadel (1996), Professor of History at Oxford University – states: "No ideology owes more to one academic than pacifism owes to Peter Brock".

In my speech I will present Peter Brock's diffuse pacifist concept relating to the creation of security in the international arena.

First part of it will be devoted to the presentation of the assumptions of this concept referring to religion and humanism in the broadest sense. In the case of the religious factor, it should be noted that the relationship between religion and war is gaining great importance nowadays. Religiously inspired thinking characterises the statements of not only religious but also political leaders. This can be seen not only in radical Islam, which inspires actions against the state of Israel, but also in the activity of the Russian Orthodox Church of the Moscow Patriarchate, which supports Russia's aggression against Ukraine.

In the second part of my speech I will discuss the directions and reception of Peter Brock's research. Requires noting that so far there has been no monograph that provides a scholarly interpretation of Brock's pacifism and the implications it generates for creating international security. Research on Brock's pacifist ideas has so far been conducted in several thematic areas - above all, from the point of view of the history of religions, particularly Christianity, the history of pacifist groups, the history of social ideas.

Thirdly, I will present historical and contemporary selected organisations referring to pacifist thought. Reflection on this issue is so important because of the fact of the uninterrupted existence of pacifist groups which, while propagating their own ideas, fit into the narratives of contemporary anti-systemic and anti-state movements. Such tendencies are evident in organizations declaring pacifism, such as Jehovah's Witnesses, Quakers, Mennonites, Seventh day Adventists.

The culmination of my speech will be the analysis of Brocke's thoughts in terms of implications for security studies.

KEYWORDS

Peter Brock; Pacifism; International security; Religion.

REFERENCES

Ceadel, M. (1996). Ten Distinctions for Peace Historians. In: *The Pacifist Impulse in Historical Perspective.* Toronto: University of Toronto Press, 17.

The state of emergency in Poland - legal regulations and reality. Carl Schmitt's concept and Polish case study

M. Kolodziejczak (1)

(1) War Studies University, Poland, malwina.e.kolodziejczak@gmail.com

The state of emergency - like the other two states - martial law and a state of natural disaster, are subject to constitutional and statutory regulations. According to Polish Constitution in situations of particular danger, if ordinary constitutional measures are inadequate, any of the following appropriate extraordinary measures may be introduced: martial law, a state of emergency or a state of natural disaster (art. 228.1.). According to art. 230, the President of the Republic of Poland may, on request of the Council of Ministers, introduce for a definite period no longer than 90 days, a state of emergency in a part of or upon the whole territory of the State in the case of threats to the constitutional order of the State, to security of the citizenry or public order. Extension of a state of emergency may be made once only for a period no longer than 60 days and with the consent of the Sejm (art. 230.1 and 230.2). Therefore, it seems that there is a complete and comprehensive procedure relating to the principles of introducing and continuing this state or even states.

Such an important situation, extraordinary after all, cannot have gaps or understatements in its regulations. But the problems appear according to substantive law and formal law too. Moreover, the premises, the procedures of introduction and even the tasks of the authorities are full of doubts. Therefore, the author will try to point out some of them and indicate partial de lege ferenda postulates at least.

What's more, the author will compare the legal provisions and the assessment of the events of 2021 with the concept of Carl Schmitt.

Main problem: What are the problematic aspects (in terms of substantive law and formal law) of the functiong of the provisions relating to the state of emergency?

Methods: system analysis, functional analysis, comparative law, dogmatic analysis, interpretation

Results: indication of provisions that should be changed, clarified together with changes at the constitutional level

Conclusions: the provisions of the state of emergency, despite extensive regulations, are insufficient and require legislative steps.

KEYWORDS

State of emergency; Martial law; Carl Schmitt's concept.

Dilemmas of representation in a study of autonomous weapon systems (AWS). A focus group perspective

J. Pekarev (1)

(1) Estonian Military Academy, janar226@ut.ee

The increasing integration of AI with weapon systems promises massive changes in warfare, as well as enormous enhancements to military arsenals. However, for nations and societies these developments also raise many concerns as the use of force, combined with decisions about life and death, become potentially delegated to lethal machines that can be operated without human input or involvement. Understanding the opinions, concerns, and attitudes of the general public towards AWS is relevant for guiding public policy decisions related to their implementation. This paper reports the findings of six focus groups (n=53), which were used to gauge the perceptions and attitudes towards the development of AWS. Understanding public opinion in terms of the way people think and talk about unmanned ground vehicles (UGV-s) for military purposes is relevant for exploring the issues related to the future development and institution of AWS. It also allows public concerns and attitudes towards AWS to be heard and recognized. The study findings indicate that the reactions to the development of AWS are not homogenous. There was, however, some degree of consensus among participants who felt that AI-embedded machines should be perceived as decision-making instruments, although with the caveat that any decisions pertaining to life and death matters should not be delegated to a machine. Among the participants there was also a general consensus that any commander in the military hierarchy giving a direct order to use AWS to carry out a mission should be primarily be held responsible for any unlawful killings that may result from that mission. In addition, there is also an often overlooked paradoxical element of autonomous weapons in that the same weapon that can be used to defend the country, can also potentially be used against it. This raises another critical issue related to the implementation of a 'patriotic code' in machines.

KEYWORDS

From religion to war and peace. A study of values that build international security

C. Smuniewski (1)

(1) University of Warsaw, Poland, c.smuniewski@uw.edu.pl

Research relating to the issues of religion and, at the same time, on the values that construct international security, is gaining importance today. This importance was increased not only by reflection on fundamentalisms, but also by the war in Ukraine. In the context of this armed conflict, Putin's religious narratives turned out to be an important part of his propaganda.

The author discusses the values that construct the international order by analyzing religiously inspired texts on security and peace. Following the thought of Adam Danel Rotfeld (director of the Stockholm International Peace Research Institute in 1991-2002), he sees values as one of the forces contributing to the international order and points to the role of moral and ethical values in making political decisions.

Reflection on values leads the author to analyze four rules of primacy in social relations: the primacy of time over space, reality over ideas, peace over conflicts, and the whole over a part. This means that "change" and "transformation" nowadays get their new position in the hierarchy of values and become one of the key values. It is about "changes" and "transformations" that take place inside states, and quickly turn out to have effects in international relations. These "changes" and "transformations" do not happen without the participation of religion - political thinking inspired by religious content.

Following Rotfeld's thought, author will analyze the Holy See's axiology of security, which as a state is bound by a series of international agreements.

The author is primarily interested in the values that have universal features, not only resulting from the Christian source of the Holy See's reflection.

The author reconstructs the collection of such values by analyzing the texts of the Popes for the "World Day of Peace" celebrated annually on January 1. These texts are a response to the current situation on the international arena. They contain not only a set of threats to contemporary security, but also a set of values that seem to have the potential to build an international order. At the heart of these values are people, their rights and dignity. Man ignites wars and builds peace, appears as the creator of threats and security. An additional feature of the reconstructed axiology of security promoted by the Holy See is its contribution to the development of security anthropology. It is by all means realistic anthropology, set in the context of history, it speaks of man in the context of his "today" (war, security, armed forces, the right to defense, state policy, international politics), which grows from "yesterday" and leads to "tomorrow". It is an anthropology that emphasizes the human ability to build communities (family, nation, state) that manifest values, defend them, demand their respect.

KEYWORDS

Values; Axiology; International security; Holy See.

The Russian ethics of war? Axiological aspects of Russian strategic documents and war propaganda in the context of the war against Ukraine

M. Skladanowski (1)

(1) The John Paul II Catholic University of Lublin, Poland, marcin.skladanowski@kul.pl

Since Vladimir Putin's speech at the Munich Security Conference in 2007 (Putin, 2007) and his declaration of an anti-Western foreign policy, a growing axiological dimension can be observed in Russian strategic documents devoted to national security. Subsequent Russian National Security Strategies contain more and more references to the values that are supposed to differentiate Russia from the liberal democracies of the West (Giles, 2019; Ivanov, 2018; Welch Larson & Shevchenko, 2014). Similarly, the language of an axiological nature concerning military action against Ukraine and a possible military conflict with NATO is present in Russian public life and media coverage fully controlled by the state. The Russian Orthodox Church, under the leadership of Patriarch Kirill, is also joining this type of discourse. The language referring to 'Russian values' in the conflict with Ukraine and the wider West took on a new dimension on 24 February 2022, the day Russia's war against Ukraine began.

This paper is the result of an axiological analysis of Russian war discourse in two stages:
  – Stage I (an ideological preparation for war) – initiated by Putin's signing of a new National Security Strategy (2 July 2021) (Strategiya, 2021) and the publication of an article questioning Ukraine's national identity and independence ('On the Historical Unity of Russians and Ukrainians', 12 July 2021) (Putin, 2021).
  – Stage II – launched with Russia's armed aggression against Ukraine. Russian documents and key statements by Vladimir Putin, Sergei Shoygu, and Sergei Lavrov were analysed. In addition, the reports of the state news agency RIA Novosti relating to the war were examined, as well as public opinion polls conducted by the Levada Centre.

The study has led to the following conclusions:
  – Both in Stage I and Stage II, military action against Ukraine and a possible war with NATO were justified by reference to the language of values. Russia is considered a particular state, different from others. The basis for this differentiation are the 'spiritual' and 'traditional' values on which Russian statehood and social life are based. In the face of external pressure, Russia's mission is to defend these values, including with military force.
  – The Russian army is presented as the defender of these values. The activities undertaken by the army are considered an important element of Russian identity policy. The ability of the Russian army to intervene in other states is an expression of Russia's desire to regain its rightful status as a superpower with its sphere of influence.
  – The military action against Ukraine is axiologically equated with the war the USSR waged against Nazi Germany from 1941 onwards, i.e. from when the Soviet-Nazi alliance broke down. These actions are always right and morally good, and their course and consequences cannot be criticised.

Ultimately, the axiological aspect of the language concerning the war in contemporary Russia allows us to pose the thesis that it makes up the process of creating a new Russian ethic of war. In this ethic of war, certain elements present in Soviet war propaganda are noticeable. These include the cult of war against Nazi Germany (1941-1945), the denial of Russian war crimes due to the assumed heroic and morally justifiable nature of the war, and the downplaying of war losses due to the priority of the interest of the community (nation/state) over the interest of the individual, which is supposed to be one of the key values distinguishing Russian culture and tradition from the West. There are also new elements in this ethic of war, unprecedented in Soviet discourse. These are primarily nationalism (the Russian army as the defender of the 'Russian world', culture, and tradition) and sacralisation (full support from the Russian Orthodox Church, recognising the war against Ukraine as a 'metaphysical war' against the decadent West).

Opinion polls conducted in Russia in 2021 and 2022 allow us to conclude that this type of discourse is accepted and supported by a significant part of Russian society.

REFERENCES

Giles, K. (2019). *Moscow Rules: What Drives Russia to Confront the West*, London: Chatham House.

Ivanov, I. (2018). *Yevropeyskiy vektor vneshney politiki sovremennoy Rossii.* Moscow: E.

Larson, D. W. & Shevchenko, A. (2014). Russia says no: Power, status, and emotions in foreign policy,. *Communist and Post-Communist Studies 47*(3-4), 269–279. doi:10.1016/j.postcomstud.2014.09.003.

Putin, V. (2007). *Speech and the Following Discussion at the Munich Conference on Security Policy*. Retrieved from http://en.kremlin.ru/events/president/transcripts/24034

Putin, V. (2021). Ob istoricheskom yedinstve russkikh i ukraintse. Retrieved from http://kremlin.ru/events/president/news/66181

Strategiya natsional'noy bezopasnosti Rossiyskoy Federatsii. (2021). Retrieved from http://publication.pravo.gov.ru/Document/View/0001202107030001

Stressed Ethics of War in the Age of Modern Military Warfare

B. Arunoday (1)

(1) Agra College, India, arunodaybajpai@gmail.com

The anarchic nature of international order breeds desire for power and the inevitability of conflict and war among nations. This realist assertion has led to two contradictory developments about the means and nature of war. The inevitability of war and conflict keeps nations inclined towards enhancing war fighting capacity with new military technology and weapons. While tank was an innovation during the First WW, we talk about drones, cyber warfare, automatic and hypersonic weapons as new military means of 21st century. These new weapons may even dehumanize the war in coming days. On the other hand, the same inevitability of war leads to another contrary tendency to humanize the war in the face of increasing destructive capacity of war. The attempts to humanize the war are articulated in the notion of ethics of war also known as just war theory. The basic premise of the idea of the just war is that war is inevitable. Hence it is to be conducted for just cause and in a just manner. Most of the premises and principles of just war theory are incorporated in the international law of war found in Hague conventions (1899 and 1907), Four Geneva Conventions (1949), statute of International Criminal Court and International customary law of war.

Thus, there is persistent struggle between the evolution of military technology and the prevailing notion of ethics of war. The just war theory tries to upgrade itself to adjust with the evolving nature of war machine. But it is not possible always in view of fast changing nature of military technology. In view of this, the present paper seeks to answer the following three fundamental questions:

- What is the present theory and practice of just war idea? Is it adequate to humanize the war in our times?
- How new military technology has impacted the ethics of war, mainly the conduct during the war.
- How the just war theory addresses the question of changing nature of war in view of ever changing military technology?

The very idea of war ethics is problematic. While realists would say that ethics has no place once war has started, but the pacifist, on the other hand would argue that there cannot be any arguments to justify the war as it results in destruction and loss of lives(Lazar: 2016). The just war theory does not justify the war, but wants to make it more humane and limited since we cannot avoid the war. It attempts to humanize and limit the war. It is most important idea to understand the ethics of war. This is a tradition going back to St. Augustine in the 5th Century and St. Thomas in the 13th Century and find wide acceptance in modern times (Moseley, 2022). The just war theory rests on the two related notions (Widdows, 2022):

- *Jus ad bellum*, meaning there should just cause for waging war by nations as a matter of last resort.
- *Jus in bello*, which denotes that the conduct of war should be just and fought with just means.

Since we are concerned with the means of war, the jus ad bellum is not directly relevant to this paper, we need to focus on the status of *jus in bello*. There are three conditions of *jus in bello* to meet the standard of just conduct of war-

- Discrimination. It means it is not permissible to target civilians or non-combatants.
- Proportionality. The collateral harm to civilians is permissible only if it is proportionate to the goals of the armed attack.
- Necessity. The collateral harm to civilians is also permissible only if the least harmful means feasible are deployed to achieve military objectives.

Walzer (2006-1977), the best modern exponent of just war theory argues that civilians or non-combatants need to be protected during the war because they have compromised their right to life unlike the combatants who have compromised this right by joining the combat forces. There is equality among combatants on this ground, hence they may harm each other. But non-combatants stand on different ground. The just war theory has faced many criticisms mainly from pacifists and realists both for justifying the war on the ground of ethical principles. It also ignores the collectivist nature of war and focuses on the conduct of individuals in the war (Babic, 2019).

While just war theory tries to limit and humanize the war as a necessity, the rapid developments in war technology like drones, autonomous weapon systems or cyber warfare pose a new challenge to ethical principles of war. There is a need to review the ethics of war in view of these technological developments. Many scholars (Horowitz, 2016; Sagan, 2016; Walzer, 2016) have analyzed the impact of technological developments of warfare on the ethics of

war. In fact, this is one of the three dimensions of the just war theory in modern times. The other two dimensions are: the application of just war principles in non-international conflicts (civil wars) and outcome and aftermath of war (*jus post bellum*). However, the scope of this paper is limited to analyze the impact of new war technology on the prevailing ethics of war mainly *jus in bello*.

KEYWORDS

War ethics; Modern warfare; *Jus in bello*; just war theory.

REFERENCES

Babic, J. (2019). Ethics of War and Ethics in War. *Conatus, 4*(1), 33-51, November 2019. Retrieved from https://www.researchgate.net/publication/336041403_Ethics_of_War_and_Ethics_in_War

Heather, W. (2022). *The ethics of warfare: Is it ever morally right to kill on a massive scale*. University of Birmingham. Retrieved from: https://www.birmingham.ac.uk/research/perspective/ethics-of-warfare-heather-widdows.aspx

Horowitz, M. C. (2016). Ethics and Morality of robotic warfare: Assessing the Debate over Autonomous Weapons. *Daedalus*, Fall. Retrieved from https://www.amacad.org/daedalus/ethics-technology-war

Lazar, S. (2016). *War*. Stanford Encyclopedia of Philosophy. Retrieved from: https://plato.stanford.edu/entries/war/

Moseley, A. (2022) *Just War Theory. Internet Encyclopedia of Philosophy*. Retrieved from https://iep.utm.edu/justwar/

Sagan, S. D. (2016). *Ethics, Technology and War, Daedalus*, Fall. Retrieved from https://www.amacad.org/daedalus/ethics-technology-war

Walzer, M., 2006 (Originally published in 1977), *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (4th edition). New York: Basic Books, 133-138.

Walzer, M. L. (2016*).* Just and Unjust War Killings: and Drone Warfare. *Daedalus*, Fall. Retrieved from https://www.amacad.org/daedalus/ethics-technology-war

Fake news as an ethical problem of building the resilience of the national security system

M. Kuczabski (1) and C. Smuniewski (2)

(1) War Studies University, Poland, m.kuczabski@akademia.mil.pl
(2) University of Warsaw, Poland, c.smuniewski@uw.edu.pl

False information is generated through methods of manipulation that use techniques that perfectly exploit the frailties of human nature, its emotionality and cognitive errors and lack of knowledge, which makes its dissemination fast and effective. The fake news paradigm requires three elements: (1) tools and services, (2) social media platforms, and (3) motivation. Tools and/or services are used to manipulate and spread fake content on social media platforms. Followers, i.e. followers or, for example, online polls, are used for this purpose. Social media platforms are where instruments and applications are used. Platforms invoke the psychological mechanisms of the viewer, confirming their hierarchy of needs and even prejudices, often use bots based on algorithms that model user data, adapting to social norms, make them more convincing and difficult to identify, track user actions, also hint and suggest Content to read or watch works continuously and can be activated, can adapt to the situation, recognizing the context - does not require human intervention. The most active bots are on Twitter. Fake news is a tool, so the motivation is based on the objectives, which may be financial or political gain or intensification of propaganda, deepening social divisions and creating information confusion. Structured fake news networks are designed for sophisticated and unidentifiable manipulation. The term is ambiguous, covering many types of disinformation, distortion of facts and circumstances. One of its varieties is the so-called FUD (Fear, Uncertainty, Doubt) - situations, events, information that cause doubts about something. The aim of such messages is to provoke fear and spread social panic. Ideologically saturated messages present a particular view of politics, so to speak, programming users who become the next link in the message. Such actions are called computational propaganda. It is one of the latest specialist strategies used to maintain social control. On the Internet, we are facing campaigns steered by the so-called trolls, i.e. people who are active online and deliberately attract the attention of other users by arousing emotions - an ideological form of interaction. They create fake accounts on social networks and represent a particular political ideology. Campaigns are thought to be the most harmful behavior on the Internet, used by extremist, nationalist, racist and xenophobic groups to harass and ridicule their opponents. The following groups are distinguished: haters, lolcows, socials and viewers. The most common activities are: denigrating government opponents, avoiding controversial topics, and raising money for support. There are organizations that employ trolls, creating 'troll farms' (e.g. Internet Research Agency funded by Putin's backers - case of Jenny Abrams, White Trolls in Turkey and China 'ziganwu'). False information in online news spreads like viruses and repeatedly emerges in mainstream media, posing a threat to state security in various areas of human activity. Users of the Internet, social media, information platforms, whose users also remain politicians and those in power, are at risk. As politics has already acquired a digital dimension, information often appears faster on Twitter than in official communications, making it all the more dangerous. The daily exposure of social media users to propaganda and disinformation campaigns has revived the need to study the phenomenon of fake news, including deep fake (fake fabricated videos), as well as local and global patterns of dissemination of different (mis)information content on social media. To be objective, it should be noted that virtually every side of the political spectrum is involved in the creation of fake news.

Objective: The aim of the study was to detect fake news, manipulation of its recognition by social media users with a question formulated as follows: what can be social resistance to fake news as a media product in the post-truth era? It has been hypothesized that fake news causes a lack of social resistance to fake news despite the declared knowledge of users about fake news and is an ethical problem in building social resilience.

Approach / Methodology / Project: The presented result of combining the analysis of secondary sources (literature, studies, reports) with the empirical part (questionnaire survey) allowed us to confirm the main thesis of the article, which is that fake news as a media product in the post-truth era causes lack of social resistance to false content.

Conclusions:. The results of the study indicate the vulnerability of social media users to fake news despite their knowledge on the subject. The conclusion points to the need for appropriate media courses, trainings, and media campaigns that will improve the knowledge of social media users making them more resistant to fake news.

WG6 – Security and Defence Policy

The role of Frontex in a changing world

P. Alonso-Rodriguez (1)

(1) Universidad Nacional a Distancia – UNED, Spain, pablo.alonsorodriguez@protonmail.com

In order to cover all relevant aspects related to the European Border and Coast Guard Agency (Frontex) a holistic approach is considered. In particular, this paper proposal states that not only defence considerations would be taken into account but also legal, geopolitical and historical considerations would be factored in. Consequently, the methodological approach is based on the interdisciplinary review of the existing setup of the agency as well as a contextualisation on the rationale for its creation and its mandate. In addition, the potential way-forward is envisaged to be tackled.

The outline of the paper proposal is composed of four main sections, apart from the introduction and concluding remarks. Section 1 would set the scene by describing the evolution of the agency, from the former European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union to the current European Border and Coast Guard Agency. Here both historical and legal considerations will be the leading aspects of this multidimensional study.

Section 2 would elaborate on the role of Frontex as regards the cooperation among the EU Justice and Home Affairs agencies network. This cooperation forum includes, apart from Frontex, other eight agencies, namely: CEPOL, EIGE, EMCDDA, EUAA, eu-LISA, Eurojust, Europol, and FRA.

Section 3 would study the current mandate of Frontex, to promote, coordinate and develop European Border Management in line with the EU fundamental rights charter and the concept of EU-integrated border management. It would also explain how Frontex provides technical and operational assistance to Member States through joint operations and rapid border interventions, as well as technical and operational assistance in the support of search and rescue operations at sea.

Finally, Section 4 would explain how Frontex should be adapted to the new realities that the agency needs to confront and the ongoing discussions in this regard as part of its Annual Risk Analysis Reports.

KEYWORDS

External border management; European cooperation; Migration; Security policy.

REFERENCES

Bossong, R. (2019). The Expansion of Frontex. *Symbolic Measures and Long-term Changes in EU Border Management*. Berlin: Stiftung Wissenschaft und Politik. Retrieved from https://www.swpberlin.org/publications/products/comments/2019C47_bsg.pdf

Ekelund, H. (2014). The establishment of FRONTEX: A new institutionalist approach. *Journal of European Integration*, *36*(2), 99-116. doi: 10.1080/07036337.2013.809345

Horsti, K. (2012). Humanitarian discourse legitimating migration control: FRONTEX public communication. In *Migrations: interdisciplinary perspectives*, 297-308. doi:10.2139/ssrn.2673046. Retrieved from https://www.researchgate.net/publication/314467677

Kalkman, J. P. (2021). Frontex: A literature review. *International Migration*, *59*(1), 165-181. doi:10.1111/imig.12729. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/imig.12729

Leonard, S. (2009). The creation of FRONTEX and the politics of institutionalisation in the EU external borders policy. *Journal of contemporary European research*, *5*(3), 371-388. Doi:10.30950/jcer.v5i3.239. Retrieved from https://www.jcer.net/index.php/jcer/article/view/239/164

Léonard, S. (2010). EU border security and migration into the European Union: FRONTEX and securitisation through practices. *European security*, *19*(2), 231-254. doi:10.1080/09662839.2010.526937. Retrieved from https://www.tandfonline.com/doi/full/10.1080/09662839.2010.526937?scroll=top&needAccess=true

Léonard, S., & Kaunert, C. (2022). The securitisation of migration in the European Union: Frontex and its evolving security practices. *Journal of Ethnic and Migration Studies*, *48*(6), 1417-1429. doi:10.1080/1369183X.2020.1851469. Retrieved from https://www.tandfonline.com/doi/full/10.1080/1369183X.2020.1851469?scroll=top&needAccess=true

Mungianu, R. (2013). Frontex: Towards a common policy on external border control. *European Journal of Migration and Law*, *15*(4), 359-385. Retrieved from https://brill.com/view/journals/emil/15/4/articlep359_2.xml

Neal, A. W. (2009). Securitization and risk at the EU border: The origins of FRONTEX. *Journal of common market studies*, *47*(2), 333-356. doi: 10.1111/j.1468-5965.2009.00807.x. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-5965.2009.00807.x?saml_referrer

Paul, R. (2017). Harmonisation by risk analysis? Frontex and the risk-based governance of European border control. *Journal of European Integration*, *39*(6), 689-706. doi: 10.1080/07036337.2017.1320553. Retrieved from https://www.tandfonline.com/doi/full/10.1080/07036337.2017.1320553

Perkowski, N. (2018). Frontex and the convergence of humanitarianism, human rights and security. *Security Dialogue*, *49*(6), 457-475. doi: 10.1177/0967010618796670. Retrieved from https://www.jstor.org/stable/26979674

Wolff, S., & Schout, A. (2013). Frontex as agency: More of the same?. *Perspectives on European Politics and Society,* *14*(3), 305-324. doi: 10.1080/15705854.2013.817809. Retrieved from https://www.tandfonline.com/doi/full

The Acolhida Operation from the perspective of human security

T. Barboza (1)

(1) Brazilian Army Staff-Officer College, tuliopb84@hotmail.com

The present work has the general objective of evaluating whether Operation Acolhida provides human security to Venezuelan immigrants. Thus, the question that guides this work is: "how has Operação Acolhida been offering human security to its immigrants?" Faced with this problem, the work proposes to categorize the actions of Operação Acolhida that took place in the state of Roraima, from February 2018 to today, within the seven aspects of human security presented by the United Nations Development Program (UNDP) in its Report of Human Development (HDR) of 1994.

Throughout the 1980s, the importance of basic human needs increased, and other aspects began to be incorporated into International Security Studies (ESI). With this, there was an expansion of the understanding of security, with the social, economic, environmental, health, development and gender concept of human security. Then comes the concept of human security, which is dedicated to the view that human beings should be the primary reference objects of security and that, therefore, the ESI should include issues such as poverty, underdevelopment, hunger and other attacks on integrity and human potential (Buzan and Hansen, 2009).

The 1994 HDR prepared by the UNDP defined that there are seven aspects of human security. They are: economic, environmental, food, health, political, personal and community. The 2009 OCHA Handbook contains indicators that allow assessing the achievement of human security in each aspect, as shown in the Table 1.

Table 1 – adapted from Human Security Unit – OCHA (2009, p. 16)

Human Security Components	Strategies to Increase Protection (Indexers examples)
Economic Security	Assured access to basic income; Public and private sector employment, salary, self-employment; Social security financing; and Diversify agriculture and the economy.
Food security	Right to food, growing it themselves, having the ability to buy it or through a public food distribution system.
Health security	Access to basic health services; Risk-sharing agreements that pool membership funds and promote communitybased insurance schemes; and Interconnected surveillance systems to identify disease outbreaks at all levels.
Environmental security	Sustainable practices that take into account natural resources and environmental degradation (deforestation, desertification); and Early warning and response mechanisms for natural hazards and/or man-made disasters at all levels.
Personal security	Rule of law; and Explicit and enforced protection of human rights and civil liberties.
Community security	Explicit and enforced protection of ethnic groups and community identity; and Protection from oppressive practices, harsh treatment of women, or discrimination against ethnic/indigenous/refugee groups.
Political security	Protection of human rights; and Protection from political or state repression, torture, ill-treatment, illegal detention and imprisonment.

Operação Acolhida is the Brazilian federal government's response to the flow of Venezuelan immigrants fleeing the crisis in their country and entering Brazil's northern border (Oliveira, 2018). In this context, Acolhida is an humanitarian aid aimed at alleviating human suffering, mitigating threats to life or risks to people, and employs military means to complement the initiatives of governments and non-governmental organizations (Brasil, 2014), dialoguing with the concept of human security by incorporating human elements into its security mission. In view of this, a documentary analysis of the reports published by the Federal

Committee for Emergency Assistance (CFAE) in the years 2020 and 2021, available on the Federal Government of Brazil website, was carried out to collect data regarding the actions taken within the scope of the operation. Such collected data were categorized according to the indicators shown in table 1, which made it possible to assess how each aspect of human security has been addressed by the operation. Finally, the classification of data according to the selected indicators made it possible to assess which aspects of human security are best served within the scope of the Acolhida, as well as to identify the aspects that deserve more attention, supporting the realization of a critique of the operation as a whole.

Going further, the data from the reports were categorized in a different way from the original, facilitating their use in future studies.

KEYWORS

Acolhida Operation; Human security; Migration.

REFERENCES

Brasil. (2014, 20 March). Nota de Coordenação Doutrinária Nr 01/2014. *Operações de Ajuda Humanitária.*

Buzan, B., & Hansen, L. (2009). *The Evolution of Internation Security Studies.* Nova Iorque: Cambridge University Press.

Human Security Unit - OCHA. (2009). *Human Security in theory and practice: Application of the Human Security Concept and the United Nations Trust Fund for Human Security.* Nova Iorque: United Nations.

Oliveira, G. A. (2018, November). *A utilização do componente militar brasileiro frente à crise migratória venezuela.* Retrieved from https://www.armyupress.army.mil/journals/edicao-brasileira/artigos-exclusivamente-on-line/artigosexclusivamente-on-line-de-2018/a-utilizacao-do-componente-militar-brasileiro-frente-a-crise-migratoria/

UNDP. (1994). *Human Development Report. An Agenda for the Social Summit.* Oxford University Press. Nova Iorque: Oxford University Press.

Best Practices for Collaboration Between Lithuanian Military and Internal Affairs System in Managing Crisis of Illegal Migrants

V. Giedraitytė (1) and R. Smaliukienė (2)

(1) General Jonas Žemaitis Military Academy of Lithuania, vidmante.giedraityte@lka.lt
(2) General Jonas Žemaitis Military Academy of Lithuania, rasa.smaliukiene@lka.lt

21st century in a global, dynamic and uncertain environment, public authorities are increasingly faced with various challenges. These challenges often arise from events that are not always accurately predicted in advance circumstances such as natural or other disasters, pandemics, etc. To all this, the challenges caused by the geopolitical environment also contribute. Such challenges, of various types, often have a significant impact on the security of the state and its citizens. So there challenges can lead to national security threats or even crises. Crisis situations from public sector institutions and bodies require not only to forecast, monitor, prepare and implement preventive measures, but also quick reactions and immediate actions to identify, manage and eliminate the effects of crises (Kapucu, 2009; Sarapuu, & Randma-Liiv, 2020).

In recent years, Lithuanian government has faced various challenges, such as managing the Covid-19 pandemic, preventing illegal migration across the border of Belarus, and providing aid to war refugees from Ukraine. These situations have shown that in crises, public authorities must make a quick effort to find new ways of managing and organizing activities that address current national security, risk, and crisis management problems. Also these situations clamed that in such cases the efforts and available resources of the institution responsible for crisis management are not sufficient. In scientific discussions, inter-institutional collaboration is identified as one of the essential means addressing such issues (Wilkins et al., 2015). Collaboration between various state institutions (from ministries, military, police, border guards to local authorities) in times of crisis, emergency, countering hybrid threats, and participating in state defense increase the readiness of state institutions to ensure the effective performance of the necessary functions (National Security Strategy of the Republic of Lithuania, 2002; 2017). Inter-institutional collaboration includes the exchange of information, sharing knowledge, and other resources, ensuring solutions and their implementation processes, based on different competencies and skills (Danzig et al., 2018).

In the context of ensuring security, collaboration between military and civilian organizations becomes especially important. Although the main function of the Lithuanian army and other institutions of the national defense system is to ensure the armed defense of the state, at the same time, the task is to carry out peacetime tasks by providing assistance to state and municipal institutions. The purpose of this presentation is to provide insights related to the best practices of collaboration between the Lithuanian military and the internal affairs system in managing crisis situations. The case of collaboration between the Lithuanian Armed Forces, the State Border Guard Service, and the Ministry of Interior in protecting the border with Belarus from illegal migrants was chosen.

The research uses the data collected by the interview method. The presentation summaries the good practices and overviews of lessons learned. The results of the study show that collaboration between the military and internal affairs institutions in managing the migrant crisis complies with the general principles of military-civilian collaboration in disaster relief. They include understanding the value of mutual collaboration, willingness to collaborate and mutual support. The essential aspects of collaboration are identified and presented, related to the distribution of functions, effective assurance of the collaboration process, changes in legal regulation, communication and information sharing, etc.

The presentation was prepared on the basis of the project "Study of the possibilities of creating an all-encompassing state defense system". The project is carried out in accordance with the 2020 order of the Minister of National Defense of the Republic of Lithuania. November 30 order no. V-925.

KEYWORDS

Inter-institutional collaboration; Military and civil collaboration; Best practices; Crisis management; Illegal migration; Lithuanian-Belarusian border.

REFERENCES

Danzig, R. J, Allen, J. R., DePoy, Ph. E., Disbrow, L. S., Gosler, J. R., Haines, A. D., Locklear III, S. J., Miller, J. N., Stavridis, J. G., Stockton, P. N., & Work, R. O. (2018). *A Preface to Strategy: the Foundations Of American National Security*. Laurel: The Johns Hopkins University Applied Physics Laboratory.

Kapucu, N. (2009). Interorganizational Coordination in Complex Environments Of Disasters: The Evolution Of Intergovernmental Disaster Response Systems. *Journal of Homeland Security and Emergency Management, 6*(1), 47. doi:10.2202/1547-7355.1498

National Security Strategy of the Republic of Lithuania (2002; 2017). Approved by Resolution No IX-907 of the Seimas of the Republic of Lithuania of 28 May 2002 (version of Resolution No XIII-202 of the Seimas of the Republic of Lithuania of 17 January 2017). Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/dc61fcd0fe8a11e6ae41f2dbc54c44ce?positionInSearchResults=0&searchModelUUID=4349d390-2854-417c-8bcf-464639d75fd9

Sarapuu, K., & Randma-Liiv, T. (2020). *Small States: Public Management and Policy - Making*. Handbook on the Politics of Small States, 55–69. doi: https://doi.org/10.4337/9781788112932.00010

Wilkins, P., Phillimore, J., & Gilchrist, D. (2016). Public Sector Collaboration: Are We Doing It Well And Could We Do It Better? *Australian Journal of Public Administration, 75*(3), 318–330. doi: https://doi.org/10.1111/1467-8500.12183

Decentralized Russia. What can we learn from the 1990s?

A. Głąb (1)

(1) War Studies University, Poland, a.glab@akademia.mil.pl

Russia has had the attribute of "federative" in its name for decades. However, at the time of the Russian Soviet Federative Socialist Republic it was federative only nominally, as it was the "federal union" for the Union of Soviet Socialist Republics. At the end of the 1980s, the political and economic processes that led to the collapse of the USSR intensified. The 1990s was a period of rapid and spontaneous search for a new form of system, using elements of the state's federal structure. The differentiation of the regional regimes also played a role. In some entities of the Russian Federation, stable systems have developed with a strong position of regional leaders, regardless of the overwhelming impression of internal "chaos".

Since 1991, the features of the political system of the Russian Federation have been difficult to be unequivocally assessed from the perspective of the concept of federalism. An efficient federal system is not only about institutions, but also about relations between them. While there are institutions in Russia which are formally necessary for the formation and functioning of the federal system, effective and stable relations have not been developed. When Vladimir Putin took the president's office, negotiations between administrative levels began to take place informally. However, through legal and political changes, the federal center wanted to increase the scope of control over regional authorities, not the effectiveness of managing federal relations as a whole.

The nature of federal relations requires entrenched democratic procedures, transparency over all institutions' decisions and trust between them. Over the past thirty years, federal and regional governments have not sought to strengthen any of these aspects. As a result, a quasi-federal system was created. It meets certain criteria of a federal state but with elements of strong centralization and authoritarian inclination weakening their significance.

The current system is a kind of prosthesis imposed on the significant differentiation of Russian entities in terms of socio-cultural, legal, economic, and political status. It remains the facade. Years of revision of the federal and regional law in order to unify it, the lack of equal economic potential as well as an inappropriate national policy have left many problems, that Russia may face as a result of weakening central control, frozen.

The trend of shifting responsibility for unpopular political decisions from the federal to the regional level began during the coronavirus pandemic. It was the heads of the regional executive power who started to be responsible for the introduction of restrictions in response to the situation within the entity. After the Russian invasion on Ukraine when the Western states began to impose economic sanctions, president Putin again ceded some competences in the field of anti-crisis policy to a lower level. However, the implementation of the rights granted requires financial resources which can be obtained mainly from the federal budget. The policy of making entities financially dependent on federal subsidies, which have been in place over the years, could not increase the regional economic potential.

Due to the complexity of this problem, it will be valuable to present the current trends within the quasi-federal state and to compare them with that observed in the 1990s, as well as to indicate the similarities and differences between them. The spectrum of the upcoming economic crisis will be another test of the relations between the center and the entities. It may become one of the most serious threats to the Russian Federation. In order to maintain political stability, the effective management of social discontent may depend on regional authorities. In return for their loyalty, they will expect financial aid from the federal authority. With growing social tension, the cost of retaining power will increase. Ultimately, this may lead to the relaxation of domestic politics and, if the federal financial and political guarantees are threatened, another spontaneous decentralization.

KEYWORDS

Russian Federation; Federal relations; Decentralization; Distribution of power; Economic crisis.

