Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2463-9575
2024 – 26/št. 2

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2463-9575
UDK 355.5(479.4)(055)
2024 – 26/št. 2

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Izdajatelj Publisher	Generalštab Slovenske vojske General Staff of the Slovenian Armed Forces
Glavna urednica Editor-in-Chief	dr. Liliana Brožič
Odgovorni urediniki Executive Editors	dr. Klemen Kocjančič dr. Viktor Potočnik dr. Pavel Vuk
Uredniški odbor Editorial Board	dr. Yusuf Abubakar, Baze University, Abuja, Nigeria dr. Zahid Anwar, University of Peshawar, Peshawar, Pakistan dr. Andrej Anžič, European Faculty of Law, Nova Gorica, Slovenia dr. Gorazd Bajc, National and Study Library, Trieste, Italy dr. Anton Bebler, Faculty of Social Sciences, Ljubljana, Slovenia višja vojaška uslužbenka XIII. razreda dr. Valerija Bernik (OF-4), Military Schools Centre, Maribor, Slovenia višji vojaški uslužbenec XIV. razreda dr. Denis Čaleta (OF-5), Knjižnično-informacijski in založniški center, Ljubljana, Slovenia dr. Maja Garb, Faculty of Social Sciences, Ljubljana, Slovenia dr. Bastian Giegerich, International Institute for Strategic Studies, London, United Kingdom dr. Irina Goldenberg, Military Personnel Research and Analysis, Canada dr. Olivera Injac, Univerzitet Donja Gorica, Podgorica, Montenegro dr. Jian Junbo, Fudan University, Shanghai, China polkovnik dr. Tomaž Kladnik (OF-5), Military Schools Centre, Maribor, Slovenia dr. Sergei Konoplyev, Harvard University, Cambridge, United Kingdom dr. Igor Kotnik, General Staff of the Slovenian Armed Forces, Ljubljana, Slovenia dr. Ivana Luknar, Institute for Political Studies, Belgrade, Serbia dr. Julie T. Manta, US Army War College, Carlise, United States dr. Thomas Mockaitis, DePaul University, Chicago, United States dr. Klaus Olshausen (OF-8, ret.), Clausewitz-Gesellschaft e.V., Hamburg, Germany dr. Jagannath Panda, Institute for Security and Development Policy, Stockholm, Sweden dr. Zoltán Rajnai, Doctoral School on Safety and Security Sciences, Budapest, Hungary dr. Tibor Szvircsev Tresh, Militärakademie an der ETH, Zürich, Switzerland dr. Viljar Veebel, Baltic Defence College, Tartu, Estonia dr. Thomas Young, Center for Civil-Military Relations, Monterey, United States dr. Yahia H. Zoubir, Kedge Business School, Paris, France
Sekretarka Secretary	višja praporščakinja Nataša Cankar (OR-9)
Prevajanje Translation	Iris Žnidarič
Lektoriranje Proofreading	Justi Carey, Marjetka Brulec, Tina Pečovnik, Vesna Vrabič
Oblikovanje Design	Skupina Opus Design
Grafični prelom Graphics	Jurko Starc
Tisk Print	Silveco, d.o.o.
ISSN	2232-2825 (tiskana različica/print version) 2463-9575 (spletna različica/online version)
Naklada Edition	300 izvodov/copies Izhaja štirikrat na leto/Four issues per year
Revija je dostopna na spletni strani Publication web page	https://sciendo.com/journal/CMC https://sciendo.com/journal/CMC
E-naslov uredništva Editorial staff´s email	svi-cmc@mors.si

Publikacija je uvrščena v bibliografsko zbirko podatkov COBISS.SI, Crossref, Military and Government Collection, EBSCO in Air University Library Index in Military Periodicals.

The publication is indexed in bibliography databases COBISS.SI, Crossref, Military and Government Collection, EBSCO and Air University Library Index in Military Periodicals.

TRANSFORMACIJA OBOROŽENIH SIL

»Potreba po transformaciji se čuti bolj kot kdaj koli prej, predvsem zato, ker prihodnjih ciljev ni več mogoče doseči z nadaljnjim prehodnim prilagajanjem strukture, nalog, organizacije in delovanja oboroženih sil.«

Upokojeni generalmajor SV Alojz Šteiner (2009), Čas je za transformacijo, Sodobni vojaški izzivi 11(3): 131

TRANSFORMATION OF ARMED FORCES

»The need for transformation is being felt more than ever before, mainly because the future objectives can no longer be attained by continuing the transition adjustment of the structure, tasks, organization and the armed forces operation.«

Alojz Šteiner, Major General (ret.), Slovenian Armed Forces (2009), It is Time for Transformation, Contemporary Military Challenges 11(3): 131

VSEBINA
CONTENTS

sciendo

Sodobni vojaški izzivi, 2024 – 26/št. 2
Contemporary Military Challenges, 2024 – 26/No. 2

Klemen Kocjančič

DOI: 10.2478/cmc-2024-0008

UVODNIK

TRANSFORMACIJA OBOROŽENIH SIL

Uvod Po koncu hladne vojne je atlantsko zavezništvo izgubilo poglavitnega nasprotnika, ko je bil ukinjen Varšavski pakt in je razpadla Sovjetska zveza. Posledično so predvsem evropske države začele krčiti obrambne proračune, kar je vplivalo na velikost, oborožitev in zmogljivost oboroženih sil.

Šele teroristični napadi na ZDA 11. septembra 2001 in (ameriško vodena) globalna vojna proti terorizmu so malenkostno spremenili trend zmanjševanja vojaških zmogljivosti, a strateško gledano se v Evropi sposobnost za (samostojno) obrambo ni spremenila. Tudi oboroženi konflikti na Bližnjem vzhodu in Kavkazu ter ruska zasedba Krima in Donbasa niso spremenili razmišljanja evropskih politikov ter gospodarstvenikov, da je treba krepiti vojaške zmogljivosti – ne samo oboroženih sil, ampak tudi vojaško industrijo.

Nova ruska invazija na Ukrajino leta 2022 je odprla oči politikov, ki so izdatno povečali obrambne proračune, kar se je preobrazilo v povečanje nakupov oborožitvenih sistemov in vojaške opreme, povečanje kadrovskega obsega, povečanje vlaganja v vojaško industrijo in proizvodnjo izdelkov z dvojno rabo ter v druge ukrepe za transformacijo oboroženih sil ter sil za zaščito in reševanje.

1 NAPREDEK NA OBRAMBNEM PODROČJU

Podobno se je zgodilo v Sloveniji. Marca 2023 je bila sprejeta nova Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2040, konec maja pa še Srednjeročni obrambni program Republike Slovenije 2023–2028. Leta 2023 je bilo za potrebe razvoja, raziskav in inovacij na Ministrstvu za obrambo namenjenih 12,5 milijona evrov, medtem ko je v letu 2024 za to področje namenjenih 23 milijonov evrov (Ministrstvo za obrambo, 2023).

V prvi polovici aprila 2024 je Ministrstvo za obrambo napovedalo delno preoblikovanje strukture in organiziranosti Slovenske vojske (SV). Načrtovano povečanje kadrovskega obsega SV bo vodilo k večjemu obsegu pogodbene rezervne sestave in s tem prostorskega dela SV, ki bo deloval izključno na nacionalnem ozemlju Slovenije. Okrepljeni prostorski del SV bo dopolnjeval manevrski del SV oz. stalno sestavo. Do poletja 2024 bo ustanovljeno Poveljstvo prostorskih sil SV, ki bo brigadne ravni in bo nadziralo ter usmerjalo načrtovani teritorialni poveljstvi ter oba obstoječa teritorialna polka. Hkrati bosta ustanovljena dva nova polka (vsak bo obsegal en jurišni odred četne ravni), nato pa bo v roku enega leta vzpostavljenih še osem novih teritorialnih polkov. V okviru Poveljstva prostorskih sil SV bo ustanovljen še učni center, ki bo deloval izključno na področju krepitve in delovanja prostorske organiziranosti SV. Napovedanim spremembam na področju prostorske organiziranosti SV bo sledila (ponovna) ustanovitev brigade vojaškega letalstva in zračne obrambe. Ponovno bodo do konca leta 2024 ustanovljeni še inženirski bataljon, bataljon jedrske, radiološke, kemične in biološke obrambe ter enota za nekinetično delovanje bataljonske ravni. Do julija prihodnje leto bo ustanovljena še enota brezpilotnih bojnih letalnih sistemov (Ministrstvo za obrambo 2024a, 2024b).

V drugi polovici aprila 2024 je Vlada Republike Slovenije sprejela še tri temeljne razvojno-usmerjevalne dokumente na obrambnem področju, in sicer Obrambno strategijo, Vojaško strategijo in Strategijo civilne obrambe. Vsi trije dokumenti temeljijo na Resoluciji o strategiji nacionalne varnosti, pri oblikovanju dokumentov pa so upoštevali najnovejše varnostne izzive, s katerimi se sooča tudi Slovenija kot članica EU in Nata (Ministrstvo za obrambo, 2024c).

Obrambna strategija narekuje uresničevanje naslednjih obrambnih ciljev: »odvrniti vojaške in druge grožnje ter tveganja za nacionalno, kolektivno in skupno varnost; obraniti neodvisnost, nedotakljivost in ozemeljsko celovitost države ter interese v okviru kolektivne in skupne obrambe; zagotoviti neprekinjeno delovanje države in družbe«. Za doseganje obrambnih ciljev je pomembna tudi nova Vojaška strategija, ki določa naslednje vojaške strateške cilje: »zagotovljeno kredibilno in uspešno odvračanje, zaščiteni, zavarovani in obranjeni suverenost, prostorska celovitost in drugi vitalni interesi RS, kredibilno prispevanje in sodelovanje v kolektivni obrambi in medsebojni pomoči, prepoznavno prispevanje k mednarodnemu miru, varnosti in stabilnosti, prispevanje k okrepljeni odpornosti države in družbe.« Vojaška strategija je pomembna tudi zaradi poudarjanja krepitve lastnih vojaških zmogljivosti, ki ima prednost pred naslanjanjem na kolektivno obrambo znotraj atlantskega zavezniška in Evropske unije. Strategija civilne obrambe Republike Slovenije dopolnjuje Vojaško strategijo tako, da v zagotavljanje nacionalne obrambe vključuje civilni del družbe, in sicer »s podporo Slovenski vojski in vojaški obrambi države, ohranjanjem neprekinjenega delovanja oblasti ter gospodarskih in drugih dejavnosti, ki so pomembne za obrambo ter preskrbo, zaščito in preživetje prebivalstva.« (Ministrstvo za obrambo, 2024c)

2 ZNANSTVENI PRISTOP K TRANSFORMACIJI OBOROŽENIH SIL

V preteklosti je bilo v *Sodobnih vojaških izzivih* objavljenih več prispevkov, ki so obravnavali transformacijo oboroženih sil z različnih vidikov: transformacijo pehotnega oddelka, voda in čete (Potočnik, 2020), zmogljivosti (Svete in Jankovič, 2009), vojaške strateške rezerve (Vegič, 2017), mirovnih operacij (Grošelj, 2009; Schmidl, 2009), zveze Nato (Šteiner, 2010, 2017), Slovenske vojske (Šteiner, 2015, 2017), madžarskih oboroženih sil (Padány in Földi, 2018) itn.

V tej številki *Sodobnih vojaških izzivov* objavljamo nove poglede domačih in tujih strokovnjakov na to tematiko.

Prvi prispevek je delo Lawrencea E. Clina z naslovom *Načrtovanje strateškega informacijskega delovanja*. Avtor v prispevku opozarja, da morajo vojaški odločevalci na področju načrtovanja in izvajanja informacijskega delovanja delovati strateško, saj trenutno veliko vojaških odločevalcev meni, da informacijsko delovanje ne sodi na vojaško področje. Hkrati izpostavlja tudi dejstvo, da je informacijsko delovanje tako ofenzivne kot defenzivne narave.

Sledi prispevek Urbana Praprotnika z naslovom *Načelo razlikovanja v kibernetskem prostoru*. Kibernetski prostor vse bolj postaja prizorišče različnih oblik napadov in drugih oblik delovanja. Avtor v prispevku opredeljuje pomen in potrebo uporabe načela razlikovanja pri delovanju v kibernetskem prostoru. To izhaja iz dejstva, da večina kibernetskih dejavnosti poteka na civilni kibernetski infrastrukturi, ki omogoča (normalno) življenje splošnemu prebivalstvu. Posledično je treba uporabljati načela mednarodnega humanitarnega prava za zaščito civilnega prebivalstva, tudi ko gre za delovanje v kibernetskem prostoru.

Guillermo López-Rodríguez in Daniel Montoya-Roldan sta avtorja prispevka *Izzivi in perspektive v urbanem bojevanju: analitični okvir*, v katerem navajata ovire, s katerimi se soočajo sodobne konvencionalne sile med bojnim delovanjem v urbanem okolju. Razsežnost vojaške organiziranosti, uporaba tehnologij za dvojno rabo in vloga civilnega prebivalstva postajajo ključni elementi pri sodobnem urbanem bojevanju. Na podlagi analize dejavnikov avtorja ponudita rešitve za prihodnje urbano bojevanje z uporabo tako kognitivnih kot tudi kinetičnih dejanj.

Prispevek z naslovom *Kumulativni učinki gonil konfliktov v regiji Sahel*, delo Jelene Juvan, analizira različne dejavnike oz. vzroke, ki vplivajo na varnostne razmere v afriški regiji Sahel. Avtorica opredeli, analizira in razvrsti dejavnike v štiri glavne kategorije, nato pa analizira prepletanje teh gonil konflikta. Pri tem se izkaže, da se konflikti širijo ne samo prek meja posameznih držav in regije, ampak tudi v sosednje regije ter celo na druge celine, zaradi česar je Sahel varnostno gledano ena najbolj problematičnih regij na svetu.

Literatura

1. *Grošelj, K., 2009. Transformacija sodobnih mirovnih operacij in vloga Slovenije. Sodobni vojaški izzivi, 11(1), str. 63–78.*
2. *Lipovec, F., 2019. Slovenska vojska do leta 2025 in naprej. Sodobni vojaški izzivi, 21(1), str. 5–34.*
3. *Ministrstvo za obrambo, 2023. Ključni dosežki na Ministrstvu za obrambo v času prvega leta 15. Vlade Republike Slovenije, Gov.si. https://www.gov.si/novice/2023-06-01-kljucni--dosezki-na-ministrstvu-za-obrambo-v-casu-prvega-leta-15-vlade-republike-slovenije/, 5. 5 2024.*
4. *Ministrstvo za obrambo, 2024a. Slovenska vojska bo letos in prihodnje leto delno preoblikovala svojo strukturo in organiziranost, Gov.si. https://www.gov.si/novice/2024-04-10-slovenska-vojska-bo-letos-in-prihodnje-leto-delno-preoblikovala-svojo-strukturo-in-organiziranost/, 5. 5 2024.*
5. *Ministrstvo za obrambo, 2024b. Letalstvo Slovenske vojske se je preoblikovalo, Gov.si. https://www.gov.si/novice/2024-05-09-letalstvo-slovenske-vojske-se-je-preoblikovalo/, 5. 5 2024.*
6. *Ministrstvo za obrambo, 2024c. Vlada sprejela tri temeljne razvojno-usmerjevalne dokumente države na obrambnem področju, Gov.si. https://www.gov.si/novice/2024-04-24-vlada-sprejela-tri-temeljne-razvojno-usmerjevalne-dokumente-drzave-na-obrambnem-podrocju/, 5. 5 2024.*
7. *Padányi, J., in Földi, L., 2018. Modernizacija v madžarski vojski. Sodobni vojaški izzivi, 20(3), str. 49–62.*
8. *Potočnik, V., 2020. The changed character of war and the transformation of infantry squad, platoon and company. Sodobni vojaški izzivi 22(3), str. 45–66.*
9. *Schmidl, E. A., 2009. Razvoj mirovnih operacij oziroma operacij v podporo miru - pregled. Sodobni vojaški izzivi, 11(1), str. 79–97.*
10. *Svete, U., in Jankovič, Z., 2009. Izkušnje Republike Slovenije pri uvajanju zmogljivosti omrežnega delovanja. Sodobni vojaški izzivi, 11(3), str. 135–157.*
11. *Šteiner, A., 2009. Čas je za transformacijo. Sodobni vojaški izzivi, 11(3), str. 117–134.*
12. *Šteiner, A., 2010. Med tranzicijo in transformacijo. Sodobni vojaški izzivi, 12(2), str. 93–109.*
13. *Šteiner, A., 2015. Za boljše razumevanje transformacijske paradigme in transformacije oboroženih sil. Sodobni vojaški izzivi, 17(2), str. 13–34.*
14. *Šteiner, A., 2017. Prispevki za analizo izzivov in prihodnjega razvoja ter obsega vojske v Sloveniji. Sodobni vojaški izzivi, 19(4), str. 35–52.*
15. *Vegič, V., 2017. Vojaška strateška rezerva in transformacija sodobnih oboroženih sil. Sodobni vojaški izzivi, 19(4), str. 53–71.*

email: klemen.kocjancic@mors.si

ORCID: 0000-0001-5206-6405

Klemen Kocjančič

DOI: 10.2478/cmc-2024-0009

EDITORIAL

TRANSFORMATION OF THE ARMED FORCES

Introduction

After the end of the Cold War, when the Warsaw Pact was abolished and consequently the Soviet Union collapsed, the Atlantic Alliance lost its main adversary. As a result, European countries in particular started to cut their defence budgets, which affected the size, weapons and capabilities of their armed forces.