Ukraine's Resilience Against Russia: Challenges and Perspectives

V. Vdovychenko (1) and J. Bērziņš (2)

(1) Borys Grinchenko Kyiv University, Ukraine, vdovychenkov@gmail.com
(2) National Defence Academy of Latvia and BA Business School, Janis.Berzins01@mil.lv

Although not necessarily new, indirect and asymmetric methods of warfare have become more common in the last 30 years. This is the result of the development of new technologies and the rise of what the West calls "hybrid warfare," with the fabrics of the nation being increasingly targeted by hostile actors to achieve the ultimate objectives of warfare in the political realm as postulated by Clausewitz.[1] Since the threat is multilayered and targets the nation's very existence, war and defense should go beyond the armed forces and involve the whole of society, as discussed by Ludendorff back in 1935.[2] Although his ideas today are considered a relic in the West, the idea of contemporary warfare being a multilayered phenomenon going beyond the military realm since it is directly aimed against the constituent factors of the nation, including its people, is an important part of the strategy of malign actors, including countries. Therefore, the whole of society is a legitime target and should take part in defense and war efforts.

Since contemporary warfare targets a nation in its totality, defense must go beyond the traditional military realm. It must include the people, information system, culture, politics, economics, and infrastructure to increase the nation's resilience. One fundamental factor determining a country's resilience is the relationship between the social and the political realms. Data from the World Values Survey shows that, before the escalation of Russia's war against Ukraine, a considerable gap existed between both realms with antagonistic characteristics./footnoteRussia has been at war with Ukraine since 2014. The current stage should be considered as the escalation of the same conflict. At the same time, despite the National Security Strategy of Ukraine emphasizing the importance of resilience, an all-encompassing and comprehensive system of national resilience able to protect the society at the central, regional, and local levels does not exist.[3] Currently, the key challenges for establishing a system of national resilience in Ukraine are:

- At the institutional level:
  - no public institutions (bodies) responsible for coordinating the interaction of state and non-statestructures in the field of national stability at the state, regional and local levels, including risk management and capacity building;
  - lack of mechanisms and permanent formats of interdepartmental cooperation on issues of national stability at the state, regional and local levels;
  - weak methods for forecasting, preventing, and responding to risks and crises at different stages of their development, as well as plans to restore sustainable operation.
- At the methodological and inter-agency level:
  - weak common methodological approaches to assess national security risks, the state of relevant capabilities for the preparation, adoption, and implementation of strategic decisions;
  - insufficient level of development of the cybersecurity system, which does not guarantee the cyberresilience of national information resources;
  - low level of awareness of public officials as well as civil society institutions about information security requirements;
  - insufficient level of means and capabilities to effectively counter the hybrid and information war against Ukraine;
  - weak communication between public authorities, local governments, and the population.

Taking the above into account, a fair question to be answered is why Russia's war against Ukraine helped consolidate the Ukrainian nation and reduced the gap between the social and political realms resulting in greater resilience. This article aims to answer this question and present alternatives and solutions for the challenges mentioned above. It concludes by presenting lessons relevant to other countries facing similar challenges, including NATO member states.

National Security of the Republic of Poland in the light of diplomatic relations with the State of Israel

T. Michalowski (1)

(1) War Studies Academy, Poland, tom.mich021@gmail.com

We have witnessed in the recent years a complete deterioration in relations between Poland and Israel. The political clash on historical and political aspects, resulted in freezing the relationship between discussed countries. As some analysts said, this conflict not only harmed relations, but also strengthened negative stereotypes. Heated discussion and mutual accusations resulted also in weakening of economic and social programs and activities that those two countries conducted together among the time.

History and the present day have a significant impact on the shaping of relations between the Republic of Poland and the State of Israel, which translates into the image of both countries on the international arena. Therefore, the aim of the research in this work is to analyze the diplomatic relations between the Republic of Poland and the State of Israel and to determine the impact of these relations on the national security of the Republic of Poland. The theoretical research methods used in the work are analysis, synthesis, comparison, opposition, and inference. The analysis and synthesis were used to verify the available scientific literature and press materials on events and activities in the studied area. The comparison and juxtaposition allowed to show the differences in the security environments of the Republic of Poland and the State of Israel, the characteristics of strategic goals and the benefits of rebuilding and strengthening relations. Inference allowed to outline partial conclusions presented at the end of each chapter and final conclusions expressed at the end of this paper. Empirical methods were also used - diagnostic survey methods, including the survey method, the survey technique, and the survey questionnaire tool. The application of this method allowed for obtaining the opinion of students of the National Security Department of the Academy of Martial Arts on the impact of relations between the Republic of Poland and the State of Israel on the national security of the Republic of Poland.

By analyzing the relationship between the Republic of Poland and its Jewish national minority, before the establishment of the State of Israel, we can see that this relationship, although sometimes turbulent, was carried out on a very good basis, and Jews in Poland could enjoy freedoms and security that in other countries were not so much. sure. The turning point for these relations was, first, the loss of independence by the Republic of Poland because of the partitions of the 17th century. This event not only disturbed the functioning of the society inhabiting the territory of the Republic of Poland, but also caused an identity crisis among these people.

To sum up, diplomatic relations between the Republic of Poland and the State of Israel, despite their relatively short relationship, have a real impact on decisions made by the Polish government in areas relevant to national security. The most important reasons for this approach are: i) a common, centuries-old history and relationship, ii) the relationship between the internal and external policies of the state and the influence of external factors on these areas, and iii) strong economic and scientific cooperation. It should also be noted that the research conducted on the relationship between the Republic of Poland and the State of Israel and the impact of this relationship on the national security of the Republic of Poland has shown the need to intensify the activities undertaken within the described relations.

KEYWORDS

Diplomacy; Israel; Poland; Conflict; International relations; Reconciliation.

REFERENCES

Berridge, G.R. (2015). *Diplomacy: Theory and practice*. Chippenham: Palgrave Macmillan.
Chojnowski, A., & Tomaszewski, J. (2014). *Izrael*. Warszawa: Trio.
Cooper, A.F. (2013). *The Changing Nature of Diplomacy*. Oxford: Oxford University Press, 41.
Kitler, W. (2011). *Bezpieczeństwo Narodowe. Podstawowe kategorie, Uwarunkowania, System*. Warszawa: AON.
Szuchta, R. (2015). 1000 lat historii Żydów polskich. Podróż przez wieki. Warszawa: Demart S.A.
Constantinou, C. (2016). *The SAGE Handbook of Diplomacy*. Londyn: The SAGE.

Constructing the security agenda: contributions for its understanding

C. Coelho (1)

(1) AECHAR, Military University Institute of Portugal, coelho.cmr@ium.pt

The interpretation of security as a semantic field that goes beyond military and strategic studies has already been accepted. Critical theorists have not only learned the language of security to address economic, health, environmental and cultural challenges, but also to shape the problems, the policy agenda, and the solutions.

Based on this framework, this paper analytically relates the contextual drivers of security creation and how problem definition and agenda building in the governmental arena are determinant for an issue to be considered important, to the point of imposing the intervention of political power and shaping its framework (Cobb, & Elder, 1971; Rochefort, & Cobb, 1993, 1994a).

Thus, the general objective of this study is to develop a critical theoretical review, whose focus, taking as a reference the process of security agenda building, is to establish a conceptual and analytical relationship between two frames of reference: the field of public policies and the theory of securitization, in the area of international relations, introduced by the Copenhagen School (Buzan, 1983; Buzan et al., 1998; Buzan, & Hansen, 2019; Wæver, 1997).

Bearing in mind that public policy analysis, as a multidisciplinary field of study, aggregates theoretical contributions from various academic disciplines (DeLeon & Martell, 2006), the analysis was based on the presentation of the main theoretical issues aimed at understanding aspects of public policy formulation, through a short and medullar theoretical reflection on the salient processes that influence the stages of problem definition and the arrangement of issues as "security threats".

As a conclusion, it was observed the presence of a clear and unequivocal link between the two frameworks, which helps to understand the process of modelling and defining the problems tending to the construction and elevation of the security agenda as a policy of exception. In addition, it was concluded that security defined as the result of the political interpretation of public problems, assumes itself as the perfect attribute to selectively present evidence, to misrepresent opposing positions and to coerce all actors, including opponents, to the accept or consent of - almost - all means to achieve the intended political ends.

KEYWORDS

Agenda; Policy Cycle; Securitization.

REFERENCES

Buzan, B. (1983). *People, States, and Fear: The National Security Problem in International Relations*. Sussex: Wheatsheaf Books.

Buzan, B., & Lene H. (2019). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Buzan, B., Wæver O., & Wilde, J. (1998). *Security: A New Framework for Analysis*. London: Lynne Rienne Publishers.

Cobb, R. W., & Elder, C. D. (1971). The Politics of Agenda-Building: An Alternative Perspective For Modern Democratic Theory. *The Journal of Politics*, *33*(4), 892–915. doi: 10.2307/2128415.

DeLeon, P., & Martell, C. R. (2006). The Policy Sciences: Past, Present, and Future. J. Pierre, & B. G. Peters (Eds.), *Handbook of Public Policy* (pp. 31-48). London: SAGE Publications Ltd.

Rochefort, D. A., & Cobb, R. W. (1993). Problem Definition, Agenda Access, and Policy Choice. *Policy Studies Journal, 21*(1), 56-71. doi: 10.1111/j.1541-0072.1993.tb01453.x.

Rochefort, D. A. & Cobb, R. W. (1994). Problem Definition: An Emerging Perspective. In *The politics of problem definition: shaping the policy agenda* (pp. 1–31). Lawrence: University of Kansas Press.

Wæver, O. (1997). *Concepts of Security*. Copenhagen: University of Copenhagen.

How to defend Norway? An inquiry into the military-strategic conceptual defence debate in Norway after 2014

H. Saxi (1)

(1) The Norwegian Defence University College, hsaxi@mil.no

This article examines the debate within the Norwegian defence sector over a new military-strategic concept in the wake of Russian aggression against Ukraine, 2014–2022. It examines the debate within the Norwegian defence sector about how Norway's military forces should best be developed, structured, and employed to ensure that the Norwegian Armed Forces contributed to credible deterrence and defence.

Three main military-strategic alternatives have dominated this debate, supported respectively by adherents of what I will term the "traditionalists", the "modernists" and the "radials". Each of these schools of thought have put forward in the debate their own operational concepts for the Norwegian Armed Forces. Due to its specialized, technical, and partially classified nature, the debate was conducted only partially in public forums.

Adherents of the "traditionalist" school of thought argue that the Norwegian Armed Forces should remain a balanced force consisting of land, air and sea forces, and that Norway should seek to meet any aggression in all domains. This requires strengthening the whole force, particularly Norway's land forces, and requires building up the presence of the armed forces in the most exposed parts of Northern-Norway. In peacetime, such a force should aim for "deterrence by denial", signaling to the opponent that any attack would be risky, costly, and unlikely to succeed. If deterrence should fail, the force would strive to maintain control over most of Norwegian territory for as long as possible until allied reinforcements arrive.

The main alternative to the "traditionalist" school can be termed the "modernists". Its adherents argue that Norway cannot afford to build the balanced military forces supported by the "traditionalists", and that the results will be a minuscule force which will not offer credible deterrence, and which will be unable to defend the most exposed parts of the country if deterrence should fail. Instead, they argue for a less ambitious military-strategic concept. If deterrence should fail, they argue that the Norwegian Armed Forces should be structured and employed to achieve "operational denial" in Finnmark county and the northern maritime areas. Enemy forces should be located and engaged with long-range precision strike weapons and special-forces-type raids, but not symmetrically engaged in the land domain by mechanized forces. The aim is to impose high costs on the adversary and signal to allies that there is an active combat situation in Norway, encouraging allies to prioritise Norway for reinforcements.

Several other and more radical alternative concepts have also been proposed, but these have fewer adherents within the defence sector establishment. To broaden the alternatives which are discussed in this project, one radical proposal will be included – a so-called "deterrence by punishment" strategic-level concept. Adherents of this approach argue that Norway should attempt conventional "deterrence by punishment". That is, to signal a willingness to employ long-range precision strike weapons deployed from combat aircraft, surface, or subsurface vessels, to target political and strategic targets of vital importance to an opponent in case of an armed conflict. The purpose is to signal a willingness to impose prohibiting costs on an adversary in order to deter aggression. This is a far more offensive strategy at the strategic-level and runs contrary to traditional Norwegian security policy and military strategic thinking.

The article will seek to describe and explain the different positions, as well as to determine who in the defence sector supported which positions and discuss why they held these views. In order to do this, the article draws on written primary and secondary source documents in Norway and selected allied countries, as well as interviews with senior Norwegian officers and officials. Some of these written and oral sources will be classified, and as such can only provide background information which cannot be utilized or acknowledged in the project's published findings.

The following research questions will be examined: What are the main arguments of the adherents of the different military-strategic concepts? What strengths do they argue that their preferred strategy have, and what weaknesses do they find with the alternative concepts? How do outside observes, who do not fall into any of the main "camps", regard these competing concepts? To what extend are Norway's NATO allies aware of these debates, and how do they evaluate the different proposals? Who are the main adherents of the different schools of thought? When, where and how did they develop and put forward their proposals? What institutional affiliations do the members of a school of thought predominantly hold? Do particular institutions favour certain military strategies and operational concepts?

If so, why? What has been the main impact (if any) of these debates on Norwegian defence policy and strategy since 2014?

KEYWORDS

Norway; Defence; Military; Security; Strategy; Ukraine; Crisis; War.

NORAD Modernization: North American strategic deterrence beyond the Cold War and Canada's role

N. Glesby (1)

(1) University of Manitoba, Canada, glesbyn@myumanitoba.ca

NORAD is the binational defence command responsible for the aerospace warning, aerospace control, and maritime warning of Canada and the United States (Government of Canada, 2021, para. 1). As the "institutional centrepiece" of joint defence, NORAD is responsible for continental defence in today's multi-domain threat environment and requires updating (Fergusson, 2015, p. 197-198).

Near-peer (or peer) adversaries in Russia and China posses weapons technology that can hold North America hostage (Brewster, 2020, para. 7-8). Hypersonic weapons means that the existing NWS is no longer able to adequately detect threats to the continent. Not only does this leave North America vulnerable to kinetic attack, but this shortfall leaves a major gap in the strategic deterrence function that continental defence ensures (Fergusson, 2020, p.6). This lack of ability to defend the continent leaves U.S.-allied and aligned states in Europe and Asia vulnerable, as their security guarantees no longer hold as much credibility. In short, North American security is the first level of the post-World War II power structure, that seeks to fight conflict outside of North America.

Strategic deterrence vis-a-vis NORAD shows to competitors in the international arena that North America is able to defend kinetic missile strikes. The post-war American-backed alliance structure is based off the safety of North America. International peace and security depends on the ability to defend the continent, in order to commit to "overseas commitments or forward defence" (O'Shaughnessy, & Fessler, 2020, p. 3, 6, 13, 14).

The solution is twofold: First, the U.S. force-wide adoption of a cross-service Joint All-Domain Command and Control (JADC2) seeks to integrate information from every domain into an artificial intelligence/machinelearning algorithm that allows for siloes to be broken and move decision-makers ability to react further left of launch (O'Shaughnessy, & Fessler, 2020, p. 10-12).

Secondly, renewed investment by Canada in defence spending is crucial, within the context of the bilateral relationship. NWS replacement and reopening of missile defence conversations means these major infrastructure requirements demand more funding (Blatchford, 2022, para. 2-3). Refocusing is key to achieve Canadian national interests, most especially as American politicians begin to publicly complain about lack of action on this file by the Canadian government (Panetta, 2022, para. 7).

Canada's quick and urgent action in committing 40% of joint resources to continental defence will mean (Murray and Viotti, 1994, p. 68): First, retainment of the cooperative nature of the special CANUS relationship during an era of enhanced and reinvigorated great power competition. Secondly, achieve American (and by proxy, Canadian) strategic deterrence options to defend North America and retain the post-World War II security and defence structures.

KEYWORDS

Canada-U.S. defence relations; NORAD Modernization; Strategic deterrence; Joint All-Domain Command and Control; Defence spending; Great Power competition.

REFERNCES

Blatchford, A (2022). *Canada taking 'comprehensive look' at joining U.S. ballistic missile defense* [Online]. Retrieved from https://www.politico.com/news/2022/05/10/canada-eyeing-bold-and-aggressive-militaryoptions -to-defend-continent-00031349.

Brewster, M (2020). *Next-generation missiles could hold leaders hostage in times of conflict: top general* [Online]. Retrieved from https://www.cbc.ca/news/politics/hypersonic-vance-missile-threat-1.5486364.

Government of Canada (2020). *March 2020 - North American Aerospace Defense Command (NORAD)* [Online]. Retrieved from https://www.canada.ca/en/department-national-defence/corporate/reports-publications/ transition-materials/caf-operations-activities/2020/03/caf-ops-activities/norad.html.

Fergusson, J. (2015). The NORAD conundrum: Canada, missile defence, and military space. *International Journal 70*(2), 196-214. Retrieved from https://www-jstor-org.uml.idm.oclc.org/stable/24709457?seq=1.

Fergusson, J. (2020). *Missed Opportunities: Why Canada's North Warning System is Overdue for an Overhaul* [Online] Retrieved from https://www.macdonaldlaurier.ca/files/pdf/20191219_NORAD_Fergusson_COMMENTARY_FWeb.pdf

Murray, D.J & Vioti, P.R. (1994). *The Defense Policies of Nations: A Comparative Study.* Washington D.C.: Johns Hopkins University Press.

O'Shaughnessy, T.J., & Fessler P.M. (2020). *Hardening the Shield: A Credible Deterrent & Capable Defense for North America* [Online]. Retrieved from https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Hardening%20the%20Shield_A%20Credible%20Deterrent%20%26%20Capable%20Defense%20for%20Nor th%20America_EN.pdf.

Panetta, A. (2022). *U.S. Senator: Canada's a freeloader on defence and it's getting tiring*. Retrieved from https://www.cbc.ca/ news/world/us-senator-canada-freeloader-1.6448053.

European Security and Defence and the Ukraine Conflict

M. Cruz (1)

(1) IUM, Portugal, cruz.maf@ium.pt

Since its foundation, matters relating to the Security and Defence of the European Union (EU) have been very conditioned by the different political views of the Member States. Among the reasons for this lack of understanding, the issue of strategic autonomy and European military dependence on NATO and the US and the establishment of a common framework of threats affecting the whole of Europe deserve to be highlighted. Although some setbacks have been made in recent years, we have seen significant progress in the areas of the Common Security and Defence Policy, in response to both internal and international crisis contexts. The last invasion of Ukraine by Russia of February (24) this year produced very significant changes in the international strategic environment, greatly influencing the objectives and ambitions of the EU and NATO strategic documents, both approved moments after this event took place.

Among the main conclusions we can mention that the Strategic Compass unequivocally identifies the main threat to European space - Russia, a circumstance that has only been seen in recent years in relation to terrorism. Russia thus assumes a centrality in the catalogue of threats identified in the new European strategy, contributing to the strengthening of internal cohesion and, consequently, to the redefinition of European security and defence priorities. Without the Ukraine conflict, the Strategic Compass would certainly be a very different document. Probably less ambitious and realistic, but above all much less supported by Member States and European citizens.

In addition to identifying the need to develop military capabilities, this conflict also promoted enhanced cooperation with NATO, after having seen moments of great tension between the two sides of the Atlantic. The Ukraine conflict has therefore caused a new context of international strategic realignments, particularly between western powers. After years of relationship crisis and, in some matters of international policy, competition, the US and EU Member States now operate a convergence at various points of understanding. The identification of Russia as a threat to the entire Western soil is an important factor of unity between policy makers and among public opinions, around the defence of Western values.

The materialisation of the EU's progress in security and defence, contemplated in the Strategic Compass, especially at the level of the targets to be achieved, is very dependent on the direction that the Ukraine conflict will take. Most of these proposed goals have as a time horizon for implementation beyond 2023. A long period in which the fatigue of the conflict between Europeans and the economic consequences may lead to a change in public opinion and, consequently, the political will to recognise Russia as the main threat unanimously. Strengthening cooperation with NATO also entails major challenges for the future of EU Security and Defence Policies, resulting from increased US influence on European soil, with a reflection not only on military issues, but also on energy and international subjects, with particular relevance to the relationship with China.

KEYWORDS

Security and Defense Policy; European Union; NATO; Ukraine.

The missing tools for peace in war with WMDs

J. Kuula (1)

(1) Emergency Services Academy Finland, Jaana.Kuula@gmail.com

Russia attacked on Ukraine without justified cause on 24th February 2022 and its brutality has been ongoing ever since. Strikes against Ukrainian defence forces, infrastructures and civilian people have been carried out with the most vicious means and methods, of which many are war crimes according to international law. Among those are also weapons of mass destruction (WMDs), even though one can argue of what precisely is their illegal use. As an example, is it only forbidden to release these particular destructive chemical, biological, radiological/nuclear and explosive agents and projectiles on built societies and people, or is also criminal to threaten and blackmail other parties with them? And, most importantly, how can anyone enforce peace by interrupting aggressive war and genocide, when the invader is ready to launch nuclear missiles at any minute?

Despite of substantial humanitarian aid and economic and material support to Ukraine, western democracies have not been able to end the war by negotiations or any other way. Particularly, due to the nuclear threat by Russia, they have been hindered from ending its hostilities towards Ukraine by direct military force. This alone raises a question, whether there is any practical way to turn down an irrational military player who has WMDs, especially nuclear weapons. In this case, Russia has also accelerated war with falsified accusations of biological weapons and threats of using chemical weapons. It has also shelled and invaded Ukrainian nuclear power plants. This kind of operation can be defined as an indirect use of nuclear weapons, because shelling nuclear power plants and making them out of order can lead into similar disasters as exploding nuclear missiles and bombs. In addition, Russia has used other unethical weapons like hypersonic, thermobaric and incendiary weapons against civilians in Ukraine, which also are comparable with WMDs.

In all, Russia's actions in Ukraine indicate that many other harmful methods in addition to chemical, biological and radiological/nuclear weapons need to be forbidden and defined as weapons of mass destruction. Additionally, not only the direct use of WMDs, but also their indirect use by triggering explosion or other uncontrolled release of critical substances should be criminalized and forbidden. Furthermore, hindering other parties from building peace and delivering humanitarian aid by threatening and blackmailing with WMDs should be made impossible and defined and judged as a war crime. Finally, outside of these measures, new technical methods should be developed for preventing the delivery and release of WMDs into the protected areas, and disabling their launch from the invader's premises. If none of these, or any other effective methods, will be taken in use, similar situations what Russia is making with WMDs and other inhumane means for Ukraine and other countries will be repeated in other countries as well. All of them will possibly not end in a peaceful manner, but in a nuclear disaster instead. Along with the climate change, and a lack of food and fresh water, referable conflicts become more likely, so it is now when the tools for making peace in case of WMDs should be taken in use.

KEYWORDS

Russian invasion; War crime; WMD; Nuclear weapon; Peace enforcement.

REFERENCES

The details and actual data of Russia's invasion to Ukraine is based on public news and professional social media in Western Europe and USA.

Evacuation or sheltering-in-place: comparative analysis of the Israeli and Ukrainian civil defence measures

J. Przybylak (1)

(1) War Studies University, Poland, j.zych@akademia.mil.pl

In most of developed countries, various types of air raid shelters and protective spaces are used for civil protection purposes. However, the level of their preparation an availability varies considerably (Kruszka, Chmielewski, Sobczyk, 2020, p. 11). After the end of the cold war, the majority of countries have significantly reduced the number of shelters, previously maintained for the case of nuclear war. The possibility of an armed conflict has never been eradicated, however, for years it has been perceived as a very limited threat. Optimistic approach to the international relations and focus on non-military challenges resulted in noticeable deterioration of civil defence systems, including the preparation of protective structures (Michailuk, 2019, pp. 137-138). Instead of that, the most prominent trend has been to focus on planning evacuation of civilians within the framework of crisis management systems, designed both for the case of military and non-military threats to the population.

The full-scale Russian aggression against Ukraine in February 2022 as well as other conflicts in the world that broke out over the last few years have proven that the military threat to the civilian population is real and it requires new approach to the problems of shelters and evacuation. In order to compare these issues in the context of regular, full-scale war between states as well as prolonged asymmetric conflict between a state and non-state actor, the examples of Ukraine and Israel were chosen for further detailed analysis. The ongoing conflict in Ukraine has proven that evacuation of the population is not always possible during hostilities, particularly in situations where the adversary does not comply with basic requirements of international humanitarian law (DFS, 2022, pp. 4, 7-8). This is also the case of Israel, where sheltering-in-place during rocket and mortar fire coming form the Gaza Strip and Southern Lebanon is favored over organized evacuation (Shaham & Elran, 2016, pp. 45-53). Therefore, the author will deliberate on the assumption that protective structures are sine qua non of effective civil protection during modern armed hostilities, regardless of the type of warfare.

In the first part of the paper the author will focus on the civil defence measures in Israel and unique Israeli approach to sheltering-in-place. Reasons for long-lasting aversion of the political and military establishment towards organized evacuation of civilians will be analyzed in the context of the most recent escalations of the Israeli-Palestinian conflict. Legal and practical solutions regarding the construction of easily accessible shelters and protective spaces will also be described and the idea of societal resilience in Israel will be discussed. Finally, the author will present the benefits and drawbacks of remaining 'on the frontline' by the majority of Israelis affected by the rocket and mortar fire. The analysis will be based on selected literature (eg. Morag, 2018; Padan & Elran, 2019; Shapiro & Bird-David, 2016) as well as the author's own empirical research conducted in SouthWestern Israel.

The second part of the paper will be dedicated to the dilemma of evacuation of civilians form war-affected Ukraine and major problems related to this issue, including the difficulties to create humanitarian corridors, noncompliance with international humanitarian law by the Russian forces and obstacles to the Ukrainian Armed Forces and other state services occurred as an effect of individual, unorganized evacuation of civilians during the first phase of the war. Significance of shelters availability for those remaining under fire will also be described. Unlike Israel, where most of households and public buildings have been equipped with private shelters or protective rooms, in case of Ukraine the majority of analysis will focus on ad-hoc temporary shelters which have never been fully prepared to play this role (such as cellars, metro stations, etc.). Since the analyzed issue refers to the most recent events that have not been researched in scientific literature yet, this part of the paper will be based mostly on reports published by various humanitarian organizations, instructions of the Ukrainian authorities (eg. Center for Strategic Communications and Information Security, 2022) as well as relevant press reports.

In the final part of the paper the author will focus on general conclusions which can be drawn from the analyzed cases and utilized in order to form recommendations for other countries dealing with the issue of outdated, inadequate civil defence systems.

KEYWORDS

Civil defence; Civil protection; Armed conflict; Shelters; Evacuation.

REFERENCES

Data Friendly Space (2022). *Ukrainian Crisis – Situational Analysis (07 June 2022).* Retrieved from https://reliefweb.int/report/ukraine/ukrainian-crisis-situational-analysis-07-june-2022.

Kruszka, L., Chmielewski, R., & Sobczyk, K. (2020). The concept of experimental research on the behavior of sand cover material for protective shelters for civilians. *Safety Engineering of Anthropogenic Objects*, *25*(1), 1116, doi: 10.37105/iboa.51.

Michailuk, B. (2019) Schrony i ukrycia: wybrane problemy współczesnego budownictwa ochronnego. In: E. Cieślak, H. & Wyrębek (Ed.). *Od bezpieczeństwa jednostki do bezpieczeństwa międzynarodowego* (pp. 137-156). Iedlce: Wydawnictwo UPH.

Morag, N. (2018). *Comparative Homeland Security*. Hoboken: Wiley.

Padan, C., & Elran, M. (2019). *The "Gaza Envelope" Communities: A Case Study of Societal Resilience in Israel (2006–2016)*. Tel Aviv: Institute for National Security Studies.

Shaham, Y., & Elran, M. (2016). Evacuation of Israeli Communities during an Emergency: Dilemmas and Proposed Solutions. *Strategic Assessment*, *19*(3), 45-57.

Shapiro, M., & Bird-David, N. (2016). Routinergency: Domestic Securitization in Contemporary Israel. *Environment and Planning D: Society and Space*, *35*(4), 637-655, doi: 10.1177/0263775816677550.

Center for Strategic Communications and Information Security (2022). *U razi nadzvychajnoji sytuatsiji abo vijny*. Retrieved from https://www.mil.gov.ua/content/pdf/NS-WAR.pdf.

The role of territorial defence in the national crisis management system. Case study: Poland

A. Bartosiewicz (1)

(1) War Studies University, Poland, adrian.bartosiewicz98@gmail.com

Wojska Obrony Terytorialnej – WOT (The Territorial Defence Forces) are the main part of the armed forces of the Republic of Poland responsible for supporting the crisis management system in Poland. The commander of The Territorial Defence Forces, in accordance with Ustawą o Obronie Ojczyzny (the Homeland Defence Act), is responsible for the overall introduction of the armed forces into counter-crisis operations. This places a new responsibility on the formation and prioritises tasks related to supporting public administration during non-military crisis situations. This seems to be a rather innovative solution due to the territorial nature of the formation, the soldiers' familiarity with the area of operations and the location of command structures on the same basis as the public administration in the country.

The aim of this study is to determine the ability of The Territorial Defence Forces to support the efforts of the public administration aimed at countering any crisis situation of a non-military nature.

The following research methods will be used: Comparative method, process tracing and case-oriented research, qualitative data analysis, empirical data analysis, participatory observation method. Crisis management theory, Ustawa o Zarządzaniu Kryzysowym (the Crisis Management Act) and Ustawa o Obronie Ojczyzny (the Homeland Defence Act) were used to conduct the research.

The results of the research allow us to conclude that The Territorial Defence Forces have specialised equipment and appropriate structures located at each level of public administration allowing for effective countercrisis actions and have the ability to bring other types of forces from the armed forces into action (Zespoły Oceny Wsparcia, Support Assessment Teams).

At the same time, it is noted the need to increase the ability of territorial soldiers to carry out actions of a non-military nature and the necessity to modernise the formation by introducing a system allowing rapid exchange of information with representatives of public administration. It is also noted the need to introduce a clear on-call system for territorial soldiers allowing them to take full advantage of their potential due to the need to combine service with private and professional life. The competence of individual soldiers should also be strictly defined in order to use their skills and experience for operations in the field.

KEYWORDS

The Territorial Defence Forces; The Crisis Management Act; The Homeland Defence Act; Crisis management; Public administration; Counter-crisis operations.

REFERENCES

Bartosiewicz A. (2020). *Porównanie koncepcji funkcjonowania obrony terytorialnej wybranych państw w kontekście kształtowania się wojsk obrony terytorialnej w Polsce*. Warszawa: Akademia Sztuki Wojennej.

Czarnecki D. (2015). Zarządzanie kryzysowe na szczeblu krajowym - organizacja i funkcjonowanie. *Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje*, 20, Warszawa.

Gąsiorek K., & Kittler W. (2005). *Wojskowe wsparcie władz cywilnych i społeczeństwa*. Warszawa: wydawnictwo Akademii Obrony Narodowej.

Goliński A., & Kędzierska M. (2013). *Planowanie cywilne w systemie zarządzania kryzysowego*. Centrum NaukowoBadawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego Państwowy Instytut Badawczy, Józefów.

Jakubczak R. (2014). *Współczesne Wojska Obrony Terytorialnej*. Warszawa: wydawnictwo Bellona.

Jakubczak R. (2020). *Powszechna Obrona Terytorialna w Bezpieczeństwie Narodowym RP*. Warszawa: wydawnictwo Fundacja Historia i Kultura.

Marczak, J. (2006). *Zadania obronne samorządu terytorialnego*. Warszawa: wydawnictwo Akademii Obrony Narodowej.

Marszałek M. (2014). *Ewolucja systemu zarządzania kryzysowego NATO*. Warszawa: wydawnictwo Akademii Obrony Narodowej.

Michailiuk, B., Stempień, J., & Denysiuk, I. (2021). *Siły Zbrojne Rzeczpospolitej Polskiej w realizacji zadań z zakresu zarządzania kryzysowego*. Warszawa: wydawnictwo Akademii Sztuki Wojennej.

Michalak A. (2020). *Działania taktyczne wojsk obrony terytorialnej*. Warszawa: wydawnictwo Akademii Sztuki Wojenne.

Morawski A. (2014). *Wykorzystanie potencjału organizacji pozarządowych w procesie zarządzania kryzysowego*. Warszawa: Uniwersytet Warszawski,.

Otwinowski W. (2016). *Podstawy zarządzania kryzysowego i systemu obronnego*. Poznań: wydawnictwo Wyższej Szkoły Handlu i Usług.

Paszyn M., Kordowski M., & Zalewski W. (2016). *Koncepcja obrony terytorialnej w Polsce*. Warszawa: Narodowe centrum studiów strategicznych.

Pawłowski J., Zdrodowski B., & Kuliczkowski M. (2020). *Słownik terminów z zakresu bezpieczeństwa*. Toruń: wydawnictwo Adam Marszałek.

Praca Zbiorowa. (2018). *Wojska obrony terytorialnej stan obecny pożądane kierunki zmian*. Warszawa: Neptun fundacja Stratpoints.

Reczkowski R. (2017). *Współczesne Wojska Obrony Terytorialnej – zadania struktura i potencjał*. Kraków: Dowództwo Wojska Obrony Terytorialnej.

Tocicka J. W. (2020). *Zarządzanie kryzysowe w społecznościach lokalnych — studium przypadku miasta stołecznego Warszawy*. Warszawa: wydawnictwo DiG.

Wojciech H., & Falkowski M. (2018). *Wojska Obrony Terytorialnej Wczoraj i dziś*. Toruń: wydawnictwo Adam Marszałek.

Załęski K. (2018). *Siły zbrojne teoria i praktyka funkcjonowania*. Warszawa: wydawnictwo Difin.

Increasing resilience against contemporary forms of warfare: comprehensive defense in Latvia

J. Bērziņš (1)

(1) National Defence Academy of Latvia and BA Business School, Janis.Berzins01@mil.lv

After Russia's actions in Crimea and Eastern Ukraine, many think-tankers, policymakers, and scholars became convinced that the next Russian military action would happen in the Baltics. The underlying presupposition is that, first, the Russian President Vladimir Putin wants to recreate the Soviet Union; second, that invading and annexing the Baltic states is one of the necessary steps for achieving this objective; third, that the Russian speaking population could be easily used to support subversive operations in a Crimea-like scenario. At the operational level, this was to be done by employing what became known as Russian Hybrid Warfare tactics, which would be based on the Gerasimov Doctrine.

A serious problem with this assumption is that it projects falsified strategic objectives and military instruments to be employed by Russia based on a narrative created by the West. The Russian strategic considerations and military concepts differ from the Western conceptualisation. The Russians have their own concepts based on their own military thought. They use the term Hybrid Warfare to refer to the allegedly American and NATO strategy of creating colour revolutions to promote social and political destabilisation in targeted countries. The Gerasimov Doctrine does not exist in Russia.[1] The Russians refer to their own way of warfare as "New Generation Warfare."[2]

Within this strategic framework, the Baltic countries are constantly under non-kinetic attack by nonmilitary and military instruments. Among these are psychological, information, and influence operations, including financing pseudo NGOs for achieving political goals, disinformation campaigns, and strong military posturing near the Baltic countries' borders. The Russian strategy for the Baltic states is multi-layered and chiefly determined by Russia considering them part of the West. As a result, since the threat is multi-layered and presents a comprehensive challenge, Latvia has developed its own comprehensive defence strategy.

The objective of this article is to analyse the evolution of Latvia's defence strategy from the 1990's until its current form of comprehensive defence. To this end, the main defence and security documents were analysed and structured to establish the process of evolution of Latvia's security policy as a reflection of the evolution of the threat perception by Latvian policy makers and experts on the matter. It presents the current system of comprehensive defense that is still being implemented.

It concludes that Non-kinetic instruments of warfare are gaining importance to achieve military strategic objectives. At the same time, kinetic instruments might be used to reach non-military strategic objectives, blurring the traditional division into military and non-military means of warfare. As a result, the first step to evaluate the instruments a country might use against an opponent is to determine its strategic objectives.

Also, that, in open-source discussions, Russia's strategic goal in the Baltic states is to stimulate a process described in literature as Finlandization. It can be achieved by kinetic or non-kinetic means, although a combination of the two is also possible. In the case of the Baltic states, Russia has chosen non-kinetic means until now. This is mostly the result of NATO's reassurance and deterrence actions, but also the Baltic states' development of new defence capabilities. Therefore, one should not underestimate the relevance of military deterrence in the region. An important point to be taken into consideration is that the operationalization of non-kinetic warfare, especially information, psychological, and influence operations, depends very much on the opponent's idiosyncratic fragilities. As a result, deterrence has to be mostly by denial. This means that it surpasses the mandate of the military and belongs in the political realm.

Finally, considering the above, the Latvian Ministry of Defence has initiated several programs to establish a reliable system of comprehensive defence, in which society's role is fundamental. The results are already noticeable. These actions have been focusing on both increasing enlistment in the National Guard and raising the society's awareness and resilience in case of military or non-military crises.

KEYWORDS

Latvia; Comprehensive Defense; Hybrid War; Society; Resilience.

Disinformation: Towards improved situational awareness

M. Alaraatikka (1), P. Koistinen (2), M. Kaarkoski (3), A. Huhtinen (4) and T. Sederholm (5)

(1) National Defence University, Finland, milla.alaraatikka@mil.fi
(2) National Defence University, Finland, pekka.koistinen@mil.fi
(3) National Defence University, Finland, miina.kaarkoski@mil.fi
(4) National Defence University, Finland, aki.huhtinen@mil.fi
(5) National Defence University, Finland,teija.sederholm@mil.fi

A vital part of modern day national and information security is the capacity of public authorities to detect and counter disinformation, and other intentional efforts of malicious information influencing. In order to succeed at detecting and countering disinformation, public authorities need to improve their situational awareness about disinformation and other malicious influencing efforts. Situational awareness refers to being aware about what's happening and what might happen next while deciding how to act. Furthermore, countering disinformation and other malicious information influencing usually includes communicating fact-based information to citizens. It is essential that public authorities can communicate clearly, on time, and in constructed manner when a possible crisis occurs. As a part of the IRWIN-project (Information Resilience in A Wicked Environment) we have studied the challenges public authorities face when communicating in disinformative and complex spaces such as social media. In addition, we have analyzed public authorities' own experiences as targets of disinformation. These studies show that public authorities face major challenges in detecting and countering malicious information influencing as well as communicating effectively in social media. Our results show that the authorities felt that open decision-making processes, as well as the transparency and openness of their organizations are factors that render them vulnerable to disinformation. From the perspective of developing improved situational awareness it is evident that public authorities need more coordinated and top-down organized strategies on how to detect and counter disinformation.

Utilizing these previous findings, we organized three security cafés around Finland. In these cafes, public authorities had an opportunity to further discuss topics relating to their situational awareness about malicious information influencing, and their preparedness in relation to future communication challenges. The applied security café - method is based on World café method, which is an efficient format for hosting group-level dialogue. It is especially useful for increasing the understanding of emerging issues. Our aim was to further investigate how to improve public authorities' capacity to recognize malicious information influencing and to communicate effectively with the public. This was accomplished by collecting ideas and thoughts from public authorities themselves. The collected data is analyzed using inductive content analysis.

We will present our findings on these discussions by focusing on three questions: 1) What challenges and opportunities public authorities feel they face when preparing for information influencing beforehand? and 2) How public authorities could gain a better situational awareness about disinformation and information influencing) 3) How communications towards citizens could be improved?

KEYWORDS

Communications; Disinformation; National security; Public authorities; Social media.

ACKNOWLEDGEMENTS

Taiwan's Security: civilian control and external threat

S.-S. Wu(1)

(1) Rabdan Academy, United Arab Emirates, shangwu@ra.ac.ae

Together, the concepts of civilian control and external threats are a pair of concepts offer fresh insight into Taiwan's defence. In the face of increasingly serious threats from China in recent decades, while Taiwan should be cautiously developing its defence, the reality is somewhat different. In the mid-2000s, Taipei slowed down its pace of defence build-ups, including failing to acquire submarines, leading to Beijing's superiority with its massive military modernisation. In the 2000s and 2010s, both ruling parties constantly marginalised conscription by adopting the all-volunteer forces (AVF) policy, also reducing Taiwan's deterrence against China. While these two issues with significant impacts on Taiwan's defence differ with regard to reasons, execution, and alternatives, both were initiated by civilian sectors. Furthermore, elected administrations have their respective defence strategies with varying. Therefore, civilian control over the military in Taiwan has been remarkable, despite some constraints. The phenomenon of elected political elites shaping Taiwan's defence against its predominant external threat, China, presents a democratic perspective on understanding the evolving security outlook of this international hotspot.

Civilian control and external threats are fundamental aspects of civil-military relations (CMRs). External threats usually offer a rationale for a country to establish and maintain armed forces, which are supposed to be strong enough to cope with potential enemies. A formidable military for external threats, however, could be detrimental to domestic society. Preventing the military from applying its coercive power domestically is the main purpose of civilian control. As civilian political leadership is accountable to the people under a democratic mechanism, it has greater legitimacy than its military counterpart in decision-making on security-related issues, despite the latter's greater knowledge on defence. Therefore, civilian leaders have the right to be wrong (Feaver, 1996, pp. 150-154). Aside from legitimacy, as civilian leaders have broader concerns, security may be compromised.

The external threat that Taiwan's civilian leadership faces is severe. Unlike other territorial disputes over a few islands and waters, China's territorial claim covers all of Taiwan; the latter consequently faces the highest level of external threat: one that targets its survival. The two regimes across the Taiwan Strait — the Republic of China (ROC) in Taipei and the People's Republic of China (PRC) in Beijing — have not formally settled their relations since the former lost the Chinese civil war and fled to the island in 1949. The PRC sees Taiwan and the ROC as a legacy from the civil war and claims its legitimacy to unify the island, with the use of force having been a policy option. This external threat was not serious in the last century, when China lacked adequate air and naval power and the potential American intervention served as a deterrent, in addition to the Strait serving as a strategic obstacle for the former's invasion. The crisis of 1995/1996 confirmed the geostrategic landscape around Taiwan, and inspired China to endeavour towards finding solutions. Thereafter, Beijing's rising military power, both to project forces across the Strait and to deny Washington's intervention, has favourably reshaped its military balance with Taipei. Whether and how long Taiwan can stand alone if China attacks, in the absence of the United States, has become a substantial issue than before.

Against this backdrop, this paper raises several questions. What are the dynamics between external threat and civilian control in Taiwan and how do these paly out? What are the pros and cons of each civilian leadership in dealing with external threats? How much leeway does the Taiwanese civilian leadership have the right to be wrong in the context of the Chinese threat? To answer these, this paper will be divided into three parts. The first section reviews civilian control and external threats as an approach to studying Taiwan's defence. Then, the dynamics between civilian control and external threats during the four civilian administrations are examined. Next, major factors and impacts in the dynamics are illustrated with an estimation of the potential development on the island.

KEYWORDS

Civilian control; External threats; Taiwan; China; Defence strategy; Conscription.

REFERENCES

Cabestan, J. P. (2016). Cross-strait integration and Taiwan's new security challenge. In G. Schubert (Ed.), *Taiwan and the 'China impact'* (pp. 282-300). London: Routledge.

Chase, M. S. (2008). Taiwan's arms procurement debate and the demise of the special budget proposal: domestic politics in command. *Asian Survey, 48*(4), 703-724. doi: https://doi.org/10.1525/as.2008.48.4.703

Cole, B. D. (2006). *Taiwan's security: History and prospects.* London: Routledge.

Feaver, P. D. (1996). The civil-military problematique: Huntington, Janowitz, and the question of civilian control. *Armed Forces and Society, 23*(2), 149-178. doi: https://doi.org/10.1177/0095327X9602300203 Fravel, M. T. (2002). Towards civilian supremacy: Civil-military relations in Taiwan's democratization. *Armed Forces & Society, 29*(1), 57-84. doi: https://doi.org/10.1177/0095327X0202900104

Jacobs, J. B. (2012). *Democratizing Taiwan.* Boston: Brill.

A Binding Model of Military Police of Santa Catarina State

A. Rodrigues (1) and J. Nascimento (2)

(1) Universidade do Estado de Santa Catarina, Brazil, ana.grillo@udesc.br
(2) Instituto Superior de Ciências Sociais e Políticas, Portugal, jlnascimento@iscsp.ulisboa.pt

Commitment in the workplace and, in particular, organizational commitment is one of the most studied outcomes in strategic human resources management (Beer, Boselie, & Brewster, 2015; Walton, 1985). Commitment is "a force that binds an individual to a course of action of relevance to one or more targets" (Meyer & Herscovitch, 2001, p. 301). Moreover, commitment may be unidimensional or multidimensional (Meyer, & Herscovitch, 2001). One of the most used models of commitment has been the Three Components of Commitment Model, established by Meyer and Allen (1991) and taken up again by Meyer and Herscovitch (2001).

However, more binding variables exist (Solinger, van Offen, & Roe, 2008). In this line, this research aims to propose and estimate a bonding model that involves the relationships between Organizational Commitment, Consent, and Entrenchment.

According to the Three Components Model (Meyer & Allen, 1991; Meyer & Herscovitch, 2001), Organizational Commitment has an Affective component, a Normative one, and a Continuance component. The affective component is an emotional linkage to the organization through identification with it and, therefore, of an emotional nature. Normative Organizational Commitment, on the other hand, has to do with the individual's duty to the organization and, therefore, is more of compliance than an emotional nature. Finally, the continuance component is more behavioral and involves the costs associated with changing the organization.

Despite being the object of various studies (Klein, Molloy, & Cooper, 2009), this model has some critics. According to Solinger et al. (2008), organizational commitment is unidimensional, corresponding only to the affective component. The normative component would reach the "normative of stealing," which corresponds to "the value of approval and the value of disapproval planned outcomes from significant others" (Solinger et al., 2008, p.77). Moreover, continuity is a "Utilitarian outcomes (i.e., potential rewards and punishments associated with the behavior) are generally assessed with an expectation-value paradigm" (Solinger et al., 2008, p.77). Along these lines, Klein, Molloy, & Brinsfield (2012) reconceptualized the

commitment construct from a one-dimensional perspective. Thus, "commitment should be viewed as a particular type of bond [...] defined [...] as a volitional bond reflecting dedication and responsibility for a target" (Klein et al., 2012, p. 131).

In the Brazilian context, several studies, based on Solinger et al. (2008), have critically analyzed organizational commitment, focusing more on organizational attachment processes (Tomazzoni, Costa, Antonello, & Rodrigues, 2020). According to Tomazzoni et al. (2020), organizational bonds are Organizational Commitment, Consent, and Entrenchment.

Given the above, the following hypotheses were formulated:
H1: Organizational Commitment positively influences Entrenchment.
H2: Organizational Commitment positively influences Consent.
H3: Consent positively influences Entrenchment.

These hypotheses support the structural model we propose to analyze and estimate in this investigation (Figure 1).

Figure 1 – Proposed model

The proposed model assumes that the influence of organizational commitment on Entrenchment is mediated by Consent.

The study contributes to a better understanding of organizational bonding processes and the relationships between the various variables associated with this process.

KEYWORDS

Organizational Commitment; Consent; Entrenchment; Military Police of the State of Santa Catarina.

REFERENCES

Beer, M., Boselie, P., & Brewster, C. (2015). Back to the Future: Implications for the Field of HRM of the Multistakeholder Perspective Proposed 30 Years Ago. *Human Resource Management, 54* (3), 427-438. doi: 10.1002/hrm.21726. Retrived from URL.

Klein, H. J., Molloy, J. C., & Brinsfield, C. T. (2012). Reconceptualizing workplace commitment to redress a stretched construct: Revisiting assumptions and removing confounds. *Academy of Management Review, 37*(1), 130-151. doi: http://dx.doi.org/10.5465/amr.2010.0018. Retrived from URL.

Klein, H. J., Molloy, J. C., & Cooper, J. T. (2009). Conceptual foundations: Construct definitions and theoretical representations of workplace commitments. In: H. J. Klein, T. E. Becker, & J. P. Meyer (Eds.), *Commitment in organizations: Accumulated wisdom and new directions* (pp. 3-36). New York: Routledge Taylor & Fracis Group.

Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resources Management Review, 1* (1), 61-89.

Meyer, J. P., & Herscovitch, L. (2001). Commitment in the workplace: Toward a general model. *Human Resource Management Review, 11*, 299-326.

Solinger, O. N., van Olffen, W., & Roe, R. A. (2008). Beyond the tree-component model of organizational commitment. *Journal of Applied Psychology, 93* (1), 70-83. doi: 10.1037/0021-9010.93.1.70. Retrieved from URL.

Tomazzoni, G.C, Costa, V.M.F., Antonello, C.S. & Rodrigues, M.B. (2020). Os Vínculos Organizacionais na Percepção de Gestores: comprometimento, entrincheiramento e consentimento. *RAC*, *24*(3), 245-258.

Walton, R. E. (1985). From control to commitment in the workplace. *Harvard Business Review, March-April*, 77-84.

Perception of security situation on the Korean Peninsula among international community

M. Blicharz (1)

(1) War Studies University, Poland, m.blicharz@akademia.mil.pl

East Asia is a region geographically far removed from Europe, but due to the globalization and international dependencies, problems on the other side of the globe have an impact on the situation in Europe and should be discussed globally. The principles of submitting this article are to indicate security determinants in East Asia and present result of research regarding perception of security situation on the Korean Peninsula among international community.

After the methodological introduction, the author will analyze the factors that have a key impact on the security situation in the region, which is main subject of research. Korea's bilateral relation with Japan, which is the important player in the region, is a complex problem in East Asia. The period of the Japanese occupation and unresolved problems of World War II including "comfort woman" issue, despite the years, are still an obstacle to the normalization of mutual relations and cooperation in the field of security. This is especially important in the context of American involvement in the region, which is based on strong alliances with both countries - Japan and Republic of Korea. Discussing security of Korean Peninsula, it is obvious to explain inter-Korean relations, which affect international security significantly and are widely commended in the world – what is important to underline – in different way than on Korean Peninsula. As a part of inter Korean relations, case of unification of peninsula into one country will be presented – being one of the important topic discussed on Korean Peninsula, but mostly ignored in other parts of the world.

Second part of the article present result of empirical research regarding security situation in the region. Author will explain data corresponding with feelings of individuals about security on Korean Peninsula, inter-Korean relations and possibility of reunifaction of divided country. The data includes variables such as respondents' gender, place of living, level of education, status of military service, knowledge of the region, experience with travelling to Korea etc.

Figure 1 – Place of residence of responders (red color)

KEYWORDS

International security; Korean Peninsula; East Asia.

The Baltic Sea Islands and Their Impact on the Regional Security

Z. Sliwa (1) and H. Helseth (2)

(1) Baltic Defence College, Estonia, Zdzislaw.sliwa@baltdefcol.org
(2) Baltic Defence College, Estonia, Hans.helseth@baltdefcol.org

Over the last decades, the islands of the Baltic Sea have proved to be an important factor due to their geostrategic location. This is reinforced by the respective Exclusive Economic Zones (EEZ), by access to natural resources and control of the Sea Lines of Communication (SLOC) – all critical aspects of the coastal states' economy. A similar situation exists elsewhere. In Asia, in the South China Sea, the multilateral and bilateral disputes are topics of concern for politicians and military leadership both regionally and globally. The same type of disputes exist with regards to the Senkaku/Dioyudao Islands and Kurile Islands. Lately, Svalbard, the Norwegian archipelago in the Barents Sea and other islands in the Arctic, have triggered quite some interest connected with the construction of military infrastructure to control naval and commercial traffic and rich natural resources. During the Russian large-scale exercise 'Zapad 2017', assumptions were made that one of the scenarios represented an amphibious invasion of Svalbard. This island group has been described as NATO's Arctic 'Achilles' Heel'. Lately, during the Russian war against Ukraine, the tiny Snake Island was seen as a symbol and at the same time strategically important for both Russia and Ukraine becoming an arena of intensive fighting.

Similarly, the Baltic Sea islands have now come back into the limelight. Dominance in the Baltic Sea Region has been inextricably linked to naval power all the way back to the age of the Vikings. Denmark, Sweden, the Hanseatic League, Germany, Russia and later the USSR, all considered the Baltic Sea an area for their exclusive interest for transportation, economic development and military operations. In no other seas has this been demonstrated more clearly, not only in a historical sense but also very much today. In a littoral sea, the coastline and in particular any islands will have very high importance, in contrast to the world's oceans.

During the Cold War, the Warsaw Pact dominated the Baltic Sea. It controlled the coastline from Travemünde to Leningrad, and Sweden and Finland remained staunchly neutral. Still, German and Danish submarines and missile boats, extensive mine warfare and maritime aircraft were present to deny the Warsaw Pact access to the North Sea through the Danish Straits, which constituted – and remains today – a strong card firmly in NATO's hands. After the end of the Cold War, and in particular after Sweden and Finland announced their intention to join NATO, the situation is completely the opposite. Russia is now squeezed into the dead-end of the

Gulf of Finland, with the exclave of Kaliningrad acting as an "island" between Poland and Lithuania. In conflict or war, NATO would control the area and be in a position to bring forward reinforcements and supplies, and conduct a wide range of operations from the sea, including amphibious landings or demonstrations and Ballistic Missile Defence. With any of the three islands of Bornholm, Gotland and Saaremaa in the hands of Russia, this task would be immensely more complicated.

Russia is dependent upon the SLOC through the Baltic Sea. Much of their trade and half of their imported food transit this enclosed sea. Interdiction of legitimate business is of course not an option in peacetime, but very much so in conflict. After an initial fight to eliminate the military capacities in Kaliningrad, the most Russia can hope for is to reduce NATO's naval effectiveness through missile attacks, either shore-based or air-launched.

Again, Russian control of an island in the middle of the Baltic Sea would make the task all the more difficult for NATO.

The purpose of this article is to analyse and clarify the geographical and military importance of the Baltic Sea main islands – Bornholm, Gotland and Saaremaa. The thesis is that as of today, Russia has limited resources to conduct a landing and occupy and fortify an island in the region. Still, a well-planned and executed attack coinciding with or launched just prior to an actual larger attack could be successful. Sweden has realised this and brought some of its armed forces back to Gotland. Bornholm and Saaremaa, on the other hand, remain more or less open and are not adequately defended today.

This article is based on publicly available information, government documents, analytical studies of think tanks and academic research works. The scope of consideration is limited to sources not covered by any confidentiality clause. It is covering the last two decades with some annotation of historical events relevant to the current context. Qualitative research applies analysis, critical synthesis, desk research and comparative studies methods. Quantitative data are used only where they concern the respective cases related to any surveys. The paper consists of an

introduction and four sections to discuss respective islands as case studies and includes regional cooperation as an important factor. It is concluded by presenting some key findings concerning the aim of the paper.

KEYWORDS

Baltic Sea islands; Bornholm; Gotland; Saaremaa; Baltic Sea Region security.

30 years of the Iraqi Kurdistan (Southern Kurdistan) de facto state: dynamic, rationale and benefits of its relations with Turkey and US

P. Sosnowski (1)

(1) University of Warsaw, Poland, p.sosnowski2@uw.edu.pl

The Iraqi Kurdistan[11] is a de facto state established unilaterally in 1992 after decades of armed struggle with Iraq. In 2005 the existence of the Kurdish Regional Government became legal and its domestic rights were defined within the Iraqi constitution. The KRG may exercise legislative, executive and judicial powers over its defined territory, except for what is listed as exclusive powers of federal authorities (Alsamee et al., 2020; Jüde, 2017; Leezenberg, 2017). However, the KRG conducts unprecedented semiformal diplomatic, economic, and military relations with the International Community (Ababakr, 2020). It is implementing policies far beyond the domestic legal framework: extraterritorial military operations, e.g., transit of heavy-armed Peshmerga[2] through Turkey to support Kurds in North-East Syria in 2015 (Barkey, 2015, p. 6; Selîm, 2018), military deployment in territories disputed with Iraqi Gov. (Chapman, 2011, pp. 224–235); concluding international agreements (Jüde, 2017; Smith, 2018); receiving external arms and military support (Aziz & Cottey, 2021; Radpey, 2014; Smith, 2018); hosts foreign armies (e.g. US, Turkey) and provides safe haven to foreign armed nonstate actors, for example, Democratic Party of Iranian Kurdistan (Hassaniyan, 2019, pp. 139, 148), Peshmerga Rojava (Lowe, 2016, p. 7). The pursuit of full sovereignty is consistent and demonstrated by the 2017 independence referendum (Palani et al., 2019).

Iraqi Kurdistan receives support (also military) from several states (e.g. the US, UK, Germany, Turkey). It has also established links with several international organizations, e.g. the EU and the UN, and plays and important role in the Global Coalition to Counter ISIL/Da'esh. However, there is no state that would provide security guarantees, so KRG does not have any full-fledged patron (unlike other de facto states e.g., Turkey and Northern Cyprus; Armenia and Nagorno-Karabakh). That differentiates Iraqi Kurdistan from other objects of grounded interest of de facto states studies (Bashir et al., 2017; Pegg, 2017). Due to the lack of security guarantees, I refer to the US and Turkey as 'quasi-patrons'.

I assume that the lack of security guarantees and therefore an asymmetrical relation with a fully-fledged patron constitutes an important circumstance allowing KRG to conduct an (empirically) sovereign security policy. From the very establishment of the KRG, its relationship with Turkey and the US has been a main factor of its survival (Ozkahraman, 2021; Park, 2004; Sosnowski, 2016). The aim of the research is to analysis and clarify and explain the dynamics, rationale, and mutual benefits of the cooperation between the de facto state (KRG) and its quasi-patrons (US and Turkey). The mutual benefits and rationale behind these cooperation have not yet been explored with sufficient consideration of Iraqi Kurdistan's agency and thus constitute a research problem. This research will contribute to the literature on the de facto states and Kurdish Studies, by setting a new way of looking at and explaining the foreign and security policy of the Iraqi Kurdistan.

KEYWORDS

Iraqi Kurdistan; *de facto* state; Security policy; Turkey; US; Iraq.

REFERENCES

Ababakr, Y. M. (2020). Iraqi Kurdistan Region: From paradiplomacy to protodiplomacy. *Review of Economics and Political Science*. doi: https://doi.org/10.1108/REPS-01-2020-0002

Alsamee, E. M. B., Wahab, H. A., & Yusof, Y. (2020). The application of federalism in the Kurdistan region under the Iraqi constitution 2005. *Journal of Critical Reviews*, *7*(5), 172-176. doi: https://doi.org/10.31838/jcr.07.05.28

Aziz, S., & Cottey, A. (2021). The Iraqi Kurdish Peshmerga: Military reform and nation-building in a divided polity. *Defence Studies*, *21*(2), 226-241. doi:https://doi.org/10.1080/14702436.2021.1888644

Barkey, H. J. (2015). On the KRG, the Turkish-Kurdish Peace Process, and the Future of the Kurds. *Global Turkey in Europe Series, Working Paper*, *12*. Retrieved from https://www.iai.it/sites/default/files/gte_wp_12.pdf

---

[11] The Iraqi Kurdistan is a commonly used name to refer to the area in northern of Iraq and used synonymously with the Kurdistan Region in Iraq and Kurdistan Regional Government (KRG). It is also called 'Southern Kurdistan'(sor. باشووری کوردستان), referring to its location in the geo-cultural region of Kurdistan and with regard to the continuity of its historical specificity. [2] Official name of the KRG security forces.

Bashir, H., Sadoon, K., & Politicsjune, M. E. (2017). *From Foreign Relations to Foreign Policy: Transformation of the Kurdish de Facto State into an Independent Foreign Policy Actor*.

Chapman, D. (2011). *Security Forces of the Kurdistan Regional Government. | National Technical Reports Library-NTIS*. Mazda Publishers. Retrieved from https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA510826.xhtml

Hassaniyan, A. (2019). Cross-border Kurdish solidarity: An endangered aspect of Kurdishness. *Kurdish Studies*, *7*(2), 135-160. https://doi.org/10.33182/ks.v7i2.484

Jüde, J. (2017). Contesting borders? The formation of Iraqi Kurdistan's de facto state. *International Affairs*, *93*(4), 847–863. doi: https://doi.org/10.1093/ia/iix125

Leezenberg, M. (2017). Iraqi Kurdistan: A Porous Political Space. *Anatoli*, *8*, 107-131. doi: https://doi.org/10.4000/anatoli.608

Lowe, R. (2016). Rojava at 4: Examining the experiment in Western Kurdistan. *LSE Middle East Centre Workshop Proceedings*. Retrieved from http://eprints.lse.ac.uk/id/eprint/67515

Ozkahraman, C. (2021). Kurdish cross-border trade between Syria and Turkey: The socio-political trajectories of Syrian Kurds. *Middle Eastern Studies*, *57*(4), 567-580. doi: https://doi.org/10.1080/00263206.2021.1874365 Palani,

K., Khidir, J., Dechesne, M., & Bakker, E. (2019). The development of Kurdistan's de facto statehood: Kurdistan's September 2017 referendum for independence. *Third World Quarterly*, *40*(12), 2270-2288. doi: https://doi.org/10.1080/01436597.2019.1619452

Park, B. (2004). Iraq's Kurds and Turkey: Challenges for US Policy. *Parameters*, *34*(November 2003), 18.

Pegg, S. (2017). Twenty years of de facto state studies: Progress, problems, and prospects. In W. R. Thompson (Ed.), *The Oxford Encyclopedia of Empirical International Relations Theory*. Oxford University Press. doi: https://doi.org/10.1093/acrefore/9780190228637.013.516

Radpey, L. (2014). The Legal Status of the Kurdistan Regional Government (KRG) in International Law. *The Journal of Social, Political, and Economic Studies*, *39*(4), 397-435. Retrieved from http://www.idosi.org/mejsr/mejsr22(1)14/9.pdf

Selîm, H. E. (2018). *Pêşmerge li Kobanê*. Pertuxana Bedirxanian.

Smith, C. (2018). *Independent Without Independence: The Iraqi- Kurdish Peshmerga in International Law*. *59*(1). Retrieved from https://ssrn.com/abstract=3003644

Sosnowski, P. (2016). Relations with Turkey as determinant of Iraqi Kurdistan economic security. *Securitologia*, *2*(24), 87-103.

WG7 – Armed Forces and Society

Public Service Motivation and Turnover in the Portuguese Air Force: The Mediation role of Loyalty

J. Duque (1), J. Nascimento (2) and C. Fachada (3)

(1) Força Aérea Portuguesa, joanaduque.grh@gmail.com
(2) CAPP/Instituto Superior de Ciências Sociais e Políticas, Portugal, jlnascimento@iscsp.ulisboa.pt
(3) CIDIUM/Instituto Universitário Militar, Portugal, fachada.cpa@ium.pt

One of the recurring problems in the armed forces is the number of troops, that is, the attraction and retention of military personnel (Charbonneau, Lévesque, Tchokouagueu, Tadjiogue, Tchinda, & Mongong, 2020). The Public Service Motivation (PSM) is one construct developed in a public context that has been studied in the military context (Ritz, Brewer, & Neumann, 2016; Taylor, Clerkin, Ngaruiya, & Velez, 2015). Following the Perry and Wise approach, the PSM is "understood as an individual's predisposition to respond to motives grounded primarily or uniquely in public institutions and organizations" (Perry & Wise, 1990, p. 368). Moreover, the PSM could be conceptualized as a multidimensional or unidimensional construct (Perry, & Vandenabeele, 2015).

Five dimensions were identified in a preliminary PSM validation study for Portugal (Fonseca, Nascimento, & Dias, 2020). Three of them are prosocial, corresponding to those initially proposed by Perry (1996) and consisting of Self-Sacrifice (SS), Civic Duty (CD), and Social Justice (SJ). The remaining two were asocial, specifically, Social Selfishness (SR) and Social Cynicism (SC). These results suggest that a high PSM implies high levels of the three prosocial dimensions and low intensity of the two asocial dimensions.

PSM is, therefore, an essential antecedent in the attraction and retention of public servants (Perry, & Vandenabeele, 2015) due to its affective, rational, and normative nature (Perry, & Wise, 1990), and it is an attraction factor for the military service. In this line, it has been a topic of great interest to study the PSM in a military context (Charbonneau et al., 2020). Additionally, it is an antecedent of a set of variables, such as performance, loyalty, or retention (Charbonneau et al., 2020; Hattke, Vogel, & Znanewitz, 2018; Perry & Vandenabeele, 2015; Ritz et al., 2016; Taylor et al., 2015). In this context, analyzing the relationships between consequent, antecedent, mediators, and moderators variables is one of the PSM's research trends, as highlighted by Perry and Vandenabeele (2015).

The present research is positioned in this theoretical framework and aims to verify the influence of PSM on Turnover, mediated by Loyalty to the Institution, namely the Portuguese Air Force. Thus, the following general hypotheses are formulated:

H1: PSM negatively influences Turnover.
H2: PSM positively influences Loyalty
H3: Loyalty negatively influences Turnover.

Based on the above, the hypotheses formulated above support the structural model proposed in the present study (Figure 1), implying that Loyalty is a variable that mediates the influence of PSM on Turnover.

Figure 1 – The proposed model

Understanding the mutual influences between the three constructs is a first contribution to the theoretical framework of PSM in general and, particularly, in a military context. On the other hand, this investigation also highlights the importance of Loyalty as a mediator of PSM's influence on Turnover. The third advantage lies in the fact that it verifies the impacts of the five dimensions of PSM on Turnover and Loyalty. Therefore, the results obtained may

contribute to better management of human resources in a military context, namely in the selection of candidates and their retention.

KEYWORDS

Military Context; Portuguese Air Force; Public Service Motivation; Turnover; Loyalty; Structural Model.

REFERENCES

Charbonneau, É., Lévesque, J. F., Tchokouagueu, F. A., Tadjiogue, Y. W., Tchinda, K. J., & Mongong, M. (2020). Camouflaged or deserted? A systematic review of empirical military research in public administration. *Asia Pacific Journal of Public Administration*. doi: 10.1080/23276665.2020.1839351. Retrieved from URL

Hattke, F., Vogel, R., & Znanewitz, J. (2018). Satisfied with red tape? Leadership, civic duty, and career intention in the military. *Public Management Review*, *20*(4), 563-586. doi: https://doi.org/10.1080/14719037.2017.1335341. Retrieved from URL

Perry, J. L. (1996). Measuring public service motivation: An assessment of construct reliability and validity. *Journal of Public Administration Research and Theory, 6*(1), 5-22.

Perry, J. L., & Vandenabeele, W. (2015). Public service motivation research: Achievements, challenges, and future directions. *Public Administration Review, 75*(5), 692-699. doi: 10.1111/puar.12430 Retrieved from URL

Perry, J. L., & Wise, L. R. (1990). The motivational bases of public service. *Public Administration Review*, *50*(3), 367-373. Retrieved from https://www.researchgate.net/profile/Patricia-Ingraham/publication/229476704_Performance_Promises_to_Keep_and_Miles_to_Go/links/5eee604d92851ce 9 e7f52f27/Performance-Promises-to-Keep-and-Miles-to-Go.pdf

Ritz, A., Brewer, G. A., & Neumann, O. (2016). Public service motivation: A systematic literature review and outlook. *Public Administration Review, 76*(3), 414-426. doi: 10.1111/puar.12505. Retrieved from URL

Taylor, J. K., Clerkin, R. M., Ngaruiya, K. M., & Velez, A. L. K. (2015). An Exploratory Study of Public Service Motivation and the Institutional–Occupational Model of the Military. *Armed Forces & Society, 41*(1), 142-162. doi: 10.1177/0095327X13489119. Retrived from URL

Finnish Independence Day 2021: who were setting the agenda on Twitter?

M. Kaarkoski (1), J. Huhtamäki (2), D. Savolainen (3), M. Alaraatikka (4), P. Koistinen (5), A.-M. Huhtinen (6), T. Sederholm (7)

(1) Finnish National Defence University, miina.kaarkoski@mil.fi
(2) University of Tampere, Finland, jukka.huhtamaki@tuni.fi
(3) Aalto University, Finland, savolainend@gmail.com
(4) Finnish National Defence University, milla.alraatikka@mil.fi
(5) Finnish National Defence University, pekka.koistinen@mil.fi
(6) Finnish National Defence University, aki.huhtinen@mil.fi
(7) Finnish National Defence University, teija.sederholm@mil.fi

In time-sensitive and complex situations, authorities and political leaders are often expected to deliver the official information to citizens quickly and accurately. From the perspective of national security, this demand is connected to influence over political discourse and agenda setting, both of which have great importance as sources of power. Social media platforms have fundamentally changed the dynamics of political agenda setting and the communicative role of authorities. A wide variety of political and societal actors now have the potential to seek attention and, hence, gain influence on topics that are discussed publicly. This influence can be used to affect how these topics and issues are framed within the public discussion. In the hybrid media system, political actors, publics and media representatives interact and construct ties, contexts and social relationships. Within these interactions in hybrid media space, the construction of meanings takes place. While information influence and disinformation have been recognized as serious threats to national security and to the work of authorities, more analytical research is needed on actors that seek and gain attention in social media, and the strategies they use.

In this paper, we are studying the roles of actors who were seeking and gaining attention on Twitter during an event that included elements of a hybrid media event. The Finnish Independence Day on December 6th is a national holiday during which the media agenda usually consist of an official celebration of the nation's independence. Traditionally, a significant part of the Finnish population has been sitting in their homes and watching a live TV broadcast by the national public broadcast company, which shows a military parade and a few hundred guests invited by the President of Finland celebrating in the presidential residence. However, the day often sparks controversies in the Finnish society, since it is simultaneously a day when a wide variety of ideologically orientated demonstrations are organized. Demonstrations and confrontations often take place on the streets and in the media, as political far right and left-wing orientated groups typically challenge things such as the state and its leadership, authorities and other topical political issues. In the year 2021, the President of Finland canceled the celebration in the castle and the military parade was cancelled as well. The volume of demonstrations during thst year was significant, and the discourse on the Covid-19 pandemic added new layers to the demonstrations and social media communications.

Twitter is a platform that connects politicians, state leaders, authorities and citizens. This is the case especially in Finland, where Twitter is the most popular social media site among political and media elites. The data of our research consists of approximately 33 000 tweets that were collected using the Twitter API. The search criteria included different security, military and healthcare authorities and political leaders, as well as terminology referring to the demonstrations. Through social network analysis, the aim was to study the role of authorities and political leaders as receivers of attention, and the strategies they used for gaining attention and setting the agenda in social media communication during this hybrid media event. It appears that authorities and political leaders gained significant attention on Twitter even though their role in communicating with the public on Twitter was rather passive. Means to seek attention included active tweeting in general and, in particular, active interaction through replies in discussion threads, as well as mentioning other actors. However, activity only had a minor impact to the received attention, which was driven primarily by actor status and existing followership.

KEYWORDS

Social media; Twitter.

Basic assumptions of security science in social sciences

R. Szpyra (1)

(1) War Studies University Warsaw, Poland, r.szpyra@akademia.mil.pl

In recent years, we have observed a systematic increase in publications on security, however, many of them concern national security or the state, treating the general theory of security marginally (Chojnowski 2015; Cieślarczyk 2011; Drabik 2013; Gierszewski 2013; Konieczny 2012; Piwowarski 2018; Smith, & Brooks 2013; Wróblewski 2017). If their authors recognize other types of security, they consider them in the context of state or national security. It is worth noting, however, that there is a general category of "security" relating to all kinds of entities and contexts of considerations. One could also consider the possibility of the existence of security sciences located in all fields of science, regardless of the existence of an independent discipline of security science in social sciences[1]. In this study, the overall essence of security was sought. The search was conducted using a critical analysis of security-related publications. The research began with an analysis of the philosophical and axiological foundations of this phenomenon.

On this basis, the general essence of security was established. It was assumed that security is an abstract category of human thinking, a relation that defines the possibility of the duration of real beings and the striving to improve the possibility of the existence of these beings. On the other hand, learning about security means examining the possibility of the existence of real beings and the search for ways to improve the possibility of the existence of these beings, i.e. to extend this existence.

Then it was established that the area of social sciences research is limited to the study of society and social phenomena and processes in which the core is man and his relations with other people and the environment. This limitation also constitutes the research field of security sciences - a discipline of social sciences.

Another research question concerned the autotelic values of social sciences. Values as a feature objectively and subjectively belonging to a given thing and values in the metaphysical sense were sought here. It was established that despite the existence of naturecentrism, ecocentrism or biocentrism, it is difficult to imagine that they would degrade man by completely reversing the hierarchy of values, putting nature at their head.

It is more about the so-called sustainable existence and development of man and nature, because some natural or man-stimulated directions of changes in nature may even make it impossible to exist. As a result, it was established that both for the social sciences and the security sciences functioning within them, the autotelic value in a static approach is man and his community, and in a dynamic approach, the existence of man and / or his community. Subsequently, the general essence of security was transformed into its understanding in social sciences. This transformation was made, however, with the universal essence of security in mind.

It was established that security is a category related to some autotelic value and its duration, therefore it was assumed that the semantic core of security in social sciences is the abstract category of human thinking, a relationship that defines the objective possibilities of the existence and development of real beings of human society and its environment, mainly of man and / or his community and striving to improve the possibilities of the existence and development of these beings.

In addition, an appropriately coherent understanding of threats, objectivity and subjectivity of security has been proposed. It was established that the essence of threats is that they hinder or even prevent the existence and development of an object, in this case of man and / or his community.

Regardless of the general subjective abilities of a human being, when it comes to answering the question of whose safety we are talking about, it is an objective aspect. In this aspect, man can also be considered. Therefore, it was assumed that the object of security will be man and his communities and the beings created by him, and in the dynamic approach, the existence of man and / or his community and the existence of beings created by him. Moreover, in the most general sense, a human being, apart from being an object of security, is also the main subject of the considered security. His existence is the main value, but also man is the only element of nature aware of his existence. Moreover, man is able to actively change his surroundings and the natural environment in which he lives. Therefore, it is man who is the main entity that consciously shapes his security. It is difficult to imagine any form of this shaping other than some human action, that is, some activity spread over time.

KEYWORDS

Security; Security Science in Social Sciences.

REFERENCES

Chojnowski, L. (2015). *Bezpieczeństwo. Zarys teorii*. Słupsk: Wydawnictwo Naukowe Akademii Pomorskiej.

Cieślarczyk, M. (2011). *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*. Siedlce: Akademia Podlaska Siedlce.

Drabik, K. (2013). Podmiotowy wymiar bezpieczeństwa. In: T. Szczurek (Ed.), *Filozoficzne i społeczne aspekty bezpieczeństwa* (pp. 137-162). Warszawa: Redakcja Wydawnictw Wojskowej Akademii Technicznej.

Gierszewski, J. (2013). *Bezpieczeństwo społeczne. Studium z zakresu teorii bezpieczeństwa narodowego*. Warszawa: Difin.

Ingarden, R. (1989*). Wykłady z etyki*. Warszawa: PWN.