It was not until the terrorist attacks on the U.S. on 11 September 2011 and the (US-led) global war on terror that the trend of military capability cuts slightly changed. However, strategically, the Europe's ability for (self) defence has not changed. Even the armed conflicts in the Middle East and the Caucasus, as well as the Russian occupation of Crimea and Donbas, have not changed the minds of European politicians and economists that military capabilities - not only armed forces, but also military industry - need to be strengthened.

The new Russian 2022 invasion of Ukraine opened the eyes of politicians, who substantially increased defence budgets, which in turn translated into increased purchases of weapon systems and military equipment, increased staffing levels, increased investment in military and dual-use industries, as well as other measures to transform the armed forces and protection and rescue forces.

1 PROGRESS IN THE FIELD OF DEFENCE

The same has happened in Slovenia. In March 2023, the new Resolution on the Long-Term Programme for the Development and Equipment of the Slovenian Armed Forces until 2040, was adopted, and at the end of May, the Medium-Term Defence Programme of the Republic of Slovenia 2023-2028 was adopted. In 2023, €12.5 million was earmarked for the needs of development, research and innovation in the Ministry of Defence, while €23 million is earmarked in 2024 (Ministry of Defence, 2023).

In the first half of April 2024, the Ministry of Defence announced a partial transformation of the structure and organization of the Slovenian Armed Forces (SAF). The planned increase in SAF manpower will lead to a larger volume of contracted reserve personnel and thus the territorial segment of the SAF that will operate exclusively on the national territory of Slovenia. The reinforced territorial component of the SAF will thereby complement the manoeuvre component of the SAF, i.e. the active component. Consequently, by the summer of 2024, an SAF Territorial Forces Command will be established at brigade level to oversee the planned territorial commands and the two existing territorial regiments. Two new regiments (each comprising one company-level detachment) will be established at the same time, followed by eight new territorial regiments within one year. A training centre will also be established within the SAF Territorial Forces Command, which will work exclusively in the field of strengthening and functioning of the SAF spatial organisation. In addition to the announced changes in the field of the SAF spatial organisation, the (re)establishment of the Aviation and Air Defence Brigade followed. By the end of 2024, the Engineer Battalion and the Nuclear, Radiological, Chemical and Biological Defence Battalion, as well as the Non-Kinetic Battalion Level Unit will be re-established. By next July, an unmanned combat air systems unit will be established (Ministry of Defence 2024a, 2024b).

In the second half of April 2024, the Government of the Republic of Slovenia adopted another three more fundamental development-orientation documents in the field of defence, namely the Defence Strategy, the Military Strategy and the Civil Defence Strategy. All three documents are based on the Resolution on the National Security Strategy, and have also taken into account the latest security challenges facing Slovenia as a member of the EU and NATO.

The Defence Strategy dictates the pursuit of the following defence objectives: "to deter military and other threats and risks to national, collective and common security; to defend the independence, integrity and territorial integrity of the state and its interests in the framework of collective and common defence; to ensure the continuity of the functioning of the state and society". The new Military Strategy is also relevant to the achievement of defence objectives, and sets out the following military strategic objectives: "credible and effective deterrence assured; sovereignty, spatial integrity and other vital interests of the Republic of Slovenia protected, secured and defended; credible contribution to and participation in collective defence and mutual assistance; visible contribution to international peace, security and stability; contribution to enhanced resilience of the state and society". The importance of the Military Strategy also lies in the emphasis on strengthening our own military capabilities and only then relying on collective defence within the Atlantic Alliance and the European Union. The Civil Defence Strategy of the Republic of Slovenia complements the Military Strategy by involving the civilian part of society in the provision of national defence, namely "by supporting the Slovenian Armed Forces and the military defence of the country, maintaining the continuity of the functioning of the authorities, and economic and other activities important for the defence and the supply, protection and survival of the population." (Ministry of Defence, 2024c)

2 THE SCIENTIFIC APPROACH TO THE TRANSFORMATION OF THE ARMED FORCES

In the past, Contemporary Military Challenges has published several articles addressing the transformation of the armed forces from different perspectives: infantry squad, platoon and company transformation (Potočnik, 2020), capability transformation (Svete and Jankovič, 2009), military strategic reserve transformation (Vegič, 2017), peacekeeping transformation (Grošelj, 2009; Schmidl, 2009), on the transformation of NATO (Šteiner, 2010, 2017), on the transformation of the Slovenian Armed Forces (Šteiner, 2015, 2017) and the Hungarian Armed Forces (Padány and Földi, 2018), etc.

In this issue of *Contemporary Military Challenges*, we are publishing new perspectives on this topic from national and international experts.

The first contribution is by **Lawrence E. Cline** and is entitled *Planning for Strategic Information Operations*. In the paper, the author points out that military decision-makers need to act strategically in the planning and execution of information operations, as many military decision-makers currently consider information operations to be outside the military domain. At the same time, it also highlights the fact that information operations are both offensive and defensive in nature.

This is followed by a contribution by **Urban Praprotnik** entitled *The Principle of Distinction in Cyber Warfare*. Cyberspace is increasingly becoming the scene of various forms of attacks and other forms of action. In his paper, the author defines the importance and necessity of applying the principle of distinction when it comes to acting in cyberspace. This is because most cyber activities take place on civilian cyber infrastructure that enables (normal) life for the general population. Consequently, the principles of international humanitarian law must be applied to protect civilians also when it comes to operating in cyberspace.

Guillermo López-Rodríguez and **Daniel Montoya-Roldan** have written a paper entitled *Challenges and Prospects in Urban Warfare: An Analytical Framework*, which outlines the obstacles faced by modern conventional forces when fighting in urban environments. The dimension of military organisation, the use of dual-use technologies and the role of the civilian population are becoming key elements in modern urban warfare. Based on an analysis of the factors, the authors offer solutions for future urban warfare using both cognitive and kinetic actions.

Jelena Juvan's paper, *The Cumulative Effects of Conflict Drivers in the Sahel Region*, provides and analysis of different factors or causes that influence the security situation in the Sahel region of Africa. The author defines, analyses and classifies the factors into four main categories, and then analyses the interplay between these drivers of conflict. In doing so, it turns out that conflicts spread not only across national and regional borders, but also to neighbouring regions as well as to other

continents, making the Sahel one of the most problematic regions in the world in terms of security.

References

1. *Grošelj, K., 2009. Transformation of contemporary peacekeeping operations and the role of Slovenia. Contemporary Military Challenges, 11(1), pp 63–78.*
2. *Lipovec, F., 2019. Slovenian Armed Forces up to 2025 and beyond. Contemporary Military Challenges, 21(1), pp 15–34.*
3. *Ministry of Defence, 2023. Ključni dosežki na Ministrstvu za obrambo v času prvega leta 15. Vlade Republike Slovenije [Key achievements of the Ministry of Defence during the first year of the 15th Government of the Republic of Slovenia], Gov.si. Available at: https://www.gov.si/novice/2023-06-01-kljucni-dosezki-na-ministrstvu-za-obrambo-v-casu-prvega-leta-15-vlade-republike-slovenije/ (Accessed: 5 May 2024).*
4. *Ministry of Defence, 2024a. Slovenska vojska bo letos in prihodnje leto delno preoblikovala svojo strukturo in organiziranost [The Slovenian Armed Forces will partially reorganise its structure and organisation this year and next], Gov.si. Available at: https://www.gov.si/novice/2024-04-10-slovenska-vojska-bo-letos-in-prihodnje-leto-delno-preoblikovala-svojo-strukturo-in-organiziranost/ (Accessed: 5 May 2024).*
5. *Ministry of Defence, 2024b. Letalstvo Slovenske vojske se je preoblikovalo [The Aviation of the Slovenian Armed Forces has transformed], Gov.si. Available at: https://www.gov.si/novice/2024-05-09-letalstvo-slovenske-vojske-se-je-preoblikovalo/ (Accessed: 5 May 2024).*
6. *Ministry of Defence, 2024c. Vlada sprejela tri temeljne razvojno-usmerjevalne dokumente države na obrambnem področju [The Government adopts three key national defence development and orientation documents], Gov.si. Available at: https://www.gov.si/novice/2024-04-24-vlada-sprejela-tri-temeljne-razvojno-usmerjevalne-dokumente-drzave-na---obrambnem-podrocju/ (Accessed: 5 May 2024).*
7. *Padányi, J., and Földi, L., 2018. Modernisation within the Hungarian Defence Forces. Contemporary Military Challenges, 20(3), pp 49–62.*
8. *Potočnik, V., 2020. The changed character of war and the transformation of infantry squad, platoon and company. Contemporary Military Challenges 22(3), pp 45–66.*
9. *Schmidl, E. A., 2009. Transformation of Contemporary Peacekeeping Operations and the Role of Slovenia. Contemporary Military Challenges, 11(1), pp 79–97.*
10. *Svete, U., and Jankovič, Z., 2009. Experience of the Republic of Slovenia in the Introduction of the Netweok Operation Capabilities. Contemporary Military Challenges, 11(3), pp 135–157.*
11. *Šteiner, A., 2009. It is time for transformation. Contemporary Military Challenges, 11(3), pp 117–134.*
12. *Šteiner, A., 2010. Between transition and transformation. Contemporary Military Challenges, 12(2), pp 93–109.*
13. *Šteiner, A., 2015. For better understanding of transformational paradigm and transformation of armed forces. Contemporary Military Challenges, 17(2), pp 13–34.*
14. *Šteiner, A., 2017. Prispevki za analizo izzivov in prihodnjega razvoja ter obsega vojske v Sloveniji. Contemporary Military Challenges, 19(4), pp 35–52.*
15. *Vegič, V., 2017. Vojaška strateška rezerva in transformacija sodobnih oboroženih sil. Contemporary Military Challenges, 19(4), pp 53–71.*

email: klemen.kocjancic@mors.si

ORCID: 0000-0001-5206-6405

Lawrence E. Cline

DOI: 10.2478/cmc-2024-0010

NAČRTOVANJE STRATEŠKEGA INFORMACIJSKEGA DELOVANJA

PLANNING FOR STRATEGIC INFORMATION OPERATIONS

Povzetek Strateško informacijsko delovanje se običajno obravnava kot vprašanje nad vojaško ravnjo. Kljub temu je bistveno za oblikovanje širšega operativnega okolja in zagotavljanje strateške pobude z izjemo vojne in zato ključno za vojaške strege. V večini zahodnih držav je bil poudarek na obrambnih ukrepih proti nasprotnikovim prizadevanjem na področju informacijskega delovanja. Takšna obrambna miselnost ima malo možnosti za uspeh. Nekateri dolgoročni vzorci in izkušnje na področju informacijskega delovanja so uporabna podlaga za kampanje obrambnega in ofenzivnega informacijskega delovanja.

Ključne besede ***Informacijsko delovanje, dezinformacije, informacijska vojna, politična vojna.***

Abstract Strategic information operations (IO) have normally been viewed as an issue above the military level. Nevertheless, they are critical both in shaping the larger operational environment and in providing a strategic initiative short of war. As such, they are crucial for military strategists. Also, in most Western countries, the focus has been on defensive measures against opponents' IO efforts. Such a defensive mindset is unlikely to succeed. Some long-term patterns and lessons learned in IO provide a useful template for both defensive and offensive IO campaigns.

Key words ***Information operations, disinformation, information warfare, political warfare.***

Introduction

Both during the Cold War and since, many countries have been subject to various forms of Information Operations (IO) campaigns. Attention among analysts has been mostly focused on how to defend against such attacks, portraying IO efforts as essentially malevolent (Dowse and Bachmann, 2022; Jones, Simon, 2018). A typical approach has been to place these campaigns under the rubric of political warfare by opponents, and to offer ways to fight them using defensive means (Bagge, 2019; Polyakova and Boyer, 2018).

Defense against IO campaigns is certainly critical, and efforts to improve counter-IO must continue. There are two issues associated with a focus on counter-IO, however. The first, to be discussed in more detail below, is that these efforts may in fact prove counterproductive. The second, broader, issue may be even more critical. This is that focusing solely on counter-IO – usually described as fighting disinformation – cedes the initiative to the opposing countries. Trying simply to counteract the efforts of others can prove to be an exercise in futility. Understanding some of the critical processes in developing IO campaigns is crucial, both to disrupt the opponents' efforts and to conduct our own IO efforts.

After briefly discussing current IO processes at the purely military level, this paper focuses on IO at the higher strategic level. Although most of these efforts are not conducted by military elements, they are critical in the broader strategic context. It may also be noted that many of the examples of IO campaigns date back to the Cold War. This is very deliberate, because there has in fact been a continuity of approaches and types of campaigns for many years. In the case of Russia in particular, much of its conceptualization continues to reflect that of the Soviet Union. The tools for dissemination have, of course, both changed and improved, making IO campaigns easier, but the tools should not be confused with the underlying thinking. The focus in this paper is on Soviet-bloc and, subsequently, Russian IO operations, both because these are viewed as the more significant threats and because there is considerable open-source information available on these efforts. Most of the threats and responses can certainly be applied more broadly, but the primary emphasis in this study is on Russia. The methodology employed is the use of available open-source historical information and current reporting and analysis.

1 INFORMATION OPERATIONS AT THE MILITARY LEVEL

The militaries of various countries have generally developed IO doctrine as part of their operational planning (*JWP 3-80*, 2002; *JP 3-13*, 2014; *MC 0422/6 NATO Military Policy for Information Operations*, 2018). Although the specifics vary, most Western militaries view IO as including "military information support operations (MISO), military deception, operations security, public affairs, electronic warfare (EW), civil affairs operations (CAO), and cyberspace" (ATP 3-13.1, 2018). One important distinction between military IO and broader efforts is that, doctrinally, military IO focuses on degrading the decision-making of opposing leaders – whether through electronic or physical disruption or through 'getting inside their heads'

– while broader strategic IO has tended to focus on the populace of opponents (*Field Manual FM 3-13*, 2003; Blackmore, 2003, p 14).

Although military IO has the most developed doctrines and operational concepts, there are issues even at this level. The first is the broadness of the missions subsumed under the title of IO. Actually trying to synchronize and operationalize these disparate skill sets into a coherent mission plan, much less a broader strategy, presents significant difficulties. Likewise, even the term "IO" remains somewhat amorphous: "As a consequence, there is little in the way of standardization across staff sections, offices, organizations, and even individuals. Many of the concepts and terms associated with IO and OIE [Operations in the Information Environment] are viewed as esoteric and are not well understood across the joint force" (Schwille et al., 2020, p 2). Beyond this, there is significant flux in basic military doctrines concerning IO, to the extent that some even have proposed that the term IO be replaced with 'operations in the information environment' (Schwille et al., 2020, p 4). Although continued doctrinal development is, of course, to be encouraged as more sophisticated analysis is conducted, trying to carry out strategic planning when doctrine is ever-changing can be very difficult.

2 THE CRITICALITY OF ANALYSIS

Whether at the operational or strategic level, for the best results a thorough intelligence analysis of the target must be conducted. This consists of three essential components: vulnerability, susceptibility, and accessibility. The vulnerability analysis focuses on who are the most likely to respond to IO efforts; susceptibility focuses on how likely they are to respond to our campaigns; and accessibility tries to maximize efforts to get the message to the intended targets. A similar argument, using a marketing approach, is provided by Jackson (2016). Likewise, Blackmore (2003) suggests using public relations procedures.

Behavioral analysis provides a good system for providing intelligence support to information operations. It should try to answer the following questions:

– What has the actor (individual or group/organization) done in the past?
– What are useful indicators in past behaviors?
– What estimative value does past behavior have?

Assessing social and political trends among segments of the populace in other countries is also critical. This is particularly important if there are existing cleavages that can be taken advantage of. In some cases, these may be evolutionary, consistent over time, or have changed significantly based on particular events. Pattern analysis using observable behaviors can be particularly useful for seeing whether common actions result in similar social or political outcomes. The underlying logic is to identify both psychological and sociological vulnerabilities which could prove susceptible to IO campaigns. As will be noted below, some of the most effective IO

campaigns in the past – and likely ongoing – have not relied on "false" information, but rather have leveraged facts in a selective fashion to try to achieve a country's goals.

The key ingredient in this is knowledge of the analysts. Lt. Gen. Dennis Crall, Director of Command, Control, Communications and Computers/Cyber and Chief Information Officer, Joint Staff, J6 emphasized this point: "Do you understand that environment? Do you speak the native language? Do you speak the number of dialects in that area? Do you understand anthropology, religion, history when it comes to context? Many of our messages that sound righteous to us fail miserably when introduced to very specific populations during different times," (Magnuson, n.d.). During the same address, he argued that the US is not in a good position with regard to these requirements at the moment; Crall said that there has been a sharp decline in information operations skills in the military. Those who honed their craft at the end of the Cold War have retired: "I've said goodbye to them years ago. They've gone on to their second careers, and many of them now are gone. We don't build information experts who have deployed and have experience in areas like we did even a decade ago" (Magnuson, n.d.).

It may also be noted that there are reportedly significant issues with the actual authorities given to both analysts and operators for 'offensive' IO measures (Jajko, 2002). To a large extent, this is a result of conflating traditional information operations campaigns with cyber warfare. Most attention in the last number of years has focused on the latter rather than the former (Schmitt and O'Donnell, 1999; Jensen, 2017; Corn, 2021). There still seem to be significant legal and regulatory gaps in the authorities granted on which populations are allowed to be targeted and the types of IO campaigns that are permitted.

3 STRATEGIC INFORMATION OPERATIONS

The discussion thus far has centered on the purely military side of IO. Arguably, IO can have (and has had) more significance at the higher strategic level. At this level – above normal military planning – the overall population of a country is targeted, rather than focusing on elements of the military. The ultimate function of IO seems primarily to create friction between the populace and the government or between segments of the populace. Over time, such efforts can have a corrosive effect on public trust and confidence in its government. Using an analogy from another era of physical sabotage, it is akin to putting sand in the gearbox of a locomotive, rather than blowing it up. Although slower, the results can be similar. Ideally, of course, such a long-term effort will be combined with more focused IO efforts for specific goals. If conducted with effective strategic planning, the larger strategic efforts will complement the more operational approaches: "information activities are strategically aligned with military activity occurring covertly at any point on the spectrum of conflict" (Hammond-Errey, 2019, p 3).

3.1 Most strategic IO has targeted populations

As noted, truly strategic IO has tended to target the populations of opposing countries. In many ways, existing points of friction have been weaponized, rather than inventing fresh 'realities'. Finding these areas of existing contention has been relatively easy, particularly in democratic societies. In fact, some have argued that democratic societies are particularly vulnerable to these efforts (Paterson and Hanley, 2020, p 440). Although the various press and speech freedoms in democratic states make broad IO campaigns easier, the multiple information transmission means now available make true control of all information flows difficult even for highly authoritarian countries.

In the case of the Soviet Union, and seemingly still in the case of Russia, efforts to identify specific segments of the population for targeting seem to be somewhat minimal. IO efforts appeared to focus more on particular themes rather than on sub-groups. As one example, the KGB's campaign to inflame US race relations was described by a senior KGB officer stationed in the United States, Oleg Kalugin, who worked undercover as a Radio Moscow correspondent in New York and Washington in the 1960s and early 1970s: "Our active measures campaign did not discriminate on the basis of race, creed, or color: we went after everybody" (Walton, 2022).

A consequence of the Soviet/Russian approach is that "It is thus not the quality of information that is important in Russian information warfare, but the quantity" (Thornton, 2015, p 46). One reflection of this system has been the Russian Internet Research Agency, which became notorious during the 2016 US presidential election. Studies of its operations indicate a group that valued output with much less concern than effectiveness (Dawson and Innes, 2019; Rid, 2020). At times, in fact, its workers – most of whom were given quotas for producing traffic – transmitted competing positions on IO themes. Although it is possible that these competing positions were intentionally designed to sow friction in the target populations, it is hard to escape the suspicion that in many ways they simply reflected poor internal controls. However well the Russians (and perhaps the Chinese) have succeeded with such 'bulk' campaigns, the resources required for this approach are unlikely to be available to many Western countries.

3.2 'Truth' versus falsehood

Most IO campaigns should be and have been based on at least kernels of truth. Even actual disinformation will be more readily accepted by willing audiences if there are pre-existing cleavages that can be taken advantage of. This has likely gotten easier in today's environment where 'authoritative' news sources – such as the *BBC, London Times, New York Times*, etc. – are less followed by significant numbers of people, who instead are getting their 'news' from various internet sources of dubious reliability. If a disinformation theme tracks with their perceived realities, it will probably be believed.

Despite having themes that are based on these perceptions of reality, there clearly has been some successful use of forgeries. In some cases, the forgeries simply have not been expected to have much credibility. Bittman noted that a Sudeten German leader was targeted by forged letters purportedly written by him asking for financial support from various foreign figures, which he then had to explain (Bittman, 1972, p 13). There seemed to be little expectation that these letters would have a long shelf life before being exposed as forgeries, but simply having to deal with exposing them created a significant distraction. One other issue with forgeries should be noted. Earlier IO campaigns in developing countries suggest that in these types of environments, even egregiously bad forgeries and what typically would be seen as false narratives could have significant implications. A good example of this approach was the Soviet campaign in many African countries in the 1980s blaming the US for the deliberate introduction of the AIDS virus (US Department of State, 1987). Even poor forgeries – and they seemed to be rather common – had potential usefulness: "Most forgeries were released to the public, with the intended victim promptly denying the authenticity, but the KGB calculated that the denial would not entirely offset the public damage" (McCauley, 2016, p 171).

Third party sources can be critical in getting narratives accepted. Ideally, these sources will have significant credibility. In the past, this would have included respected journalists, newspapers, and other media sources. Currently, it might be more important to focus on social media influencers or popular websites. The actual credibility of the initial source reporting might not always be significant as long as the stories are picked up by foreign press that can spread (and preferably amplify) them. McCauley provides a good example of this from the Cold War, using the example of how the Burmese press was used to plant stories which then grew (McCauley, 2016, pp 155-156).

In many cases, existing groups – whether mainstream or radical – can be the best conduits for getting the message disseminated. Bittman noted that in a disinformation campaign in Germany in an effort to discredit the German government as being influenced by Naziism, a false flag operation in the 1960s using Neo-Nazi propaganda had some actual Nazis distributing the material thinking it was authentic (Bittman, 1972, p 3). At the same time, using such radical groups which, in fact, may not support the political goals (not to mention the ideology) of the government using IO can be problematic. In the same campaign to emphasize the "Nazi" leanings of the German government, the KGB instructed the Stasi officers supervising the campaign: "Our comrades must, however, continue to work amongst Nazis with the greatest skill to prevent them from unwittingly helping to strengthen Nazi movements". It ended by warning that "effective countermeasures would have to be taken at the slightest indication that matters were beginning to get out of hand" (Rid, 2020, p 129).

This also can be a problem with the covert IO support of groups that are in general ideological supporters of the goals of the IO-sponsoring country. Perhaps the largest open-source example of this was the Soviet support for various peace movements

in Europe during the Cold War: "The difficulty was balancing Kremlin control of the [front] groups while appearing independent in order to attract non-Communist support" (McCauley, 2016, p 88). This certainly applies to campaigns against countries such as Russia; too close a public identification of movements within these countries can easily lead to them being branded as 'foreign agents' and significantly reduce their potential impact.

3.3 What is viewed as public diplomacy by one country can be viewed as disinformation by opponents

A corollary to the previous paragraph is that public support for foreign opposition groups which is too overt can boomerang on the country providing it. This may be particularly critical in ongoing IO campaigns directed by Russia and the US against each other. One aspect of IO and disinformation which is commonly not given sufficient attention by observers is the extent to which other countries view the US and other Western countries as a major user of these techniques. Typically, the US government stresses terms such as public diplomacy and support for democratic trends, but these efforts can begin to look a lot like disinformation to those opponents against whom they are directed. In fact the US has, of course, conducted significant disinformation and clandestine operations in the past, such as the early Cold War operations in East Germany, the early post-World War II Italian elections, and clandestine support for the Solidarity movement in Poland.

This last operation – known as QRHELPFUL – was particularly wide-ranging and reportedly received support (however unwittingly) from US labor unions, the Catholic Church, and some humanitarian organizations. Throughout the operation, despite both suspicions and accusations of the CIA 'running' the Solidarity movement, QRHELPFUL achieved one significant goal: "the CIA wanted to smuggle materials in such a way that Solidarity members never definitively knew the CIA was providing aid. Solidarity's legitimacy would have been severely undermined if there was unequivocal evidence of CIA assistance" (Jones, 2018, p 6).

Such history continues to be germane to the IO conflict between the US and Russia. The so-called Gerasimov Doctrine in fact focuses on defense against US IO operations (Gerasimov, 2016). As a further example of the Russian military's almost-fixation on the possibility of US disinformation:

The main objective of information war is to capture the consciousness of the population of the Russian Federation, to undermine the moral-fighting potential of the armed forces; i.e., to set the stage for political, economic, and military penetration. With this goal in mind, both secret information and psychological operations (actions) are being prepared and continuously conducted, not just by designated state structures of traditional enemies of Russia, but also by its allies and friendly countries (Korotchenko, 1996).

The same source provides several other examples of this argument. This is not to argue for moral equivalency or to suggest that current US IO efforts are in fact as significant as the Russian sources claim (given the issues with the lack of qualified personnel noted earlier); it does however indicate that, for at least the Russian military and almost certainly for the larger Russian security apparatus, the view is that IO is a tit-for-tat conflict. Thomas (1998) provides a detailed examination of the Russian structure for counter-IO operations. As such, expecting a reduction in IO efforts is futile.

3.4 Official reactions to IO campaigns to try to counter them may increase their effectiveness

Counter-IO efforts are virtually inevitable and in fact are necessary. The issue, however, is how well these are planned and implemented. One such effort during the Cold War – the Active Measures Working Group – has typically been used as an example of how counter-IO can be achieved. Among other efforts, the organization provided regular public reports on Soviet propaganda efforts (US Department of State, 1987). In a detailed study, Schoen and Lamb (2012) provided a very positive judgement of the operations of the Active Measures Working Group.

More recently, in 2016, the US State Department established the Global Engagement Center with the mission to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations" (Global Engagement Center, 2024). Others have argued that the counter-IO effort should in fact be even more formalized and strengthened, with the establishment of a full-time multi-agency center akin to the National Center for Counterterrorism (Walton, 2022).

Unfortunately, efforts to counter disinformation can often simply reinforce the IO campaign by giving it increased airtime: "Therefore, debunking false information and refuting provided data as incoherent and leading to false assumptions is ineffective in countering disinformation campaigns. Also, the more the data seems credible despite being disinformation, and the more it is tailored to seduce the opponent's cognitive biases, the more effective it is" (Bagge, 2019, p 37). Perhaps the most prominent example of this issue was the plethora of official US government reports on Russian interference in the 2016 elections and the potential for further interference (Mueller, 2019; National Intelligence Council, 2021). The conclusions of these reports could easily lead to considerable cognitive dissonance among members of the public; at the same time as government officials were stressing the reliability of the election process, they were warning of the extent of Russian interference. It would have been very easy for at least segments of the population to conclude that the government either was not being honest with them about the safety of the electoral process, or that the threat was overstated. Either way, the result could be decreased public trust in the government. Again, the immediate results might not be dramatic, but the corrosive

effect could be important over time: "This is because the perception of interference can be just as damaging as actual interference, and thus beneficial to Russia's central aim of creating chaos to erode trust in democracy, and degrade western societal and political legitimacy" (Paterson and Hanley, 2020, p 443).

3.5 Actually measuring the effectiveness of strategic IO campaigns has been virtually impossible

Many approaches for assessing how well IO efforts have worked have been suggested, but no useful metrics have resulted. One review of the available literature concluded that the impact of persuasive campaigns has been limited (Wallenius, 2022). Likewise, another study concluded that "Contrary to past and present claims about foreign malign "hidden hands" in U.S. domestic affairs, in fact the Soviet Union's disinformation strategy, and its impact, were limited: it targeted and amplified existing divisions within American society, doing nothing more than magnifying them" (Walton, 2022).

Even at the operational level, the actual impact of IO, at this level probably better viewed as propaganda, has been difficult to quantify. At their simplest (and perhaps simplistic), tactical efforts have been measured by the number of enemy troops surrendering who present surrender chits[1] or the like. Clearly, there is no simple one-to-one relationship between a tactical IO campaign and troops wanting to give up the fight. In many instances, even in such 'simple' environments, the efficacy of a particular campaign remains unknown until after it is over. Also, of course, what might work well at a particular point in time or in a particular environment may be ineffective or even counterproductive in a different time or environment. Some measurement tools may be useful at lower levels in relatively benign environments, such as peacekeeping missions; one approach that has been suggested is the use of corporate public relations measurement techniques (Blackmore, 2003).

Conclusion

In the United States, some proposals have been put forth that because the Defense Department already has some authorities for IO, it should be the proponent for all national IO policies and operations (Hatch, 2019, pp 73-85). How well other government agencies would view this approach – particularly for the 'darker shades' of IO – is questionable. More broadly, most Western countries would likely view such organizational structures as not being conducive to appropriate civil-military relations. Nevertheless, military strategists must take into account the broader strands of strategic IO in their strategic planning.

Most Western countries have focused on defensive measures against IO campaigns conducted against them. As noted, this may be counterproductive in many cases, and more broadly, may in fact be a poor strategic decision. Ceding the initiative to an opponent is unlikely to ever succeed in the strategic longer term. Certainly,

[1] *Highly visible sheets of paper distributed among enemy troops which promise safe conduct and good treatment for those who surrender*

efforts to counter disinformation will remain necessary, but a case-by-case approach will never provide a coherent counter campaign. Understanding previous patterns and strategic approaches are required both for defensive and possible offensive information operations campaigns.