Konieczny, J. (2012). O pojęciu bezpieczeństwa. Bezpieczeństwo. *Teoria i Praktyka, 2012*(1), 7-20. Retrieved from http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.mhp-45da9458-d624-4545-adf4-5cab49cd1600.

Korzeniowski, L. (2012). *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem*. Warszawa: Difin.

Piwowarski, J. (2018). *Nauki o bezpieczeństwie. Między kulturą bezpieczeństwa a studiami bezpieczeństwa*. Warszawa: Difin.

Rutkowski, C. (2018). *Podstawy nauk o bezpieczeństwie z elementami naukoznawstwa*. Warszawa: Szkoła Główna Służby Pożarniczej.

Smith, C.L., & Brooks, D.J. (2013). *Security Science. The Theory and Practice of Security*. Amsterdam: ELSEVIER.

Wróblewski R. (2017). *Wprowadzenie do nauk o bezpieczeństwie*. Siedlce: Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach.

Conscription as Part of Life Course: an Ethnographic Study

E. Lillemäe (1)

(1) Estonian Military Academy/University of Tartu, eleri.lillemae@ut.ee

Conscript service is often seen by young people as a period when they fall behind their peers and give up a year in their lives. In contemporary societies, individual values are emphasized and every experience is part of building a personal portfolio. Armed forces on the other hand, are based on collective values and limited agency, which leads to tensions between the obligation to go through the conscript service and values prevalent in society. In the context of the countries whose state defence is built on the comprehensive defence and reserve army principle, conscript service forms the base for future reservists, whose skills, knowledge and will to defend is central in defending the country. Therefore, it is important to study how young people today perceive conscription and which aspects turn it into a meaningful experience and which ones to a futile obligation.

In order to study this question in depth, an ethnographic study was carried out. The study is based on the Estonian conscription system, which is one of the few countries with mandatory military service in Europe. Its small population and position on the NATO's eastern flank have led to maintaining conscription as the most effective model for state defence. In the ethnographic study the focus was on young people's expectations on conscription and how they emerged and changed during the service.

In the study 14 young men were followed throughout their service in 2021-2022 for a year, combining interviews, diary keeping, video recordings and observations. Based on the data collected, narrative analysis was used to understand how participants constructed their stories and what affected their service - relations with other conscripts, commanders, family and friends; events occurring in their unit and private lives; security situation; attitudes, etc. During the one-year study period, it was found that conscripts previous attitudes towards the military and state defence had a central role in how they perceived their service. As the start of the Ukrainian war was in the middle of their training process, the understanding of state defence and their role in it shifted as well.

KEYWORDS

Conscription; Life course; Ethnography; Agency.

From conscript service to active duty – the realization of intentions in Estonia

K. Kasearu (1)

(1) University of Tartu, Estonia, kairi.kasearu@ut.ee

After the end of the Cold War, the military reforms spread over the world. The role of the armed forces changed significantly in the 1990s with broad technological, geostrategic and societal changes, which challenged the utility and legitimacy of mass armies and conscription. Ng (2008) argues that although from economic perspective conscription might not be efficient, the equilibrium can be found, which makes conscription acceptable. He claims that in case of a high demand for manpower in military sphere where the recruitment pool from all-volunteer force would not be sufficient, conscription might be more favourable solution both from an individual and a societal perspective compared to the all-volunteer force. Anna Leander (2004) makes similar point, the estimation of economic costs depends on the type of conscription, how many are drafted on what terms, and what would be the costs of alternative solutions. Recent geopolitical developments are stressing the need to increase the resources on defence including human resources. The questions of recruitment and retention are turning to be the hot topics again.

Estonia, a small country between Baltic Sea and Russian Federation, with very small geographical and social size (population 1.3 million) has maintained the conscript system. Conscripts are providing a pool for regulars and reserves and to an extent for locality-based but nationally organized voluntary defence organization. This situation means that Estonia is a good example to explore how and what role the conscription plays in recruiting process of the active duty members. The aim of the research project is to explore how the intention to join the Estonian Defence Forces (EDF) after the period of conscription develops, changes and will be turned to the action. The data are gathered within the Estonian Conscript Survey. Annual Estonian Conscript Survey (ECS) is carried out since 2016 in cooperation between University of Tartu and Estonian Military Academy. Every year about 3000 conscripts enter the conscription and they are surveyed twice in their service period, during the first and last month. The data of this study are representing the conscripts, who started their service in 2020 and finished in 2021. To the data set was added the information about their professional military career – whether they joined the EDF within 6-month period or not.

Our research shows that there are two main paths to join the EDF. The first and more dominant is the realization of military propensity and orientation to EDF, it is associated with internal motivation and institutional values. The second path is adaptation and finding own place. The intention to join EDF is formalized during the conscription and is initiated by external motivation – good salary, action, active life-style. We described it as occupational motivation. Beside the individual motivation, the realization of intention to join the EDF is shaped by structural conditions and barriers, e.g. education and language proficiency.

KEYWORDS

Estonia; Conscription; Recruitment; Longitudinal data.

REFERENCES

Leander, A. (2004). Drafting Community: Understanding the Fate of Conscription. *Armed Forces & Society*, *30*(4), 571-599. Retrieved from https://www.jstor.org/stable/48608613

Ng, Y.-K. (2008). Why is the military draft common? and increasing returns. *Annals of Economics and Finance*, *9*(2), 373-384. Retrieved from https://www.researchgate.net/publication/227388255_Why_is_the_Military _Draft_Common_Conscription_and_Incr easing_Returns

The present and future of conscription in the 21st century

V. Česnuitytė (1), T. Ferst (2), E. Jonsson (3), K. Kasearu (4), E. Lillemäe (5), J. Novagrockienė (6), M. Salo (7), M. Salminen (8), T. Sederholm (9), F. B. Steder (10), S. Svensén (11), T. Szvircsev Tresch (12), T-T. Truusa (13), J. Österberg (14)

(1) General Jonas Zemaitis Military Academy of Lithuania, vida.cesnuityte@lka.lt
(2) Military Academy at the ETH Zurich, Switzerland, thomas.ferst@vtg.admin.ch
(3) Swedish Defence University, emma.jonsson@fhs.se
(4) University of Tartu, Estonia, kairi.kasearu@ut.ee
(5) Estonian Military Academy/University of Tartu, eleri.lillemae@ut.ee
(6) General Jonas Zemaitis Military Academy of Lithuania, jurate.novagrockiene@mil.lt
(7) Finnish Defence Forces, mikael.salo@mil.fi
(8) Finnish Defence Research Agency/Finnish National Defence University, mikko.k.salminen@mil.fi
(9) Finnish National Defence University, teija.sederholm@mil.fi
(10) Norwegian Defence Research Establishment, frank.steder@ffi.no
(11) Swedish Defence University, sofia.svensen@fhs.se
(12) Military Academy at the ETH Zurich, Switzerland tibor.szvircsev@vtg.admin.ch
(13) University of Tartu, Estonia, tiia-triin.truusa@ut.ee
(14) Swedish Defence University, johan.osterberg@fhs.se

While most of the European countries have moved towards an all-volunteer force in the recent decades, there is a number of countries who have retained conscription. Although the general principle of mandatory military service is universal, mechanisms for recruiting and training as well as adapting and legitimising conscript service in increasingly neoliberal and individualistic societies is varied. In the context of recent events in Ukraine, the discussion about state defence models and conscription has become a central topic of discussion. The same mechanisms that propelled the transformation away from conscription today motivate the keeping or reinstating of conscription. This research draws from the experience of six European countries, of which four have continuously kept conscription (Estonia, Finland, Norway, and Switzerland), and two re-established conscriptions in recent years (Lithuania and Sweden). Since 2020, these six countries have worked together in a joint research group to explore further the viability of mandatory military service model and the reasons and mechanisms behind the choice of retaining/reinstating it. A comparative research has been carried out based on official documents, academic literature and a shared survey. The aim of the presentation is to give an overview of the research project, introduce, and discuss the first results.

Our research shows that reasoning for maintaining or reinstating conscription in these countries is similar, although the meaning and position of conscription in these societies is different. The effect of conscription to societies can be described through two mechanisms: (1) the share of drafted individuals in the birth cohort, (2) recruitment and share of female conscripts. While the first one is related to socializing effect of conscription through the number of people who are related to military (families, friends, schoolmates), the second one exemplifies applying societal values in the military (e.g. gender equality). Based on these factors we claim that conscription systems can be characterised through three types: (1) wide, representative, and heterogeneous (in motivation and values), but rather male dominant (Estonia, Finland, and Switzerland); (2) narrow, homogenous and male dominant (Lithuania); (3) narrow, selective, homogenous, and gender neutral (Sweden, Norway).

In the following years, all of these countries aim to increase their number of conscripts and include more women in the service. These aims might be accelerated due to the changed security situation and motivation to increase military capacities in the near future. This in effect could lead to broader discussion on state defence models and change the existing conscription systems, shifting them from one type to another.

KEYWORDS
Conscription; Recruitment; Retention; Changing societies.

The Finnish Model of Conscription – A Successful Policy to Organize National Defence

J. Kosonen (1) and J. Mälkki (2)

(1) Army Command Finland, jarkko.kosonen@mil.fi
(2) Finnish Defence Force´s Research Agency, juha.malkki@mil.fi

The Finnish conscription model dates to the end of the 19th century when Finland was still an autonomous Grand Duchy of the Russian Empire. Conscription has maintained its legitimate role as the basis of the armed defence of Finland ever since. The unpublished research I offer to be presentation at ISMS conference explores Finland's conscription program as a policy success over time and covers which factors have fortified the endurance of the program for over a hundred years. It also discusses the counter narratives that have been used to challenge the policy success of the successful policy programme of conscription.

Finland is a Nordic welfare state where all citizens are subject to a national defence obligation by constitutional law.

Conscription is mandatory for men, and their service completion rate varies due to political, social, and health reasons. The current goal is to train the entirety of male ages cohort, while about 70 percent of young men successfully complete their conscription or civil service. A central reformation of the conscription programme started in 1995, when the law for volunteer military service for women came into effect. The number of women who have completed conscription has steadily increased, although it is still only a few percent of the total female age cohort.

Conscription in Finland forms the basis for a political programme of national defence. The armed defence of the state is part of Finland´s national defence policy and comprehensive security. The endurance and legitimacy of conscription has traditionally held strong support among politicians and public opinion.

The conscription model has been challenged in the political sphere with either the opportunity to transition to a professional standing army or to a mandatory, gender-neutral national service model which would subject the entire age group to service. For a small nation like Finland, which has to contend with both resource and geopolitical realities, a professional standing army would be a costly alternative compared to an economically efficient conscription model.

It was supposed that due to the previous year´s politically contentious issue of gender neutrality and equality in conscription the future a gender-neutral national service model would become relevant in political discourse. Recent fundamental changes in security policy in Europe have changed the emphasis of the citizen´s emotions, societal debate and political discourses in conscription in Finland. According to recent national opinion poll (ABDI, The Advisory Board for Defence Information) citizens' will to defend the country has clearly strengthened; over 80 per cent want

Finland defended by military means if it is attacked. This is the highest score that has ever measured in Finland since 1970s. (ABDI 2022, p. 9–10, 29.) Due to the current security policy situation in Europe, the debate on conscription, military service and national service for all citizens is likely to continue in Finland.

KEYWORDS

Citizenship; Conscription; Defence policy; Military service; National defence; National defence obligation.

REFERENCES

ABDI (2022). Finns' Opinions on Foreign and Security Policy, National Defence and Security. The Advisory Board for Defence Information. *Bulletins and reports, 3*, 2022. Retrieved from https://www.defmin.fi/en/the_advisory_ board_for_defence_information_abdi/bulletins_and_reports/finns_opinions_on_foreign_and_security_policy_ national_defence_and_security_2022.12756.news).

Kosonen, J, & Mälkki, J. (will be published in 2022). The Finnish Model of Conscription – A Successful Policy to Organize National Defence. In: C. De La Porte, G. Bjokeydal, J. Kauko, D. Nohrstedt, P. Hart, & S. Tranøy, B. (Eds.), *Successful Public Policy in the Nordic Countries*. Oxford: Oxford University Press.

Trust in the Latvian National Armed Forces among Russian-speakers in Latvia

L. Berzina (1)

(1) National Defence Academy, Center for Security and Strategic Research, Latvia, ieva.berzina@mil.lv

An essential prerequisite for effective security policy is trust in the military as it is one of the critical factors affecting society's will to defend its country. This paper analyses the lower trust among Latvia's Russian-speakers in the Latvian National Armed Forces when compared to people whose mother tongue is Latvian. The study examines the issue in the context of the Latvian media environment which consists of media in both the Latvian and Russian languages, including Kremlin-controlled media, a situation whereby Latvian residents receive information about the activities of both the Latvian and Russian armies. The study investigates three information-environment related factors that could potentially decrease trust in the Latvian army among Russian-speaking audiences.

The extensive consumption by Latvian Russian-speakers of media content in the Russian language, especially from Kremlin-controlled media, encouraged the formulation of three assumptions, which were tested empirically. Firstly, the Official Language Law (2000) stipulates that state communication with the public must take place only in Latvian. Therefore, one of the possible explanations for the research problem is that the public, which uses only the Russian language information space, receives less information about the Latvian National Armed Forces than the public which uses Latvian language information sources. Secondly, according to the Latvian State Security Service (2020: 26), the Russian media under the Kremlin's control aims "to improve Russia's image and provide support in discrediting other countries, including Latvia." It may, therefore, be assumed that the Russian media contain negative information about the Latvian army. Thirdly, the Kremlin controlled media disseminate information about the Russian Armed Forces, the military capabilities of which exceed the military capabilities of Latvia as a small country many times. It may be assumed that the perception of the asymmetry of military power affects the image of the Latvian army within the Russian speaking audience negatively.

The paper's theoretical framework is based on studies of the interaction between the media and the military. The issue of trust in the military will be analysed in the context of the increasing role of the media in various aspects of social life, which is described as mediatization in the theoretical literature. The basic idea of mediatization is that the media are not only the intermediaries between the audience and the communicator, but that they form the very environment in which communication takes place. The military is no exception; therefore, the concept of mediatization has also been applied to warfare (Crosbie, 2015; Hiebert, 1991; Horten, 2011; Hoskins & O'Loughlin, 2010, 2015; Maltby, 2012; McQuail, 2006).

Furthermore, empirical data indicating and comparing the image of the Latvian and Russian military within Russian-speaking audiences in Latvia were obtained in focus group discussions in 2020. The main conclusion of the paper is that Russian-speakers' trust in the Latvian National Armed Forces can be reduced to a specific range of factors: a lack of sufficient information about the Latvian army; the strong and positive image of the Russian Armed Forces; the influence of Kremlin-controlled media content on the perception of Latvia's overall security policy as a small country.

KEYWORDS

Media and military; Trust in the armed forces; Russian-speaking community.

REFERENCES

Crosbie, T. (2015). Scandal and military mediatization. *Media, War & Conflict, 8*(1), 100–119. doi: https://doi.org/10.1177/1750635214531108

Hiebert, R. E. (1991). Public relations as a weapon of modern warfare. *Public Relations Review, 17*(2), 107-116. doi: https://doi.org/10.1016/0363-8111(91)90049-Q.

Hoskins, A. & O'Loughlin, B. (2010). *War and Media: The Emergence of Diffused War*. Cambridge: Polity Press.

Hoskins, A. & O'Loughlin, B. (2015). Arrested war: the third phase of mediatization. *Information, Communication & Society, 18*(11), 1320-1338. doi: 10.1080/1369118X.2015.1068350

Horten, G. (2011). The Mediatization of War: A Comparison of the American and German Media Coverage of the Vietnam and Iraq Wars. *American Journalism, 28*(4), 29-53. doi: http://dx.doi.org/10.1080/08821127.2011.10677801

Latvian State Security Service. (2020). *Annual Report*. Retrieved from https://vdd.gov.lv/en/?rt=documents&ac=download&id=59

Maltby, S. (2012). The mediatization of the military. *Media, War & Conflict, 5*(3), 255-268. doi: https://doi.org/10.1177/1750635212447908

McQuail, D. (2006). On the Mediatization of War: A Review Article. *International Communication Gazette, 68*(2), 107118. doi: https://doi.org/10.1177/1748048506062227

Official Language Law (2000). Retrieved from https://likumi.lv/ta/en/en/id/14740

Adolescents and the dark side of social media - Threats to individual and to societal security

J. Äijälä (1), R. Riikonen (2), A-M Huhtinen (3) and T. Sederholm (4)

(1) National Defense University, Finland, juho.aijala.19@alumni.ucl.ac.uk
(2) University of Eastern Finland, Finland, reetta.riikonen@uef.fi
(3) National Defense University, Finland, aki.huhtinen@mil.fi
(4) National Defense University, Finland, teija.sederholm@mil.fi

Adolescents remain the most active users of social media (Statistics Finland, 2020). Adolescence is a period of development and of identity formation, during which peer pressure plays an increased influence. Thus, adolescents might be more vulnerable to risk-taking, emotional motivation and peer pressure (Dual-systems theory: Shulman et al., 2016). The adverse effects social media can have on societal and individual well-being are well documented. Adolescents especially face various risks: cyberbullying, online abuse, exposure to negative content (Willoughby, 2018), disinformation, coordinated information influencing and political polarisation (Norri-Sederholm et al. 2020). Due to being in the process of biological and psychological maturation, adolescents might be more vulnerable to this dark side of social media. Thus, due to: (1) being the most active user group of social media (2) being more vulnerable to the dark side of social media, adolescents might act as targets for malevolent actors on both on individual and societal levels.

Our research has identified threats Finnish adolescents face on social media, and their effect on both individual and societal well-being, with a focus on national security. We performed semi-structured interviews with officers from the Finnish preventive measures police unit (conducted December 2019), who regularly work with adolescents online. The officers were recruited from three police districts representing distinct geographical areas in Finland. Due to their professional experience, police officers are expertly suited to evaluate the risks adolescents face from the point of view of national security. To analyse these interviews, we employed qualitative content analysis in two phases. In the first phase we employed data-driven analysis to identify the main threats that arose from the interviews. In the second phase, we employed the Honeycomb-model of social media (Baccarella et al., 2018) as theoretical framework to breakdown the identified threats. This was done to get a more nuanced picture of how the threats are present in social media.

The first phase analysis revealed three primary threats: polarization, disinformation, and social media as a pathway to illegal activities. Polarisation was thought to effect adolescents' attitudes to other users, and it was reported to be present as radicalisation and extremist propaganda, and as a strong ingroup/outgroup bias present within different groups and sub-cultures on social media. Disinformation was related to the prevalence of disinformation on social media platforms and the (lack of) capabilities of adolescents in detecting it. In addition, the officers emphasised the effect of confirmation bias and the long-term impact this could have on the worldviews of adolescents. Moreover, some adolescents were identified as active producers of disinformation. Social media as a pathway to illegal activities was related to the ways social media could lead adolescents to criminal activities: committing offences such as defamation or criminal threats, the ease with which even younger people can be involved in either selling or buying drugs via social media. Moreover, the possibility for extremist groups to manipulate or recruit adolescents via social media was discussed as a serious threat.

The second phase of our analysis broke down these threats using the honeycomb-model as a theoretical framework. This approach can be used to organize and represent the threats as the functionalities of social media, which in turn can be used to better understand and counter them. An example of the identified threat

"Disinformation", broken down to its functionalities can be seen in Figure 1.

Figure 1 – A Sankey diagram presenting an example of how the identified threat "Disinformation" can be broken down into smaller pieces using the Honeycomb-model

Our presentation will focus on how these functionalities are present on social media, and how they give rise to the identified threats. Moreover, we will discuss how the threats have evolved since 2019, and how our approach can be used to predict how they will evolve in the future.

KEYWORDS

Social media; National security; Adolescents.

REFERENCES

Baccarella, C. V., Wagner, T. F., Kietzmann, J. H., & McCarthy, I. P. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal, 36*(4), 431-438.

Norri–Sederholm, T., Norvanto, E., Talvitie–Lamberg, K., & Huhtinen, A. M. (2020). Misinformation and Disinformation in Social Media as the Pulse of Finnish National Security. In *Social Media and the Armed Forces* (pp. 207–225). Springer, Cham.

Shulman, E. P., Smith, A. R., Silva, K., Icenogle, G., Duell, N., Chein, J., & Steinberg, L. (2016). The dual systems model: Review, reappraisal, and reaffirmation. *Developmental cognitive neuroscience, 17*, 103-117.

Statistics Finland (2020) The use of information and communication technology, [online], Statistics Finland. Retrieved from http://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_tau_021_fi.html

Willoughby, M. (2019). A review of the risks associated with children and young people's social media use and the implications for social work practice. *Journal of Social Work Practice, 33*(2), 127–140.

Young Finns' discourses on conscription and willingness to defend in the context of the war in Ukraine

M. Kaarkoski (1) and T. Tallberg (2)

(1) Finnish National Defence University, miina.kaarkoski@mil.fi
(2) Finnish National Defence University, teemu.tallberg@mil.fi

European security is strongly affected by the military aggression of a great power with an alternate political system and opposing values. Currently, Finland and Sweden are applying for a Nato membership, which is a remarkable decision for the two Nordic countries that have traditionally relied on policies of conscription and military nonalignment. As an institution, conscription not only provides means to counter external threats, but it also relates to profound cultural and historical issues, while connecting citizens to armed forces. This connection has been traditionally expressed through speaking about and measuring people's willingness to defend their country and nation. In Finland, opinion surveys conducted during the spring of 2022 indicated that people's willingness to defend Finland was stronger than ever. However, scholars have recently criticized the tradition of measuring citizens' willingness to defend with only one or two questions, since it offers a very narrow view of the relationship between citizens and national defence.

More analytical approaches have been developed to study the complexity and nuances of how citizens relate to national defence. A new model of citizens' relationship to national defence has been proposed as an attempt to respond to this scholarly criticism. The model describes factors that may connect citizens to national defence and explain their thoughts about their willingness to defend their country.

Inspired by this model, we interviewed young Finns' (aged 18-29) about their views on conscription and willingness to defend Finland during the spring 2022, when the war in Ukraine set a new kind of context on studying people's ideas about national defence and their own role in it. Our study examines the conceptions and the language used by the younger generation to describe the variety of meanings assigned to conscription within the European context.

The results highlight conscription as a societal construct that requires the continued acceptance of citizens who consider equality and freedom of choice as the core values when contemplating their own role in national defence. Based on our analysis, we will consider the theoretically-orientated model of citizens' relationship to national defence.

KEYWORDS

View of youth generation in Poland to European Union mediation in resolving conflict between Serbia and Kosovo in 2011-2020

U. Jaśkiewicz (1)

(1) War Study university, Poland, urszulaja@gmail.com

The Serbian government's long-standing policy of discrimination (dismissing Albanians from their jobs for origin, depriving them of their right to ownership of land, denying respect for human rights) against Albanians in Kosovo led to the outbreak of armed conflict in 1998. Open-armed conflict and ethnic cleansing have forced the international community to intervene to stop the violence. An air operation was carried out by NATO and then international supervision over Kosovo was established. According to the assumptions of Resolution 1244, Kosovo continued to be part of Serbia as its autonomous district, under the management of United Nations Interim Administration Mission in Kosovo. However, political tensions continued between the Serbs and Kosovars, leading to Kosovo's unilateral declaration of independence in 2007. This decision has triggered a political conflict between Serbia and Kosovo, in which the European Union has been mediating since 2011, in accordance with a UN General Assembly resolution. The mediation was multi-phase, and in their opinion the main one was to normalise relations between Serbia and Kosovo.

The aim of the research is (i) to examine the current state of knowledge of the young generation in Poland on the mediation of the European Union in resolving the conflict between Serbia and Kosovo in 2011-2020, (ii) to analyze the assessments of the young generation in Poland on the mediation of the European Union in resolving the Serbian-Albanian conflict in 2011-2020 and to indicate the reasons for the current level of knowledge of the young generation in Poland about the conflict. The methods used to conduct the research are: case study, diagnostic survey made using the Google Forms online form and a research tool such as a survey questionnaire, as well as inference and generalization. The research was based on the theory of conflict management through mediation developed by Jackob Berecovitch and theory of conflict regulation according to Morton Deustch.

The conducted research indicates that the general state of knowledge of the young generation in Poland about the mediation of the European Union in the conflict between Serbia and Kosovo in 2011-2020 is high. The respondents were able to identify the key factors of the conflict between Kosovo and Serbia, but they were not able to clearly indicate whether the European Union is a reliable mediator in this conflict. The research shows the need to increase social education, especially among the younger generation, on mediation by the European Union in the conflict between Serbia and Kosovo in 2011-2020. It is necessary to increase public awareness of this conflict and to undertake broader social debates on the regulation of political as well as armed conflicts in the contemporary environment of state, regional and global security.

KEYWORDS

European Union; mediation; Kosovo; Serbia; Conflict; Resolving conflicts.

REFERENCES

Bercovitch J. (2009). Mediation success or failure: a search for the elusive criteria, Cardozo Journal of Conflict Resolution, *7*, 289. Retrieved from https://sfinc.ch/wp-content/uploads/2018/09/SFINC-Mediation-Success-orFailure.pdf

Bercovitch J., & Jackson R. (2009). *Conflict resolution in the Twenty-first Century – principles, methods and approaches*. University of Michigan Press.

Bergmann, J. (2020). The European Union as International Mediator. Brokering Stability and Peace in the neighborhood. Basingstok: Palgrave Studies in European Union Politics.

Deutsch, M. (2006). Cooperation and Competition. In: M. Deutsch, P. T. Coleman, & E. C. Marcus (Eds.), *The Handbook of Conflict Resolution. Theory and Practice*. San Fransisco; Jossey-Bass a Wiley Imprint.

International Court of Justice (ICJ) (2010). *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*. Advisory Opinion.

Londano, L.C.M. (2003). The Effectiveness of International Mediation –The current debate. *International Law: Revista Colombiana de Derecho Internacional*, 2. Retrieved from https://www.redalyc.org/pdf/824/82400210.pdf

Stanicek B. (2021). *Belgrade-Pristina dialogue. The rocky towards a comprehensive normalization agreement.* Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689371

Society's readiness to defend against possible aggressor's invasion: the case of Lithuania

Česnuitytė (1)

(1) General Jonas Žemaitis Military Academy of Lithuania, vida.cesnuityte@lka.lt

ABSTRACT

Military actions in Ukraine highlighted a need to revise Lithuania's readiness to defend the country in case of possible aggressor's invasion. As a separate question, the readiness of society to defend the state arose. A peaceful life during the last few decades has "put the society to sleep", delegating defence issues to the Lithuanian army and NATO. On the opinion of the population, Lithuania own would not be able to defend itself against an external invasion, only the help of NATO would provide such an opportunity. Though, Ukrainian example reveal importance of the society members' role, and their contribution in defence of the country with and / or without gun.

The research aim is to explore readiness of Lithuania society's members to contribute to the state's defence in case of possible aggressor's invasion.

KEYWORDS

Armed Forces; Society; Aggressor's.

RESEARCH METHODOLOGY

The following research hypotheses formulated: H1: Members of Lithuania society intend to defend the state in case of possible aggressor's invasion. H2: Considering long years of peace in Europe, most habitants of Lithuania aren't prepared for the defence of the state from external invasion.

The hypotheses test is based on the empirical data collected within the implementation of the research project "Sociological studies of the development of the Lithuanian Armed Forces in the changing international security environment" that is funded by the Ministry of National Defence of Lithuania. A field-work of this representative quantitative survey was conducted in October-November, 2021. In total, 1053 respondents of 15+ years of old were questioned face-to-face. A standardized questionnaire as a survey instrument was used.

MAIN FINDINGS

While asked which groups' security worn them, the survey participants mostly focused own nuclear and extended families, in average – on local community and population of Lithuania, and less – on European and World population. If an enemy attacks Lithuania or there is a real threat of attack, 54% of the respondents state that they defend the country with or without a gun, and only 11% would leave the country. At the same time, 58% of the respondents state that they definitely don't know or rather don't know how to what they should do to protect themselves and own family in the threat of war. The answers differ according to social-demographic characteristics of the respondents: a little bit greater knowledge and awareness to defend the country was demonstrated by individuals between 20-49 years of old, with Higher education, and better financial situation in the household / family; in the meantime, variations according to ethnicity or size of the living place not detected.

The low percentage of the latter calls for investment on habitants' knowledge about defence. Four fifths of the respondents would accept lectures on country defence at schools, and almost three quarters would accept such lectures at workplace. The mostly accepted possible lectures on the topics how the population will be evacuated from the war zone (59%), what to do if someone, not being a soldier, appear in a war zone (48%), which public services will be accessible and how (34%), how society's members can contribute to defence without being a soldier (28%), and how will the mobilization of the population into the military forces and aid squads be organized (25%). To be noted that topics on what to do if someone, not being a soldier, appear in a war zone, how society's members can contribute to defence without being a soldier, what will be your duties to contribute to national defense at your workplace, and how will the mobilization of the population into the military forces and aid squads be organized were more accepted by the younger respondents blow 49 years of old. Meanwhile, the topics on how the population will

be evacuated from the war zone, and which public services will be accessible are more interesting for those of 50 or more years of old.

CONCLUSIONS

The research results proved hypothesis H1, and revealed of at least most of Lithuania society's intention to contribute to the state's defence in case of possible aggressor's invasion. Also hypothesis H2 was proved by showing that almost half of population lack of proper knowledge how to defend the country with or without gun.

To be noted, that attitudes and knowledge on the issues much related to social-demographic characteristics of the society's members, therefore for improvement of the situation, the applied methods should be differentiated.

The survey was conducted in pre-Ukrainian war time, therefore it can be presumed that answers of the survey participants were not affected by the escalation of the security situation. Now, research results, likely, would be different, and it is reason for continuation of the research.

Security for "the people": Populism's potential impact on the EU's security agenda

D. Gal (1)

(1) Institute for Political Studies of Defense and Military History, Romania, galdorin07@gmail.com

Populism is establishing itself as one of the ideas with the most potential of influencing modern-day international relations and defense initiatives, both inside conference rooms and outside of them. Positioned firmly within the realm of liberal democracy, its general image is that of a discourse that is not only critical of society's elites(Müller, 2017, p. 2) and demands that power be given back to the people, but also as a volatile and "thincentered" ideology (Mudde, 2004, p. 544).

This volatile nature allows populists to tailor their speech for increased popular support, making them particularly dangerous to actors vulnerable to it such as the European Union. Considering the EU's new Strategic Compass and aims to become a reliable security provider, this paper looks to prove the negative impact that populism can have on the Union's security and defence initiatives, and on international military cooperation as a whole. With approximately 40% of current European populist parties being against increased defence cooperation within the EU's framework (De Spiegeleire, Skinner, & Sweijs, 2017, p. 85), this is a risk that must be carefully managed.

This paper doesn't solely take into account the discourse of populist political parties, but also the general feeling of the population in regard to these issues, particularly since populists can bypass the standard political spectrum through the use of social media platforms. As a result, any defence initiatives that rely on consensus and public acceptance are at risk. Using data gathered from academic sources and documents regarding the political use of social media, I will use the EU's Strategic Compass as a case study, postulating potential scenarios.

The aim is to emphasize the way in which both populist actors and tendencies can constrain European defense cooperation. They can use it as an issue through which to mobilize the electorate and win votes, particularly since both left-wing and right-wing populist parties emphasize ideas that can challenge European cooperation in this field (Henke & Maher, 2021, p. 393). While it's worth noting that such attitudes result more from their overall Eurosceptic viewpoint rather than their doubts about defence cooperation, the populist discourse has the potential to impact this area as much as it did the efforts of European federalization a few years ago.

KEYWORDS

Populism; Defence; European defence.

REFERENCES

De Spiegeleire, S., Skinner, C., & Sweijs, T. (2017). *The rise of populist sovereignism: What it is, where it comes from, and what it means for international security and defense.* The Hague Centre for Strategic Studies.

Henke, M., & Maher, R. (2021). The populist challenge to European defense. *Journal of European Public Policy, 28*(3), 389-406. doi: https://doi.org/10.1080/13501763.2021.1881587

Mudde, C. (2004). The populist zeitgeist. *Government and opposition, 39*(4), 541-563. doi: https://doi.org/10.1111/j.1477-7053.2004.00135.x

Mudde, C., & Kaltwasser, C. R. (2017). *Populism: A very short introduction.* Oxford University Press.

Müller, J.-W. (2017). *What is populism?* Penguin.

The role of Securitization in maintaining national security: Balkan perspective influenced by Afghan refugees

V. Katerina (1)

(1) MIT University – Skopje, Faculty of Security Sciences, Macedonia, veljanovska_katerina@yahoo.com

Following the rise of Taliban forces to power in Afghanistan, governments in Albania, Kosovo, and North Macedonia have accepted a US request to provide temporary shelter to some political refugees fleeing the country for fear of retaliation. This is a need for analysis of several aspects, ie logistical, technical, security and social issues that is crucial to be taken into account (Arboleda, & Hoy, 1993, p. 69). What is in focus is that the United States is a major ally and strategic partner of North Macedonia, on the basis of which the country has accepted civilians from Afghanistan who need evacuation but who are allowed to stay in the country until a lasting solution is found for them. All this is in the spirit of North Macedonia in international relations as a country of solidarity, providing support and assistance in large-scale disasters.

This situation is in fact a lesson from the Afghan experience of the proclaimed security and stabilization policies, as well as relations with the United States and other regional powers, the issue of migration and other open areas circulating in this area. More specifically, according to Clayton (2021), it is an analysis of the immediate security implications for Europe, but also an analysis of the wider role of the United States in the Middle East, including the impact on ongoing stabilization efforts (Graham, & Poky, 2000).

Within this paper, an analysis from several relevant sources, as well as primary empirical research is implemented. The scientific analysis is based on the empirical research framework that refers to the Republic of North Macedonia, includes the application of qualitative research, implemented by a group of 20 experts, university professors, media representatives and government officials. Additionally, a focus group of 20 students which are educated in the frame of security studies are included, regarding a discussion on current trends within the migration crisis.

The International Organization for Migration is especially relevant with the positive popularization of the migrant movement in a country, in order to find a way of understanding and acceptance by the domestic population (Fernie, Pitkethly, 1998). Additionally, Bigo (2002, p. 70) states that migration provides a series of positive benefits for one region (in this case Balkan region), i.e. encouraging social and economic development through migration, and above all by meeting the operational challenges of this global phenomenon from which no country is left out.

According to Clarke (1972), mobility in conditions of migration is especially needed in globalization and development of its benefits. However, there was an almost unified view that all countries needed to work together to ensure orderly, safe, regular and responsible migration and mobility (Graham, & Poky, 2000). According to Bogue. only in this way it can be brought under control and realized in a way that will not allow human rights violations (1959).

According to the above, hate speech has been noticed in a certain domain on social networks, but all this is due, above all, to the spread of misinformation. As an example of untruths are some claims that the new wave of refugees will bring in the Balkan an increase in crime and rape rates, as well as that migrants are terrorists who will greatly endanger the state and the security of the population.

According to Balzacq (2011), securitization theory analyses the construction and deconstruction of threats as a social reality by using speech acts, images, tools and practices. Ratha and collaborators (Ratha, Mohaptra, & Scheja, 2011), considers security as a 'speech act', which is not given but constructed through a discursive process. The Copenhagen School considers traditional approaches insufficient to understand post-Cold War security challenges including civil strife, illegal migration, refugee crisis, environmental degradation, climate change, transnational terrorism, and health epidemics. Knudsen (2001), has thus widened the scope of security to other spheres other than military including economic, environmental, societal, and political sectors. According to Davies (2008), sectors of securitization help us better analyze which referent objects are framed as being subject to an existential threat. Chandna (1998), identify states, sovereignty or the ideology of states, national companies, collective identities such as nations and religions, and individual species and climate as the possible referent objects in the military, political, economic, societal and environmental sectors, respectively.

According to Aradau (2004, p. 391), securitization is measured by the expression of public satisfaction/dissatisfaction. Furthermore, in the case of Afghan refugees, the discourse of "securitization" is used to identify Afghan refugees as deepening economic problems and a threat to the country's domestic stability and security. Also, Afghan refugees themselves are securitized by presenting themselves as vulnerable and poor people (Hughes, 2007).

The main focus and goal of this scientific paper is to analyse securitization as important for strengthening national security from external influences, such as migration wave.

KEYWORDS
Securitisation: Afghan; Refugees; Balkan; National; Security.

REFERENCES
Aradau, C. (2004) Security and the Democratic Scene: Desecuritization and Emancipation. *Journal of International Relations and Development, 7*(4), 388-413.

Arboleda, E., & Hoy, I. (1993). The Convention Refugee Definition in the West: Disharmony of Interpretation and Application. *International Journal of Refugee Law, 5*(1), 66-90.

Bogue, D. J. (1959). *Internal Migration.* In: P. M. Hauser, & O. D. Duncan (Eds), *The Study of Population.* Chicago: University of Chicago Press.

Bigo, D. (2002). Security and Immigration: Towards a Critique of the Governmentality of Unease. *Alternatives, 27* (Special Issue), 63-92.

Clarke, J. I. (1972). *Population Geography* (2nd Ed.). Oxford: Pregamon Press.

Clayton, T. (2021). *U.S. Military Withdrawal and Taliban Takeover in Afghanistan: Frequently Asked Questions.* Congressional Research Service. Report.

Chandna, R.C. (1998). *Population.* New Delhi: Kayani Publishers

Davies, J.A. (2008). Clashing Civilizations or Conflicting Interests?. *Geopolitics, 13.*

Fernie, J., & Pitkethly, A. (1998). *Resources, environment and policy.* London: Harper and Row.