References

1. *Babbage, R., 2019. Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail. 2 vols. Washington DC: Center for Strategic and Budgetary Assessments.*
2. *Bittman, L., 1972. The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare. [1st ed. Syracuse, N.Y.]: Syracuse University Research Corp.*
3. *Blackmore, T. R., 2003. Assess the Importance of Measures of Effectiveness (MOE) for the Further Development of UK Information Operations. Defence Studies 3(3), September 2003, pp 9–37. https://doi.org/10.1080/14702430308405075 (Accessed 17 January 2024).*
4. *Dawson, A., and Innes, M., 2019. How Russia's Internet Research Agency Built Its Disinformation Campaign. The Political Quarterly 90(2), June 2019, pp 245–256. https://doi.org/10.1111/1467-923X.12690. (Accessed 17 January 2024).*
5. *Dowse, A., and Dov Bachmann, S., 2022. Information Warfare: Methods to Counter Disinformation. Defense & Security Analysis 38(4), October 2, 2022, pp 453–469. https://doi.org/10.1080/14751798.2022.2117285. (Accessed 17 January 2024).*
6. *Gerasimov, V., 2016. The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Translated and Reprinted in Military Review, February 2016, pp 23–29.*
7. *Global Engagement Center, 2024. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (Accessed 17 January 2024).*
8. *Hammond-Errey, M. 2019. Understanding and Assessing Information Influence and Foreign Interference. Journal of Information Warfare 18(1), Winter 2019, pp 1–22.*
9. *Hatch, B., 2019. The Future of Strategic Information and Cyber-Enabled Information Operations. Journal of Strategic Security 12(4), January 2019, pp 69–89. https://doi.org/10.5038/1944-0472.12.4.1735 (Accessed 17 January 2024).*
10. *Headquarters, Department of the Army, 2003. Field Manual FM 3-13.*
11. *Headquarters, Department of the Army, 2018. ATP 3-13.1. The Conduct of Information Operations.*
12. *Jackson, C. F., 2016. Information Is Not a Weapons System. Journal of Strategic Studies 39(5-6), September 18, 2016, pp 820–46. https://doi.org/10.1080/01402390.2016.1139496 (Accessed 17 January 2024).*
13. *Jajko, W. A., 2002. Critical Commentary on the Department of Defense Authorities for Information Operations. Comparative Strategy 21(2), April 2002, pp 107–14. https://doi.org/10.1080/01495930290043074 (Accessed 17 January 2024).*
14. *Jones, S. G., 2018. Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare. Washington DC: CSIS Brief.*
15. *Jones, S., 2018. Combating Information Operations: Developing an Operating Concept. Cambridge, MA: Harvard Belfer Center.*
16. *Klein, H., 2018. INFORMATION WARFARE AND INFORMATION OPERATIONS: RUSSIAN AND U.S. PERSPECTIVES. Journal of International Affairs 71(1.5), pp 135–142.*
17. *Korotchenko, E. G., 1996. Informatsionno- Psikhologicheskoye Protivoborstvo v Sovremennykh Usloviyakhn [Information - Psychological Confrontation under Modern Conditions]." Voennoye Mysl [Military Thought], February 1996, pp 19–26.*

18. *Magnuson, S., 2022. US Still Playing Catch Up in Information Operations. National Defense Magazine, February 11, 2022. https://www.nationaldefensemagazine.org/articles/2022/2/11/still-playing-catch-up-in-information-operations (Accessed 17 January 2024).*
19. *Ministry of Defence, 2002. Joint Warfare Publication 3-80 Information Operations. Swindon, UK: The Joint Doctrine & Concepts Centre, Ministry of Defence.*
20. *Mueller, R., 2019. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Washington DC: Department of Justice, March 2019.*
21. *National Intelligence Council, 2021. Foreign Threats to the 2020 US Federal Elections. Washington DC, March 10, 2021.*
22. *NATO, 2018. MC 0422/6 NATO Military Policy for Information Operations. Brussels.*
23. *Polyakova, A., and Boyer, S. P., 2018. The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition. Washington DC: The Brookings Institution.*
24. *Rid, T., 2020. Active Measures: The Secret History of Disinformation and Political Warfare. First edition. New York: Farrar, Straus and Giroux.*
25. *Schoen, F., and Lamb, C. J., 2012. Strategic Perspectives 11: Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. Washington DC: National Defense University.*
26. *Schwille, M., Atler, A., Welch, J., Paul, C., and Baffa, R. C., 2020. Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities between Intelligence and Information Professionals. Santa Monica, CA: RAND.*
27. *Sieting, L. A., 2003. Intelligence Support to Information Operations: Today and in the Objective Force. Military Intelligence, September 2003, pp 56–60.*
28. *Thomas, T. I., 1998. Russia's Information Warfare Structure: Understanding the Roles of the Security Council, Fapsi, the State Technical Commission and the Military. European Security 7(1), March 1998, pp 156–172. https://doi.org/10.1080/09662839808407354 (Accessed 17 January 2024).*
29. *Thomas, T. L., 1997. Russian Information-Psychological Actions: Implications for U.S. PSYOP. Special Warfare 10(1), Winter 1997, pp 12–19.*
30. *Thornton, R., 2015., The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. The RUSI Journal 160(4), July 4, 2015, pp 40–48. https://doi.org/10.1080/03071847.2015.1079047 (Accessed 17 January 2024).*
31. *United States Department of Defense, 2014. Joint Publication 3-13 Information Operations. Washington DC: Department of Defense.*
32. *United States Department of State, 1987. "Soviet Influence Activities: A Report of Active Measures and Propaganda, 1986-1987," August 1987.*
33. *United States Department of State, 1987. Soviet Influence Activities: A Report of Active Measures and Propaganda, 1986-1987. Washington DC: United States Department of State.*
34. *United States Department of State, 2024. "Global Engagement Center 'Mission & Vision,'" January 17, 2024. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (Accessed 17 January 2024).*
35. *Wallenius, C., 2022. Do Hostile Information Operations Really Have the Intended Effects? A Literature Review. Journal of Information Warfare 21(2), Spring 2022, pp 21–35.*
36. *Walton, C., 2022. Old Is New Again: Cold War Lessons for Countering Disinformation. Texas National Security Review, Fall 2022. N. d.*

email: lawcline@gmail.com

ORCID: 0000-0002-6174-325X

sciendo

Sodobni vojaški izzivi, 2024 – 26/št. 2
Contemporary Military Challenges, 2024 – 26/No. 2

Urban Praprotnik

DOI: 10.2478/cmc-2024-0011

NAČELO RAZLIKOVANJA V KIBERNETSKEM VOJSKOVANJU

PRINCIPLE OF DISTINCTION IN CYBER WARFARE

Povzetek Kot eno temeljnih načel mednarodnega humanitarnega prava za zaščito civilnega prebivalstva, načelo razlikovanja določa, da morajo vpleteni v sovražnosti vselej razlikovati med civilnimi objekti in vojaškimi cilji, ter civilisti in borci. Članek z analizo uporabe tega načela naslovi vprašanje o zadostnosti zaščite, ki jo načelo ponuja v kibernetski domeni. Velika odvisnost vojska od civilne kibernetske infrastrukture namreč razširi nabor vojaških ciljev na sisteme, na katere se zanašajo ključne civilne dejavnosti. Nejasnosti se pojavljajo tudi pri zadostitvi na videz enostavnim pogojem za status borca ter udeležbi civilistov pri izvajanju kibernetskih operacij.

Ključne besede ***Načelo razlikovanja, kibernetsko vojskovanje, mednarodno humanitarno pravo, izbira vojaških ciljev.***

Abstract Principle of distinction, one of the fundamental principles of international humanitarian law dictates, that participants in hostilities at all times distinguish between civilian objects and military objectives, as well as between civilians and combatants. This article addresses the adequacy of the protection offered by the principle in the cyber domain. Great reliance of militaries on civilian cyberinfrastructure expands the range of military objectives to the systems which key civilian activities depend on. There are many unknowns in fulfilling even the simple conditions for the combatant status, as well as in regulation of civilian direct participation in hostilities.

Key words ***Principle of distinction, cyber warfare, international humanitarian law, targeting.***

Uvod

Informacijsko-komunikacijska tehnologija nudi številne priložnosti za razvoj civilne družbe, zaradi česar se ta nanjo čedalje bolj zanaša. Vseprisotnejša digitalizacija širi napadalno površino za kibernetske operacije, kar pomeni povečano ranljivost (ICRC, 2020, str. 33). Nekatere kibernetske operacije so že povzročile veliko ekonomsko škodo (Nash idr., 2018), dosedanji napadi na kritično infrastrukturo pa razkrivajo ranljivost ključnih civilnih storitev na kibernetske napade (ICRC, 2020, str. 47–50). Zaradi potencialno uničujočih kibernetskih operacij za visokotehnološkega nasprotnika, sta varnost lastnega in dominiranje nad nasprotnikovim kibernetskim prostorom za sodobne oborožene sile ključnega pomena. Razumeti gre torej stališče Odprte delovne skupine za razvoj na področju informacij in telekomunikacij v kontekstu mednarodne varnosti (OEWG), da se bo uporaba kibernetskih operacij nadaljevala tudi v prihodnosti (Generalna skupščina Združenih narodov, 2021, odst. 16).

Bistvena značilnost kibernetskega prostora je medsebojna povezanost (*interconnectivity*) naprav, ki ga tvorijo. Večina vojaških omrežij se zanaša na civilno kibernetsko infrastrukturo, kot so podmorski kabli in sateliti. In obratno, civilna tehnologija se zanaša na vojaško. Nadzor ladijskega in zračnega prometa je tako denimo odvisen od vojaških satelitov. Medsebojna povezanost zato predstavlja nevarnost, da kibernetski napadi prizadenejo ključno civilno infrastrukturo (Droege, 2012, str. 538–539). Prepletenost vojaške in civilne sfere je tipična tudi za udeležence v kibernetskem vojskovanju,[1] za katerega je v primerjavi z drugimi domenami značilna večja vključenost nedržavnih in zasebnih akterjev.

V luči pomena kibernetskih operacij v sodobnem vojskovanju (Microsoft, 2022, str. 35), ter posledic, ki jih lahko povzročijo civilnemu prebivalstvu, je treba biti pozoren na njihovo pravno ureditev. Vsaka civilizacija je namreč poznala nekatere najbolj temeljne omejitve za zaščito civilnega prebivalstva v vojni, ki so veljale, še preden je mednarodno pravo dobilo celovito podobo. V sodobnem mednarodnem humanitarnem pravu (MHP) je za zaščito civilistov primarno pomembno načelo razlikovanja, ki je zasnovano na temelju mednarodnih pogodb, običajnega prava in splošnih pravnih načel (Sancin idr., 2009, str. 49, 57), predstavlja pa tudi običajno mednarodno pravo v obeh vrstah oboroženega spopada (ICJ, 1996, odst. 78).[2] Najnatančneje je opredeljeno v Prvem dopolnilnem protokolu k Ženevskim konvencijam (DP-I), določa pa, da morajo vpleteni v oboroženi spopad vselej razlikovati med civilnimi objekti in vojaškimi cilji, ter civilisti in borci. Temu ustrezno morajo usmerjati svoje

---

[1] *Univerzalno sprejete definicije kibernetskega vojskovanja ni, Mednarodni odbor Rdečega križa (MORK) pa ga definira kot izvajanje kibernetskih operacij, ki kot sredstva ali metode vojskovanja dosežejo prag oboroženega spopada, ali se odvijajo v njegovem okviru (ICRC, 2013, str. 1). ZDA definirajo kibernetske operacije kot uporabo kibernetskih zmogljivosti, katerih glavni namen je doseganje ciljev bodisi v kibernetskem prostoru, ali z uporabo kibernetskega prostora (DoD, 2021, str. 55). Rusi in Kitajci z izjemo prevodov iz tujih besedil pojma kibernetsko vojskovanje ne uporabljajo, govorijo pa o informacijskem vojskovanju, ki je širši pojem od definicije MORK in ZDA (Connell in Vogler, 2016, str. 3). Podobno definicijo uporablja tudi Šanghajska organizacija za sodelovanje (Shanghai Cooperation Organisation, 2009, str. 9).*

[2] *Oborožen spopad obstaja, ko pride do uporabe oborožene sile med državami oz. v primeru dolgotrajnega oboroženega nasilja med vladnimi oblastmi in organiziranimi oboroženimi skupinami ali med takšnimi skupinami znotraj države (ICTY, 1995, odst. 70).*

akcije zgolj zoper objekte, ki so vojaški cilji, ter borce in tiste civiliste, ki neposredno sodelujejo v sovražnostih. Namen članka je preučiti, ali načelo razlikovanja nudi zadostno zaščito tudi v kibernetski domeni. To stori z analizo uporabe načela razlikovanja pri objektih in osebah in izpostavitvijo najbolj perečih problemov, ter sprotno obravnavo predlogov stroke za njihovo rešitev.

1 RAZLIKOVANJE MED CIVILNIMI OBJEKTI IN VOJAŠKIMI CILJI V KIBERNETSKEM PROSTORU

1.1 Prispevek k vojaškemu delovanju

Vojaški cilji so skladno z 52. členom DP-I definirani kot objekti,[3] ki zaradi svoje narave, lokacije, namena ali uporabe pomembno prispevajo k vojaškemu delovanju in katerih popolno ali delno uničenje, zavzetje ali nevtralizacija daje v danih okoliščinah jasno vojaško prednost. Civilni objekti so vsi objekti, ki ne zadostijo definiciji vojaških ciljev.[4] Identificiranje vojaških ciljev po kriterijih narave in lokacije se v kibernetskem vojskovanju v bistvenem ne razlikuje od kinetičnega, razlike pa se pojavijo pri kriterijih uporabe in namena.

Večino kibernetskega prostora sestavljajo objekti, ki so v osnovi civilni, npr. podmorski kabli. Velika odvisnost vojska od civilne kibernetske infrastrukture je znatno razširila nabor objektov, ki so lahko napadeni, vključujoč sisteme, na katere se zanašajo ključne civilne dejavnosti. Legitimni vojaški cilji denimo postane civilni satelitski sistem za navigacijo ali pridobivanje slike v realnem času, če ga nasprotnik uporablja za pridobivanje posnetkov ali informacij o lokaciji vojaških objektov. Legitimne tarče predstavljajo tudi objekti, ki zaradi svoje prihodnje uporabe izpolnijo kriterij namena. Če stran v spopadu razpolaga z zanesljivimi informacijami, da bo nasprotnik pridobil računalniško opremo, ki bo prispevala k njegovemu vojaškemu delovanju, se taka oprema šteje za legitimni vojaški cilj (Schmitt, 2017, str. 440, 447).

Način izbiranja tarč je v kibernetski domeni specifičen, saj se pri izbiri tarč bolj kot na same podatke, ki potujejo po kibernetskem prostoru, osredotoča na njihovo pot - zlonamerno kodo je namreč zaradi minimalnih razlik v primerjavi z običajno kodo, ter visoke hitrosti prenosa, med njeno potjo praktično nemogoče najti. Zato se v kibernetskem vojskovanju napada fizična kibernetska infrastruktura.[5] Ker je že na začetku oboroženega spopada jasno, da se bo za izvajanje kibernetskih operacij uporabljala civilna kibernetska infrastruktura, praktično nemogoče pa je predvideti, katero milisekundo bo pri izvajanju neke vojaške operacije uporabljen

[3] *Objekt je nekaj vidnega in oprijemljivega, v čemer se razlikuje od pojmovanja v računalniški znanosti, kjer je termin definiran širše (Schmitt, 2017, str. 437).*

[4] *Definicija se pojavlja v več virih, ki veljajo v obeh tipih oboroženih spopadov, npr. v tretjem in četrtem odst. 1. člena Protokola o prepovedih ali omejitvah uporabe zažigalnih orožij.*

[5] *Geiss in Lahmann navedeno ponazorita s primerjavo vojskovanja v zračnem in kibernetskem prostoru. Pri prvem se ne cilja zraka, temveč zrakoplove, pri drugem pa je tarča medij, po katerem potuje zlonamerna koda (Geiss in Lahmann, 2012, str. 389).*

njen določen segment (Geiss in Lahmann, 2012, str. 386), tako vojaški cilji denimo postanejo vsi komunikacijski kanali, usmerjevalniki in strežniki, preko katerih bodo potovali, ali se na njih nahajali vojaški podatki (Schmitt, 2015, str. 19). Zlasti zaradi izpolnitve kriterijev uporabe in namena, bi tako vojaški cilj postala popolnoma vsa kibernetska infrastruktura (Pascucci, 2017, str. 438). Idealna rešitev te praktično nevzdržne situacije bi bila dosledna fizična delitev kibernetske infrastrukture na vojaško in civilno, za kar si trenutno prizadeva Mednarodni odbor Rdečega križa (MORK) (ICRC, 2023, OP 10). V hladni vojni je bila denimo ločitev na MILNET in ARPANET, ki sta se kasneje razvila v omrežje za vojaške komunikacije in internet (Šarf, 2017, str. 84), še izvedljiva, danes pa zaradi vseprisotne soodvisnosti vojaške in civilne kibernetske infrastrukture, ni uresničljiva. Bolj realistična bi bila zgolj ločitev objektov, ki so v MHP posebej zaščiteni, oziroma morebitna širitev njihovega nabora na druge objekte kritične infrastrukture.

1.2 Jasna vojaška prednost

Na videz odprto definicijo vojaškega cilja utegne zamejiti njen drugi del, ki v drugem odstavku 52. člena DP-I poleg prispevka k vojaškemu delovanju zahteva, da njegovo popolno ali delno uničenje, zavzetje ali nevtralizacija v danih okoliščinah daje jasno vojaško prednost. Tok podatkov je namreč odporen na motnje - če so nekateri komunikacijski kanali uničeni, lahko podatki do svojega cilja samodejno najdejo pot po preostalih kanalih. Tako je možno zagovarjati stališče, da civilna kibernetska infrastruktura, kljub svojemu pomembnemu prispevku k vojaškemu delovanju, ne more postati vojaški cilj, saj njeno uničenje, zavzetje ali nevtralizacija, resneje ne ogrožajo nasprotnikove zmožnosti izvajanja operacij in zato ne dajejo jasne vojaške prednosti. Jasna vojaška prednost bi bila podana kvečjemu z uničenjem vseh, ali vsaj večjih komunikacijskih poti (Mavropoulou, 2015, str. 44).[6] V praksi je ta dilema razvidna iz analize bombardiranja stavbe Radiotelevizije Srbije (RTS), pri katerem se je Nato zavedal, da bo bombni napad prekinil oddajanje zgolj za nekaj ur, kar je v Končnem poročilu tožilcu s strani odbora, ustanovljenega za pregled bombardiranja Zvezne republike Jugoslavije (ZRJ), s strani Nato sprožilo vprašanje o jasni vojaški prednosti takšnega napada. Strateška tarča (omrežje poveljevanja nadzora in komunikacij ZRJ) je bila namreč kompleksna mreža, ki je ni bilo možno onesposobiti v enem napadu. Nato je doseganje jasne vojaške prednosti opravičeval s trditvijo, da je bil napad na RTS zgolj del večje operacije zoper več podobnih objektov (poleg stavbe RTS tudi električno omrežje, radijske in televizijske relejne postaje v Novem Pazarju, Novem Sadu in Kruševcu) (ICTY, 2000, odst. 78).

Kibernetska infrastruktura torej ne more postati vojaški cilj, razen v primeru, da se uniči njen večinski del. Iz povedanega denimo sledi, da bi se zaradi inherentne odpornosti interneta, pogosto uporabljenega v vojaške namene, katere posledica

[6] *Talinski priročnik omrežje dvojne rabe, pri katerem se ne ve, katere njegove dele bodo prečkale vojaške komunikacije, ponazori z analogijo s cestnim omrežjem, pri katerem se ne ve natančno, kateri obvoz bodo ubrala vojaška vozila v primeru cestne blokade - v tem primeru celotno cestno omrežje šteje za vojaški cilj, oz. vsaj tisti njegov del, po katerem je pot vojaških vozil visoko verjetna (Schmitt, 2017, str. 446).*

je možnost pridobitve jasne vojaške prednosti zgolj z oviranjem večjega dela komunikacijskih poti, lahko kot vojaški cilj kvalificiral tudi internet v celoti (Mavropoulou, 2015, str. 54).[7] Takšen sklep, ki ne dopušča vmesnih nians, se zdi neživljenjski.

2 RAZLIKOVANJE MED CIVILISTI IN BORCI V KIBERNETSKEM PROSTORU

Poleg vojsk in vladnih agencij, kibernetske operacije pogosto izvajajo tudi zasebne institucije in posamezniki.[8] Nekateri nedržavni akterji so že pokazali kibernetske zmogljivosti, do nedavnega dostopne le državam (Generalna skupščina Združenih narodov, 2021, odst. 16), njihova vloga pa se bo v prihodnosti verjetno še povečevala in še bolj zameglila ločnico med vojaškimi in civilnimi osebami (ICRC, 2020, str. 34). Štrucl opaža, da je tudi rusko-ukrajinska vojna pokazala, da dejanske kibernetske zmogljivosti držav poleg vojska in državnih organov ležijo tudi v zasebnem sektorju (Štrucl, 2022, str. 117). Skladno s 3. členom Zakona o obrambi vojaško obrambo v Republiki Sloveniji (RS) izvaja Slovenska vojska (SV), civilno obrambo pa državljani, samoupravne lokalne skupnosti, državni organi, gospodarske družbe, zavodi in druge organizacije. Kibernetsko obrambo skladno s 24. členom Zakona o informacijski varnosti (ZInfV) izvajajo Urad Vlade RS za informacijsko varnost, skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, Ministrstvo za obrambo in drugi nacionalni organi, torej je moč podobno trditi tudi za RS. Velja opomniti, da se borce, ter zgoraj omenjene civiliste, ki so neposredno udeleženi v sovražnostih, lahko napade tako kibernetsko, kot tudi kinetično.[9]

2.1 Borci

Splošno sprejeta definicija borca izhaja iz 1. člena Haaškega pravilnika, za potrebe upravičenosti do statusa vojnega ujetnika jo je prevzel tudi 4. člen Ženevske konvencije o ravnanju z vojnimi ujetniki (ŽK-III). Skladno z obema pravnima viroma, so borci pripadniki oboroženih sil ene od strani v spopadu, ter pripadniki drugih milic in drugih prostovoljnih enot, vključno s tistimi pripadniki organiziranih odporniških gibanj, ki pripadajo eni od strani v spopadu,[10] ob izpolnjevanju naslednjih pogojev: poveljuje jim poveljnik, ki je odgovoren za svoje podrejene, imajo na

---

[7] *Skupina strokovnjakov za Talinski priročnik se je tega problema sicer zavedala in takšno rešitev v teoriji dopustila, vendar je menila, da okoliščine, ki bi napravile celoten internet vojaški cilj, zaenkrat še ne obstajajo. Nasprotno, vsak napad na internet kot tak, bi moral biti omejen le na njegove manjše segmente (Schmitt, 2017, op. cit. 14, str. 446).*

[8] *Eden izmed udeležencev srečanja strokovnjakov MORK je postavil tezo, da države s ciljem izogibanja nekaterim obveznostim in zaradi nepoznavanja MHP s strani obveščevalnih agencij, izvajanje kibernetskih operacij morda namenoma premikajo izven delokroga oboroženih sil (ICRC, 2020, str. 14).*

[9] *To se je denimo zgodilo v NMOS med Izraelom in Hamasom, v katerem se je Izrael na kibernetski napad Hamasa odzval z zračnim napadom na stavbo izvora napada (Doffman, 2019).*

[10] *Patriotski hekerji, ki izvajajo kibernetske operacije iz osebnih simpatij do strani v spopadu, zaradi prešibke povezave s stranjo v spopadu statusa borca ne uživajo.*

daljavo viden razpoznavni znak, odkrito nosijo orožje in izvajajo svoje operacije v skladu z zakoni in običaji vojne. V RS tej definiciji denimo zadostijo pripadniki Enote za komunikacijske in informacijske sisteme SV, ki je namenjena zagotavljanju delovanja komunikacijskih in informacijskih sistemov ter podpori poveljevanja in kontrole na strateškem in operativnem nivoju SV.

Stroka glede pogojev za status borca sicer ni enotna. Stališče MORK je, da je običajnopravna definicija borca zapisana v DP-I, namen definicij iz Haaškega pravilnika in ŽK-III pa naj bi bil zgolj določiti pogoje za status vojnega ujetnika, ki pa ne sovpada nujno s statusom pripadnika oboroženih sil (Henckaerts in Doswald-Beck, 2005, str. 15). Borec skladno z DP-I zaradi narave sovražnosti, ki včasih ne omogoča razlikovanja od civilnega prebivalstva, obdrži svoj status, če odkrito nosi orožje med vsako vojaško akcijo in dokler ga nasprotnik lahko vidi med vojaško pripravo pred napadom, v katerem bo sodeloval. DP-I tako v svojem 44. členu črta zahtevan pogoj nošenja na daljavo vidnega razpoznavnega znaka za status borca. V kontekstu kibernetskega vojskovanja je tak pristop smotrnejši, saj se borci pri kibernetskem vojskovanju fizično niti ne soočijo (Döge, 2010, str. 495). Čeprav Talinski priročnik[11] priznava obstoj kibernetskih orožij,[12] je strokovna skupina ugotovila, da zahteva po odkritem nošenju orožja v kibernetski domeni ni realna (Schmitt, 2017, str. 406). Opozoriti velja, da zgolj neuporaba konvencionalnega orožja s strani kibernetskih borcev še ne spreminja pravne ureditve, ki je v tem primeru popolnoma jasna. Kibernetski napadalci se v bistvenem ne razlikujejo od ostalih pripadnikov oboroženih sil, katerih primarna naloga ni boj z nasprotnikom (inženirji, kuharji, pravniki, ipd.). Našteti so prav tako oboroženi z lahko osebno oborožitvijo, s čimer zadostijo zahtevi po odkritem nošenju orožja.

Status borca pripada tudi pripadnikom *levée en masse* (množični odpor), ki so definirani kot prebivalci neokupiranega območja, ki se z oboroženo silo spontano uprejo bližajočemu nasprotniku, ne da bi se imeli čas organizirati v redne oborožene sile. Skladno z 2. členom Haaškega pravilnika štejejo za borce če odkrito nosijo orožje, ter spoštujejo zakone in običaje vojne, niso pa podvrženi zahtevi po nošenju razlikovalnega znaka ali druge razlikovalne oprave. Kibernetski *levée en masse* bi tako lahko sestavljali t. i. »hacktivisti« oz. »patriotski hekerji,« saj niso pripadniki oboroženih sil in na lastno iniciativo izvajajo kibernetske napade zoper nasprotnika. Čeprav to počno brez avtorizacije ali nadzora njihovih držav, zasledujejo iste politične cilje (Turns, 2012, str. 293). Zgoraj omenjeni pogoj odkritega nošenja orožja je v primeru *levée en masse* posebnega pomena zaradi odsotnosti zahteve po uporabi razlikovalnega znaka (ICRC, 2021, odst. 1021–1023).

---

[11] *Talinski priročnik je trenutno najbolj celovit dokument, ki med drugim obravnava uporabo MHP v kibernetski domeni. Lahko ga štejemo za nauk uglednih strokovnjakov za mednarodno pravo, torej služi kot pomožno sredstvo pri ugotavljanju in razlagi pravnih pravil.*

[12] *Za potrebe Talinskega priročnika so kibernetska orožja sredstva bojevanja, ki so uporabljena, dizajnirana ali namenjena povzročitvi smrti ali poškodb ljudem, oziroma uničenja ali poškodb objektom (Schmitt, 2017, str. 452).*

Čeprav Talinski priročnik priznava, da pogoj nošenja orožja v kibernetski domeni nima realne uporabe, pa brez vidnega orožja ni jasnega načina ločitve teoretičnega kibernetskega *levée en masse* od civilnega prebivalstva (Wallace in Reeves, 2013, str. 659). Prenosni računalniki in mobilni telefoni se lahko sicer nosijo odkrito, vendar je vprašljivo, če zaradi njihove vseprisotnosti med civilnim prebivalstvom zadostijo potrebi po razlikovanju (Turns, 2012, str. 293). Argument glede nošenja orožja pri *levée en masse* je v kibernetski domeni sicer enak tistemu v zvezi s pripadniki oboroženih sil, predstavljenim zgoraj. V Talinskem priročniku obstaja tudi dilema glede globine ozemlja pod sovražnim nadzorom, v katero *levée en masse* še sme izvajati kibernetske operacije (Schmitt, 2017, str. 409).

Zgodovinsko gledano *levée en masse* namreč ni izvajal operacij globoko v sovražno ozemlje, temveč je bil njegov namen zaustaviti nasprotnika na frontni liniji. Zato so nekateri avtorji mnenja, da se kibernetske operacije ukrajinske »IT armade,« katerih tarče se nahajajo na različnih koncih Rusije, ne morejo šteti kot akcije *levée en masse* (Buchan in Tsagourias, 2022). Zgodovinsko *levée en masse* sicer niti ni bil sposoben izvajanja napadov v globino sovražnega ozemlja, danes pa kibernetska orodja omogočajo povzročanje škode v nasprotnikovemu zaledju, ki lahko pripomore tudi k njegovi zaustavitvi na frontni liniji. Zaradi opisanih nejasnosti pri globini ozemlja pod sovražnim nadzorom, v katero se še smejo izvajati kibernetske operacije, ter vsebini pojma odkrite nošnje orožja v kibernetski domeni, kot konstitutivnih pogojev *levée en masse*, je zaslediti predloge popolne ukinitve te kategorije borcev za kibernetsko vojskovanje. Namesto nje naj bi se od vseh kibernetskih borcev zahtevalo upoštevanje štirih kriterijev iz Haaškega pravilnika in ŽK-III (Wallace in Reeves, 2013, str. 664). Omenjeni predlog spregleda kriterija spontanosti in neorganiziranosti, ki sta bistvena elementa *levée en masse*, nekatere kibernetske borce pa prikrajša statusa borca, saj bi se v tem primeru kvalificirali kvečjemu kot civilisti, ki se neposredno udeležujejo sovražnosti.

2.2 Civilisti

Za civiliste se skladno s 50. členom DP-I štejejo vsi, ki niso pripadniki oboroženih sil ali *levée en masse.* Njihova uporaba je v kibernetskem kontekstu mamljiva zaradi oteževanja pripisljivosti, njihovega tehničnega znanja in razpolaganja s kibernetskimi orodji, ki niso predmet tipičnega vojaškega inventarja (Hathaway idr., 2011, str. 854). Zgoraj omenjen opis kibernetske obrambe po ZInfV, ki jo izvajajo številni nacionalni organi, nakazuje, da je tudi pri kibernetski obrambi v oboroženem spopadu, katerega stran bi bila RS, pričakovati poudarjeno vlogo civilistov. Civilisti skladno z 51. členom DP-I postanejo legitimne vojaške tarče, kadar so neposredno udeleženi v sovražnostih. Zaradi vseprisotne uporabe civilistov (van Benthem, 2023), so v kibernetski domeni pravila o neposredni udeležbi v sovražnostih nadvse pomembna. Mednarodno pogodbeno pravo definicije neposredne udeležbe ne ponuja, obstaja pa dovolj strinjanja glede osnovnih parametrov Interpretativnih smernic o pojmu neposredne udeležbe v sovražnostih v MHP (*Interpretive Guidance on the Notion of Direct participation in Hostilities under International Humanitarian Law* – Interpretativne smernice), da te lahko služijo kot temelj za razpravo o neposredni

udeležbi v sovražnostih. V tem smislu so Interpretativne smernice avtoritativne (Turns, 2012, str. 286).

Same sovražnosti so v Interpretativnih smernicah definirane kot kolektivna uporaba sredstev in metod vojskovanja strani v spopadu. Ne zahteva se nujno uporaba oborožene sile zoper nasprotnika, ali povzročitev smrti, poškodb ali uničenja (Melzner, 2009, str. 47), kar pomeni, da pojem sovražnosti pokriva velik spekter kibernetskih operacij. Eden izmed zadržkov glede Interpretativnih smernic, ki je zaradi zamegljene ločnice med civilisti in borci v kibernetski domeni še toliko bolj utemeljen, je, da definirajo neposredno udeležbo preširoko (Goodman in Jinks, 2010, str. 639). V nadaljevanju bo predstavljeno, da temu ni nujno tako.

V Interpretativnih smernicah so identificirani trije konstitutivni elementi neposredne udeležbe v sovražnostih - nastanek škode, neposredna vzročna zveza, ter povezava s sovražnostmi.

2.2.1 Nastanek škode

Da se ravnanje kvalificira kot neposredna udeležba v sovražnostih, mora biti take narave, da lahko specifično škoduje vojaškim operacijam ali vojaškim zmogljivostim nasprotne strani v oboroženem spopadu, ali alternativno, povzroči smrt, poškodbo, ali uničenje. Zgolj nevšečnosti, kot je manipulacija civilnega računalniškega ali električnega omrežja, čeprav lahko resno vplivajo na javno zdravje, varnost, ali trgovino, ne dosežejo nivoja zahtevane škode (Melzner, 2009, str. 50). Motnja računalniškega sistema za nadzor železniškega omrežja, bi lahko omrežje torej ohromila in onemogočila potovanja v ciljni državi, ne bi pa dosegla zahtevanega nivoja škode.[13] Če bi enaka motnja ohromila transport moštva, oborožitve ali opreme, bi bil zaradi škodovanja vojaškim operacijam ali vojaškim zmogljivostim rezultat drugačen. Kibernetski napad v Estoniji leta 2007, ki je povzročil motnje vitalnih računalniških sistemov v administraciji, finančnem, ter socialnem sistemu, tako ni dosegel zahtevanega nivoja škode, saj ni prišlo do poškodb na objektih ali ljudeh. Napad z virusom Stuxnet pa bi zaradi nastanka fizične škode na centrifugah v Natanzu, kriteriju škode zadostil.[14]

2.2.2 Neposredna vzročna zveza

Interpretativne smernice neposredno vzročno zvezo pogojujejo z enim korakom med ravnanjem in nastankom škode. Tako kot delavec v tovarni orožja, za katerega so bili avtorji Interpretativnih smernic soglasni, da v sovražnostih ne sodeluje neposredno, naj neposredno ne bi sodeloval niti razvijalec kibernetskih orožij (Melzner, 2009, str. 53). Kibernetska orožja so v tem smislu lahko specifična – zaradi nasprotnikove nepričakovane ali spreminjajoče-se aktivne kibernetske

[13] *To se je denimo zgodilo v Nemčiji v oktobru 2022 (Thurau, 2022).*

[14] *Opomniti velja, da niti v Estoniji, niti v Iranu, ni potekal oboroženi spopad. Obenem tudi ni povsem jasno, kdo stoji za napadoma.*

obrambe, lahko obstaja neprestana potreba po nadgradnji kibernetskih orožij tekom samega napada. Takšne nadgradnje zahtevajo globlje sodelovanje med napadalcem in razvijalcem kibernetskega orožja, kar poveča intenzivnost razvijalčeve udeležbe v samem napadu. Nekatera ravnanja razvijalcev programske opreme tako lahko dosežejo prag neposredne vzročne zveze, saj so od škode oddaljena zgolj en korak (Matheson, 2019, str. 39). Interpretativne smernice v takšnem scenariju torej dajejo zelo življenjski rezultat.