Graham, D.T., & Poky, N.K. (2000). *Migration globalization and human security.* London: Routledge.

International Migration Law. (2004) *Glossary on Migration.* Geneva.

Hughes, B. (2007). Securitizing Iraq: The Bush Administration's Social Construction of Security. *Global Change, Peace and Security, 19*(2), 83-102.

Knudsen, O. F. (2001). Post Copenhagen Security Studies: Desecuritizing Securitization. *Security Dialogue, 32*(3), 355-368.

Ratha, D., Mohaptra, S., & Scheja, E.(2011). *Impact of migration on economic and social development: a review of evidence and emerging issues.* Policy Research Working Paper.

Building resilience to disinformation disseminated in social media

D. Domalewska (1)

(1) War Studies University, Poland, d.domalewska@akademia.mil.pl

Interference in the current affairs of democratic countries has long been known as a harmful process. It is a strategy for mostly covert, secret manipulation of the strategic interests of other states. The best example is disinformation and propaganda which are spread in a target country to interfere in its domestic politics, to promote certain agenda, to influence the decision-making capacity, to increase polarization, and to cause chaos. Due to the severity of consequences of hybrid threats to state security, building societal resilience is of utmost importance. The most effective way of fighting hybrid threats is to be prepared for them. Based on the investigation of past actions, democratic states may draw up legislation whereas independent organizations can strengthen fact-checking initiatives and educational activities. However, since hybrid threats, especially disinformation, are most often disseminated through social media, it is important to consider how social networking sites can fight interference and malicious activities.

Based on the analysis of Facebook posts and tweets published during presidential elections and social protests taking place in Poland in 2020 (N=3,014M), I will discuss current malicious activities carried out on social media, focusing on disinformation disseminated through automatic social media accounts (malicious bots) and its effect on the public opinion. The study has proved the activity of a large amount of accounts exhibiting unethical behaviour (most probably bots) engaged in public discussion in social media, in particular during social protests and to a lesser extent during the 2020 presidential elections.

Given a wide range of malicious behaviour present in social media, I will discuss strategies for building societal resilience. First, I will discuss fact-checking as an initiative to detect and debunk fake news. In Poland fact-checking is mainly carried out by media companies and non-governmental organizations. Through the content analysis of fake news identified by these initiatives in 2020, substantial differences in the amount and content of false information identified by the fact-checkers have been observed, which leads to interesting conclusions on their efficiency as far as disinformation detection is concerned. Finally, I will give examples of activities carried out by social networking sites to decrease the extent of malicious activity and lower its effect on the public.

KEYWORDS

Strategic communications; Social media; Hybrid threats; NATO.

9862

Armed Forces challenges in new disruptive socio-ecological scenarios of the 21st century Anthropocene

H. Júnior (1) and M. Santos (2)

(1) University of Vigo (Spain) and CIDIUM/IUM (Portugal), handradejunior@gmail.com
(2) UTAD, Portugal, mgsantoss@gmail.com

The Armed Forces are organizations traditionally prepared for security and defence matters, covering a spectrum of actions in extreme and crisis situations of various orders. The military apparatus in human and material terms has an eminently destructive function, where science and the art of war merge, from the beginning of military school learning. Throughout contemporary history, military personnel have studied technical and tactical aspects of psychological, biological, chemical, nuclear (WW I and II) and cyberwarfare. As an example, warfare with a socio-ecological impact was used in Vietnam by the US and by Saddam Hussein in the Gulf War, with the deliberate burning of oil wells. Other impacts of fearful repercussions continue to occur in the Ukraine War. Thus, military actions bring notable environmental impacts, wherever they go. It is suggested that such organizations assume the socio-ecological responsibility for their actions in a global and not just rhetorical way. Their forces, skills and resources directly applied to the alleviation of vectors as pandemics, migrations, hunger, ethnic conflicts and in natural and man-made disasters are needed. Around the world, concrete cases of applied competence of the armed forces in environmental tragedies are known. Thus, the contribution of this article is amplify a discuss that the armed forces of each country, acting together in international cooperation or in non-military aliances, would be better able to mitigate the socio-ecological impacts caused by them, going to more in addition. As an international call in the context of the Anthropocene XXI, military personnel will commonly be requested for preparation, training and logistics to face extreme situations and this is already guaranteed frequency. Extreme situations include the pandemics, pitfalls and threats caused by climate change such as floods, fires, earthquakes, landslides, severe storms or major natural erosion. The general population, in these states of chronic environmental crisis, will need specialized help for their rescue, for the losses suffered within a large number and range of systemic disruptions, such as the lack of electrical energy, the commitment of the fuel supply, the reduced food supply or disrupted telecommunications/digital networks. These are undoubtedly challenges for militaries around the world, as the threats will come from various dimensions and from all sides, and not just from an environmental perspective. As they are crisis-prepared institutions that are sometimes created by themselves, they should be further discussed in the socioecological framework of the Anthropocene and beyond.

KEYWORDS

WG8 – Defence Management and Economics

Requirements Management in the Portuguese Navy – An Application to Shipbuilding Projects

G. Ferreira (1) and P. Água (2)

(1) Escola Naval, Portugal, marques.ferreira@marinha.pt
(2) Escola Naval, Portugal, pedroagua@gmail.com

Nowadays, project management has an impact on world GDP bigger than ever, and organizational project management maturity is a critical capability for organizations to address the challenged posed by projects. In the defence context and due to the nature of defence projects, which are highly adaptive, characterised by innovation, uncertainty, and risk, such organizations demand the finest project management capabilities. Within project management, Requirements Management is considered a critical capability which is accountable for a big slice of a project's success. Since the Portuguese Navy is willing to ensure the acquisition (and building) of new ships to guarantee its numerical and qualitative presence in its operational environments, requirements management has become crucial for projects' goals achievement. The aim of this study was to find "where" and "what" it can be improved towards the Navy's improved requirements management.

This research is framed according to William Dettmer's Constraint Model Management (Dettmer, 2003), and associated logical thinking tools, using the following steps: (1) defining the paradigm, (2) analysing the mismatches, (3) creating a transformation, (4) designing the future, and (5) planning the execution. In order to get a realistic perception of the current reality of the Navy's requirements management practices, in-depth interviews were performed to core member of the Navy's project management teams (Boyce & Neale, 2006).

This investigation allowed some findings; specifically, that the main causes for the underperformance of projects are related to organizational issues, such as teams' resilience and training, absence of internal instructions for requirements development, weak engagement with stakeholders and the inadequate requirements statements definition (Hood, Wiedemann, Fichtinger, & Pautz, 2008; INCOSE, 2012). This is causing undesirable effects such as overbudgeting, delay and missed scope of the project, and also loss of project management knowledge and disengagement with stakeholder, in an organizational viewpoint. Consequently, the solution for these concerns relies in the implementation of new strategic guidelines. The implementation of the proposed solution is expected to ensure and adequate requirements management in order to effectively ensure budget, schedule, and scope conformance. Moreover, it also intends to encourage the growth of organizational knowledge concerning requirements management and to enhance a cooperative environment that ensures an appropriate stakeholder engagement (PMI, 2016).

The solution suggests several specific measures or lines of action; from the suggestion for a revision of Public Procurement policies, in order to improve project management activities in highly adaptive projects (as is the nature of shipbuilding projects), to the implementation of standards for requirements writing and process development are also recommended, in order to establish common practices that are globally employed and that can ensure proper execution guidelines. A new strategic guideline related with the deployment of a requirements management tool/software could also guarantee a more accountable and effective management of requirements and, consequently, an improved requirements change management process. Similarly, the implementation of a stakeholders management tool, capable of doing the adequate register, characterization, and grouping of stakeholders; could avoid or minimize the lack of some stakeholders engagement. Finally, the last suggested measures are concerned with the personnel certification in project management standards or methodologies since the certification of core members of projects teams could represent an increment to the quality of project development in practice. Figure 1 summarises some of the findings within the accomplished study.

Figure 1 – Executive Summary Tree of the New Strategic Guidelines

Moreover, this study also considered the potential adoption of the Model Based Systems Engineering (MBSE) approach as the next step to improve the way defence acquisition and systems engineering develops in order to ensure the finest project management performance within the context of defence projects. A few *de facto* approaches are setting the standard (e.g., *SysML, IBM Raphsody* or *Capella*) and following associated success cases would be advised for overall requirements management improvement as well as project management proficiency in the context of defence.

KEYWORDS

Constraints Management Model; Project Management; Requirements Management; Strategy Analysis.

REFERENCES

Boyce, C. & Neale, P. (2006). Conducting in-depth interview: a guide for designing and conducting in-depth interviews for evaluation input. *Pathfinder International Tool Series, Monitoring and Evaluation* (2). Retrieved from https://nyhealthfoundation.org/wp-content/uploads/2019/02/m_e_tool_series_indepth_interviews-1.pdf

Dettmer, W. H. (2003). *Strategic navigation: a systems approach to business strategy.* Milwaukee: ASQ Quality Press

Hood, C., Wiedemann, S., Fichtinger, S., & Pautz, U. (2008) *Requirements management: the interface between requirements development and all the other systems engineering processes.* Berlin: Springer

INCOSE (2012). *Guide for writing requirements.* International Council on Systems Engineering. San Diego: CA.

PMI (2016). *Requirements management: a practice guide.* Pennsylvania: Project Management Institute, Inc.

5136

Dynamic Maintenance in Ships

S. Lampreia (1), V. Lobo (2) and V. Vairinhos (3)

(1) CINAV, Portugal, suzana.paula.lampreia@marinha.pt
(2) CINAV, Portugal, vlobo@novaims.unl.pt
(3) CINAV, Portugal, valter.vairinhos@sapo.pt

ABSTRACT

One of the main objectives of naval mechanical engineers is to guarantee good maintenance of the ship's equipment and avoid unplanned downtime. This is a very important issue both in warships and merchant ships. In an environment with limited resources, optimizing and prioritizing maintenance actions is crucial and will contribute to reduce costs and increase the ship's availability and performance. Condition Based Maintenance policies have proven to be the most efficient in accomplishing that optimization, but they require a lot of data, and this data must be well organized in an appropriate data structure. Since a ship is complex system in constant modification, the maintenance priorities will change as more recent data is collected, giving rise to Dynamic Maintenance systems, that impose certain conditions on those data structures. In this paper we discuss the data structures for maintenance actions that should be available to enable efficient implementation of analysis, prediction, and planning algorithms to support Dynamic Maintenance Systems.

KEYWORDS

Maintenance; Database; Dynamic; Ship.

INTRODUCTION

All mechanical systems require maintenance, so there is a lot of research in this area, with an increasing number of scientific papers published in this area. For example, a search for the keyword "Maintenance" (M) in Google Scholar, will yield approximately 5.7 million papers. Our interest in this area stems from the need of enhancing maintenance process performance, due to the lack of material and human resources.

DYNAMIC MAINTENANCE

There are several types of approaches regarding the different types of maintenance policies. In this paper we used the framework described in the European Standard for Maintenance Terminology EN (2017). This standard considers two types of maintenance, preventive, and corrective. The first one can be systematic, condition-based and on demand, and the second can be immediate or postponed.

Aside from considerations of existing types of maintenance, considering condition-based and data-based maintenance, various statistical and software approaches can be applied.

It is believed that modern maintenance can't be carried out without an implement condition-based maintenance system and decision based in algorithm that process selected data from equipment's and systems.

Dynamic Database-Driven value has been exposed by Davis and Robbins (2022) in a basis that dynamic database should always be available online and the systems must be constantly actualized because of the change in electronic sensors and resources.

By implementing intelligent systems in maintenance management in ships, these systems should be integrated in the Information Security Management Systems (ISMS) that are being implemented in merchant ships, and where should be implemented applied cybersecurity rules (DNV.GL, 2021) to mitigate eventual cyberattacks.

CASE STUDY - MAINTENANCE DATABASES

In the organization understudy there is a System of Data Treatment Collection (SRTD) (Marinha, 1984), that nowadays are represented by a software that supports the surface-ships maintenance requests and reports, SICALN.

The SICALN has various documents, the one used for requests and report maintenance is the DSM58, the one for time functioning, operationality report, and marine gasoil and lubricant consumption, it has also the DSM60 that are used for spare parts requests.

The database is constantly actualized, so the future applied decision algorithm results will be variable accordingly data variation

CONCLUSIONS

Due the objective of high performance in companies and organizations, although means restriction, the maintenance responsible´s are changing maintenance philosophies and automatizing systems and databases processing.

The organization understudy already has a system of data treatment collection.

It is possible to develop a database that receive data from the already existing software, SICALN, and treat the information.

It was presented the sub-databases that should constitute the main database. Further work will be developed for conceive a decision-making system.

ACKNOWLEDGMENT

REFERENCES

EN (2017). *EN 13306 – Maintenance Terminology*. Europe: European Standards.

Marinha (1984). *Data Collection and Processing System Manual (Manual do Sistema de Recolha e Tratamento de Dados (SRTD)) (ILMANT512)*. Alfeite: Direção de Navios.

Global, I. (2022). *IGI Global - Publisher of Timely Knowledge*. Retrieved from https://www.igiglobal.com/dictionary/dynamic-maintenance-chinagrid-support-platform/8509

Davis, F., & Robbins, L. (2022). Potentials of Dynamic Database-Driven Web Sites.

He, Z., & Darmont, J. (2005). Evaluating the Dynamic Behavior of Database Applications. *Journal of Database Management, 16*(2), 25. doi:10.4018/jdm.2005040102.

MIT (2021). *Machine Learning Course.* Massachusetts Institute of Technology - Massachusetts - USA: MIT-Professional Education.

DNV.GL (2016). *Cyber security resilience management for ships and mobile offshore units in operation. Recommended Practice - DNVGL-RP-0496*. [Online]. Retrieved from https://www.dnv.com/maritime/dnvgl-rp-0496-recommended-practice-cybersecurity-download.html

Portuguese Army Additive Manufacturing. Capability Development – Preliminary Study

P. Pinheiro (1), L. Quinto (2), A. Machado (3), M. Leite (4), É. Chambel (5), P. Peças (6), A. Ribeiro (7) and P. Fernandes (8)

(1) Regimento de Manutenção, Portugal, pinheiro.pmb@exercito.pt
(2) Academia Militar, Portugal, luis.quinto@academiamilitar.pt
(3) Unidade de Apoio Geral de Material do Exército, Portugal, machado.ajsc@exercito.pt
(4) Instituto Superior Técnico, Portugal, marcoleite@tecnico.ulisboa.pt
(5) Academia Militar, Portugal, enio.chambel@academiamilitar.pt
(6) Instituto Superior Técnico, Portugal, ppecas@tecnico.ulisboa.pt
(7) Instituto Superior Técnico, Portugal, relogio.ribeiro@tecnico.ulisboa.pt
(8) Regimento de Manutenção, Portugal, fernandes.pjn@exercito.pt

Many organizations maintain significant spare parts inventories to avoid equipment downtime due to component failure. Because of the nature of military operations, component failure can result in financial losses, the cancellation of planned operations, or even the risk of military and civilian personnel's lives. Military operations can take place anywhere in the world, under various external conditions, influencing equipment in unpredictable ways. Large quantities of spare parts are transported to mission regions to avoid costly system downtime, yet critical components sometimes fail, and spare parts are not always available (Boer, Lambretchs , & Krikke, 2020). In such cases, spare parts must then be shipped from the home country depots or purchased from external suppliers. In some cases, lead times could be weeks or months long.

Additive Manufacturing (AM) has been identified as a promising sourcing option for manufacturing parts on-site, close to the point of demand (Begley, 2017). AM can be used to temporarily provide spare part availability until a standard or conventional spare component becomes available, decreasing system downtime and enhancing strategic autonomy (Costa, Silva, Velloso, Amador, & Dâmaso, 2019).

In this context, in 2020, the Portuguese Army (PRT Army) developed the Army Logistic Support through Additive Manufacturing (ALSAM) research project. Its main objective is to capacitate the PRT Army with methodologies and resources that allow for the manufacture of dual-purpose components to support the Military Operations (e.g., spare parts supply for deployed contingents or during supply chain shortages) and for civilian support (e.g., during catastrophes). The project includes three research activities, namely: 1) state-of-the-art and identification of case studies; 2) design and development of components to support the PRT Army; 3) development and testing of prototypes both in the laboratory and in field conditions. This work focuses on the state of the art and identification of case studies to analyze and implement maintenance methodologies based on AM. For that purpose, extensive research has been conducted to identify the best practices and lessons learned by key international organizations and several other nations.

The subject of AM has been studied by several international organizations, including the North Atlantic Treaty Organization (NATO) and the European Defence Agency (EDA). NATO identifies AM as one of the main areas of research and development with disruptive potential (Reading and Eaton, 2020). This organization has already developed documentation on the future of manufacturing technologies for military applications (Busachi et al., 2018) and is currently studying the interoperability of AM in combined operations (NATO, 2022). Meanwhile, EDA presents AM as a key technology for European military capabilities, with several related activities underway, namely the Additive Manufacturing for Logistic Support (AMLS) (EDA, 2021).

In addition to international organizations, states have been conducting research programs for the application of AM in their Armed Forces or at a governmental level. For example, the Department of Defense (DoD) of the United States has published a strategy for implementing AM (DoD, 2021a), as well as a policy for the use of AM in the DoD (DoD, 2021b). Furthermore, in mid-2018, the US Army defined its Additive Manufacturing Implementation Plan, whose objective was to develop an overarching strategy and framework to integrate and synchronize Army AM capabilities to enable its warfighting capabilities (Goodly, 2018). More recently, the US Army has included in its Maintenance Operations Doctrine the use of additive manufacturing technologies to support the tasks of Maintenance, Repair & Operations (MRO) (Department of the Army, 2019).

As for Canada, after weighing the benefits and drawbacks of AM in its deployed land forces, the Canadian Armed Forces concluded that this technology will be significant and that its development cannot be neglected (Levac, 2018).

By implementing such technology, the Royal Netherlands Army (RNLA) expects to reduce the required on-site storage space and enhance asset availability in the mission area (Westerweel, Basten, Boer, & Houtum, 2021). Considering the economic impact of AM, in several cases, overall cost reductions of more than 50% have been achieved. (Westerweel et al., 2021). As a result, on-site AM provides a strategic advantage, reducing the RNLA's reliance on insecure supply lines and allowing them to operate more efficiently and effectively in foreign missions (Westerweel et al., 2021).

In 2021, the PRT Army deployed AM capability to the Central African Republic. Different case studies have been identified, and several parts have been produced *in loco* and applied to repair various types of equipment, resulting in an increased readiness level. Based on the lessons learned from these case studies, the following steps will involve the revision of the current doctrine, aiming to include AM in the PRT Army's Logistic Doctrine.

KEYWORDS

Additive Manufacturing; 3D printing; Defence; Military Logistics; Armed Forces.

ACKNOWLEDGMENTS

REFERENCES

Begley, L. (2017). *Increasing Capabilities and Improving Army Readiness trough Additive Manufacturing Technologies*. Army War College.

Boer, J., Lambrechts, W., & Krikke, W. (2020). Additive manufacturing in military and humanitarian missions: Advantages and challenges in the spare parts supply chain. *Journal of Cleaner Production*, 257.

Busachi, A., Kuepper, D., Brunelli, J., Heising, W., Moeller, C., Fischer, D., Watts, C., Drake, R., Salter, K., & Banfi, S. (2018). *Additive Manufacturing – Rapid Support System (AM-RS2): Concept Design of a deployable AM unit for War Theatre*. NATO Science and Technology Organization.

Costa, G., Silva, M. C., Velloso, N., Amador, P., & Dâmaso, T. (2019). Impactos da impressão 3d num futuro próximo. *IUM Atualidade*, 17. Lisboa: Instituto Universitário Militar.

Department of Defense. (2021a). *Department of Defense Additive Manufacturing Strategy*. Washington: Office of the Under Secretary of Defense for Research and Engineering.

Department of Defense. (2021b). *DoD Instructions 5000.93 – Use of Additive Manufacturing in the DoD. Office of the Under Secretary of Defense for Research and Engineering*. Washington.

Department of the Army. (2019). *ATP 4-33 Maintenance Operations*. Washington: US Army.

European Defence Agency. (2021). Additive manufacturing – A capability enabler for logistic support. *Fact Sheet*.

Levac, M. (2018). *3D printing and its implications on army sustainment*. Canada: Canadian Forces College.

NATO. (2022). *2022 Collaborative Program of Work*. NATO Science and Technology Organization

Reding, D. F., & Eaton, J. (2020). *Science & Technology Trends 2020-2040*. Brussels: NATO Science & Technology Organization.

Westerweel, B., Basten, R. J. I., Boer, J., & Houtum, G. J. (2021). Printing spare parts at remote locations: fulfilling the promise of additive manufacturing. *Production and Operations Management, 30*(6), 1615–1632.

Delivering more competition and less protectionism? - Estimating the effects of Directive 2009/81/EC on European defence markets

L. Kananoja (1), J-M. Lehtonen (2), J. Kosonen (3) and J. Lintunen (4)

(1) Finnish National Defence University, lauri.kananoja@mil.fi
(2) Finnish National Defence University, juha-matti.lehtonen@mil.fi
(3) Finnish National Defence University, jesse.kosonen@mpkk.fi
(4) Finnish National Defence University, julia.lintunen@mpkk.fi

European defence markets are duplicative and fragmented, and EU member states protect their national defence industries (Hartley 2003; Hartley 2011). European Commission (2013) estimated that over 80 percent of the defence materiel by the member states were procured from national firms. Furthermore, different offset policies have been used to support national industries (Hartley 2003; Kanniainen & Lehtonen 2019). Without more collaborative projects creating economies of scale (Trybus 2014) and more competition, economic benefits reduce. To solve this, European Commission introduced directive 2009/81/EC, aimed at providing transparent and equal treatment and competitive tendering for defence and security contracts, once applicable and valued above certain thresholds. However, Article 346 TFEU provides possibility to exempt procurement of military equipment from the EU public procurement rules. As a result, most defence and security contracts are awarded based on national rules of member states, hindering the establishment of European defence markets. (European Commission 2016).

This paper examines the effects of the directive 2009/81/EC. We consider the directive and its national legislative implementations as a policy change and reflect our results against the policy targets. We first use national defence industrial strategies of the EU member states before and after the policy change to analyze how member states take into account the directive. Furthermore, we group the member states as protectionist or nonprotectionist based on their strategic documents. We then use a panel dataset of the official reported EU defence materiel exports from 2004 to 2020 to estimate the competition increase and protectionism decrease. Our null is that competition has increased and protectionism decreased, based on the reports of the European Commission (2016) that the directive adds value in a form of more competition, transparency, non-discrimination and less exemptions.

For modeling competition increase in the EU defence markets, we use a fixed effects model. We model the number and value of licenses issued for all the member states. We use defence budgets, defence materiel and R&D investments, industry and military force sizes and alliance dummies as regressors and control for member state characteristics. As a result, we find the effect of national implementation of the directive for the competition increase for each member state inside European defence markets. For a robustness check and comparison, we further apply the model for exports from EU member states to United States and Canada and for exports to non-EU member states in Europe.

For modeling protectionism in the EU defence markets, we use a difference-in-difference method. We take the directive 2009/81/EC as a treatment and use the strategy analysis grouping member states as protectionist or non-protectionist. We expect the protectionist member states not being affected by the treatment, making these our control group. Accordingly, we expect the non-protectionist member states being affected by the treatment, making these our treatment group. Taking domestic procurement (= investments – imports) as an outcome we get a proxy for protectionism. As a result, we find evidence of the treatment effect for the member states.

Provided the results for competition increase and protectionism decrease, we discuss whether the results correspond to the strategies analysed in the first part of the paper. Combining strategy analyses and econometric modeling provides us a sufficient framework for EU wide policy suggestions with respect to improving the effectiveness of the directive 2009/81/EC. Recent legal framework related papers have focused on firm performance (Callado-Muñoz et al. 2022) or export performance of firms in the defence sector (Castellacci & Fevolden 2014), restructuring of the defence sector (Arteaga 2014), or partial strategic autonomy (Lundmark 2022), making our approach unique.

KEYWORDS

European Union, defence markets, competition, protectionism, econometrics.

REFERENCES

Arteaga, F. (2014). A Proposal for restructuring the security and defence sector in Spain. *Defence and Peace Economics, 25*(1), 69-83. doi:https://doi.org/10.1080/10242694.2013.857463.

Callado-Muñoz, F.J., Hromcová, J., Sanso-Navarro, M., Utrero-González, N., & Vera-Cabello, M. (2022). Firm Performance in Regulated Markets: The Case of Spanish Defence Industry. *Defence and Peace Economics, 33*(2), 201-218. doi:https://doi.org/10.1080/10242694.2020.1783622.

Castellacci, F., & Fevolden, A. (2014). Capable companies of changing markets? Explaining the Export Performance of Firms in the Defence Industry. *Defence and Peace Economics, 25*(6), 549-575. doi: https://doi.org/10.1080/10242694.2013.857451.

Hartley, K. (2003). The future of European defence policy: An economic perspective. *Defence and Peace Economics, 14*(2), 107-115. doi: https://doi.org/10.1080/10242690302921.

Hartley, K. (2011). *The Economics of Defence Policy. A new perspective*. London: Routledge.

European Commission (2013). *Towards a more competitive and efficient defence and security sector. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions*. Brussels, 24.7.2013. COM(2013) 542 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0542&from=EN

European Commission (2016). *Evaluation of Directive 2009/81/EC on public procurement in the fields of defence and security. Commission Staff Working Document*. Brussels, 30.11.2016. SWD(2016) 407 final. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/b3a0e4a2-b6f4-11e6-9e3c01aa75ed71a1/language-en/format-PDF

Kanniainen, V., & Lehtonen, J-M. (2019). Offset Contracts as an Insurance Device in Building the National Security. *Defence and Peace Economics, 30*(1), 85-97. doi: https://doi.org/10.1080/10242694.2017.1335366.

Lundmark, M. (2022). The Evolution Towards the Partial Strategic Autonomy of Sweden's Essential Security Interests. *Defence and Peace Economics, 33*(4), 399-420. doi: https://doi.org/10.1080/10242694.2021.1992713

Trybus, M. (2014). *Buying Defence and Security in Europe*. Cambridge: Cambridge University Press.

The impact of the composition of defence expenditure on economic development in the Baltic countries

G. Dudzevičiūtė (1)

(1) General Jonas Žemaitis military academy of Lithuania, gitana.dudzeviciute@lka.lt

Growing internal and external security threats and Russia's war in Ukraine are forcing countries to revise their defence budgets, with increased allocations and a reallocation of funds among defence activities. The Baltic countries are no exception, where the focus on defence funding has increased since Russia invaded and annexed Crimea in 2014.

In a scientific context, the question is whether rising defence funding will harm economic development. Which defence financing activities have an impact on economic growth? Over the past years, many researchers (Almajdob, & Marikan, 2021; Becker, & Dunne, 2021; Dimitraki ,& Win, 2021; Gentilucci, 2020; Nugroho, & Purwanti, 2021; Raju, &Ahmed, 2019; Santamaria, Garcia, & Gonzalez, 2021; Susilo, Sari, Putra, & Pratiwi, 2022) have investigated the link between defence spending and economic development, with mixed results in the countries studied.

The results are contradictory, and four possible effects can be identified, namely positive, negative, no relationship, and the impact of economic growth on defence spending (Santamaria, Garcia & Gonzalez, 2021).

The author then goes on to present the results of some studies. The study by Dimitraki and Win (2021) revealed positive short-run and long-run relationships between defence expenditure and economic growth in Jordan between 1970 and 2015. Santamaria, Garcia, and Gonzalez (2021) examined the impact of defence expenditure on the growth of NATO's countries in 2005 – 2018. The results confirmed that the existence of five different groups can be identified in NATO countries.

Moreover, it can be argued that the impact is greater in the nuclear countries than in the other groups. The investigation by Susilo, Sari, Putra and Pratiwi (2022) revealed that defence expenditure had a positive and significant impact on the value of GDP during the COVID-19 pandemic in 40 developing countries with upper-to-middle-income levels. The research of 27 lower-middle income countries from 2002 to 2018 suggested that the military expenditure had a negative impact on economic growth, although the results are not significant (Nugroho, & Purwanti, 2021). Becker and Dunne (2021) noted that research rarely examines defence spending by major categories such as personnel, equipment, infrastructure, and other. However, they can be expected to have different impacts on economic development.

This investigation aims to assess the impact of defence expenditure by main categories in Lithuania, Latvia, and Estonia. The study covers the period between 2004 and 2021. The author uses automatic linear modelling (ALM), which allows to process the data with several automatic methods and to select the appropriate forecasting model.

The results show that in the three Baltic States, total defence spending has a significant positive impact on economic development. In Lithuania, it explains 76.2% of the variation in real GDP per capita, 78.3% in Latvia, and 77.6% in Estonia. Looking at the impact of defence spending on economic development by main categories, it was found that in Lithuania spending on equipment positively impact on economic development. In Latvia, spending on personnel is the main contributor to economic development, while in Estonia it is operating and maintenance expenditure.

These insights could be useful for the implementation of the Sustainable Development Goal (SDG) on economic growth in the Baltic States.

KEYWORDS

Defence expenditure; Economic development; Baltic countries.

REFERENCES

Almajdob, M. S., & Marikan, D. A. A. (2021). The Impact of Military Spending on the Economic Growth of Arab Spring Countries. *International Journal of Academic Research in Business and Social Sciences, 11(3), 1436-1451*. doi:10.6007/IJARBSS/v11-i3/9276. Retrieved from https://hrmars.com/index.php/IJARBSS/article/view /9276/The-Impact-of-Military-Spending-on-TheEconomic-Growth-of-Arab-Spring-Countries.

Becker, J., & Dunne, J.P. (2021). Military Spending Composition and Economic Growth. *Defence and Peace Economics.* doi: 10.1080/10242694.2021.2003530. Retrieved from https://www.tandfonline.com/doi /full/10.1080/10242694.2021.2003530.

Dimitraki, O., & Win, S. (2021). Military Expenditure Economic Growth Nexus In Jordan: an Application of Ardl Bound Test Analysis in the Presence of Breaks. *Defence and Peace Economics, 32 (7),* 864-881. doi: 10.1080/10242694.2020.1730113. Retrieved from https://www.tandfonline.com/doi/full/10.1080/ 10242694.2020.1730113.

Gentilucci, E. (2020). A Causality Analysis. Military Expenditures and Economic Growth in USA and China. *MPRA Paper No. 104848*. Retrieved from https://mpra.ub.uni-muenchen.de/104848/.

Nugroho, D.A., & Purwanti, E.Y. (2021). Impact of Military Expenditure on Economic Growth: Encouraging or Constraining? *JEJAK: Jurnal Ekonomi dan Kebijakan*, 14(1). doi:https://doi.org/10.15294/jejak.v14i1.26062. Retrieved from https://journal.unnes.ac.id/nju/index.php/jejak/article/view/26062/11440.

Raju, M.H., & Ahmed, Z. (2019). Effect of Military Expenditure on Economic Growth: Evidences from India Pakistan and China Using Cointegration and Causality Analysis. *Asian Journal of German and European Studies, 4*(3). Retrieved from https://link.springer.com/article/10.1186/s40856-019-0040-6.

Santamaria, P. G-T., Garcia, A.A., & Gonzalez, T.C. (2021). A Tale of Five Stories: Defence Spending and Economic Growth in NATO´s Countries. *PLoS ONE, 16 (1):* e0245260. Retrieved from https://doi.org/10.1371/journal.pone.0245260.

Susilo, A.K., Sari, D.W., Putra, I. N., & Pratiwi, N. A. (2022). Economic Growth and Military Expenditure in Developing Countries during Covid-19 Pandemic. *Applied Econometrics and International Development, 22*(1), 19-38. Retrieved from https://www.usc.es/economet/reviews/aeid2212.pdf.

3514

Security financing - priority investments of the Three Seas Initiative (3SI) in the context of the needs of Central and Eastern Europe and the war in Ukraine

M. Gębska (1)

(1) War Studies University, Poland, m.gebska@akademia.mil.pl

The concept of creating the 3SI emerged as early as 2012-2013, during talks between Polish businessmen and Ian Brzezinski - an American expert in the field of security and international politics. They reflected on the further development of Poland and the Central and Eastern European region. The result of the talks was the finding that the political and organizational changes in the countries of the region since 1989 need to be continued in the form of further investment in infrastructure. It was also concluded that membership in the EU and NATO must be accompanied by adequate economic development, deepening the region's security (Trójmorze. D. Fried, I. Brzezinski, G. Mosbacher, https://trimarium.pl/en/fried-mosbacher-brzezinski-what-is-the-three-seas-initiativefrom-vision-to-action/).

In November 2014 The Atlantic Council (AC) and Central Europe Energy Partners published an 83-page report entitled: "Completing Europe. From the North-South Corridor to Energy, Transportation, and Telecommunications Union" (*Completing Europe...* 2014). The report's authors highlighted the security environment in Central and Eastern Europe in the 21st century, including geopolitical, geo-economic factors affecting the region's changing security and future. In particular, the report highlighted three elements of Europe's security system and environment. The first was Europe's political and economic situation. The authors of the report stated that Europe was under pressure from external and internal forces, and centrifugal political and economic forces challenged its cohesion and unity. The second thesis stated that the European Union faced a number of external threats, such as a resurgent Russia, increasing global economic competition and geopolitical upheavals, which are affecting the EU's diminishing resilience, resulting in serious implications for the transatlantic community. According to the third thesis of the report's authors, economic growth and energy security are pillars of EU resilience.

Although the Atlantic Council report did not mention the name "3SI" or any other name associated with this form of cooperation, and the recommendations did not include incentives for the creation of a new form of cooperation in Europe, the report was undoubtedly familiar to the originators of the 3SI. Recommendations in the areas of energy, transport and digitization overwhelmingly coincided with the goals of the 3SI declared during its summits . Also, the chapter on finance reflected many of the practical solutions implemented and promoted by the Initiative.

The 3SI was officially announced in 2015 by Polish president Andrzej Duda and Croatian president Kolinda Grabar-Kitarović, and began operations in 2016. It is not an international organization, but a platform for cooperation, it is just forming its identity, developing forms and scopes of cooperation, and beginning to be visible and recognizable in the international security community. The 3SI implements its investment projects not only using the Three Seas Initiative Investment Fund (3SIIF), but primarily through the use of domestic funds, from the EU and the European Bank for Reconstruction and Development. In the case of this type of financing, it is the states, together with the co-financiers, that decide the order in which the projects are to be implemented, taking into account the priorities of the 3SI, the main objective of which is to improve the economic security of the countries that form it and the region as a whole, including, above all, the reduction of energy dependence and the development of infrastructure, including critical infrastructure.

3SIIF is a fund combining public and private entities, created for the purpose of making investments in 3SI. The willingness to use the resources of the 3SIIF has been expressed by all member countries, except Austria. The fund operates on a commercial basis and operates under Luxembourg law, like many other funds bringing together international investors. The 3SIIF collects and disburses the funds of the 3SI. The funds are earmarked for priority investments in energy, transportation and digitization infrastructure. The 3SIIF is operated and managed by Amber Infrastructure Group (Amber), which is an independent private international manager, handling some 150 investments from around the world, 50 of which are greenfield in 2021. 3SIIF-funded investments are to come from the following sources:
- National funds from the state budget for the implementation of specific investments;
- Funds from the European Union (and potentially other international organizations);
- Funds from private investors recognizing the possibility of profit from a specific investment.

241

It is estimated that the 3SIIF is able to raise between 3 and 5 billion euros to subsidize investment projects in the medium term, which is why it is looking for potential investors to co-finance it. In 2021, discussions were underway about 3SIIF's financing from sources including: EIB, EBRD, World Bank, Nordic Investment Bank, pension funds and investors from Canada, Japan, South Korea, the Netherlands and Finland. The IFC has also pledged the possibility of contributing financially to the Fund. In February 2020, U.S. Secretary of State Mike Pompeo pledged $1 billion in financial support as part of two supporting institutions - US International Development Finance Corporation (DFC - U.S. International Development Finance Corporation. *U.S. International Development Finance Corporation Begins Operations*, https://www.dfc.gov/media/pressreleases/us-international-development-finance-corporation-begins-operations) and the Blue Dot Network program. 3SSIF is seeking investment funds from private entities as well.

The 3SI takes on particular importance in the context of Russia's aggression against Ukraine in February 2022. Even before Russia's aggression, the 3SI was planning to implement several infrastructure projects involving Ukraine, but also Moldova and Georgia. The intensive cooperation of countries within the Initiative encourages countries outside the Initiative to join the 3SI and the EU and resolve conflicts peacefully, but also Russia's aggressive and destabilizing actions in its neighborhood. Ukraine's aspirations to join 3SI, were expressed by Volodomyr Zelensky and the Ukrainian parliament in October 2020, and demonstrate the attractiveness of the EU and the 3SI. The EU as a whole and the 3SI will be of exceptional importance once the war is over and in rebuilding Ukraine after its victory over Russia. Ukraine's European aspirations and the importance of the 3SI for regional security were reaffirmed in June 2022 at the Seventh Summit in Latvia and with the recognition of Ukraine as an official EU candidate country on June 23, 2022.

KEYWORDS

Security; Three Seas Initiative; Investments; Ukraine; Critical infrastructure.

REFERENCES

Atlantic Council and CEEP. (2014). *Completing Europe. From the North-South Corridor to Energy, Transportation, and Telecommunications Union*. Washington.

Fried, T. Brzezinski, I., & Mosbacher, G. (n.d.). *Fried, Mosbacher, Brzezinski: What is the Three Seas Initiative? From Vision to Action*. Retrieved from https://trimarium.pl/en/fried-mosbacher-brzezinski-what-is-the-three-seas-initiative-fromvision-to-action/

Defense Resources Management in the 21st Century: A Research from the Strategic Management Perspective

E. Caymaz (1)

(1) Canakkale Onsekiz Mart University, Turkey, ebru.caymaz@comu.edu.tr

ABSTRACT

Defense resources management can be broadly defined as the effective and efficient allocation of resources to achieve a country's defense goals. The majority of studies on defense resources management either focus on the allocation of financial resources or examine defense resources from a financial perspective. However, today's rapidly changing conditions have necessitated a more comprehensive framework in which the dimensions of strategic management, its antecedents as well as its components entail a dynamic and flexible management process consisting of strategic planning, capability planning, resource planning, and supply chain planning. Currently, as an integrative management field, strategic management of defense resources benefits from a wide variety of disciplines including finance, organizational behaviour, marketing, and human resources management. Accordingly, this study aims to critically outline the process of defense resources management from the strategic management perspective.

INTRODUCTION

Defense organizations cannot be established independently of a state's political, administrative, and cultural phenomena. Developing, reforming, and transforming a national defense organization requires the maturation of a coherent concept with sufficient breadth and depth to effectively and efficiently carry out the politically determined tasks and functions. On the other hand, the core concept of a defense organization is supposed to reflect national management culture and traditions, the existence of managerial capacity at the political, macro-organizational, and performance levels, the private business environment, educational capacities, and its society's readiness to accept innovations and comprehensive changes. However, allocation of defense resources while ensuring transparency is a subtle task even in competent defense planning systems in which decision-making processes are dominated by a rational approach (Bucur-Marcu et al., 2009; Tillman et al., 2010). Furthermore, the failure to establish a systematic process has become the most common problem in defense resources management.

In order to address the recent challenges in the defense environment, this study dwells on the theoretical background of strategic management. In the broadest sense, strategic management is defined as managerial decisions and practices which determine the long-term performance of an organization (Kenny, 2006). Propelled by technology, today's rapidly changing conditions have necessitated a more comprehensive framework in which the dimensions of strategic management, its antecedents as well as its components entail a dynamic and flexible management process consisting of strategic planning, capability planning, resource planning, and supply chain planning. These planning processes and their subcategories have strategic aspects extending from medium to high levels that complement each other. Accordingly, being an integrative management field, strategic management of defense resources benefits from a wide variety of disciplines including finance, organizational behaviour, marketing, and human resources management. The next session further discusses defense resources management in the 21st century from the strategic management perspective.

DEFENSE RESOURCES MANAGEMENT IN THE 21ST CENTURY

Up to the present, the defense field has mainly been dominated by two major fields: the economy and security issues (Ibanez et al., 2020). However, the types of threats, the operational environment, management techniques as well as organizational structures have undergone a major transformation (Berzins, 2020; Magula et al., 2022; Taylor, 1990). In a previous study by Tagarev (2006, p.69), defense resource management was examined from the program-based implementation framework and the common problems experienced both by new NATO members as well as Partner states were outlined as:
- The lack of sufficient defense planning experience especially in business process management,

- Insufficiency in the assessment of cost-effectiveness and design of defense programs,
- Organizational resistance,
- The lack of commitment from senior executives.

In addition to developments especially within the field of AI technologies, the contemporary operational environment presents several challenges and opportunities. Therefore, there has been a paradigm shift within the initial scope of the term "resource" and it has acquired strategic aspects through the term "asset" (Taillard, 2014). Asset management mainly focuses on budgets, work management, and lifecycle activities. The growing number of asset management studies also indicate a multilateral organizational setting in which a holistic approach towards all types of defense resources has been recognized (Taillard, 2014). Herein, from a strategic management perspective, budgets involve key performance indicators including maintenance costs and current performance while work management involves human resources, skills, and capability development. Aside from reliability, availability, safety, and dependability of assets, lifecycle activities contain asset care with a special focus on asset condition, location, interventions, as well as life extension.

CONCLUSION

Defense resource planning, along with talent and acquisition planning, constitutes two of the four main planning processes in the defense management system. In order to ensure security and the use of limited resources allocated to defense effectively and efficiently, it is imperative for every state to develop a unique, dynamic, modern, and comprehensive defense resource management process. This study concludes that developing a defense resources management framework in which assessment management is successfully being implemented is highly significant to address the security challenges associated with the 21st century. Strategic leadership becomes another significant issue in this process in which developing the ability to foster competing demands and enduring competencies rather than teaching perishable skills becomes prominent.

REFERENCES

Berziņs, J. (2020). The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *The Journal of Slavic Military Studies, 33*(3), 355–380.

Bucur-Marcu, H., Fluri, P., & Tagarev, T. (2009). Defence management: An Introduction. *Security and Defence Management*, 1. Geneva; DCAF.

Ibanez, J. S., Garraton, M. C., & Soto Meca, A. (2020). A Literature Review of DEA Efficiency Methodology in Defence Sector. *Academia Revista Latinoamericana de Administración, 33*(3/4), 381403.

Kenny, J. (2006). Strategy and the Learning Organization: A Maturity Model for the Formation of Strategy. *The Learning Organization, 13*(4), 353-368.

Magula, J., Rouland, M., & Zwack, P. (2022). *NATO and Russia: Defense and Deterrence in a Time of Conflict*. Defence Studies.

Tagarev, T. (2006). Introduction to Program-Based Defense Resource Management. *Connections, 5*(1) (Spring-Summer), 55-56.

Taillard, M. (2014). Asset management. In: Analytics and modern warfare. New York: Palgrave Macmillan. Retrieved from https://doi.org/10.1057/9781137407870_16.

Taylor, T. (1990). Defence Industries in International Relations. *Review of International Studies, 16*(1), 5973.

Tillman, M. E., Gollwitzer, A. H., Parlier, G. H., Fletcher, C. V., & Hinkle, W. P. (2010). *Defense resource management studies: introduction to capability and acquisition planning processes*. Institute for Defense Analyses, IDA Document D-4021.

3D printed guns – a threat or a possibility

S. Rautio (1) and M. Broms (2)

(1) Finnish National Defence University, samu.rautio@mil.fi
(2) Tampere University, Finland, mika.broms@tuni.fi

Additive Manufacturing (AM) - more commonly 3D printing - has emerged as a potential manufacturing method alongside traditional manufacturing methods (Lemu, 2019). AM can be used to make parts and tools, not only for friendly but also for damaging use, such as weapons (Walther, 2015). Manufacturing weapons with a new manufacturing method can affect various security authorities such as the military, police, border guards, customs, and security services. On the other hand, it can allow 3D printed weapons to be used for authorities' own regular needs or special situations (Sensiba, 2021). On the other hand, it may pose a threat to their tasks (Daly, Mann, Squires & Walters, 2021).

The first 3D printed weapon that become widely known to the public was the "Liberator" developed by Cody R. Wilson in May 2013. At the time, 25-year-old university student Cody R. Wilson was rebelling against gun laws. He designed a 3D printing of a weapon invisible in a metal detector. He released digital models of the weapon freely available on the Internet. It can be said that the digital revolution in the manufacture of 3D printing utility weapons had begun and it had achieved one of its major but worrying crossings (Wilson, 2017). Since 2013, various 3D printable gun models have been published both freely available on the Internet and as development projects of different organizations. See Table 1.

Table 1 – Sample of 3D printed gun concepts and parts

Gun model / part	Designer	Model	3D printed parts	Printing time	Material	Year
Liberator	Cody Wilson	Pistol	14	approx.20 h	ABS	2013
AR15 Lower Receiver	Cody Wilson	Part of AR-15 semi-automatic rifle	1	approx.9 h	ABS	2013
1911 DMLS 9mm	Solid Concepts Inc	9mm pistol	33	approx.34 h	Stainless steel, Inconel 625, PA12	2013
Glock body	Deterrence Dispensed	Glock 9mm pistol body	1	approx.11 h	ABS	2016
Rapid Additively Manufactured Ballistics Ordnance (RAMBO)	The Armament Research, Development, and Engineering Center (ARDEC)	40mm grenade launcher pistol	30-40	approx.48 h	4340 steel, Aluminum, ABS, PL12	2016
FGC-9	Jacob D / Deterrence Dispensed	9mm submachine gun	17	to all parts approx.90 h	PLA+	2020

In March 2020, the Deterrence Dispensed group released 3D models of a printable self-loading submachine gun. With models, the group had drawn up detailed manufacturing instructions for printable parts and parts to be procured. The purpose of the group was to make the most efficient and easy-to-manufacture homemade semiautomatic weapon available to people with limited weapons manufacturing skills and equipment (CTRLPEW, 2022). This 3D gun model has spread around the world (Defcad, 2021) and is designed to produce a usable weapon. In Finland, in June 2021, customs unveiled a weapons factory where nine printers printed FGC-9 gun parts. Customs considered seized 3D printed weapons quite useful (Kerkelä, 2021). With the development of 3D printing technology and materials, the potential of the method for the production of usable weapons has increased.

The aim of the study is to find out how the spread of 3D printed weapons and their use can affect the authorities dealing with weapons. The study examines the potential of the new manufacturing method and whether it poses a threat to their operation. On this basis, conclusions can be drawn about the changes in policies that research is causing.

The method of the study is Delphi - more specifically, future scenario planning (Crawford & Wright, 2016). Thus, 3D printed weapons are a new phenomenon, the future is difficult to predict. Therefore, researchers have created three key future scenarios for the manufacture and use of 3D printed weapons: most likely, potential, and most dangerous development. Experts gathered from various Finnish authorities, respond and reflect to the statements based on these scenarios. The survey results are collected through a web-based system with two or more rounds of survey comments.

In the study, we follow four basic Delphi principles: 1. Anonymity - experts do not know about the participation of other experts, 2. iterative activities - experts can shape or change their opinion or view throughout the iteration cycle 3. controlled and open data processing - all respondents see and comment on each other's answers and 4. the research is carried out on a qualitative basis - qualitative methods are generally used as methods for analyzing the data, although quantitative sampling of the data is possible (Linstone & Turoff, 2002).

Based on the expected preliminary results of the study, different authorities have different perspectives on the use of 3D printed weapons. Printing parts of weapons can improve the user experience of their own weapons in use, as well as develop the individual features needed for them. On the other hand, the unpredictability of the 3D printed weapons can pose risks to both users and the authorities facing the weapons. Militarily, the rapid manufacture of weapons - even tailored to their intended use - can enable completely new ways to utilize weapons in their operations.

Legal factors related to 3D printed weapons have been published in several studies (Talbot & Skaggs, 2021; Tran, 2014). The study of the use itself from the point of view of the authorities and especially the soldiers have hardly been published. This study brings a new perspective to the use of 3D printed weapons - not only from a criminal or anti-government perspective but also from the perspective of how authorities can take advantage of this new technology. At the same time, it brings new perspectives to the debate on how their use should be taken into account in training, and operations.

KEYWORDS

Additive manufacturing; 3D printing; 3D printed guns; Military Technology.

REFERENCES

Crawford, M. M.;& Wright, G. (2016). Delphi Method. In StatsRef, *Statistics Reference Online,* 1-6.
CTRLPEW. (2022, 20 April). *Print Every Weapon*. Retrieved from: https://ctrlpew.com/
Daly, A., Mann, M., Squires, P., & Walters, R. (2021). 3D printing, policing and crime. *An International Journal of Research and Policy, 31*(1).
Defcad. (2021, 16 April). *FGC-9 Mk2 9mm Pistol*. Retrieved from https://defcad.com/library
Eromäki, V. (2021, 9 June). *Mitä tamperelaisesta 3D-asetehtaasta tiedetään nyt? Tullin valvontajohtaja: "Valtaosan aseesta pystyy printtaamaan"*. Retrieved from https://yle.fi/uutiset/3-11972755
Lemu, H. G. (2019). On Opportunities and Limitations of Additive Manufacturing Technology for Industry 4.0 Era. In K. Wang, Y. Wang, J. Strandhagen & T. Yu, *Advanced Manufacturing and Automation VIII. IWAMA 2018. Lecture Notes in Electrical Engineering.* Singapore: Springer.
Linstone, H. & Turoff, M. (2002). *The Delphi Method - Techniques and Applications.*
Sensiba, J. (2021, 11 December). *Gun Control's Death Throes: Burmese Rebels Use FGC-9 3D-Printed Guns to Resist Army Coup*. Retrieved from: https://www.thetruthaboutguns.com
Talbot, T. & Skaggs, A. (2021). Regulating 3D-Printed Guns Post-Heller: Why Two Steps Are Better Than One. *The Journal of Law, Medicine & Ethics*. doi: https://doi.org/10.1177/1073110520979407
Tran, J. L. (2015). The Law and 3D Printing. *The John Marshall Journal of Information Technology and Privacy Law 505*, *31*(4).
Walther, G. (2015). Printing Insecurity? The Security Implications of 3D-Printing of Weapons. *Science and Engineering Ethics, 21*, 1435–1445. doi: https://doi.org/10.1007/s11948-014-9617-x
Wilson, C. (2017). *Come and Take It: The Gun Printer's Guide to Thinking Free.* Gallery Books .

Contributions to the decarbonization of military activity

M. Matos (1), P. Água (1) and A. Frias (1,2)

(1) CINAV/IUM, Portugal, marlene.elisabete.matos@marinha.pt
(2) CINAV/IUM, Portugal, pedroagua@escolanaval.pt
(3) CINAV/IUM, Portugal, silva.frias@marinha.pt

INTRODUCTION

Sustainability dominates the concerns of today's society. Within military activity is also an important research topic, witnessing a trend that favors multidisciplinary approaches to the detriment of a focus on one of the pillars of sustainability (Smaliukiene, 2018). The adoption of solutions to improve the sustainability of military installations and operational activity may require different approaches, given its own specificity (Borglin et al., 2010; Saritas & Burmaoglu, 2016).

This work aims to identify solutions that allow the Portuguese Navy to become more sustainable: reduce expenditure on energy acquisition and its environmental footprint, while fostering social development. Using comparative analysis, intends to identify good practices adopted by other entities, which may be transferable to the reality under study.

Lisbon Naval Base (BNL) occupies an area of approximately 2.4 km^2 where it houses the Portuguese Navy main infrastructures. More than 3800 people work there. Due to its dimension and relevance, improving the sustainability of the activities can contribute positively to the sustainability of the region.

EXTRAPOLATIVE COMPARATIVE STUDY

The breath and diversity of the activities developed at BNL allow multiple lines of action towards its sustainability.

Green energy production

To support its activity, BNL consumes more than 20 million kW/year. In addition to numerous roofs and coverings where it would be possible to install photovoltaic panels, there are more than 50,000 m^2 for car parking.

In 2019, one of the national TV broadcasters (RTP) implemented a photovoltaic plant for self-consumption in a car park, with an installed power of 234 kWp. Taking as a reference the expected production values for the described RTP project, it would be possible to produce more than 5.8 million kWp/year. This corresponds to around 30% savings in total annual electricity consumption, in addition to other associated advantages.

Sustainable gardens

Porto Business School created what is considered the largest urban garden in the country on a building roof. With an estimated production of about 3 ton/year of food, this project aimed to reduce the carbon footprint, water consumption and production of organic waste. Production is intended for the preparation of meals, distribution by employees and donation by social institutions (Agrotec, 2021).

BNL has vast spaces to implement sustainable gardens. The creation of community gardens to be distributed to active military personnel, reserve and reform would be a way of promoting social intergenerational integration and the corporate image of the Navy.

Management of the Alfeite Green spaces

BNL has a considerable green area that needs intervention, namely reforestation by native plants, control of invasive species and the forest fuel mass that potentiates the occurrence of fires.

The creation of partnerships with entities specialized in reforestation with native species such as FUTURO -Project (CRE.Porto) and the application of regenerative agriculture procedures (Antunes, 2022), can be beneficial.

Other areas

Intervention possibilities are not limited to the identified areas. Activities such as mobility, water management, energy efficiency of buildings or waste collection are fields where there are also possibilities for improvement.

CONCLUSION

BNL has physical, infrastructural and population conditions, which allows the adoption of various measures to improve sustainability, thus contributing to society and to the corporate image of the Navy.

Energy dependence, due to its economic weight and impact on different areas, can be reduced using photovoltaic production.

The need to carry out a correct management of the existing green spaces constitutes an opportunity to implement measures that improve sustainability and fire risk. The existence of community gardens can bring social, economic and environmental benefits.

Areas such as water and waste management are likely to present good examples with the potential to be applied at BNL, contributing, as a whole, to reducing the Navy's carbon footprint and increasing local sustainability.

KEYWORDS

Decarbonization; Green energy; Military activities; Sustainability.

REFERENCES

Agrotec (2021). *Porto Business School e Noocity unem-se para cultivar a maior horta urbana do país* [Página online]. Retrieved from http://www.agrotec.pt/noticias/porto-business-school-e-noocity-unem-se-para-cultivar-a-maiorhorta-urbana-do-pais/

Antunes, A. (2022) Agricultura regenerativa "O truque do maneio está no equilíbrio". *Revista Ruminantes, 45*, 016-020. Retrieved from https://issuu.com/ruminantes/docs/_book_45_ld/s/15404798

Borglin, S., Shore, J., Worden, H., & Jain, R. (2010). An overview of the sustainability of solid waste management at military installations. *International Journal of Environmental Technology and Management, 13*(1), 51-83. doi: https://doi.org/10.1504/IJETM.2010.032534

ECO.AP (2020). *Central Fotovoltaica para Produção de Energia Elétrica em Autoconsumo* [Página online]. Retrieved from https://www.barometroecoap.pt/wp-content/uploads/2020/04/01.-Artigo-Fotovoltaico_VF_02.pdf

CRE. Porto (2022). *Futuro: O projeto das 100.000 árvores* [Página online]. Retrieved from https://www.100milarvores.pt/

Saritas, O., & Burmaoglu, S. (2016). Future of sustainable military operations under emerging energy and security considerations. *Technological Forecasting and Social Change, 102*, 331-343. doi: https://doi.org/10.1016/j.techfore.2015.08.010

Smaliukiene, R. (2018). Sustainability Issues in the Military: Genesis and Prospects. *Journal of Security & Sustainability Issues, 8*(1), 19-32. doi: https://doi.org/10.9770/jssi.2018.8.1(2)

NORAD: A specialization of the joint-products model

O. Secrieru (1), U. Berkok (2) and K. Lee (3)

(1) Royal Military College of Canada, oana.secrieru@rmc.ca
(2) Royal Military College of Canada, berkok-u@rmc.ca
(3) Royal Military College of Canada, kaminpeyrow@gmail.com

NORAD (North American Defence Command) is a two-country alliance of Canada and United States against potential missile attack. The Northern Warning System (NWS), an early detection mechanism, was created in 1957 to centralize operational control of continental air defenses against the threat of Soviet bombers. The installation consisted of the Distant Early Warning Line (DEW Line) and the mechanism of aerospace control for North America. In the late 1980s the DEW Line was replaced by the current NWS of 47 radar sites spanning the North American land mass from the Atlantic to the Pacific Oceans. Since threats have evolved over time and more drastically recently with the addition of supersonic gliding vehicles that can launch missiles from afar and at supersonic speeds, NORAD capabilities had to be modernized.

Beyond the technological ageing of the current system, a spatial challenge arose as a result of the recent expansion of the Canadian ADIZ (Air Defence Identification Zone) in 2018. The modernized NORAD may not only have to expand its sensors layer to far out into the Arctic but also cope with that challenging environment to surveil with a wide range of threats from multiple adversaries, traditionally Russia and now China with its global ambitions in the Arctic environment. Moreover, a new generation of multi-mission sensors that can detect a spectrum of threats have to be installed into harsh climate conditions in vast spaces with no existing infrastructure to support them, unlike modifications to the existing NWS radar stations. While space-based sensors can complement the ground and underwater based censors in the surveillance of the Arctic, new challenges and tradeoffs may arise in terms of right orbits needed to build the new multi-layered system.

The requirement for this bundle of high-tech equipment and the engineering challenges of the new defences will necessitate budgets in the range of tens of billions of dollars. The burden-sharing becomes critical to the modernization of the alliance technology.

The original joint-products model cannot capture this NORAD bilateral alliance between Canada and the U.S. due to the asymmetric nature of fundamental inputs into the surveillance and early-warning system. Namely, Canada's contribution of land and U.S.'s contribution of technology generate a "specialize and trade" NORAD organization, which requires differentiation of Canada's contribution beyond a mere defence activity. For clarity, we use a quasi-linear utility function to compensate for an augmentation of defence activity into two inputs into the public and private defence goods. The jointness of the private and public goods components of the alliance output will then determine the extent to which free-riding will be alleviated as the publicness of the alliance output then depends on the tradeoff between technology transfer and land use.

KEYWORDS

Joint products; Alliances; Burden-sharing; Defence budgets.

Analysing the Portuguese military managers personal background association with management control systems use

L. Godinho (1)

(1) Portuguese Air Force and ISEG, godinho.lmm@afa.ium.pt

Recent military organizations reforms were implemented with the goal of improving organizational adaptation and learning processes to increase flexibility and innovation processes, transforming them into agile organizations based on networking (Eisenberg et al., 2018). Public sector extant literature findings support that higher Management Control Systems (MCS) use is associated to sustainability, efficiency, effectiveness, economic, and balanced decision-making processes (Heinicke, & Guenther, 2020; Martyn et al., 2016; Simons, 1995). Additionally, a balanced MCS use enables organizational adaptation and innovation capabilities, augment and sustain resiliency, promotes organizational learning and management attention to improve strategic goals performance (Bracci, & Tallaki, 2021; Simons, 1995). Military Defence organizations are relevant within countries central budget (Felício et al., 2021), but in MCS literature they are the least studied as the organizational unit (Godinho, & Gonçalves, 2020; Navarro-Galera et al., 2014).

I build upon Simons' Levers of Control (LOC) framework (Simons, 1995) to study MCS use in Portuguese military organizations, and understand how military managers emphasize MCS use, adopting a contingency-based approach (George et al., 2019). The objective is to test empirically the military managers' different perceptions of LOC inter-dependencies and complementarities, and the upper echelon theory effect of age and military core training personal characteristics (Hambrick, 2007; Hambrick, & Mason, 1984). The questionnaire is adapted from extant literature (Naranjo-Gil, & Hartmann, 2006; Widener, 2007) to the convenient sample of Portuguese Armed Forces military in management functions, at different Services and subunits. The 281 valid responses were received from May to July of 2021. I test Simons' LOC complementarity and the impact of military manager's personal characteristics on the perceived MCS use hypothesis, using partial least squares structural equation modelling (PLS-SEM) and multigroup analysis.

 I find support for Simons' LOC use complementarity and inter-dependency, similar to private and public extant literature (Heinicke et al., 2016; Pilonato & Monfardini, 2020; Widener, 2007). The mean values for each Lever of Control reveal medium emphasis, and are lower than those found in public sector extant research (Heinicke & Guenther, 2020; Matsuo et al., 2021; Naranjo-Gil, 2016; Naranjo-Gil & Hartmann, 2006, 2007). Results support the older managers association to higher interactive use emphasis, similar to public higher education organizations (Bobe, & Kober, 2020), but opposite to public hospital sector (Naranjo-Gil et al., 2009). Additionally, through PLS-SEM multigroup analysis, I find significant differences (p < 0,05) in MCS use between younger and older military managers, with the older subgroup revealing greater Levers of Control emphasis. The remaining military managers' demographic characteristics, rank and education level, do not reveal significant differences (p > 0,05) in MCS use between their subgroups.

I identify limitations associated to the study design, as are the single-sector and single-country participants, and cross-sectional data collection, that do not allow findings generalization.

This research contributes to the Defence economics and management studies, public sector MCS literature (Chenhall, 2003; Otley, 2016; Van der Kolk, 2019), and fills a literature gap in military organizations studies as the organizational unit (Godinho & Gonçalves, 2020). I identify relevant findings to academics and practitioners. To military managers, I identify relevant and significant MCS use emphasis (p < 0,05), and associations between Levers of Control and managers' personal background, supporting Simons' Levers of Control propositions (Simons, 1995) and upper echelon theory (Hambrick, 2007; Hambrick, & Mason, 1984). To military sciences scholars, identifying future research paths to increase knowledge regarding military organizations as organizational units, and how to promote performance. Scholars and military managers may use these findings to better understand military organizations managers MCS use and its differences to other organizational settings, public or private. The military organization's units may need, more than ever, to be studied as health care organizations are, recognizing Defence and management studies, as health economics and management are today, to assist military managers' goals in their specific setting to maintain or increase resilience capability, sustainability, and efficiently support the decision-makers.

REFERENCES

Bobe, B. J., & Kober, R. (2020). University dean personal characteristics and use of management control systems and performance measures. *Studies in Higher Education, 45*(2), 235–257. doi:10.1080/03075079.2018.1504911

Bracci, E., & Tallaki, M. (2021). Resilience capacities and management control systems in public sector organisations. *Journal of Accounting & Organizational Change, 17*(3), 332-351. doi:10.1108/JAOC-102019-0111

Chenhall, R. H. (2003). Management control systems design within its organizational context: findings from contingency-based research and directions for the future. *Accounting, Organizations and Society, 28*(2-3), 127-168. doi: 10.1016/S0361-3682(01)00027-7

Eisenberg, D. A., Alderson, D. L., Kitsak, M., Ganin, A., & Linkov, I. (2018). *Network Foundation for Command and Control (C2) Systems: Literature Review*. IEEE Access, 6, 68782–68794. doi:10.1109/ACCESS.2018.2873328

Felício, T., Samagaio, A., & Rodrigues, R. (2021). Adoption of management control systems and performance in public sector organizations. *Journal of Business Research, 124* (June 2020), 593-602. doi: https://doi.org/10.1016/j.jbusres.2020.10.069

George, B., Van de Walle, S., & Hammerschmid, G. (2019). Institutions or Contingencies? A Cross-Country Analysis of Management Tool Use by Public Sector Executives. *Public Administration Review, 79*(3), 330- 342. doi:10.1111/puar.13018

Godinho, L. M., & Gonçalves, T. (2020). Defense Organizations Budgeting and Management Control Systems in Restrictive Budgets Context – Literature Gaps. *Smart Innovation, Systems and Technologies, 181*, 391-397. doi:10.1007/978-981-15-4875-8_34

Hambrick, D. C. (2007). Upper Echelons Theory: An Update. *Academy of Management Review, 32*(2), 334-343. doi: 10.5465/amr.2007.24345254

Hambrick, D. C., & Mason, P. A. (1984). Upper Echelons: The Organization as a Reflection of Its Top Managers. *Academy of Management Review, 9*(2), 193–206. doi: 10.5465/amr.1984.4277628

Heinicke, A., Guenther, T. W., & Widener, S. K. (2016). An examination of the relationship between the extent of a flexible culture and the levers of control system: The key role of beliefs control. *Management Accounting Research, 33*, 25-41. doi: 10.1016/j.mar.2016.03.005

Heinicke, X., & Guenther, T. W. (2020). The Role of Management Controls in the Higher Education Sector: An Investigation of Different Perceptions. *European Accounting Review, 29*(3), 581-630. doi: 10.1080/09638180.2019.1619603

Martyn, P., Sweeney, B., & Curtis, E. (2016). Strategy and control: 25 years of empirical use of Simons' Levers of Control framework. *Journal of Accounting & Organizational Change, 12*(3), 281-324. doi: 10.1108/JAOC-03-2015-0027

Matsuo, M., Matsuo, T., & Arai, K. (2021). The influence of an interactive use of management control on individual performance: mediating roles of psychological empowerment and proactive behavior. *Journal of Accounting & Organizational Change, 17*(2), 263-281. doi: 10.1108/JAOC-06-2020-0079

Naranjo-Gil, D. (2016). Cómo los equipos de dirección usan los sistemas de información y control en la gestión hospitalária. *Gaceta Sanitaria, 30*(4), 287-292. doi: 10.1016/j.gaceta.2015.12.009

Naranjo-Gil, D., & Hartmann, F. (2006). How Top Management Teams Use Management Accounting Systems to Implement Strategy. *Journal of Management Accounting Research, 18*(1), 21-53. doi: 10.2308/jmar.2006.18.1.21

Naranjo-Gil, D., & Hartmann, F. (2007). How CEOs use management information systems for strategy implementation in hospitals. *Health Policy, 81*(1), 29-41. doi: 10.1016/j.healthpol.2006.05.009

Naranjo-Gil, D., Maas, V. S., & Hartmann, F. G. H. (2009). How CFOs Determine Management Accounting Innovation: An Examination of Direct and Indirect Effects. *European Accounting Review, 18*(4), 667-695. doi: 10.1080/09638180802627795

Navarro-Galera, A., Muñoz-Leyva, F., Maturana, R. I. O., & Rubio, J. L. (2014). Factors influencing the modernization of military-investment economic appraisal systems. *Defence and Peace Economics, 25*(6), 577-604. doi: 10.1080/10242694.2013.804671

Otley, D. (2016). The contingency theory of management accounting and control: 1980–2014. *Management Accounting Research, 31*, 45-62. doi: 10.1016/j.mar.2016.02.001

Pilonato, S., & Monfardini, P. (2020). Performance measurement systems in higher education: How levers of control reveal the ambiguities of reforms. *The British Accounting Review, 52*(3), 100908. doi: 10.1016/j.bar.2020.100908

Simons, R. (1995). *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*. Harvard Business School Press. Retrieved from https://www.hbs.edu/faculty/Pages/item.aspx?num=257

Van der Kolk, B. (2019). Management control packages: a literature review and guidelines for public sector research. *Public Money & Management, 39*(7), 512-520. doi: 10.1080/09540962.2019.1592922

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations and Society, 32*(7-8), 757-788. doi: 10.1016/j.aos.2007.01.001

WG9 – Military Education

Training of Gendarmes from the Sahel Region: GAR-SI Sahel project

A. García (1), R. Prieto (2) and J.-I. Antón (3)

(1) Universidad Nacional de Educación a Distancia (UNED), Spain, adcastro@poli.uned.es

(2) Universidad Nacional de Educación a Distancia (UNED), Spain, rgaona1@alumno.uned.es

(3) Universidad de Salamanca (Usal), Spain, janton@usal.es

With the pressing scenario of terrorist cells from the Sahel threatening Europe, the European Union has tried to train the members of the security apparatus of those countries which constitute that area.

In that context, the EU funded GAR-SI Sahel project builds the necessary structure and programs for training of African Gendarmes both in Europe and Africa to assure the necessary tools and procedures for that task to be able to be completed. In that regard, it gives Spanish Guardia Civil, Portuguese Guardia Nacional Republicana (GNR), French Gendarmerie and Italian Carabinieri the task to train and support the Sahelian Gendarmeries. Based on their experience countering organized crime and terrorism.

Nevertheless, these activities and initiatives are under-studied and significantly under-theorized. Therefore, this conference article examines the EU GAR-SI Sahel project as one of the last European capacity building efforts in the Sahel gendarmeries.

This conference examines and evaluates several parts of the project:

- Part of the training that took part in the *Centro de Adiestramientos Especiales* (CAE) in *Logroño* (Spain) focusing on lessons learned and on how following editions can benefit from a public polity evaluation.
- Training that took place in Burkina Faso in 2021, which allows us to make the necessary comparison with training in European soil.
- The International Security/International Relations theoretical framework that can be used to analyze the initiative. In particular the relationship with the dogmas present in Security Sector Reform (SSR).
- The intelligence aspects of the project. Its link with the historical origins of the Guardia Civil throughout the "*Cartilla del Guardia Civil*" .

In sum, this conference presentation has a triple intention, firstly to outline the main findings of the study, secondly to benefit from the knowledge of other participants in this activity and thirdly to inspire some similar research from Portuguese and international scholars.

KEYWORDS

International Security; European Union; Sahel; Gendarmerie Training.

A Trainer's Guide to Sustainable Security

K. Trochowska-Sviderok (1)

(1) War Studies University, Poland, k.trochowska@akademia.mil.pl

The recent global climate and health crises along with the 2022 war made us starkly realize that the contemporary global security paradigm is brutally unjust and absolutely unsustainable. We need a solid re-orientation of philosophical approaches, knowledge and education systems, principles, values, governance arrangements, management practices and behaviors to ones that:
- Embrace and make an asset of diversity;
- Build resilience;
- Center around sustainability.

In this way, we can navigate towards a holistic and synergistic system that will work not only for privileged minorities and regions, but for all of the biosphere.

Therefore, in the years 2018-2021, I was working on the novel Sustainable Security Paradigm (SSP), along with practical training, teaching and policy-making tools that would aid its implementation. The SSP was featured in the "Sustainable Security: Revolution or Utopia?" article in the European Research Studies Journal (IF 1,57) (Trochowska-Sviderok, 2021). I centered the theoretical framework around three pillars: the scientific study of the socio-ecological systems of the Anthropocene, a holistic understanding of security, and genuine realization of the UN's Sustainable Development Goals.

My presentation will briefly feature the paradigm and analyze the application of a variety of approaches, training tools and projects I have been realizing with my civilian and military students at the War Studies University and while working with the NATO Science and Technology Office and NATO Innovation Hub. Those solutions include:
- Training soft skills such as communication, cooperation, cultural and gender competence, diversity management and radical empathy in security and defense organizations.
- The use of serious gaming and Proteus effect in military and civilian training.
- Design and conduct of the open *Critical Thinking Course* for NATO Innovation Hub within the *Cognitive Warfare Project* (NATO Innovation Hub, 2022).
- The activity of *Gender, Peace and Sustainable Security Exploratory Team ET-197* that I lead for the NATO Science and Technology Organization (NATO STO ET-197, 2022).

The latter is of particular significance. The 2020 Women in the Armed Forces report (NATO Science and Technology Organization, 2012) found that soft skills in leadership and leader development, play a key role in the effective integration of service women into the armed forces, as well as contributing to the culture of organizations and the prevention of sexual harassment and assault. It also highlighted the importance of training of service members as critical to the prospects of service women in a range of areas, including in the integration of women into combat roles and the enhancement of women's physical performance (NATO Science and Technology Organization, 2012). However, it is important to note that current understanding of "gender perspective" is the integration, inclusiveness and integrity in the context of women only. And gender perspective is so much more than this - it is also about masculinities, sexuality and Sexual Exploitation and Abuse, cultural narratives & norms, and LGBTQ+ issues - from the individual perspective, as well as through the organizational to transnational level. Diversity in the armed forces has become prominent due to the adherence to the principle and laws of equality, respect for human rights and the elimination of discrimination. In developed countries diversity is becoming a democratic imperative in that the professional army reflects the composition of the entire population, women constituting more than 50% of the population in almost all countries. The realization that women are actually the majority but treated by organizations and society as a minority and a 'niche' leads to the inevitable realization that without women's central involvement in peacekeeping processes, sustainable peace and security are not possible.

The practical tools that I am planning to discuss provide a way to bridge the gender and cultural gaps. In this way diversity is an asset that contributes to a truly sustainable security environment on and off mission.

KEYWORDS

Military education and training; Sustainable security; Soft skills.

REFERENCES

NATO Innovation Hub (2022). *Cognitive Warfare*. Retrieved from https://www.innovationhub-act.org/content/cognitive-warfare

NATO Science and Technology Organization (2012). *Women in the Armed Forces*. Brussels: Office of the Chief Stientis.

NATO STO ET-197 (2022). *Gender, Peace and Sustainable Security*. Retrieved from https://www.sto.nato.int/search/Pages/activities_results.aspx?k=gender%2C%20peace&s=Search%20Activities

Trochowska-Sviderok, K. (2021). Sustainable Security – Revolution or Utopia?. *European Research Studies Journal*, *XXIV*(2), 369-395. Retrieved from https://www.ersj.eu/journal/2132

CyberAcademy of the Ministry of National Defense as a bridge to increase the level of state cybersecurity

G. Pilarski (1)

(1) War Studies University, Poland, g.pilarski@akademia.mil.pl

The War Studies University, in accordance with its strategy, meets the needs of the Polish Armed Forces in the field of education of senior command staff and civilian employees employed in the state and private sectors acting for the defense and security of the state. Since the Ministry of National Defense has identified activities related to cyberspace security as a priority, it should be assumed that one of the areas to which special attention should now be paid is cybereducation. The fact that the North Atlantic Treaty Organization recognized cyberspace as the fifth dimension of the struggle was also important in this respect. Cyberspace is exposed to many threats, which is reflected in the emergence of newer and newer methods of attack on the information resources of various organizations. Knowledge in this field is essential, because it allows you to build awareness that it is possible to counteract these threats. This knowledge should be possessed by the staff responsible for the security of ICT networks, the administrators of these networks, and so that ordinary users of ICT services.

On the basis of the above issues, a doubt arises, which the author formulated in the form of the following research question: how to ensure a high-quality education process in the area of "cyber"?

On the basis of the acquired knowledge and research results, the author in the scope of the above research question proposes to take the following assumption for further consideration: the complex relationships of functioning in cyberspace force the establishment of specific cybercoopetition relationships in the field of education. This is a key element enabling the creation of an entity in the Ministry of National Defense called CyberAcademia MoD. The purpose of such an institution would be to educate highly qualified specialist staff and to shape awareness of the entire military and civilian status of the MoD in the field of functioning in cyberspace. It should be assumed that the appropriate selection of specialized courses, the transfer of appropriate language skills and the creation of an IT platform supporting cybereducation will allow to improve the quality of education of command and staff for the needs of the Polish Armed Forces, which in turn will enable the preparation of MoD staff to implement activities in cyberspace in the contemporary realities of the battlefield. The area of research indicates a multifaceted approach to this process of implementing cybereducation.