2.2.3 Povezava s sovražnostmi

Pogoj povezave s sovražnostmi (*belligerent nexus*) zahteva, da dejanje v svoji zasnovi podpira eno stran v spopadu v škodo nasprotne strani (Melzner, 2009, str. 59). V kibernetski domeni pomaga razlikovati med patriotskimi hekerji, ki želijo pomagati svoji državi, ter skupinami, kot je recimo *Anonymous*. Oboji izvajajo podobne akcije, vendar zadnji tega ne počno s ciljem pomoči strani v spopadu. Pogoj povezave s sovražnostmi v izjemnih primerih vzame v obzir subjektivne lastnosti napadalca, kot je naklep,[15] kar se v kibernetskem scenariju zgodi v primeru »botneta«, specifično načrtovanega za izvajanje napadov porazdeljene zavrnitve storitve (*distributed denial of service* – DDoS) preko ugrabljenih civilnih računalnikov. Lastniki teh računalnikov se ne zavedajo njihove zlorabe, torej obdržijo svojo zaščito, čeprav njihovi računalniki postanejo vojaški cilji. Gre za še eno kibernetsko situacijo, ki s strani avtorjev Interpretativnih smernic morda ni bila predvidena, a zanjo Interpretativne smernice ponujajo praktično rešitev.

2,2,4 Ugotovitve o udeležbi civilistov v kibernetskem vojskovanju

Nabor aktivnosti, ki se štejejo za neposredno udeležbo v sovražnostih, je v kibernetski domeni širok, zaradi česar je v sodobnih oboroženih spopadih delež civilistov, ki predstavljajo legitimne tarče, večji, kot smo vajeni v klasičnih vojnah.[16] Ker pa operacije, ki sicer resno vplivajo na javno zdravje, varnost ali trgovino, ne dosežejo nujno nivoja zahtevane škode, razen če rezultirajo v uničenju civilne infrastrukture ali civilnih poškodbah, in ker Interpretativne smernice neposredno vzročno zvezo pogojujejo tudi z enim korakom med ravnanjem in nastankom škode, kar pri kibernetskih operacijah ni tipično, tvorijo visok prag za neposredno udeležbo

---

[15] *Te so vzete v račun le v izrednih okoliščinah, ko se civilist niti malo ne zaveda svoje vloge v izvajanju sovražnosti (voznik, ki nevede prevaža daljinsko vodeno bombo), ali pa, ko fizično niti ne ravna (mu je povsem odvzeta fizična svoboda - neprostovoljni človeški ščiti) (Melzner, 2009, str. 60).*

[16] *Skupina strokovnjakov za Priročnik iz Osla o izbranih temah prava oboroženih spopadov (Oslo Manual Manual on Select Topics of the Law of Armed Conflict) je bila soglasna, da se za neposredno udeležbo v sovražnostih štejejo: kibernetske aktivnosti, zasnovane za neposredno povzročitev poškodb ali uničenja nasprotni strani v spopadu, kibernetska obramba vojaških ciljev, prispevanje k postopkom izbire ciljev, udeležba v načrtovanju kibernetskih napadov, ter zagotavljanje oz. prenos taktično pomembnih informacij s ciljem pomagati bojnim operacijam. Zgolj pridobivanje vojaško pomembnih informacij še ne šteje za neposredno udeležbo, avtorji pa niso mogli določiti jasne meje med zbiranjem in procesiranjem pridobljenih informacij, ki pa že šteje kot neposredna udeležba v sovražnostih (Dinstein in Willy, 2020, pravilo 28).*

v sovražnostih.[17] Civilisti torej lahko izvajajo kibernetske operacije z znatnimi posledicami za civilno prebivalstvo, ne da bi postali vojaške tarče. Interpretativne smernice časovno okno neposredne udeležbe v sovražnostih poleg izvajanja sovražnosti omejijo še na pripravljalna dejanja in vrnitev z aktivnosti (Melzner, 2009, str. 65).

V kibernetskem vojskovanju je to nepraktičen standard, saj z izjemo operacij bližnjega dostopa, ni prihoda ali odhoda z operacije. Sama izvedba kibernetske operacije tipično poteka hitro, tako da pred njenim zaključkom napadalca običajno niti ni mogoče identificirati (Dinniss, 2013, str. 270). Obstoječa ureditev zaradi manjše verjetnosti zajetja, ki sicer izvotli pomen borčevskega privilegija, tako predstavlja iniciativo za neupoštevanje načela razlikovanja (Padmanabhan, 2013, str. 301).

2.3 Posebej zaščitene osebe

Zdravstveno osebje, pripadniki civilne zaščite, versko osebje, in druge posebej zaščitene osebe, uživajo svojo zaščito tudi v kibernetski domeni. Kot dodatna kategorija posebej zaščitenih oseb, bi se v tej domeni lahko šteli tudi pripadniki skupin za odzivanje na elektronske grožnje (*computer emergency response teams* – CERT). Skladno z ZInfV so v RS to skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Po Pravilih odgovornega obnašanja v kibernetskem prostoru (*UN Norms of Responsible State Behaviour in Cyberspace*), naj takšne skupine ne bi bile vojaške tarče.[18] Sodelujoči na srečanju strokovnjakov o izogibanju civilni škodi v vojaških kibernetskih operacijah v oboroženih spopadih (*Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts*) so o potrebi, da se CERT v kibernetskem prostoru zaščiti podobno kot bolnišnično osebje, ki v kinetičnem vojskovanju nudi prvo pomoč, razpravljali leta 2020. Več strokovnjakov je izpostavilo, da je takšno analogijo težko vzpostaviti, saj sta vlogi prvih poleg saniranja škode tudi identifikacija vira napada in zaustavitev samega napada (ICRC, 2020, str. 28). Pravila odgovornega obnašanja v kibernetskem prostoru vsekakor predstavljajo dober nastavek za nadaljnje delo na področju ustanavljanja ekvivalentov bolničarjem, gasilcem, ali pripadnikom civilne zaščite v kibernetski domeni, pod pogojem da se njihove naloge zameji zgolj na zmanjševanje škode. V primeru izvajanja protinapada bi, podobno kot preostale zaščitene osebe, svojo zaščito začasno izgubili.

---

[17] *Turns na primeru desetih hipotetičnih kibernetskih operacij ugotavlja, da zgolj tri dosežejo prag neposredne udeležbe v sovražnostih. Najlažje je vzpostaviti pogoj povezave s sovražnostmi, najtežje pa neposredno vzročno zvezo (Turns, 2012).*

[18] *UN GGE je to predlagala v svojem poročilu GS OZN št. A/70/174, odst. 13(k), kasneje je GS OZN poročilo soglasno podprla v resoluciji št. 70/237. Pravila odgovornega obnašanja v kibernetskem prostoru sicer niso zavezujoča, državam pa služijo kot smernice pri ravnanju z IKT (Generalna skupščina Združenih narodov, 2021, odst. 25).*

Zaključek

Spoštovanje načela razlikovanja je v kibernetskem vojskovanju zahtevnejše kot v ostalih domenah vojskovanja. Naletimo namreč na več ovir, tako pri ločevanju civilnih objektov od vojaških ciljev, kot civilistov od borcev.

Zaradi velike odvisnosti vojska od kibernetskega prostora bi ob upoštevanju zlasti kriterijev uporabe in namena, lahko bil nabor civilnih objektov, ki se v kibernetskem vojskovanju spremenijo v vojaške cilje, izjemno širok in bi vključeval sisteme, na katere se zanašajo ključne civilne dejavnosti. Idealna rešitev je dosledna fizična delitev kibernetske infrastrukture na vojaško in civilno, ki pa zaradi njune vseprisotne soodvisnosti ni uresničljiva. Bolj realistična je zgolj ločitev objektov, ki so v MHP posebej zaščiteni, oziroma širitev njihovega nabora na druge objekte kritične infrastrukture. Odprto definicijo vojaškega cilja zamejuje zahteva po jasni vojaški prednosti, ki pa v zvezi s kibernetskimi omrežji ponuja neživljenjski zaključek, da bi bila jasna vojaška prednost podana zgolj z uničenjem vseh, ali vsaj večjega dela komunikacijskih poti.

Problemi pri ločevanju civilistov od borcev se pojavijo že pri konstitutivnih pogojih vizualnega razlikovanja za določene skupine oseb, tako ali drugače udeleženih v kibernetskem vojskovanju. Ker se borci pri kibernetskem vojskovanju fizično ne soočijo, je zahteva po nošenju na daljavo vidnega razpoznavnega znaka, po mnenju nekaterih avtorjev, utemeljeno, odveč. Del stroke meni tudi, da v kibernetski domeni nima realne uporabe zahteva po odkritem nošenju orožja. A zgolj neuporaba konvencionalnega orožja s strani kibernetskih borcev še ne spreminja popolnoma nedvoumne pravne ureditve. Če se odkrito nošenje orožja pri trenutni ureditvi še lahko zanemari pri večini borcev, se tega ne da storiti pri kibernetskem *levée en masse*, pri katerem je pogoj odkritega nošenja orožja edini element razlikovanja od civilistov. Obenem pa trenutno ni jasno, kaj se v kibernetski domeni sploh lahko šteje kot odkrito nošenje orožja.

V kibernetskem vojskovanju je delež civilistov, neposredno udeleženih v sovražnostih, večji, kot smo vajeni v klasičnih vojnah, kar je skladno z našo zakonodajo pričakovati tudi v RS, saj kibernetsko obrambo izvajajo Urad Vlade RS za informacijsko varnost, skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij in drugi nacionalni organi. Uslužbenci teh organov lahko pod pogoji, identificiranimi v članku, postanejo legitimne vojaške tarče, v primeru zajetja s strani nasprotnika, pa so lahko zaradi odsotnosti njihovega borčevskega statusa tudi kazensko preganjani po nasprotnikovi zakonodaji.

Obenem pa tipične kibernetske operacije, katerih tarča je civilno prebivalstvo in lahko resno vplivajo na javno zdravje, varnost ali gospodarstvo, ne dosežejo nivoja zahtevane škode, razen če rezultirajo v uničenju civilne infrastrukture ali civilnih poškodbah. Civilisti torej lahko izvajajo kibernetske operacije z znatnimi posledicami za nasprotnikovo civilno prebivalstvo, brez nevarnosti, da bodo postali vojaški cilji. Obstoječa ureditev je do takšnih civilistov torej preveč prizanesljiva, saj jim nudi večjo zaščito kot osebam z borčevskim privilegijem.

V odsotnosti mednarodne jurisprudence na temo kibernetskega vojskovanja, je razjasnitev v članku identificiranih problemov zaenkrat odvisna od akademikov in bodoče prakse držav. Zaradi izpostavljenih pomanjkljivosti uporabe načela razlikovanja pri kibernetskem vojskovanju, ki posegajo v njegovo bistvo do te mere, da v nekaterih primerih ostane praktično brez zaščitne vrednosti, načelo razlikovanja osebam in objektom, zaščitenim v kinetičnem vojskovanju, v kibernetski domeni ne nudi zadostne zaščite. Kljub temu zaščita civilistov in civilnih objektov ni nujno nezadostna. Ugotovitev se namreč nanaša zgolj na načelo razlikovanja, ki pa podobno kot v drugih domenah vojskovanja, vselej deluje v kombinaciji z drugimi načeli MHP, zlasti načeloma previdnosti in sorazmernosti.[19]

Obstaja tudi nekaj dobrih predlogov dopolnitve obstoječe pravne ureditve, med katerimi velja poleg že omenjene ločitve v MHP posebej zaščitenih objektov, ter širitve njihovega nabora, izpostaviti tudi možnosti zaščite CERT z nekaterimi omejitvami pri izvajanju protinapadov, na podoben način, kot je zaščiteno zdravstveno in versko osebje, kar bi v RS lahko omogočalo zaščiten status skupinam za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij.

Literatura

1. *Buchan, R., in Tsagourias, N., 2022. ‚Ukrainian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?'. https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/ (26. 2. 2024).*
2. *Connell, M., in Vogler, S., 2016. Russia's Approach to Cyber Warfare, CNA's Occasional Paper series, https://apps.dtic.mil/sti/pdfs/AD1019062.pdf (28. 2. 2024).*
3. *Department of Defense, 2021. Dictionary of Military and Associated Terms, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf (28. 2. 2024).*
4. *Dinstein, Y., in Willy, D. A., 2020. Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary. Springer.*
5. *Doffman, Z., 2019. Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First. Forbes, 6. maj, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=50d4edacafb5 (26. 2. 2024).*
6. *Döge, J., 2010. Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime. Archiv des Völkerrechts, 48(4), str. 486-501.*
7. *Droege, C., 2012. Get off my Cloud: cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), str. 533–578.*
8. *Geiß, R., in Lahmann, H., 2012. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. Israel Law Review, 45(3), str. 381–399.*
9. *Generalna skupščina Združenih narodov, (2015). The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2015 (A/70/174). Z dne 22. julija 2015.*
10. *Generalna skupščina Združenih narodov, (2021). OEWG Final Substantive Report (A/AC.290/2021/CRP.2). Z dne 10. marca 2021.*

[19] *Kibernetske operacije lahko s svojo nesmrtonosno naravo omogočijo napadanje vojaških ciljev z manjšo postransko škodo, kot jo povzročijo njihove kinetične alternative, zato so lahko ob odgovorni uporabi primernejše od kinetičnih. Glej npr stališče Združenega Kraljestva (UK, 2020, točka B).*

11. *Goodman, R., in Jinks, D. P., 2010. The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law: An Introduction to the Forum, New York University International Law and Politics, 42, str. 637–640.*
12. *Harrison Dinniss, H., 2013. Participants in Conflict: Cyber warriors, patriotic hackers and the laws of war. V: D. Saxon, ur. International Humanitarian Law and the Changing Technology of War, str. 251–278. Leiden: Boston: Martinus Nijhoff Publishers.*
13. *Hathaway, O. idr., 2011. The Law of Cyber-Attack. California Law Review, 100, str. 817–886.*
14. *Henckaerts, J., in Doswald-Beck, L., 2009. Customary International Humanitarian Law, Vol. 1 – Rules. Cambridge: Cambridge University Press.*
15. *Human Rights Watch, 2003. International Humanitarian Law Issues in a Potential War in Iraq. Human Rights Watch Briefing Paper. Washington DC.*
16. *ICRC, 2013. Cyberwarfare and international humanitarian law: the ICRC's position, https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (28. 2. 2024).*
17. *ICRC, 2020. Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting, 21–22 January 2020, Geneva, https://shop.icrc.org/avoiding-civilian-harm-from-military-cyber-operations-during-armed-conflicts-icrc-expert-meeting-21-22-january-2020-geneva-pdf-en (27. 2. 2024).*
18. *ICRC, 2021. Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War. Cambridge: Cambridge University Press.*
19. *ICRC, 2022. Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions. ICRC, Ženeva.*
20. *ICRC, 2023. Preventing and minimizing digital threats to people affected by armed conflict, Draft Elements of Resolution, November 2023. ICRC, Ženeva.*
21. *International Court of Justice (ICJ), 1996. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion). I.C.J. Reports, 226.*
22. *International Criminal Tribunal for the Former Yugoslavia (ICTY), 1995. The Prosecutor v. Dusko Tadić, IT-94-1-AR72 (Appeals Chamber, Decision).*
23. *International Criminal Tribunal for the Former Yugoslavia (ICTY), 2000. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. International Legal Materials, 39(5), str. 1257–1283.*
24. *Matheson, C., 2019. From Munitions to Malware: A Comparative Analysis of Civilian Targetability in Cyber Conflict. Journal of Law & Cyber Warfare, 7(2), str. 29–66.*
25. *Mavropoulou, E., 2015. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. Journal of Law & Cyber Warfare, 4(2), str. 23–93.*
26. *Melzer, N., 2009. Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. International Committee of the Red Cross (ICRC), Ženeva.*
27. *Microsoft, 2022. Microsoft Digital Defense Report 2022. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (27. 2. 2024).*
28. *Nash, K. S., Castellanos, S., in Janofsky, A., 2018. One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs. The Wall Street Journal, https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 (27. 2. 2024).*
29. *Padmanabhan, V. M., 2013. Cyber Warriors in the Jus in Bello. International law studies, 288(89), str. 288-308.*
30. *Pascucci, C., 2017. Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution. Minnesota Journal of International Law, 26(1), str. 419–460.*