In cyberspace, there is a constant struggle that allows you to achieve various goals, such as being better, leading, allowing you to gain prestige, priority or the status of being innovative. Since entities in cyberspace have their own separate, divergent goals, cooperation is not possible to achieve. By deciding to openly define their goals, these entities have a chance that despite competitive activities they will be able to find a sphere of mutual cooperation, where cyberspace will be the base platform. Such an area is certainly the defense and security of the state. A tangible example of cyber cooperation is the functioning of the North Atlantic Alliance, where we observe a long-term action of cooperation between individual countries in some areas on the one hand, and competition in others on the other. Cooperation is intertwined with competition, which is why the authors propose to use the concept describing various dependencies in cyberspace by using the term cybercoopetition. The author defines cybercoopetition by claiming that it is conducting or preparing activities in cyberspace with the participation of entities (actors) remaining in simultaneous and interdependent relations of competition and cooperation in a specific time horizon.

Taking as the basic criterion the effect of the impact as a result of the functioning of cybercoopetition can be divided into: positive cybercoopetition and negative cybercoopetition. Assuming as an axiom functioning in cyberspace without signs of cybercrime, i.e. ethical action that does not cause any negative impact on the functioning of other entities in cyberspace, with respect for private life and communication, this type of activity can be classified as a positive type. On the other hand, actions that are completely different, unethical and leading to negative effects will be qualified for negative activities. An example of positive cyber cooperation may be the implementation of cybereducation in MoD. Thanks to education, we are able to influence the perception of cyberspace, its advantages, but also the threats associated with it. Cybereducation allows us to improve our thinking by accurately perceiving reality and events in relation to time and space. At the same time, it enables the interpretation of these events and their consequences. To sum up, education improves our situational awareness (observation, planning and prediction skills) in the area of cyberspace. As a consequence, this change also affects the possibility of implementing specific activities in the sphere of observation and/or response, which directly translates into an improvement in the area of defense and state security.

The development of ICT affects the constant need to have qualified staff in the field of development, operation, maintenance and ensuring safety in these innovative solutions. According to a study by Frost & Sullivan, the dramatic growth of products and services by 2025 will be driven by three major megatrends: connected living, big data clouds and smart cities. In each of these three main areas, it will be necessary to ensure the safety of use, which is why it was noted that with the development of these technologies, the demand for specialists in this industry will increase. The result may be the creation of a skill gap (a skills gap and in fact a shortage of employees with this type of skills and competences in relation to the expectations of employers) in the area of cybersecurity. According to these predictions, in the near future, shortages of qualified staff in the "cyber" area may have a significant impact on the security of citizens in cyberspace in various areas of social life. One of the ways to reduce the "cyber skill gap" is undoubtedly the introduction of specific activities in the field of cybereducation.

On the basis of the research carried out on the need to conduct courses and trainings in the area of "cyber" at the War Studies University (a survey among military students at WSU, the question was: in your opinion, should the War Studies University conduct trainings / courses on the issues of military activities in cyberspace?) nearly 68% of respondents supported this initiative (definitely yes – 25%; rather yes – 43.3%; it is difficult to say – 16.3%; rather not – 8.7%; definitely not – 6.7%). Similar indicators were obtained in the question concerning the creation of a CyberAcademy in the Ministry of National Defense (the question was: In your opinion, should a competence training center should be created in the Ministry of National Defense to educate in the field of military activities in cyberspace, e.g. CyberAcademy?): more than half of the respondents voted in favour – 52.5% (definitely yes – 20.2%, rather yes – 32.7%; it is difficult to say – 18.3%; rather not – 17.5%, definitely not – 11.5%).

The issue of cybereducation is currently one of the leading topics discussed on the national and international arena. The multifaceted nature of this research problem indicates the need to conduct research and debate covering the conditions to be met in order to strive through cybereducation to cyclically increase the level of cybersecurity in the area of defense and state security.

KEYWORDS

Cyberspace; Cybersecurity; Cybereducation; Cybercoopetition.

REFERENCES

Brandenburger A. M. & Nalebuff B. J. (1996). *Co-opetition, 1. A revolutionary mindset that combines competition and cooperation. 2. The game theory strategy that's changing the game of business*, New York: Currency Doubleday. ISO/IEC 27003:2017, Information technology – Security techniques – Information security management systems – Guidance.

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls Łączn. 1000/99 (1999). *Tymczasowa instrukcja organizacji projektowania, wdrażania i eksploatacji systemów informatycznych w resorcie Obrony Narodowej*, Warsaw: Sz. Gen. 1341/88.

Pilarski G. (2020). *Cyberprzestrzeń – relacje w wojnie hybrydowej*. Warsaw: War Studies University.

Pilarski G., & Pilarska M. (2020). *Wieloaspektowość cyberedukacji*, In: Marczyk M. (Ed.) Militarne aspekty cyberbezpieczeństwa państwa w czasie działań hybrydowych przeciwko RP (pp.95-113). Warsaw: War Studies University.

Raport, (2017). *Global Information Security Workforce Study Bench-marking Workforce Capacity and Response to Cyber Risk*, Frost & Sullivan.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2020). Warsaw.

Military Education – the scientific role in the integral education

M. Cavique (1) and A. Mourão (2)

(1) Naval Academy, Portugal, cavique.santos@escolanaval.pt
(2) NOVA School of Science and Technology, Portugal, ajfm@fct.unl.pt

In Europe, there has been an effort to integrate military high-education (MHE) into the high-education system (Callada-Muñoz, 2019). Therefore, the MHE shares the classical missions of the University, preserving, transmitting, and creating knowledge. The role of preserving knowledge reduced in the last century. Recently giving "a contribution to society" appears to be a new University mission (Compagnucci, 2020), which has always been part of the military ethos.

The "contribution to society" is a consequence of integral education. Integral education aims to create a Man in all human dimensions, physical, emotional, rational, and spiritual - adapted from Ferrer (2005). This kind of education has always been the focus of MHE, which Universities now share.

Future officers will decide in a more "incomprehensive" world than before. As an example, the strategical concept of NATO regarding Russia changed in less than twelve years (NATO, 2010, 2022).

The ability to conceive new solutions will be a challenge for future officers. They will need to be right-first-time – in many states of affairs, there is no second opportunity. Moreover, cyber as a new warfare dimension will create extra challenges. In warfare, artificial intelligence (AI) will run over a cyber environment with unusual and sometimes inconceivable solutions. Human decisions must overcome any lethal decision taken autonomously by AI in military contexts (Kissinger, 2021, p. 172, 175). A conceptual framework needs to be in the officer's mind to allow him to decide. Requirements, physical solutions, and humanity constraints will come along in the decision process.

To conceive a solution is to make a Design. Design is a synthesis process. The most common reasoning process developed in Universities is the deduction ($p \rightarrow q$; if p, then q). However, in the synthesis process, the abduction ($p \rightarrow q$; if q, may p), induction ($p_1 \rightarrow q_1$; $p_2 \rightarrow q_2$; then $p_n \rightarrow q_n$), and induction, an induction in different fields of knowledge, prevail.

The university syllabus usually only describes the topics of the learning modules. The syllabus must cross with reasoning processes (Mourão, 2011). Some courses define the level of learning achievement as "to know", "understand", and "apply".

Research universities usually address extensive fundamental matters and some technical issues. Applied universities may give the necessary scientific basis to address specific technical problems. Some Universities courses may even have no explicit applications. They may give a broad knowledge of philosophy, physics, mathematics, art, ethics, and law.

The specificity of MHE is to mix wide-ranging knowledge in many fields with specific applications. The students need to apply in detail the specific applications. Moreover, there is a need to instruct quick decisions in harmful environments. This type of training asks for quick thinking. However, quick-thinking restrain values. On the contrary, slow thinking is needed to understand Science and Knowledge and requires effort and time (Maffei, 2014, p.90, 91).

Creativity and innovation occur by merging both types of thinking in the conception of something new, a new design. Axiomatic Design is a scientific theory of design that relies on two axioms regarding the independence of achieving the functional requirements and the probability of success (Suh, 1990). This theory has been applied to engineering, AI, design of organizations, etc., and can be a tool to solve future challenges for humanity (Suh, 2021).

Regarding the rational scientific field, MHE might have two areas or cycles. One is dedicated to learning broad fundamental matters focusing on analysis — the other on applications with a synthesis reasoning. The second area, or cycle, should address innovation, creativity, and strategy anchored in design theories. Design theories and applications should be the focus of the second area to train new officers to solve odd problems. They will need these types of skills during their lifelong careers.

KEYWORDS

Integral Education; Reasoning; Design; Axiomatic Design; Innovation.

REFERENCES

Callada_Muñoz, F.J., & Utrero-González, N. (2019). Integration in the European higher education area: the case of military education. *Defence Studies*, doi: 10.1080/14702436.2019.1681897

Compagnucci, L., & Spigarelli, F. (2020). The Third Mission of the University: A systematic literature review on potentials and constraints. *Technological Forecasting & Social Change*, 161, doi: 10.1016/j.techfore.2020.120284

Ferrer, J. N., Romero, M.T., & Albareda, R.V. (2005). Integral Transformative Education: A Participatory Proposal, *Journal of Transformative Education*, *3*(4), 306–330. doi: 10.1177/1541344605279175

Kissinger, H., Schmidt, E., & Huttenlocher, D. (2021). *The Age of A.I.*. Publicações Dom Quixote.

Maffei, L. (2014) *Elogio della lenteza*. Edições 70.

Mourão, A., Cavique, M., Gonçalves-Coelho, A. (2011). Different Perspectives in Education According to the Mission – The Balance between Analysis and Synthesis. *The 17th International Scientific Conference Knowledge-Based Organization*, November 24-26, Sibiu, Romania.

NATO (2022). *Strategic Concept*, NATO Summit in Madrid, 29 June.

NATO (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, NATO Summit in Lisbon, 19-20 November.

Suh, N.P. (1990). *The Principles of Design*. New York, NY, USA: Oxford University Press.

Suh, N.P., Cavique, M., & Foley, (2021). *Design Engineering and Science*. Cham, Switzerland: Springer Nature.

Towards a posthumanist professional military education

B. Ateş (1) and Ç. Dedeoğlu (2)

(1) Turkish National Defence University, barisates@gmail.com
(2) Yorkville University, Canada, dedeoglucagdas@gmail.com

Humanism places human beings at the center of the world and therefore subordinates everything else to them, and even leads to distinctions between humans such as superhuman, less human, or underdeveloped human. Posthumanism, on the other hand, emphasizes that human beings are not unique and that every human, and even every living thing, is equal in this diversity of life. Posthumanism, when defined as a vault that includes scientific, philosophical, and artistic ways of knowing and knowledges, it can be applied to bring a fresh perspective to a wide variety of fields, from philosophy to technology. As its name implies, posthumanism's rejection of conventional Western humanism is one of its distinguishing characteristics. In this way, violence by a group of people (usually Western white, healthy male) by seeing others, by definition, as less human for physiological, political, and ethnic reasons can be challenged (at least onto-epistemologically). In other words, stopping human violence against humans or other living things can be accepted as one of the goals of posthumanist perspectives, which decry the humanist positioning of the non-white and non-Western people as less than human. Obviously, this also has ethical implications for geopolitics, security politics, war, and diplomacy.

However, it is evident that in the modern era, which is decorated with humanist principles, unnecessary violence has not been avoided so far. For example, the number of people who lost their lives due to wars during the 20th century is around 110 million, of which 23 million people lost their lives during the Cold War. These numbers prove that unnecessary violence could not be prevented despite humanist values. Therefore, it would not be an exaggeration to argue that humanistic values are insufficient to prevent violence. In addition, military conflicts and wars are considered among the important causes of the 6th Mass Extinction, as well as the loss of cultural heritage. These aspects can also be seen as the effects of "humanist" violence on the planet that is mostly ignored.

At first glance, it may seem logical to locate the soldiers who manage and execute organized violence in the antiposthumanist camp – if there is one. Because it may appear that minimising violence while also managing and practising it is an impossible task for the military organization. However, one may argue that there is complete harmony between posthumanism and the ideals of military education. In fact, modern armies and their officer corps aim to end the war with the least possible violence. But to achieve this goal, soldiers need a critical and creative professional military education (PME), which is immune to hyper-individualism and techno-solutionism.

The modern era PME seems to be characterized by a rather classical modernist view of education based on universalism, structuralism, and objective knowledge and aims to foster a sense of shared identity. It, therefore, fosters a learning environment with scenario-based pre-planned exercises as ways to conduct military operations with a uniform understanding. However, it is seen that this understanding of education is changing. Because the new era requires able soldiers who think analytically and critically, those soldiers should also be able to cope with uncertainty. These features are in line with posthuman values.

In this presentation, we claim that an understanding that does not place human beings at the center of the universe or fall into the trap of super/underdeveloped humans will prevent unnecessary violence in wars and crises. After all, it should not be forgotten that humanity, from Westphalia to Solferino, or from the UN to the ICTY, has spent the last few centuries pursuing this goal. However, despite these efforts, the Srebrenica massacre, the events in Abu Ghraib, and the slaughter of innocent and mostly civilian people in Ukraine are examples of unnecessary violence that can be listed at first glance. In short, despite all efforts, unnecessary violence could not be prevented. Besides legal or political solutions, can unnecessary violence be prevented by introducing a posthuman understanding into the education of soldiers? Of course, an intervention at the onto-epistemological level is not enough to stop wars, but isn't it possible to combine PME and posthumanism to limit violence in future wars? This study makes a pragmatic effort to show that this might be possible.

Posthumanist politics and posthumanist war as an extension of it are already discussed in the relevant literature. In this presentation, we aim to bring a critical posthumanist perspective to military education and make a case for the posthumanist military education. We find this discussion valuable in that, on the one hand, military power can be redesigned for peace and security; on the other hand, politic – and military politics – can be handled with a transpersonal and transdisciplinary understanding. Moreover, this new form of education can help mediate the

soldier's purpose of existence, namely the management of organized violence, to prevent violence that is not necessary by bringing in posthuman values.

KEYWORDS

Posthumanism; Professional military education; Organized violence.

REFERENCES

Aloni, N. (2011). Humanistic Education: From Theory to Practice. In: W. Veugelers (Ed.), *Education and Humanism: Linking Autonomy and Humanity*. Rotterdam: Sense Publishers, 35-36.

Bolter, J.D. (2016). *Posthumanism*. In K. B. Jensen, & R. T. Craig (Editors-in-Chief). *The International Encyclopedia of Communication Theory and Philosophy*. John Wiley & Sons, Inc.. Retrieved from https://onlinelibrary.wiley.com/doi/10.1002/9781118766804.wbiect220

Snaza, N. et. al. (2014). Toward a Posthumanist Education. *Journal of Curriculum Theorizing*, *30*(2), 39-55.

Sookermany, A.M. (2017). Military Education Reconsidered: A Postmodern Update. *Journal of Philosophy of Education*, *51*(1), 310-311.

Veugelers, W. (2011). Introduction: Linking Autonomy and Humanity. In: W. Veugelers (Ed.), *Education and Humanism: Linking Autonomy and Humanity, Sense Publishers*. Rotterdam.

Doctorate in Military Science: Solution or Trojan Horse?

D. Last (1)

(1) Royal Military College of Canada, last-d@rmc.ca

Several countries' military staff colleges are challenged to provide military faculty with the academic qualifications necessary to teach at the graduate level, according to the standards now widely accepted within the European Higher Education Area. Eastern European countries, including Romania, Hungary, Czech Republic, and Serbia have defence university programs with civilian partnerships, and offer doctoral degrees in military technical subjects including ballistics, military chemistry, and armaments. However, doctoral, terminal or troisième cycle programs for professional officers are not readily available in defence universities in most western countries. This paper explores a potential solution and considers institutional reactions which challenge implementation. The solution might be professional doctoral degrees like those available in business, education, or engineering. Evident reluctance of defence universities and staff colleges to pursue this solution might be t he result of normal impediments to innovation, or it might reflect institutional interests that make the solution look like a "trojan horse" to key military and academic stakeholders. The research for this paper draws on interviews and primary policy documents.

Discussions with the European Security and Defence College (ESDC) and with mid-career staff colleges in 2015-2017 suggested that civilian universities are focused on academic degrees that prepare professional researchers and university teachers, while the need at staff colleges is rather for faculty with professional degrees that prepare military officers and defence civilians to contribute to research and teaching within the profession. A discussion paper circulated to ISMS members in 2017 made the case for a professional Doctor of Military Science (DMilSci) offered cooperatively by several countries' defence universities.

Professional doctorates are well established as an alternative to the academic PhD, particularly in the fields of business (DBA), Engineering (Eng.D) and Education (D.Ed). They build on applied science as defined by the OECD Frascati manual (2015). They aim to produce practitioners who contribute to the profession through research on practical problems. In the military context, these would be career officers or defence civilians who remain at a degree-granting defence university for a portion of their career, then cycle back to practice, where they apply research skills to professional challenges. The paper compares existing doctoral programs in War Studies and Military Science to the two archetypes of the academic PhD and the professional doctorate (Bourner et al, 2001).

The paper discusses modalities. Who is the target audience? When, where, and how would programs be delivered? How would graduates be employed? International cooperation between defence universities might include an agreed framework for major fields in military sciences and a menu of courses, supervisors, and resources available to share internationally. This follows work led by the Norwegian Defence University College to establish the boundaries of military science in a major reference work (Sookermany, 2019). National accreditation based on international resources is more likely to succeed than multinational degrees for which there is no designated accreditation body. ISMS members might contribute to a common DMilSci by appointing adjuncts and sharing courses and resources including supervisors, examiners, and grey literature to support research.

The proposal for a DMilSci has not advanced since 2017 but new information from interviews suggests two fundamental barriers. Academics invested in defence universities may see the DMilSci as a trojan horse to introduce less academically qualified instructors into hard-won academic positions. Conversely, military instructors at defence universities may see the DMilSci as a trojan horse to introduce more academics to the world of professionally credible practitioners. Survey research on an open international platform aims to shed light about resistance and support for the idea of a DMilSci.

KEYWORDS

Doctorate; Practitioner; Soldier-scholar; Staff college; DMilSci.

KEYWORDS

Bourner, T., Bowden, R., & Laing, S. (2001). Professional doctorates in England. *Studies in higher education, 26*(1), 65-83.

Fulton, J., Kuit, J., Sanders, G., & Smith, P. (2013). *The professional doctorate: A practical guide*. Palgrave Macmillan.

OECD (2015). *Frascati Manual: Guidelines for Collecting and Reporting Data on Research and Experimental Development.* Organization for Economic Cooperation and Development.

Marilyn, R., McIntosh, S., & Junke, M. (2011). *The Professional Doctorate: An Overview*. Faculty of Graduate Studies, Brock University.

Sookermany, A. (2019) *Handbook of Military Sciences*. Springer.

A reasoned response to an unpredictable situation: the education of officer cadets in military academies

D. Parenteau (1)

(1) Collège militaire royal de Saint-Jean, Canada, danic.parenteau@cmrsj-rmcsj.ca

As vocational schools, military academies are established to train officers for the armed forces with a comprehensive training programme, usually based on distinctive pillars: military, physical fitness, education, character and sometimes language (second language training for officially bilingual countries or English). Military academies are work-oriented institutions (Paillé, 2011), as officer-cadets are trained for the work responsibilities that await them upon graduation. The educational pillar is generally multidisciplinary and mobilises several academic fields, ranging for example from political science, history, natural sciences, engineering or literature. In this sense, the profession of officer is the only one that does not have its own "science", i.e. a specialised and exclusive academic field for educating their candidates, whereas, for example, studies in medicine lead to the profession of the same name or studies in law lead to the profession of lawyer. There is indeed a field called "military sciences", but it is far from being unified and has no vocational purpose either.

This pedagogical choice of multidisciplinarity is undoubtedly due to the singular nature of this profession, in that officers are by definition generalists. In the course of their career, officers are called upon to perform an extreme plurality of tasks in the most diverse positions, in the form of relatively short and successive postings. No other profession organises the career path of its members in such a way that they change assignment, level of responsibility, and sometimes even environment, every two or three years. The generalist nature of the university education offered to officers also stems from the singular nature of the activity domain on which they exercise their expertise; that of military operations. The military academy must train officers for the ultimate purpose of any armed force, which is to prepare for war. Yet war is a domain dominated by chaos (Beaumont, 1994; Gallant, 2021), unpredictability (LindleyFrench & Boyer, 2014; Marshall, 2000), uncertainty (Due et al, 2015) and increasingly by complexity (Manwaring, 2012). No specific and exclusive educational programme can prepare someone for this unique field of activity. Also, for the sociologist Bernard Boëne, "When complexity and uncertainty of the future dominate, the only worthwhile bet is to invest in the capacity for situational intelligence, which refers to a more rigorous selection and a diversified general culture (Boëne, p. 49)." In the same sense, for the historian Reed Bonadonna, "In here role as tactician, the thinking of an officer is perhaps less tied to rule and more dependent on flexibility and mental agility than that of any other professional activity. Neither procedures, principles, nor doctrine provide the solution to any tactical problem. Unlike the lawyer, to whom the words of which laws are made are all-important, the engineer, who must abide by known rules of stress and structure, or the physician, whose training inculcates strong guidelines for diagnosis and procedure, the military officer-as-tactician must consider a multitude of uncertainties tied to only a few givens (Bonadonna, p. 143)."

This paper is intended as a free reflection on the challenges for military academies of developing in officer cadets the intellectual capacity, or rather the singular mindset, to prepare them for what is by definition unplanned, beyond the reach of predictability, and strongly marked by complexity. Our reflection will be based on a general distinction, inspired by the formula of the historian Ron Haycock, according to which "instruction aims at a predictable response to a predictable situation", whereas "education aims rather at a reasoned response to an unpredictable situation (Haycock)". How to train officer cadets intellectually to deal with the reality of war? What type of knowledge or intellectual tools are best suited for the development of their expertise? Our reflection will not dwell on the emotional preparation that this requires – even if this "character" education seems to us to be just as essential— but on the intellectual preparation. This reflection will mostly mobilizes works of sociology on the profession of officer, of war studies and of military pedagogy.

KEYWORDS

Officer's education; Military academy; Complexity of War; Critical thinking.

REFERENCES

Beaumont, R. (1994). *War, Chaos, and History*. Westport. Conn.: Praeger.

Bonadonna, R. (2020). *How to Think Like an Officer. Lessons in Learning and Leadership for Soldiers and Other Citizens*. Latham, MD: Stackpole Books.

Due, J., Finney, N., & Byerly, J. (2015). Preparing Soldiers for Uncertainty. *Military Review*, January-February, 26-30.

Gallant, T. (2021). War is War: The Relevance and Practicality of The Principles of War for Future Combat. *The Canadian Military Journal, 21*(4), 51-60.

Haycock, R. (2011). Clio and Mars in Canada: The Need for Military Education. Presentation to the Canadian Club, Kingston, Ontario, 11 November 1999. In: B. Horn (2011). A rejection of the need for warrior scholars. *The Canadian Military Journal, 11*(2), 48-53.

Lindley-French, J., & Boyer, Y. (2014). The unpredictability of war and its consequences. In: J. Lindley-French & Y. Boyer (Eds.). *The Oxford Handbook of War* (pp. 663-668). Oxford: Oxford University Press.

Manwaring, M. G. (2012). *The Complexity of Modern Asymmetric Warfare*. Norman, OK: The University of Oklahoma Press.

Marshal, S.L.A. (2000). *Men against Fire: The Problem of Battle Command (1947)*. Norman, OK: The University of Oklahoma Press.

Paile, S. (2011). *Europe for the Future Officers, Officers for the Future Europe. Compendium of the European Military Officers Basic Education*, Polish Ministry of National Defence.

Education for the Ideal Lieutenant: Canada's Military Colleges

A. Dizboni (1), J. McKay (2), P. Jolicoeur (3) and H. Breed (4)

(1) Royal Military College of Canada, dizboni-a@rmc.ca
(2) Royal Military College of Canada, James.Mckay@rmc.ca
(3) Royal Military College of Canada, Pierre.Jolicoeur@rmc.ca
(4) Royal Military College of Canada, Hans.Christian.Breede@rmc.ca

This presentation is based on a manuscript published by the presenters in the Parameters Journal as part of Parameter's strategic lieutenant series. The aim of the text is to answer the following question: what leads governments to reform entry-level officer professional military education: the global strategic environment or the domestic political environment? Renewed emphasis on post-secondary education was due to domestic reactions to incidents that occurred in Somalia in 1993. Reforms were not only shaped by resource constraints as part of government efforts to economize and reduce debt in response to globalization but also by shifting government priorities over time. Our presentation looks at how domestic context creates the conditions for reform to a greater extent than the global strategic context. In the case of Canada's post–Cold War era, the Canadian Armed Forces (CAF) officer education was reformed because of demands in the national and operational environments generated in Ottawa and the court of Canadian public opinion. Our presentation begins with a summary of how entry-level military education is delivered in Canada, then examines perceived changes in the global strategic and domestic environments and assesses that changes and reforms tended to come from the domestic environment.

In conclusion, for our military college graduates, changes in the global strategic context since the Cold War, including globalization, America's challenges, China's initiatives, and environmental threats have not led to a renaissance in professional military education in Canada. The domestic context has eclipsed the global strategic context. The demands of the future are less certain and more fluid than those of the past, which creates a need for professional military education throughout an officer's career. The education provided at the entry level is foundational and should prepare future officers for uncertain and fluid situations. This means playing the long game associated with an evolving global strategic context even when the domestic context forces one into the short game of an evolving domestic context when it comes to resources.

KEYWORDS

Strategic lieutenant; Canada military college; Military education; Domestic context; Global strategic context.

Training transfer factors: study in military context

N. Loureiro (1)

(1) Faculdade de Ciências e Tecnologia and IUM, Portugal, nuno.a.loureiro@gmail.com

The effectiveness of training is a critical success factor for organizations, given the necessary investments and expected results. This issue is particularly relevant to the Armed Forces that must empower their workforce to meet the challenges of a volatile, uncertain, complex and ambiguous world, knowing that military vocational education and training helps establish the conditions for military success by creating the intellectual architecture to make military operations more effective. Based on this effectiveness, mostly, on the effective transfer of training to the workplace, the mastery of the factors that influence it is relevant.

This study is part of a broader ongoing investigation, which aims to study the transfer of training to the workplace in a military context, considering factors related to the individual characteristics of the trainees, the organizational context, the conception of training, the culture of learning, organizational commitment, and career development expectations. The relationships established between these factors will contribute to identify and understand a new paradigm for training throughout the military career, underpadding a formative model more adjusted to the current and future needs of the Armed Forces.

Having as objectives the study of the factor structure of the transfer of training in the military context, and the analysis of statistically significant differences in the mean score of the factors in relation to demographic and socio-professional variables (gender, age, branch, seniority, function, qualifications, course, and time elapsed since the last course attended), exploratory and confirmatory analyses were performed on the results of Bate's Learning Transfer System Inventory answered by 672 military personnel of the permanent staff of the Navy, Army and Air Force who completed career promotion courses.

The results showed a latent factorial structure different from the original version, as well as the existence of significant differences according to the demographic and socio-professional dimensions of the study population. Some practical implications for the human resources officers of the Military Institution were also discussed.

KEYWORDS

Adult Education and Training; Armed Forces; LTSI; Training Transfer.

Learning military leadership through literature: Reflections from project LITTLED

A. Hagen (1) and J. Kibsgaard (2)

(1) Norwegian Defence University College, annemhagen@mil.no
(2) Norwegian Defence University College, jkibsgaard@mil.no

Bridging the gap between experiential knowledge and theory is a perennial challenge in professional military education (PME). It concerns how to facilitate the acquisition of professional knowledge and the development of a professional identity within a training environment, and it concerns how to facilitate the development of a type of competence that enables officer cadets to put into practice the knowledge, skills and attitudes they have learned. Fiction is used as a didactic tool in several practice-orientated programmes such as law, engineering, social work, and medicine (Rydén Gramner, 2022; Tarkiainen et al., 2021). Both civilian and military leadership studies incorporate fiction (see, for example, Kaurin, 2014; Samet, 2007).

At the Norwegian Military Academy (NMA), the reading programme LITTLED (Literature and Leadership) has been developed as a method to help cadets identify with the profession and reflect on challenges of military leadership. The cadets are organised into reading groups across all branches of service as a vehicle for aiding socialisation into the profession and the development inter-service bonds. In addition to discussing the set novel in reading groups, the cadets write individual learning reflections centring on this book and military leadership.

Reading fiction is associated with increased social and cognitive skills such as empathy, perspective-taking, critical thinking and decision-making (Bal & Veltkamp, 2013; Hollis, 2021; Kidd & Castano, 2013). These skills are important for leadership and thus relevant for officer cadets in the process of developing a wider officer competence (Roennfeldt, 2017). The underlying concept is that literature is defamiliarizing and dehabituating; that is, it invites us to consider frames for thinking and feeling about the world that are unfamiliar to us, which in turn aid the consequent modification of the reader's personal understanding (Fialho, 2019; Miall & Kuiken, 1994; Shklovsky, 1917).

In addition, the social reading context brings benefits. It forms the basis for social practices and using a work of fiction to express their own experiences and reflections has positive effects for individual readers (see e.g. Fuller & Rehberg Sedo, 2015; Skjerdingstad & Rothbauer, 2016). LITTLED facilitates a reading experience where readers can explore and negotiate understandings of the military profession and concepts of military leadership.

This presentation gathers resources for thinking about fiction as a site for the development of professional skills that are relevant for the military. The presentation also sets out methods and concepts for exploring how cadets engage with ideas of military leadership through social, critical reading of fiction. Finally, the presentation offers some reflections from the 2022 LITTLED programme.

KEYWORDS

Leadership; Professional military education; Professional higher education; Professional identity; Reading; Literature.

REFERENCES

Bal, P.M., & Veltkamp, M. (2013). How does fiction reading influence empathy? An experimental investigation on the role of emotional transportation. *PLoS ONE, 8*(1), e55341. Retrieved from https://doi.org/10.1371/journal.pone.0055341

Fialho, O. (2019). What is literature for? The role of transformative reading. *Cogent Arts & Humanities, 6*(1), 1692532, doi: https://doi.org/10.1080/23311983.2019.1692532

Fuller, D., & Rehberg Sedo, D. (2015). *Reading beyond the book: The social practices of contemporary literary culture*. London: Routledge.

Hollis, H. (2021). An investigation into the relationship between fiction and nonfiction reading exposure, and factors of critical thinking. *Scientific Study of Literature*, *11*(1), 108-141. doi: https://doi.org/10.1075/ssol.20014.hol Retrieved from An investigation into the relationship between fiction and nonfiction reading exposure, and factors of critical thinking | John Benjamins (jbe-platform.com)

Kaurin, P. (2014). *The warrior, military ethics and contemporary warfare: Achilles goes asymmetrical*. New York: Routledge.

Kidd, D. C., & Castano, E. (2013). Reading literary fiction improves theory of mind. *Science*, *342*(6156), 377- 380. Retrieved from Reading Literary Fiction Improves Theory of Mind (science.org)

Miall, D.S., & Kuiken, D. (1994). Foregrounding, defamiliarization, and affect: Response to literary stories. *Poetics, 22*, 389-407. Retrieved from Miall & Kuiken -- Foregrounding, Defamiliarization, and Affect: Response to Literary Stories (southampton.ac.uk)

Roennfeldt, C. (2019). Wider officer competence: The importance of politics and practical wisdom. *Armed Forces & Society, 45*(1), 59-77. doi: https://doi.org/10.1177/0095327X17737498. Retrieved from Wider Officer Competence: The Importance of Politics and Practical Wisdom - Carsten F. Roennfeldt, 2019 (sagepub.com).

Rydén Gramner, A. (2022). *Cold heart, warm heart: On fiction, interaction, and emotion in medical education*. (Ph.D. dissertation.) Linköping Studies in Behavioural Sciences no. 240. Linköping: Linköping University Electronic Press. Retrieved from Cold Heart, Warm Heart : On fiction, interaction, and emotion in medical education (diva-portal.org)

Samet, E. (2007). *Soldier's heart: Reading literature through peace and war at West Point*. New York: Farrar, Straus & Giroux.

Shklovsky, V. (1917/1997). Art as technique. In K.M. Newton (Ed.), *Twentieth-century literary theory: A reader* (pp. 3-5). London: Palgrave.

Skjerdingstad, K., & Rothbauer, P. (Eds.). (2016). *Plotting the reading experience: Theory/practice/politics*. Waterloo, Ontario: Wilfrid Laurier Press.

Tarkiainen, L., Heino, E., Tapola-Haapala, M., & Kara, H. (2021). Students' learning reflections when using works of fiction in social work education. *Social Work Education*. doi: 10.1080/02615479.2021.1928624. Retrieved from https://doi.org/10.1080/02615479.2021.1928624

Contributions to the development and integration of the Portuguese Military University Institute's internal quality assurance system

D. Dores (1)

(1) Instituto Universitário Militar, Portugal, dores.dz@ium.pt

Internal quality assurance is a structuring and integrating element of higher education institutions (HEIs).

Portuguese Military University Institute (PMUI) and its schools have demonstrated, with the Higher Education Assessment and Accreditation Agency (A3ES), that they have quality assurance mechanisms in place for the accreditation of their study cycles. Additionally, PMUI and its schools have their own Internal Quality Assurance System (IQAS), which are independent and are not certified. For this reason, within the scope of the institutional accreditation of the PMUI by A3ES, which took place in 2019, the creation of a IQAS was recommended that would integrate all the schools (A3ES, 2018).

Taking into account the need to create PMUI's IQAS, this study aimed to: propose contributions to the creation of the PMUI's IQAS, including all the schools, in order to comply with the standards defined for quality in higher education. The study was limited to: the period in which IQAS certifications by A3ES took place (since 2013); to PMUI and its schools, its European counterparts and Portuguese university institutions, with a certified IQAS and a structure similar to that of the PMUI; the use of national and European standards for the certification of HEI's IQAS. Documental review and interviews were used as research instruments.

In order to verify existing knowledge regarding IQAS, a literature review was carried out, where it was found that the existing norms in Portugal, for the certification of IQAS, are wider than the European norms (SmartQual, 2021). Thus, the essential elements of the study were obtained, fundamentally, from document review referring to Portuguese IQAS.

The first phase of the study included the analysis, in a new perspective, of the existing documentation regarding the IQAS certification. The dimensions of the study were defined, associated with the specific areas of analysis of the A3ES audit process (A3ES, 2020) and characterizing elements (EC) of these dimensions were identified. Additionally, constraints to the IQAS implementation were identified, associated with the dimensions of the analysis.

The second phase of the study included IQAS analysis of PMUI and its schools, as well as of European counterparts. In the latter case, information on these institutions was compiled and it was deduced that institutions from Norway and Finland were the only ones that fit the current study (EQAR, 2022). In Norway there is a decentralized IQAS structure in the schools and commissions that integrate the Defence and Armed Forces Branches. With regard to the PMUI and its schools, the existence of specific EC was found, e.g. Branches are the main customers, instead of students. The analysis of the quality manuals, complemented with the analysis of the information obtained in the interviews, made it possible to identify similarities in the IQAS of these institutions, reflected in the EC and in the constraints to their implementation.

The third phase of the study included the analysis of the IQAS of University of Algarve, University of Évora, University of Minho and University of Trás-os-Montes e Alto Douro. The analysis carried out on the quality manuals of these institutions, consolidated with the interviews with the respective responsible for quality, made it possible to structure EC, among which are highlighted: IQAS models are aligned with the dimensions of the current study, which facilitated the certification process; one member of the rectoral team is responsible for coordinating IQAS; IQAS is supported by an information system that is an integrating element; and, a meta-assessment of the IQAS is carried out every year.

The combination of the results obtained in the three phases gave rise to contributions to the creation of the PMUI's IQAS, which includes: appointment of PMUI's Commander as responsible for the implementation and management of the IQAS; creation of a IQAS monitoring commission; creation of subcommittees for quality in each school as well as by area of intervention (e.g. education, research); creation of a decentralized structure for the Evaluation and Quality Office; creation of a strategic plan for the PMUI, including schools, and a quality policy; implementation of a IQAS meta-assessment; creation of monitoring, evaluation and continuous improvement mechanisms transversal to the PMUI, supported by procedures and instruments; implementation of an information system that integrates all IQAS information; and, implementation of PMUI's IQAS instruments, being systematized and automated through the information system.

Additionally, constraints were identified for the implementation of IQAS, which should lead to implement measures conducive to their mitigation (e.g. creation of mechanisms to minimize the effects of the high turnover of PMUI human resources [Callado-Muñoz and Utrero-González, 2019]).

Current study made it possible to propose contributions to structure PMUI's IQAS, also contributing to the knowledge in this area of study, identifying EC of HEI's IQAS, to be taken into account in its conception and operationalization, associated with the specific areas of analysis of the A3ES audit process, as well as constraints for its implementation.

KEYWORDS

Military Higher Education; Portuguese Military University Institute; Internal Quality Assurance System.

ACKNOWLEDGMENTS

REFERENCES

Agência de Avaliação e Acreditação do Ensino Superior. (2018). *AINST/16/00034 - Avaliação Institucional do IUM - Relatório final da CAE*. Retrieved from https://www.a3es.pt/pt/resultados-acreditacao-94

Agência de Avaliação e Acreditação do Ensino Superior. (2020). *Auditoria dos Sistemas Internos de Garantia da Qualidade nas Instituições de Ensino Superior - Manual para o processo de auditoria*. Lisboa: Autor. Retrieved from https://www.a3es.pt/pt/acreditacao-e-auditoria/guioes-e-procedimentos/auditoria-de-sistemas-internos-de garantia-da-qualidade

Callado-Muñoz, F., & Utrero-González, N. (2019). *Integration in the European higher education area: the case of military education. Defence Studies, 19*(4), 373-391. doi:10.1080/14702436.2019.1681897.

European Quality Assurance Register for Higher Education. (2022, 1st of april). *Database of External Quality Assurance Results* [*online*]. Retrieved from https://www.eqar.eu/qa-results/search/by-institution/

Smart-Qual. (2021). *IO1.A1 - State of the Art of the Quality Management System of HEIs - Clustering Document*. Retrieved from https://smartqual.eu/#use-our-results

The consolidation of the military polytechnic higher education in Portugal

R. Romão (1)

(1) IUM, Portugal, romao.rmj@ium.pt

The new legal requirement for Portuguese Armed Forces (PAF) Non-Commissioned Officers (NCOs) and Republican National Guard (RNG) NCOs to have level 5 of the national qualifications' framework to join ranks, is a fundamental shift in their education. The rules that govern the NCOs teaching are now the ones that apply to higher education in general and not those of the traditional Schools and Training Centers from the PAF Branches and the RNG.

The mission of educating NCOs with the qualification level 5, within the scope of military polytechnic higher education, was assigned to the Military Polytechnic Unit (MPU) in 2019. The MPU is subject to the legal framework that regulates the higher education in Portugal while at the same time it needs to take into consideration the specificities of the military education and training. The MPU is in the development phase until 2023 and the success of its consolidation is of relevance, not only for NCOs, the PAF and the RNG, but also for the institutional accreditation of the Military University Institute.

Therefore, the problem this study sought to solve, which equals to the research question, was to know how to consolidate the new model of the military polytechnic higher education in Portugal, in the context of the specificity of the military higher education and the legislation applicable to it. The main goal of the research was to offer concrete guidelines leading to the military polytechnic higher education consolidation in Portugal.

With this objective in mind the hypothetical-deductive reasoning was selected for the methodological procedure, along with a mixed research strategy and a case study for research design. The data collection was based on an in-depth document analysis and on interviews with key entities to better understand the research object, which is the MPU.

The research revealed the faculty body of the MPU is adequate. This means the faculty body is academically qualified, specialized, and sufficient in number, considering the existing number of students and the current teaching offer, presently corresponding to the level 5 and not the level 6 of qualification, as required by the Portuguese law. On the other hand, the MPU faculty body is not stable enough, due to the high number of existing courses and curriculum units and to the fact that the military teachers perform their duties in addition to other tasks in the PAF Branches. This instability compromises the MPU and the quality of the teaching provided.

Second, the study data also showed that the MPU research capabilities are still in their preliminary stages of development. Although practice-based research activities are part of the MPU's mission and it is one of the relevant criteria to evaluate polytechnic institutions, there is no collective understanding among the MPU Departments on what practice-based research activities should be or how they should be implemented. The study revealed that the process associated with the MPU research capabilities is not yet consolidated and that practice-based research is not conducted either by teachers or students.

Lastly, the research also revealed there is no consensus among the PAF Branches and the RNG as to the need or purpose for the MPU to offer a higher education first cycle, even when the law requires it.

The study concluded the MPU must stabilize its faculty body, must conduct guided research properly, and must offer a first cycle of higher education to be accredited by the Portuguese Higher Education Assessment and Accreditation Agency. However, the research also determined the MPU, and the Military University Institute have the option of choosing the timeframe to do so and the legislative framework that best suits the reality of the Portuguese Armed Forces, the Republican National Guard, and the growing complexity of the operational environment as well. With these investigation results in consideration, it presents concrete solutions and specific guidelines to consolidate the new model of military polytechnic higher education in Portugal, in the context of the specificity of the military higher education and the legislation applicable to it.

KEYWORDS

Exploring Self-Help: Using International Societies to Enhance Professional Military Education in Africa

M. Mahela (1) and D. Last (2)

(1) School of Military Science at the University of Namibia, mmahela@unam.na
(2) Royal Military College of Canada, david.last@rmc-cmr.ca

How can defence education institutions chart a course appropriate to national circumstances in the new international environment? The authors describe alternative models for enhancing PME from an African perspective. Many countries have accepted "supply side" help from major powers. In this model, the nature of assistance is determined by the providing state. There may be long-term consequences for accepting training and education assistance. Some states have sought "demand driven" assistance, in which the recipient determines the gaps that are to be filled, but then accepts available help which may not be a perfect fit for the gap. Each approach has drawbacks in the Namibian experience of developing PME, but each has been useful and necessary. Self-help drawing on international organizations provides an alternative deserving further exploration. The paper describes the experiences of the Namibian School of Military Science (SMS) in the context of Namibian training and education. The authors discuss the availability of supply side and demand driven educational assistance to Namibia, and the roles and potential of three international organizations: the African Conference of Commandants, the International Association of Military Academies (IAMA) and the International Society of Military Sciences (ISMS). The paper compares the composition, capacity, and volition of these organizations, and their connection to bilateral and multilateral assistance channels available to Namibia and other non-aligned countries. Implications for confronting new security challenges and further research questions are suggested. Namibia offers a case study of self-help in its efforts to chart a course appropriate to Namibian defence and security needs within its limited resources. Its military forces originate in the 1989 blending of SWAPO and forces that had supported the SADF. Early officer training was conducted abroad. The School of Military Studies for undergraduate officers was established in 2012 and the Chinese-funded National Defence College at Okahandja was opened in 2019.

Supply-side help is determined by providers. With needs in almost every category, Namibia accepted whatever help was offered in 1989. This included Commonwealth, American, and even North Korean assistance. Since 1989, donor countries have provided seats on foreign training courses, equipment and logistics help, peacekeeping training, and borrowed doctrine and course packages. Supply side help often serves supplier interests. Donated equipment is linked to maintenance contracts or long-term purchase of parts and replacements. Borrowed organizations and doctrine shape the missions that forces might undertake in the future. Officers who receive training and education abroad form values, attitudes, and beliefs about how the world works, who are the country's friends, and what the country and the defence force need for security. Demand driven help tends to be bilateral. The recipient asks for help in specific areas that match policy priorities and perceptions of need. Response is still by countries with interests in providing help, but the help matches or approximates the needs of the recipient. Assistance often comes in small increments: training teams, project funding, or seats on specialized foreign courses.

Self-help is distinct from demand-driven help because the recipient controls the whole process, taking advice and support from domestic and international sources to develop the capabilities needed. Self-help implies providing an incentive to those actors who need to be engaged, starting with those in the home institution and working out to build a network of support – military, civilian, domestic, and foreign. Self-help often begins with finding appropriate models and mentors: what are comparable countries with comparable problems and how do they solve them? The variety of security and educational challenges facing small democratic countries means that the pool for potential inspiration is large but excludes major powers with regional interests. Prior work identifies potential regional hubs (Last, Emelifeonwu, & Osemwegie, 2015). The paper explores Namibia's relations with those hubs and tests the proposition that regional self-help is possible.

Three sections address the roles and potential of international organizations in supporting self-help: the African Conference of Commandants, the International Association of Military Academies, and the International Society of Military Sciences. The paper reports on Namibia's engagement in cooperative self-help engagements in these organizations.

KEYWORDS

Military education; Professional education; Namibia training and education.

WG10 – Strategy

The Russia-Ukraine conflict: a strategic perspective

N. Calhaço (1)

(1) Military University Institute, Portugal, calhaco.nmsr@ium.pt

The started conflict on February 24th, 2022, in Europe, represents another turning point on the old continent geopolitics and history. Russian aggression against Ukrainian sovereignty, was long being expected, especially from 2020, faced Ukraine's comittement to North Atlantic Treaty Organization (NATO) accession to be formalized.

However, the COVID19 pandemic caused by the respiratory infection COVID19 "postponed" that clash, between the main world land powers, Russia and China, in one side, against main maritime powers, led by the United States of America, along with other European powers. For a clearer understanding of the present conflict, with the possible impartially, it is important to understand the true strategic objectives of both contenders in this war, and how they structure their multidimensional strategy, to achieve them.

On the other hand, it is important to understand the main reasons that led Western countries, to seek support Ukraine Government over the last few years, to achieve their strategic objectives in this region, namely by European Union and NATO.

In this way, we will try to infer about the various military objectives of the campaign verified so far, where, clearly, we assist a conflict between the Western and the Eastern countries (Russia and China). This clash and cleavage, between world power blocs, brings the international dispute between the world superpowers, United States of America, and the rising "superpower", China, projected in this conflict between Russia and Ukraine, as a true test of balance of power between the continental and maritime powers. At this point, the United States withdrawal from Afghanistan, in August 2021, and the embarrassment caused in Western countries, faced AUKUS project, reveals the grand strategy undertaken by the maritime powers, in order to "contain" China by sea, and now, by land.

Regardless the outcome of the current conflict, between Russia and Ukraine, the dispute over areas of influence in the globe, are more heated since the end of the Soviet Union, given the current situation, a serious perspective of a future conflict between Western countries, belonging NATO and European Union countries, against "Eastern Bloc", facing Russia and China, as well their how satellite countries. Therefore, it is important to create the conditions for Western countries to be able to be prepare, in all dimensions, and to be prepared for that future and unpredictable conflict, between West and Eastern countries.

KEYWORDS

War; Russia; Ukraine; Western powers; Eastern powers.

Space Deterrence: A New Theory of War and Peace for the Information Age

A. Foerster (1)

(1) Royal Military College of Canada, andreasfoerster23@gmail.com

The purpose of this presentation is to explain the revolution in grand strategy brought about by the new Space Race and coming age of Space Warfare. Understanding this revolution begins with the realization that we live in an unprecedented age of interdependence and reliance on information technology (in the great powers, that is, and especially in the West). Therefore, the grand strategy in the Information Age revolves around a new form of total war: Unrestricted Warfare, wherein all aspects of society are weaponized. This concept is actualized in the breakout of conflict through hybrid warfare, where conventional and unconventional tactics are so intertwined the distinction is no longer clear. The key to dominating these battlespaces naturally, is the information environment. The key to conflict in the information environment is cyber warfare, for it can attack an enemy from afar and with minimal resources. This conflict occurs in grand strategy constantly, but without escalation towards the true destructive potential of cyber capabilities, just as proxies provided a means for great powers to compete in the Cold War while avoiding nuclear war. However, if such conflict were to become direct and total, both sides' centre of gravity would be their access to satellites. Without these tools, a state would effectively become "blind, deaf and dumb", which guarantees defeat in wars so dependent upon the information environment. However, cyber warfare cannot be completely relied on to either attack or defend such essential targets in an all-out war. This is because the grand strategic nature of cyber conflict, as already discussed, necessitates the concealing of true capabilities, for once they are used, a defence will quickly be created to counter them. Moreover, to completely throw back an attack robs one of the opportunity to study their methods, or track the attacker back to their origin. Therefore, the most logical course of action in cyber warfare is to focus on disruption and intelligence gathering, rather than the most powerful forms of attack and defence. These means are reserved for the case of all-out conflict, so the chances of there being a counter to them is minimized. This creates a problem: without knowledge of the enemy's true capabilities, or how one's own will work once deployed, it would be foolish to rely fully on them in a zero-sum game. Therefore, a secondary option for disabling enemy satellites and protecting one's own must be developed. This option must be as disconnected from the information environment as possible. These weapons must then be kinetic in nature. Naturally, an arms race must occur, and all the tenets of deterrence as applied to nuclear weapons can be used for space warfare. This is Space Deterrence, the actualization of concepts and technological developments that gave birth to the Information Age.

The outline of this presentation will follow the argument laid out above, covering each of the premises in detail, while also examining the concepts and capabilities currently being developed in these areas, before concluding with some remarks concerning complex deterrence theory as it will apply to space warfare.

KYWORDS

Space; Cyber; Deterrence.

What Makes a Good Strategic Concept?

L. Milevski (1)

(1) Leiden University, Netherlands, lukasmilevski@gmail.com

Some social science scholars lament the neglect of concepts and conceptual analysis, which results in an overall incapacity to assess the value of new or existing concepts (Daigneault, 2012). This certainly appears to be true for the study of military strategy, which has witnessed an incessant parade of new concepts of varyingly dubious worth, from Cold War-era limited war to the revolution in military affairs, hybrid warfare, and gray zone warfare, among others. It is therefore prudent to explore what makes any strategic concept good, a question which is distinct from what makes a concept good.

One should begin such an exploration by assessing concepts as such, upon which the social sciences have already reflected. John Gerring has offered eight criteria for assessing concept formation: familiarity, resonance, parsimony, coherence, differentiation, depth, theoretical utility, and field utility (Gerring, 1999). Giovanni Sartori did not provide such a criteria-based framework, but he did provide two other aspects. First, he suggested general guidelines for conceptual analysis (Sartori, 1984). Second, he consistently argued that the barrier to entry for new concepts should be high due to the amount of contextualizing intellectual work which must be undertaken in order to introduce a new concept responsibly (Sartori, 1975). Social scientists have tended not to reflect on how their understanding of theory affects their understanding of the concepts which make the theory.

Although these general contributions are useful for defining good concepts, they are insufficient for good *strategic* concepts; the latter needs to satisfy quality requirements for both 'concept' and 'strategic.' This requires defining 'strategic', a plausibly unrestrained task depending on how one interprets the various dimensions of strategy (Gray, 1999, ch. 1). Although there is a clear sense in which logistical, economic, geographical, societal, etc, concepts are also inherently strategic, in that these dimensions inevitably clearly influence strategy, this approach may nonetheless dilute 'strategic' to insubstantiality.

Crucial to defining 'strategic' is Bernard Brodie's remark that, "(a)bove all, strategic theory is a theory for action" (Brodie, 1973, p. 452). As a result, strategic studies recognizes two levels of theory: strategy as a general theory and strategy as specific theories of victory practiced by particular polities in time and space. This two-level, mutually-interactive strategic theoretical context affects how a concept's quality should be judged.

Two considerations result. First, general theory should be systemic, whereas actionable theory is inherently ad hoc. A general-level concept fit should within the system while simultaneously being able to generate ad hoc concepts for application—for example, to be able to go from 'operations' to Air Land Battle. However, too many modern ad hoc concepts have unwarranted and unjustified systemic implications. Second, strategy is a form of discovery and way-finding, and so must be thought and practiced abductively. Ad hoc concepts for application must combine into ad hoc, multi-dimensional, actionable theories which explain the logic of how the desired goals are to be achieved. Strategists using these ad hoc theories built out of ad hoc concepts must thereby be capable of generating appropriate orders to their subordinates, to implement the strategy tactically, logistically, etc.

Good strategic concepts must simultaneously fit two distinct measures of quality. First is the academic gauge, which prioritizes elements such as parsimony, coherence, depth, etc. Many of these are inherently valuable to practitioners as well, although they undoubtedly put less effort into ensuring the academic quality of their concepts. Second is the strategic gauge, which emphasizes conceptual transferability from general, systemic theory to ad hoc theory for action, and then from ad hoc theory for action to tactical orders. These two measures of quality are not inherently mutually contradictory, and to a certain degree may actually be mutually reinforcing. Nonetheless, they are distinct and the best strategic concepts fit both quality gauges.

KEYWORDS

Strategy; Concept; Theory; Practice.

REFERENCES

Brodie, B. (1973). *War & Politics*. New York: Macmillan.

Daigneault, P-M. (2012). Introduction to the symposium 'Conceptual analysis in political science and beyond'. *Social Science Information, 51*(2), 183-187.

Gerring, J. (1999). What Makes a Concept Good? A Criterial Framework for Understanding Concept Formation in the Social Sciences. *Polity, 31*(3), 357-393.

Gray, C.S. (1999). *Modern Strategy*. Oxford: Oxford University Press.

Sartori, G. (1984). Guidelines for Concept Analysis. In: G. Sartori (Ed.), *Social Science Concepts: A Systematic Analysis* (pp. 15-85). Beverly Hills: Sage Publications.

Sartori, G. (1975). The Tower of Babel. In: G. Sartori, F.W. Riggs, & H. Teune. *Tower of Babel: On the Definition and Analysis of Concepts in the Social Sciences* (pp. 7-37). Pittsburgh: International Studies Association.

Russia's corrosive policies beyond Europe: What with Russian proxies and military presence in the Sahel?

C. Kozera (1) and M. Marszałek (2)

(1) University of Warsaw, Poland, kozeracyprian@gmail.com
(2) War Studies University, Poland, m.marszalek@akademia.mil.pl

In the proposed presentation, the authors analyse Russian military and proxy involvement in the Sahel in the context of Moscow's attempts at restituting its status as a global power.

The post-Cold War return of Russia into Sub-Saharan Africa, and specifically the Sahel, is characterised by mixed or arm sales and military contract. These, however, cannot match the competing Chinese or French deals or restitute the extent of the Soviet presence in Africa. In order to balance its lack of resources, Russia is proposing another means of military cooperation, namely mercenary services of its proxies: the so-called Wagner group. This quasi-state and quasi-organised crime entity serves as means of projecting Russia's power into disfranchised and often post-coup states that seek security solutions alternative to democratic and liberal means proposed by the international system.

By employing proxies such as the Wagner Group and acting in the grey area of international politics, Russia has been able to obtain results that would not be obtainable otherwise with the same financial or political cost. As the presented case study of Russian involvement in the Republic of Mali shows, Moscow managed to force the traditional and privileged international partner of Mali, France, to hastily withdraw from the country. By installing state-backed mercenaries and military instructors, Moscow not only forced the French out, yet also destabilised the entire European and French-led counterterrorism operation in the Sahel, and severely weakened Paris' position in the region. Considering the financial and political cost of such involvement, and comparing it with the results — it was a great strategic success of Moscow. Such proxy-based political warfare proved very cost-efficient for Moscow.

The authors further argue that allowing such illiberal behaviour, that contradicts all the accepted norms, can encourage further Russian interventions in Africa and other parts of the world, undermining democratic system and international peace — and especially in times when Moscow is waging an illegal war in Ukraine. Last but not least, the authors aim at presenting recommendations for the international community.

The Need for Constructive, Traceable and Auditable Methods for Strategy Analysis and Operations Planning and Execution

A. Carreira (1), J. Mendes (2) and P. Mendes (3)

(1) NOVA School of Science and Technology, Portugal, amp.carreira@fct.unl.pt
(2) Premium Minds, Lda., Portugal, jmendes@premium-minds.com
(3) CENTEC - University of Lisbon, Portugal, p.mendes@tecnico.ulisboa.pt

Given a mission, Armed Forces produce an Operations Plan and put it in place. The expected outcome of the planned military operations, however, is not guaranteed. The reasons for success or failure, be it total or partial, are not always easily identifiable. This is particularly noticeable when the operation fails, although the fundamentals of the operational apparatus have followed established, approved norms and been deemed appropriate for the mission, with no caveats.

Uncertainty in military operations, as in any decision-making rich endeavor, brings risks in itself and a properly planned operation already deals with that, at least by wisely estimating its risk exposure.

However, sometimes the mission goal is ill-posed, loosely described, or both, adding an external, upper layer of uncertainty to the whole of the mission. This often happens due to the intrinsic conflict of interests and ambiguities that permeate the political process that triggers the strategic action, like in international multi-lateral bodies, notably the UN. And yet, more coherent entities, including firmly bound regional organizations, e.g., the EU, or an alliance like NATO, are susceptible to such unavoidable particulars.

Even if the military operation is successful in itself, the political goals behind it may not be achieved. "Lessons Learned" special organizations seek to explore existing information on mission statement, operations planning, setup, unfolding and outcome, and external factors, in order to come to meaningful relationships that may shed new light on the military process, from strategy to tactics, and improve military knowledge. Results look modest, even for traceability and auditability of such a complex process, much less for the providing of predictive-able theories and methods.

If this was not the case, unaccomplished military missions probably would have been successful because their strategic rational, operational apparatus and enabled tactics would have been properly adapted in time and substance whenever those theories or methods, confirmed by matching field data, dictated so.

New planning approaches have been tried, like in the NATO Training Mission – Afghanistan (Zweibelson 2012), which, among others, highlights the organizational-dependent communicational difficulties in the planning process, whose goal was somewhat new, requiring a new approach, with which everyone was essentially inexperienced, and had its own intrinsic limitations.
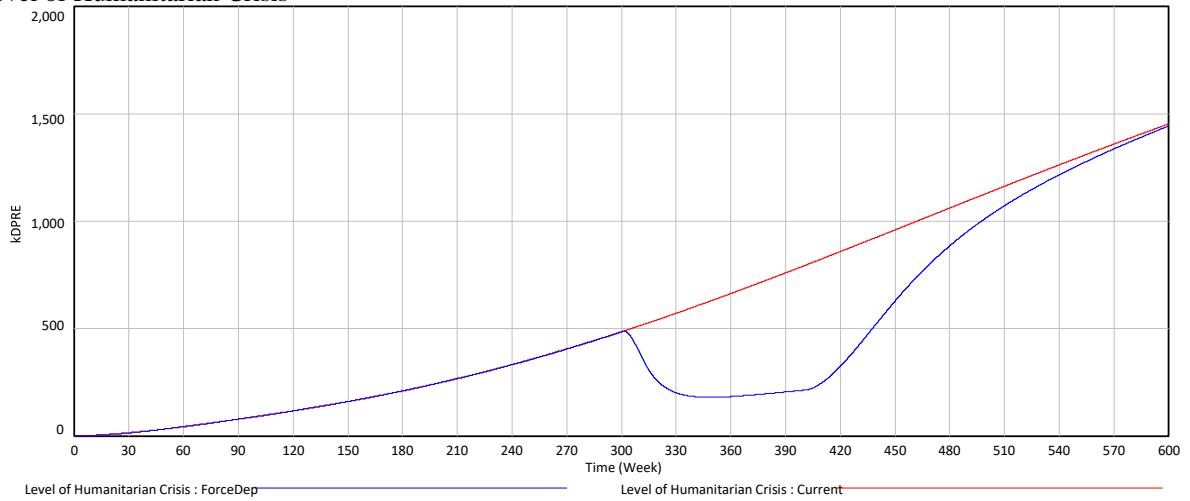
But limitations of current approaches are also visible in such essential actions, like the definition of a Force's strategic objectives and the corresponding identification of operational requirements and needs, as in the case of the new "East of Asia only" proposed view for the US Marine Corps future engagements, with the adoption of a new operational perspective, which proved to be not appropriate for the current geopolitical and military landscape redefined by the war in Ukraine (Mcgee 2022).

Mendes et al. (2016) propose the use of a constructive method to create traceable, auditable and easily updatable models of strategic problems, using Systems Modelling Language. SysML mposes objectivity and provides ease of communication. The proposed method enforces the owners of the problem to identify all the elements of the system (variables and relationships among them). The method provides for simulation to understand the dynamics of the situation. This approach was applied to NATO's Zoran Sea operations planning training case (Orvis 2009), departing from its pure operations purpose and obtaining the model of the systemic structure that explains the problem comprehensively.
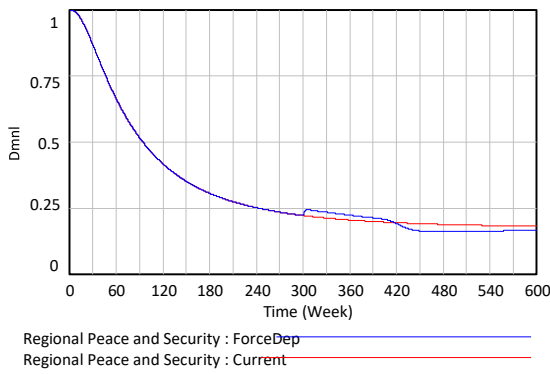
The behaviors over time (BOT) of the four key indicators are depicted on Figure 1. The NATO peace force operation (weeks 300 to 400) only bought time, bringing little more than some relief to DPREs, due to a lack of effective tools in the decision-making political process that was unable to go further than merely order the operation.

The proposed method spotted this failure just by appropriately modelling the system behind the situation. This represents a major possibility for the military process, at the strategic, operational and tactical levels, be it in short or long time frames.
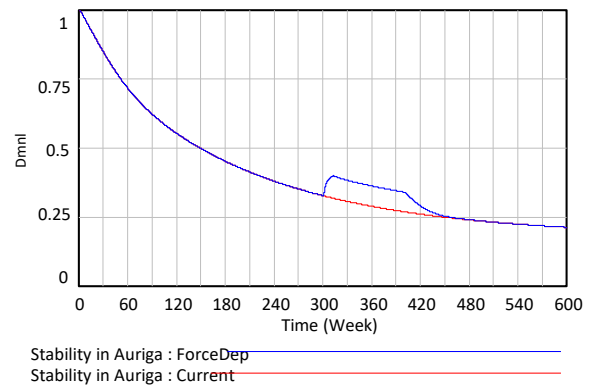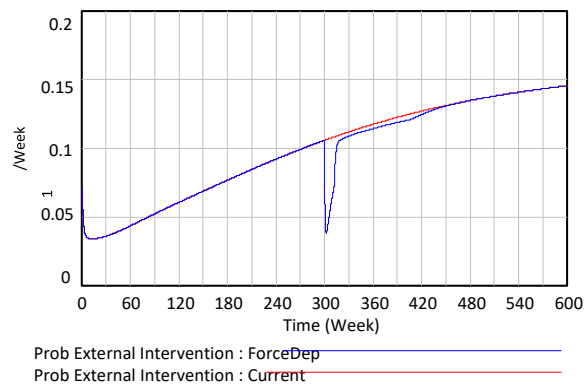
Level of Humanitarian Crisis

Figure 1 – Behaviors Over Time of the key variables. The NATO operation lasts from week 300 through week 400

KEYWORDS

Strategy; Operations; Planning; Method; Constructive method; Traceability; Auditability; Dynamics; Model; Simulation.

REFERENCES

Mcgee, W. (2022). forcing design or designing force ? the reinvention of the Marine Corps. *Small Wars Journal*. Retrieved from https://smallwarsjournal.com/jrnl/art/forcingdesign-or-designing-force-reinvention-marine-corps

Mendes, J., Carreira, A., Aleluia, M. & Mendes; J.P. (2016). Formulating Strategic Problems with Systems Modeling Language. *Journal of Enterprise Transformation, 6*(1), 23–38. doi: 10.1080/19488289.2016.1210705.

Orvis, R. (2009). Back to Basics for HQ Planning Staff. *Nrdc-Ita Magazine,* (14), 11–13.

Zweibelson, B. (2012). Military design in practice: A case from NATO training mission-Afghanistan in 2012. *Small Wars Journal*. Retrieved from https://smallwarsjournal.com/jrnl/art/military-design-in-practice-a-case-from-nato-training-missionafghanistan-in-2012 .

The (new) challenges of maritime security in the Atlantic Ocean

A. Alexandre (1)

(1) Military University Institute of Portugal, amgalexandre527@hotmail.com

The oceans' contribution to human development can be summarized to four main attributes: for the resources they contain; for its utility for trade and shipping; for its importance as a means of information exchange; and as a source of power and dominance (Till, 2009). For the pursuit of all the attributes listed above, Till (2009, p. 286) believes that there is a need for a "good order at sea" as they face, per se, several risks and threats that may jeopardize their contribution to human development. We will focus on just one of those attributes (the oceans as a source of power and dominance).

Maritime security is a concept coined at the end of the last century, which has become well-known at the beginning of this century with the occurrence of terrorist attacks carried out in different maritime spaces (as was, for example, the case of the attack on the USS Cole in the Yemeni port of Aden in 2001) and, above all, with the vertiginous evolution of piracy incidents, especially from 2007 onwards in the Horn of Africa region (Bueger, 2015; Bueger & Edmunds, 2017). It refers to the risks and threats existing in the maritime domain, whether in relation to the territorial integrity of states (which includes security against crimes committed at sea) or in relation to intentional and illegal damage caused to the marine environment (such as illegal dumping of waste or depredation of natural resources) (UNSG, 2008). Maritime security threats are often used in discourses (with a strong geopolitical slant) as an argument (among others) to justify the projection of security beyond the external borders of states. In this sense, ensuring the security of the global commons, for example, legitimizes the projection of naval forces beyond the spaces of jurisdiction of states (Germond, 2015).

The global strategic environment has been marked in the recent past by the return of systemic rivalry, particularly with the rise of China and the persistently aggressive Russia (NATO, 2020). In the Atlantic region, the challenges to maritime security that have been posed by these global powers are being felt in a concrete way.

China's current military strategy is based on active defense, a concept that adopts the principles of strategic defense combined with offensive action at the operational and tactical levels. Active defense is rooted in the principle that a given power intends to avoid the outbreak of armed conflict but be ready to respond if (and when) challenged (Office of the Secretary of Defense, 2020). On the other hand, Beijing has been increasing its People's Liberation Army Navy with modern and flexible means as it has focused in recent years on replacing previous generations of ships with limited capabilities with new multifunctional combatant platforms. While marine resources and trade are seen as the primary reason why Beijing should lean (more) towards the Atlantic, Chinese strategists have assumed that faced with a situation where Washington increases pressure and containment of China's strategic space (in the Indo-Pacific region), the Atlantic is likely to become a new strategic penetration space for Beijing's power in distant seas. And the fact is that China has been trying to penetrate through the South Atlantic, seeking to establish another military base out of doors and investing heavily in African countries participating in the belt and road initiative - whose end points are, by the way, all in the Atlantic (Goldstein, 2020).

Russia's 2015 maritime doctrine identifies the Atlantic as one of the main regional priority areas of Moscow's national maritime policy. It is based on the implementation of long-term objectives in the Atlantic Ocean itself and in the Baltic, Azov, Black and Mediterranean Seas, of which the most relevant are: ensuring a consistent naval presence in the region; and developing the volume of shipping, fishing, marine scientific research and marine ecosystem monitoring, and increasing geological exploration efforts (in the area under Russian jurisdiction) of polymetallic sulphides from the seabed (Russia Maritime Studies Institute, 2015). Moscow will not allow significant superiority of other states' naval forces over its navy and will strive to ensure that it remains the second most capable in global terms. To do so it must possess powerful and balanced fleets in all strategic areas, consisting of ships designed to carry out missions in near and distant maritime regions and ocean areas, as well as naval aviation assets and coastal forces equipped with high-precision strike weapons (Davis, 2017).

We argue that the guarantee of maritime security in the Atlantic basin, given the geopolitical disputes that are foreseen in that region in view of the foreseeable projection of power by the two global actors (China and Russia), will necessarily imply a much more assertive posture on the part of two Western international organisations (NATO and the European Union).

KEYWORDS

Atlantic Ocean; maritime security; China; Russia, NATO; EU.

REFERENCES

Bueger, C. (2015). What is maritime security? *Marine Policy 53*, 159-164.

Bueger, C., & Edmunds, T. (2017). International Affairs 93: 6. *Beyond seablindness: a new agenda for maritime security studies*, 1293-1311.

Davis, A. (2017). *English Translation of the Fundamentals of the State Policy of the Russian Federation in the Field of Naval Operations for the Period Until 2030*. Newport. Rhode Island: Russia Maritime Studies Institute. United States Naval War College.

Germond, B. (2015). The geopolitical dimension of maritime security. *Marine Policy 54*, 137-142.

Goldstein, L. J. (2020). *Would the Chinese Navy Dare Sail In the Atlantic Ocean?* The National Interest. Retrieved from https://nationalinterest.org/blog/reboot/would-chinese-navy-dare-sail-atlantic-ocean-167256

NATO. (2020). *NATO 2030: United for a New Era.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-FinalReport-Uni.pdf

Office of the Secretary of Defense. (2020). *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China.* Washington: US Department of Defense. Retrieved from https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWERREPORT-FINAL.PDF

Russia Maritime Studies Institute. (2015). *Maritime Doctrine of the Russian Federation*. Newport: United States Naval War College.

Till, G. (2009). *Seapower. A Guide for the Twenty-First Century* (Second ed.). New York: Routledge.

UNSG. (2008). *Oceans and the law of the sea : report of the Secretary-General.* United Nations. Washington: UN General Assembly. Retrieved from https://www.refworld.org/docid/48da24e72.html

Designing Strategy from Complexity. The modeling of National Security through System Dynamics

A. Figueiredo (1)

(1) Instituto Universitário Militar, Portugal, figueiredo.ama@ium.pt

At the hearth of the Information Age, where Nations, Organizations, and different Societies are increasingly interconnected and interdependent, adaptability and evolution become critical to steer a world that Jamais Cascio describes as brittle, anxious, non-linear and incomprehensible. It is within this highly dynamic context that Nations seek to design strategies in order to bring coherence on their efforts to achieve National Interests, with an increased adoption of comprehensive approaches that orchestrate the Instruments of Power towards an acceptable condition of National Security. Yarger (2006) rightfully points out the importance of Strategy in this context "as it helps discipline our thinking in order to deal with the complexity and volatility of the strategic environment". But as the paradigms of looking at reality change, so must the tools and methods follow that trend.

When traditional, linear, deterministic models no longer suffice to study reality, the focus on not only the individual entities but also the connections and relationships between them becomes vital to study the fabric of the systems that define our world. Such endeavor has been explored by the field of Complex Systems Science. Siegenfeld and Bar-Yam (2020) state that complex System Science consider systems with many components, either physical, biological, or social, and while most scientific disciplines focus on the components themselves, complex system science studies how the components within a system are related to one another. As the subfields of interest have increased, ranging from Physics and Economics to Ecology and Sociology, so have different approaches to the study of complex systems emerged along the years (Mitleton-Kelly, Paraskevas, & Day, 2018). Of particular interest for this research is the field of System Dynamics (SD). SD is a major systems science approach initially developed by Jay Forrester in the late 1950s that has continued to grow and gain acceptance in all types of organizations (Richardson, 2020).

Strategy and complexity are indissociable. The wok of Osinga (2007) sheds light on how important the study of complex adaptive systems was on shaping the strategic thinking of John Boyd. Cabayan et al. (2012) show how relevant the study of complexity is for strategists in the field of National Security. Building from those insights, and leveraging the wide range of SD applications on Business Strategy and Policy Making (Rahmandad, 2015), this PhD thesis project aims at (1) analyzing how complexity defines the physical, human and social dimensions and their implications for Strategy formulation; (2) model National Security as a complex system through the use of System Dynamics methodology; (3) create a conceptual framework that integrates the study of complex systems into National Security Strategy design.

KEYWORDS

Strategy; National Security; Complexity; System Dynamics.

REFERENCES

Cabayan, H., Adelman, J., Amir-ghessemi, A., Astorino-Courtois, A., Berns, G., Bragg, B., & Busch, W. (2012). *National Security Challenges: Insights from Social, Neurobiological, and Complexity Sciences*. Retrieved from https://apps.dtic.mil/sti/citations/ADA565602

Mitleton-Kelly, E., Paraskevas, A., & Day, C. (2018). *Handbook of research methods in complexity science : theory and applications*. Cheltenham, UK: Edward Elgar Publishing.

Osinga, F. P. B. (2007). *Science, strategy and war : the strategic theory of John Boyd*. New York, NY: Routledge.

Rahmandad, H. (2015). Connecting strategy and system dynamics: an example and lessons learned. *System Dynamics Review, 31*(3), 149-172.

Richardson, G. P. (2020). Core of System Dynamics. In B. Dangerfield (Ed.), *System Dynamics: Theory and Applications* (pp. 11-20). New York, NY: Springer US.

Siegenfeld, A. F., & Bar-Yam, Y. (2020). An introduction to complex systems science and its applications. *Complexity, 2020*. doi: https://doi.org/10.1155/2020/6105872

Yarger, H. R. (2006). *Strategic theory for the 21st century : the little book on big strategy*. Strategic Studies Institute, U.S. Army War College.

Russian Federation's strategy in the Central African Republic

M. Correia (1)

(1) Portuguese Army, correia.mjp@exercito.pt

This paper aims to analyse Russian Federation's strategy in the Central African Republic (CAR). The goal of the first moment is to contextualize the operational environment in CAR, describing the current operational environment, and identifying and highlighting the factors that motivate the presence of the Russian Federation in the CAR. The goal of the second moment is to characterize the Russian Federation's conception of Hybrid Warfare and describe the differences between the Russian and Western conceptions of Hybrid Warfare. The third moment characterizes and analyses the practical applicability of two of the Hybrid Warfare instruments in the CAR, mainly the Russian Federation's activities in the Information Environment and the use of Russian Private Military Companies (PMC) while reflecting on the changes introduced and the consequences resulting from the implementation of the Russian Federation's Strategy in the CAR.

The African continent presents itself as a stage of opportunity for the Russian Federation. Expanding the Russian Federation's influence in Africa can reduce the impact of coercive sanctions, provide an additional revenue stream, and can also support the expansion of its military presence and influence in the informational space.

The outcome of the UN General Assembly vote resolution against Ukraine invasion on the 2nd March of 2022 allows the assessment of Moscow's diplomatic influence in Africa. The narratives of historical support for the selfdetermination of African countries and the unconditional support for their empowerment - materialized by Russia's military presence through bilateral agreements, PMCs, arms supplies - coupled with the efficient information campaign that underpin the high dependence of autocratic governments on Kremlin. The Russian Federation cannot compete militarily with other global powers, but it can serve as a permanent destabilizer of their interests by applying its instruments of power and influence. The CAR is the perfect setting to bring about this imbalance by supporting the increase and expansion of Russian diplomatic influence in the region. The Russian Federation leverages CAR as a base of support and uses the income generated by natural resources as the primary source of funding and incentive for Russia's mercenary forces, which present themselves as a fundamental tool by shaping people's perception of reality and thus contributing decisively to the pursuit of the Russian Federation's goals.

KEYWORDS

Africa; Central African Republic; Russian Federation's; Hybrid Warfare; Information campaign; Private Military Companies.