31. *Protokol o prepovedih ali omejitvah uporabe zažigalnih orožij, Uradni list Socialistične Federativne Republike Jugoslavije, Mednarodne pogodbe, št. 3/82.*
32. *Sancin, V., Švarc, D., in Ambrož, M., 2009. Mednarodno pravo oboroženih spopadov. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.*
33. *Schmitt, M. N., 2015. The Law of Cyber Targeting. Naval War College Review, 68(2), Article 3, str. 1–20.*
34. *Schmitt, M. N., 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2. izd. Cambridge: Cambridge University Press.*
35. *Second International Peace Conference, The Hague, 1907. Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land. International Conferences (Haag), z dne 18. oktobra 1907.*
36. *Shanghai Cooperation Organisation, 2009. Agreement on Cooperation in Ensuring International Information Security. Jekaterinburg, 16. junija.*
37. *Šarf, P., 2017. Legality of Low-Intensity Cyber Operations Under International Law. Sodobni vojaški izzivi, 19(3), str. 81–93.*
38. *Štrucl, D., 2022. Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare. Sodobni vojaški izzivi, 24(2), str. 103–123.*
39. *Thurau, J., 2022. Germany's Critical Infrastructure Is Poorly Protected. DW, https://www.dw.com/en/germanys-critical-infrastructure-is-poorly-protected/a-63505983 (26. 2. 2024).*
40. *Turns, D., 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. Journal of Conflict and Security Law, 17, str. 279–297.*
41. *Ur. l. SFRJ, 1978. Dopolnilni protokol k ženevskim konvencijam z dne 12. avgusta 1949 o zaščiti žrtev mednarodnih oboroženih spopadov, z dne 8. junija 1977 (DP-I), mednarodne pogodbe, št. 16/78.*
42. *van Benthem, T. J., 2023. Privatized Frontlines: Private-Sector Contributions in Armed Conflict. 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Talin, Estonija, str 55–69. DOI: 10.23919/CyCon58705.2023.10182177.*
43. *Wallace, D. A., in Reeves, S., 2013. The Law of Armed Conflict's ‚Wicked' Problem: Levée En Masse in Cyber Warfare. International Law Studies, 89, str. 646–668.*
44. *Združeno kraljestvo, 2020. Response to Chair's Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security, April 2020.*
45. *Ženevska konvencija o ravnanju z vojnimi ujetniki, z dne 12. avgusta 1949. (1950). Ur.l. Prezidijuma LS FLRJ, št. 6/50.*

email: urban.praprotnik@mors.si

Guillermo López-Rodríguez,
Daniel Montoya-Roldan

DOI: 10.2478/cmc-2024-0012

IZZIVI IN PERSPEKTIVE V URBANEM BOJEVANJU: ANALITIČNI OKVIR

CHALLENGES AND PROSPECTS IN URBAN WARFARE: AN ANALYTICAL FRAMEWORK

Povzetek Število prebivalcev v mestih po svetu se bo v naslednjih desetletjih povečalo. Konvencionalne vojaške sile se bodo v večji meri uporabljale na omejenih območjih, kjer njihove visokotehnološke zmogljivosti ne prinašajo prednosti. Ta raziskava zagotavlja analitični okvir za razumevanje glavnih izzivov urbanega bojevanja za konvencionalne sile. Analiza kot ključne dejavnike opredeljuje vojaško organizacijsko razsežnost, tehnologije z dvojno rabo, ki spreminjajo pravila bojevanja, in vlogo civilnega prebivalstva v urbanih okoljih. Ugotovitve podajajo nekatera priporočila v zvezi s strategijami usposabljanja in komuniciranja. Perspektive urbanega bojevanja bo zaznamovala kombinacija kognitivnih in kinetičnih ukrepov.

Ključne besede ***Urbano bojevanje, vojaške organizacije, vojaške operacije.***

Abstract The population living in cities around the world will increase in the next decades. Conventional military forces will deploy more in constrained areas where their high-tech capabilities are not an advantage. This research provides an analytical framework for understanding the main challenges of urban warfare for conventional forces. The analysis identifies the military organizational dimension, dual-use technologies as game changers, and the role of civilian population in urban environments as key factors. The conclusions provide some policy recommendations concerning training and communication strategies. The prospects of urban warfare will be defined by a combination of cognitive and kinetic actions.

Key words ***Urban warfare, military organizations, military operations.***

Introduction

Urbanization has been identified as a key megatrend for future warfare (Stringer et al, 2023), due to a likely increase of 2.5 billion people in densely populated areas by 2050 (UN DESA, 2018). Uncontrollable urban growth could provoke a governmental failure in providing basic services, which could be used by armed groups to implement revisionist agendas (US Army, 2014). Prospective analysis has shown a clear tendency towards the concentration of the population in large urban areas (DCDC, 2016), which will identify cities as one of the main operational environments. Economic development in the global south has contributed to the urbanization process, which has implications in the social, political and military dimensions (Konaev, 2019).

Cities and metropolitan areas are relevant spaces for economic development and productive sectors, as there is a high concentration of industry, business and institutional headquarters (Sampaio, 2016). However, despite the positive outcomes of urbanization, it can also contribute to increasing violence and political instability due to state fragility or economic crisis (Rosenau, 1997). Urban areas are defined by their density, as they concentrate heterogeneous and diverse groups with different ideological or ethnic affiliations (Elfversson et al., 2023). These elements reinforce the role of urban populated areas as potential targets for military operations, and their size increases operational complexity.

The academic literature with regard to urban warfare also identifies confrontations between different violent actors. Among the vast number of actors involved, there have been recent conflicts between conventional militaries and non-state actors in Aleppo and Raqqa in Syria, high-intensity terrorist activities in Paris, France, and military operations against organized crime in Rio (Brazil) or Tijuana (Mexico) (Konaev, 2019). Due to the complexity and relevance of urban terrain for military operations, specialized literature in military affairs has identified the main implications for the success and failure of operations.

Because of this, it is relevant to ask: What are the main challenges of urban warfare for conventional military forces? This article provides a qualitative analysis of relevant trends in the deployment of conventional military forces in urban environments. The aim of the research is to focus on the offensive approach, as it allows the proposal of policy recommendations for military forces. The analysis provides a research framework which analyzes the main implications at the organizational level, the impact of double-use technologies, and the role of the civilian population in the operational environment. This study does not analyze specific case studies, instead focusing on general trends which can be extrapolated in further research. The conclusion includes further research on urban warfare, as well as policy recommendations from a political science perspective.

1 ANALYZING MILITARY FORCES IN URBAN WARFARE

Urban warfare is not a new phenomenon, as throughout the 20th Century there have been significant conflicts in urban areas, including in the Spanish Civil War and in the Sino-Japanese War, acquiring a larger dimension throughout World War II. Some self-determination projects during decolonization also involved urban warfare operations in Algeria and Indochina, as well as counterinsurgency activities in Northern Ireland (Konaev, 2019). As the end of the Cold War changed the logics of contemporary conflicts, some systematic violent intra-state actions occurred in cities such as Sarajevo and Mostar (Bosnia and Herzegovina) during the Balkan War (Kaldor, 1999), and in Grozny (Chechnya) and Mogadishu (Somalia) (Rossenau, 1997). Later experiences evidenced the relevance of cities to conventional militaries, including the US operations in Baghdad and Fallujah in Iraq between 2003 and 2011 (Konaev, 2019).

Some of the most recent urban operations have been defined by the conflict between conventional and non-conventional forces, as occurred in Aleppo (Syria), Mosul (Iraq) and Donetsk (Ukraine) (Sampaio, 2016; Bin Inam & Rauf, 2024), as well as in Sanaa (Yemen) or Raqqa (Syria) (Konaev, 2019). Due to the constant presence of a civilian population, conventional forces have limited operational alternatives, being constrained to avoid collateral damage and civilian casualties (Hahn & Jezior, 1999). The characteristics of the urban environment have implied high levels of violence against combatants and non-combatants, affecting both people and infrastructure (Sampaio, 2016).

This research provides an analytical framework for studying the challenges and prospects of conventional forces in urban warfare from an offensive approach. This perspective limits the available options, as providing the analysis from a defensive approach against a foreign adversary would imply multiple alternatives conditioned by the specific characteristics of each case. The research design is structured in several qualitative categories, the main category being the challenges of urban warfare for conventional military forces. This analytical category is further sub-divided into the following core categories: (1) The organizational dimension, (2) Dual-use technologies and (3) The role of the local population.

The analysis is structured around the core categories, divided into sub-categories according to the main challenges posed for military forces. The specific characteristics of the urban environment conditions the command and control structures, as well as requiring a high level of mobility and interoperability of forces, due to the need to conduct combined operations. The presence of violent non-state actors in urban environments increases the relevance of dual-use technologies, especially those employed for surveillance and reconnaissance, and those communication and information technologies with impact in the cognitive domain. The presence of the local population in urban warfare poses challenges related to targeting, as well as a high level of incertitude with regard to local support for violent actors. The

availability of information technologies for the local population also has an impact on the cognitive domain, which is taken into account in the analysis.

Table 1: Research design (Source: Authors)

Main Category	Core categories	Sub-categories
The challenges of urban warfare for conventional military forces	The organizational dimension	Command & Control Mobility & tempo Interoperability of forces
	Dual-use technologies	Surveillance & Reconnaissance The cognitive domain
	The role of the local population	Risks of targeting Support to local actors The cognitive domain

The analysis is structured around the core categories, divided into sub-categories according to the main challenges posed for military forces. The specific characteristics of the urban environment conditions the command and control structures, as well as requiring a high level of mobility and interoperability of forces, due to the need to conduct combined operations. The presence of violent non-state actors in urban environments increases the relevance of dual-use technologies, especially those employed for surveillance and reconnaissance, and those communication and information technologies with impact in the cognitive domain. The presence of the local population in urban warfare poses challenges related to targeting, as well as a high level of incertitude with regard to local support for violent actors. The availability of information technologies for the local population also has an impact on the cognitive domain, which is taken into account in the analysis.

2 THE CHALLENGES OF URBAN WARFARE FOR CONVENTIONAL MILITARY FORCES

The deployment of forces in urban environments implies several challenges that are analyzed in the following section. According to the research design, the first section discusses the challenges related to the organizational dimension; the second section analyzes the implications of dual-use technologies; and the final section focuses on the role of the local population and their potential impact on military operations. As fighting in cities provides several advantages to the defenders against the attacking force, especially when engaging in combat in the streets (Stone, 2009), initiative and

technological capabilities are limited for the attackers (Hahn & Jezior, 1999). This can be explained by an asymmetry of intelligence, as the defenders have a better knowledge of the streets and rooftops, which is even more important in the case of operations in shanty towns without formal maps (Rossenau, 1997).

2.1 The organizational dimension: small teams and combined operations

Military operations in urban areas are defined by a complexity and multiplicity of elements. In order to achieve operational objectives, armies require combatant awareness and readiness to deploy in complex environments under stress. As Khan & Romaniuk (2023) state, the complexity of the operational environment is defined by the multidimensionality of the physical spaces, involving underground, surface and vertical actions. The urban environment is composed of multiple micro-environments which require tempo, intensity and decentralization of command (Konaev, 2019; Rossenau, 1997). In addition to the physical features, deployed armies must take into account the presence of additional actors and informal networks in a local environment connected to the global arena (Khan & Romaniuk, 2023). The presence of additional actors can sometimes lead not only to fighting against but also to cooperating with local actors when conducting urban operations (Stringer et al., 2023).

The characteristics of urban environments make it difficult to deploy large formations of troops, which implies the division of units into smaller groups and also the decentralization of operations. These facts increase the relevance of low-echelon leadership and command, especially at the company and platoon levels (Rossenau, 1997). Different experiences in urban warfare show how the achievement of objectives is conditioned by small-unit leadership, specialized equipment, and the quality of intelligence (Konaev, 2019). The success of urban operations is based on the degree of training and the operational experience of small units.

When military organizations are deployed in urban areas, armies must take into account the lethality and mobility of the units, the survivability of their troops, and the logistic sustainability of the military equipment (Hahn & Jezior, 1999). This means that the more complex the operational environment, the higher the range of options for combatants there should be, and both the tactics and the rules of engagement must be clear (Niksch, 2017). The achievement of these requirements is essential in order to limit operational mistakes and unexpected outcomes.

With regard to the different types of objectives, conventional armies usually carry out a diverse range of functions in the urban environment. Within the different possibilities, the literature identifies policing operations, raids to evacuate hostages, and sustained military combat against irregular forces defending the city (Bin Inam & Rauf, 2024). Urban warfare requires armies to develop the ability to conduct combined operations. In this sense, a modern military must combine light infantry and mechanized and armoured units (Konaev, 2019); it is essential that light infantry

support armoured units to prevent ambushes and clashes (Rosenau, 1997). Due to the high density of urban terrain, both special operation forces and snipers can contribute to intelligence and reconnaissance activities (Konaev, 2019), providing relevant insights to improve the command and control of the operation (Hahn & Jezior, 1999).

2.2 Dual-use technologies in urban warfare

This section analyzes the main challenges with regard to unmanned vehicles and informational technologies. Both are identified as dual-use technologies available in civilian markets, and they can be used by both conventional and non-conventional actors. The main challenge is that when operating in cities, non-state adversaries will be able to use advanced capabilities such as artificial intelligence, UAVs, cyber capabilities and robotics (Khan & Romaniuk, 2023). These have constantly been used by ISIS combatants in Syria (Ball, 2017) and Iraq (South, 2018). In the case of information technologies, they have already been used for recruitment, propaganda and information exchange (Bin Inam & Rauf, 2024).

The use of technology is a relevant dimension in modern warfare, and its importance has led western societies towards a cult of technology that in some cases has voided the success of the operations (Van Creveld, 1991). The characteristics of urban terrain can limit the advantage of the attacker over the defenders, which could not only lead units to fragmentary operation, but also leave them without technological support. This limits the situational awareness of command structures in operations, as command and control require updated information about enemy positions and the movement of civilians on the ground (Hahn & Jezior, 1999).

2.2.1 The use of UAVs in surveillance and reconnaissance

Contemporary warfare has limited the aerial superiority of conventional armies, due to the availability of unmanned aerial vehicles to non-state armed groups (Konaev, 2019). This diffusion of technology has transformed the available resources, limiting the asymmetry between conventional military and other violent actors. UAVs have mainly been used for intelligence purposes and combat support, reducing the numbers of casualties in surveillance and reconnaissance actions (Bin Inam & Rauf, 2024).

As drones are usually equipped with cameras and high-definition sensors, they are used to improve combat support by obtaining intelligence from images, signals and signatures in urban areas (Chulilla-Cano, 2023; Morales-Morales, 2023). When deployed in densely populated cities, they are able to monitor physical areas and identify the selected targets. This aerial support can improve the deployment and performance of land forces. At the tactical level, the use of drones contributes to the flexibility of deployed troops, as drones can navigate between buildings, expanding the visual range of ground forces.

With regard to the future of urban operations, current drones pose some challenges that must be taken into account by military forces (Pérez-González et al., 2019). Armies will need to develop advanced data management systems to filter, analyze and diffuse real-time information. In this sense, the use of machine learning, cluster analysis and neural networks would offer significant advances towards improve decision-making processes at tactical levels.

In order to prevent non-authorized access to the information, UAVs would require strong encryption systems to build a multiple encryption layer between the drone and the operator. This defence would be complemented by proactive measures such as anti-malware software and intrusion detection systems. UAVs would also need anti-jamming technology to avoid provoked or accidental interferences. To this purpose, UAVs would require alternative frequencies to avoid interception and congestion, as well as advanced navigation systems not only dependent on GPS.

2.2.2 Communication and information technologies

The use of information technologies not only affects communications between deployed units, but also has a core influence over the cognitive domain. Dual-use technologies will keep transforming the dynamics of military operations, especially in urban warfare. If UAVs condition reconnaissance and targeting (Ball, 2017), information technologies would condition military performance and social support to deployments in urban areas.

Due to the density of the population and the infrastructure in urban areas, the damage derived from military operations is usually high (Khorram-Manesh & Brukle, 2022). In addition to its direct effects on military performance, the psychological and visual impact of the destruction can easily be instrumentalized on social media by non-state actors, to promote their narratives and gain support against the deployed forces (Bin Inam & Rauf, 2024). As objective facts are substituted by emotions and beliefs, information flows are even more relevant than in the past, as they define the levels of support to the conducted operations (Mölder & Sazonov, 2018). The impact of information can shape perceptions which can be turned into coordinated kinetic actions (Shallcross, 2017).

As global patterns of migration and connectivity have increased the diversity of cities across the globe (Elfversson et al., 2023), information flows not only impact the operational environment against the deployed forces, but also the homeland territory of the nation carrying out the operation or other nations supporting the military actions. Recent conflicts in Syria, Gaza, Nagorno-Karabakh or Ukraine have been characterized by the carrying out of several urban operations, involving a high number of civilian casualties, people displacement and infrastructure destruction. The availability of smartphones has allowed a constant exchange of information, and the organization of action networks in different locations has been a force multiplier in urban operations (Bin Inam & Rauf, 2024).

2.3 The role of local population

The density of urban environments is not only related to the physical infrastructure, but also to a greater presence of the civilian population than in rural areas. This is a key factor for military forces when deploying urban operations, as it constrains the available operational alternatives in order to avoid civilian casualties. Despite the fact that in some cases there has been a primacy of achieving military objectives, decision-makers must take into account the political outcomes of civilian casualties of urban warfare. The presence of civilians in urban operations poses challenges in blockade and siege operations, as well as in urban combat.

This dimension is critical, as in many urban operations there is a blurred difference between members or sympathizers of non-state violent groups and civilians (Sampaio, 2016). Even disregarding the ideological affiliation of civilians to the deployed conventional forces, it is clear that the presence of non-combatants affects the immediate operational phases and the further steps of the military campaign (Rosenau, 1997). In divided societies with previous experience of communal violence this factor is even more relevant (Elfversson et al., 2023b), as civilian groups must be considered as heterogeneous actors with different political agendas.

The presence of civilians in operating environments intensifies the need to correctly verify military targets (John-Hopkins, 2010), and means that the conventional rules of engagement impose restrictions on heavy artillery and air support (Konaev, 2019). Both capabilities are essential to the support of the deployed forces, so these restrictions, thanks to the need of international or local support, increase the chances of fighting in the streets. International humanitarian law demands that conventional forces apply precision fire to minimize civilian casualties and damage to infrastructure (Konaev, 2019). In addition to this, militaries are required to follow the principle of proportionality in the use of force, which also obliges modern armies to previously communicate attacks which will affect civilians (John-Hopkins, 2010). This last element not only reduces the initiative of the attacker, but also allows defenders to use civilians for combat purposes (Stone, 2009).

The civilian population can also be affected by several strategies of the deployed forces, especially in cases where humanitarian law is not respected. In some cases, attackers have blocked cities, cutting off supply chains to cause starvation in the civilian population, like in Syria, or shutting down water and electricity, like in Sarajevo (Hägerdal, 2020). These strategies have often been rejected not only due to their impact on the local population, but also due to the negative effects on public opinion. In addition to these specific actions, fighting in cities has led to other relevant problems related to infrastructure destruction (Bin Inam & Rauf, 2024); the destruction of essential infrastructure to provide water, sanitation, heat or electricity has usually led to later difficulties in terms of a refugee crisis or generalized health issues in the local population.

Access to social media and communications by civilians can also generate informal information networks by the use of instant message services as WhatsApp, Telegram or Snapchat (Konaev, 2019). This can provide real-time intelligence to defenders, increasing the vulnerability of the deployed troops. The presence of civilians in urban operations also has a clear impact on the cognitive domain of armed conflicts. As civilian casualties can be instrumentalized by media and social media campaigns, local and international public opinion can turn against the deployed actor (Bin Inam & Rauf, 2024). As pointed out earlier, confusion in clearly identifying the role of each group has several implications both for targeting and for recruitment by local non-state actors (Konaev, 2019; Bin Inam & Rauf, 2024). Particularly in those cases where conventional armies are fighting against non-state actors, the distinction between combatants, sympathizers, collaborators and non-combatants blurs, increasing the complexity of the military operations.

Conclusion

The urbanization process is a key trend which will continue to condition future military operations. Cities present specific characteristics which differ from operations in rural areas, as not only physical structures but also the diversity of civilians living in urban areas must be taken into account. Deployment in urban environments also affects non-combatants, who can be both the victims and the supporters of the involved actors, especially when the deployed troops can be considered as an occupying force. Carrying out urban operations is also more complex when analyzing offensive actions, and fighting in the streets often implies a higher number of casualties. In this sense, urban warfare involves all the organizational, technological and humanitarian challenges which have been analyzed in this article.

Conventional forces must operate in small teams, combining capabilities from various branches. In urban scenarios, infantry has a core role, and combatants require great physical and psychological strength in order to carry out rapid tactical actions, with decentralized command and multilevel environments. The technological dimension identifies UAVs as a key advantage for both combat and surveillance. According to this analysis, armies should take into account data management, information encryption and anti-jamming systems to achieve operational success. The humanitarian dimension is also key in urban warfare, as it imposes restrictions concerning the use of force. This can be even more problematic where non-combatants could be instrumentalized by defenders, confusing their categorization as victims or collaborators. All this poses communication challenges in which public opinion and different media play a key role.

As per some policy recommendations, militaries need to update their tactics, techniques and procedures for urban warfare. In environments defined by large cities and dense metropolitan areas, conventional forces must adapt themselves to constrained spaces with fragmented combat lines. Training of combatants must be taken into account, focusing on physical and psychological performance. Western militaries require urban facilities to test urban warfare procedures. This is not a new proposal, as some NATO armies already have them, but it would be advisable to

design and build full-scale urban testing areas with multiple facilities to test specific procedures in, for example, train station, airport and underground operations.

Lessons learned in urban warfare require armies to have an appropriate level of technical instruction for the use of new weapons systems and other tools for surveillance and reconnaissance. In some cases, this can require abilities from the civilian arena, especially with regard to hardware and programming, which would allow the inclusion of reservists who could provide their civilian expertise in dual-use technologies. At the same time, the need to control communication flows is essential in the operational environment. In this sense, conventional armies, even more than before, require the presence of civil-military communication and public relation teams to improve narratives in media and social media. Solid communication strategies about operational activities would improve social and political support to guarantee the success of operations in urban environments.

This article provides a basis for the development of further research following the provided analytical framework. It would be relevant to apply this framework to the study of the characteristics of several urban operations as case studies, or even from a comparative perspective. The identification of relevant categories also allows a systematic literature review in these specific categories. Due to the consolidation of information technologies as tools for propaganda, recruitment and organization, it is important to study their effects on urban operations. Further research in the field of political communication would be advisable, by applying algorithm-based techniques. This would increase understanding of impacts from the cognitive domain on physical actions in operational environments.

References

1. *Ball, R. J., 2017. The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications. Livermore, CA: Lawrence Livermore National Lab, Livermore, United States.*
2. *Bin Inam, Z., and Rauf, S., 2024. Understanding Urban Warfare and its manifestation in the Russia-Ukraine War. Institute of Strategic Studies Islamabad, 10 January 2024.*
3. *Chulilla-Cano, J. L. C., 2023. Presente y futuro de los drones comerciales letalizados [The present and future of lethal commercial drones], Revista General de Marina, 284(5), pp 673-684.*
4. *DCDC, 2016. Strategic Trends Programme: Future Operating Environment. Ministry of Defence. United Kingdom.*
5. *Elfversson, E., Gusic, I., and Rokem, J., 2023. Peace in cities, peace through cities? Theorising and exploring geographies of peace in violently contested cities. Peacebuilding, 11(4), pp 321-337.*
6. *Hägerdal, N., 2020. Starvation as siege tactics: urban warfare in Syria. Studies in Conflict and Terrorism, 46(7), pp 1-22. DOI: 10.1080/1057610X.2020.1816682.*
7. *Hahn, R. F., and Jezior, B., 1999. Urban Warfare and the Urban Warfighter of 2025. Parameters, Summer, pp 74-86.*
8. *Hartrich, J. P., 2016. Adapting the Army to win decisively in Megacities. US Army Press. APOJ 15-7.*

9. *John-Hopkins, M., 2010. Regulating the conduct of urban warfare: lessons from contemporary asymmetric armed conflicts. International Review of the Red Cross, 92(878), pp 469-493.*
10. *Kaldor, M., 1999. Nuevas Guerras. Violencia Organizada en la era global [New and Old Wars: Organized Violence in a Global Era]. Planeta.*
11. *Khan, U., and Romaniuk, S. N., 2023. Urban Warfare. In Romaniuk, S. N. et al. (eds.), The Handbook of Homeland Security, pp 477-488. Routledge.*
12. *Khorram-Manesh, A., and Burkle, F. M., 2022. Civilian population victimization: a systematic review comparing humanitarian and health outcomes in conventional and hybrid Warfare. Disaster Medicine and Public Health Preparedness, 17 (e192), pp 1-11.*
13. *Konaev, M., 2019. The future of urban warfare in the age of megacities. IFRI. Focus Stratégique 88.*
14. *Mölder, H., and Sazonov, V., 2018. Information warfare as the Hobbesian concept of modern times – the principles, techniques and tools of the Russian information operation in the Donbass. Journal of Slavic Military Studies, 31(3), pp 308-328.*
15. *Morales-Morales, S., 2023. El reto de los drones comerciales a la seguridad física y a la protección de la fuerza [The challenge of commercial drones for safety and force protection]. Revista General de Marina, 285(12), pp 1049-1060.*
16. *Niksch, C. A., 2017. The strategic challenges of urban warfare. Electronic thesis and dissertations, 1285. University of Denver.*
17. *Pérez González, J. M., Roquero Bravo, J. M., and Peraza Geist, T. D., 2019. Inteligencia computacional aplicada a vigilancia con una flota de drones. [Computational intelligence applied to drone swarms with surveillance purposes]. Thesis. University of the Republic (Uruguay).*
18. *Rosenau, W. G., 1997. 'Every room is a new battle': The lessons of modern urban warfare. Studies in Conflict and Terrorism, 20(4), pp 371-394.*
19. *Sampaio, A., 2016. Before and after urban warfare: conflict prevention and transitions in cities. International Review of the Red Cross, 98(1), pp 71-95.*
20. *Shallcross, N. J., 2017. Social media and information operations in the 21st century. Journal of Information Warfare, 16(1), pp 1-12.*
21. *South, T., 2018. The Future Battlefield: Army, Marines Prepare for 'Massive' Fight in Megacities, Military Times. https://www.militarytimes.com/news/your-army/2018/03/06/the-future-battlefield-army-marines-prepare-for-massive-fight-in-megacities/, 18 March 2018.*
22. *Stone, D. R., 2009. Stalingrad and the evolution of Soviet Urban Warfare. Journal of Slavic Military Studies, 22(2), pp 195-207.*
23. *Stringer, K. D., and Hooiveld, J. J., 2023. Urban Resistance to Occupation: An Underestimated Element of Land Warfare. Parameters, 53(3), pp 99-115.*
24. *UN DESA – Department of Economic and Social Affairs, 2022. World Population Prospects 2022. Summary of Results.*
25. *Van Creveld, M., 1991. Technology and War. From 2000 B.C. to the Present. Free Press.*

email: guillermolopez@ugr.es

ORCID: 0000-0001-8704-9007

email: danirolmonto@correo.ugr.es

Jelena Juvan

DOI: 10.2478/cmc-2024-0013

KUMULATIVNI UČINKI GONIL KONFLIKTOV V REGIJI SAHEL

THE CUMULATIVE EFFECTS OF CONFLICT DRIVERS IN THE SAHEL REGION

Povzetek Članek analizira zapletene varnostne razmere v regiji Sahel ter ugotavlja vzroke in gonila conflictive v regiji. Osrednja hipoteza, na kateri temelji članek, je, da na varnostne razmere v regiji Sahel vpliva več različnih vzrokov in gonil/povzročiteljev konfliktov, ki imajo kumulativne učinke, zaradi česar je reševanje konfliktov izjemno težko. Prvi del članka opredeljuje vzroke in dejavnike konflikta ter jih razvršča v štiri glavne kategorije. V drugem delu članek prikazuje, kako se vzroki in gonila prepletajo, kar ustvarja številne učinke prelivanja v sosednje države, v sosednje regije in tudi na druge celine, zaradi česar je regija Sahel ena najbolj problematičnih regij na svetu.

Ključne besede ***Sahel, varnost, gonila konfliktov.***

Abstract This article reflects on the complex security situation in the Sahel region, identifying the causes and drivers of conflicts. The main hypothesis underlying the article is that the security situation in the Sahel region is influenced by several different causes and conflict drivers which have cumulative effects, making conflict resolution extremely difficult. The first part of the article identifies the causes and drivers of conflict and classifies them into four main categories. In the second part, the article shows how the causes and drivers are interwoven, creating multiple spillover effects, making the Sahel region one of the most problematic regions in the world.

Key words ***Sahel, security, drivers of conflicts.***

Introduction

Although, since the end of February 2022, the attention of the international community has been focused on the war in Ukraine, Russia's military aggression, and its consequences for European and global security, and currently also on the Middle East where the conflict between Israel and the Hamas terrorist group is escalating, we must not forget or ignore the other conflict regions around the world. All the other armed conflicts have not ceased to exist with the advent of these two new ones; it is only that public and media attention has been shifted. It is therefore even more important to continue to discuss and analyse the other conflict-stricken regions in the world, and the Sahel region is undoubtedly one of them. A concerning trend can be identified in the Sahel region: the internationalization of internal armed conflicts, including civil wars. Over the past decade, the region has become fertile terrain for geopolitical competition between the great powers and for further penetration by moderate powers.

"Violent conflicts have also become more complex and protracted, involving more non-state groups and regional and international actors" (World Bank and United Nations, 2018, p V). They are increasingly linked to global challenges such as climate change, natural disasters, cyber security, and transnational organized crime (Avis, 2019, p 2). Today, conflicts have become more complex and last longer. About 2 billion people, about a third of the world's population, now live in countries affected by conflict. Violent conflicts are no longer defined by national borders (Schafer, 2018).

The main hypothesis underlying this article is that the security situation in the Sahel region is influenced by several different causes and conflict drivers[1] which have cumulative effects, making conflict resolution extremely difficult. The first part of the article identifies the causes and drivers of conflict and classifies them into four main categories: the environment as a conflict driver; economic conditions as a conflict driver; political conditions as a conflict driver; and historical/ethnic tensions as a conflict driver. In the second part the article shows how the causes and drivers are interwoven, creating multiple spillover effects and making the Sahel region one of the most problematic regions in the world.

The main purpose of this article is to raise an alert about the complex security situation in the Sahel region, and to identify the causes of the conflicts in order to be more effective in resolving them. Gaining deep knowledge of the causes of conflicts is the only way to move towards a potential successful resolution; however, in the case of the Sahel region, several other important factors, such as the spillover effects, must also be taken into consideration. The article is based on an analysis of the existing documents and academic literature on the subject.

[1] *The term 'drivers' is used as it implies the dynamic nature of the factors and processes that contribute to violent conflicts.*

1 THE SAHEL REGION AS THE SPINAL CORD OF THE AFRICAN CONTINENT

The Sahel region represents the spinal cord of the African continent's geopolitical body, and as such the phenomena of its security puzzle pose a real security threat to Africa. In addition, the spillover effects have become a global security nuisance, particularly for the European continent and the European Union. The Sahel security puzzle, a crisis emanating from the old-fashioned political order and risky arrangements of the region, is now not only generating a deeper and wider self-destructive momentum, but is also sending far-reaching shockwaves of hazards which severely affect the entire continental security system, as well as its spillovers affecting the whole globe. Serving as home to more than one-third of Africa's population, the Sahel is the origin of most of Africa's civil wars. The Sahel's geographic scope and the unfortunately violent and volatile realities of its component countries have made it the host of the largest international peacekeeping forces.

The Sahel region stretches from the Indian Ocean and the Red Sea coast in the east to the Atlantic Ocean in the west. With a width of 7,034 km from Mogadishu in Somalia to Dakar in Senegal, the region includes several countries, each with its own security issues and challenges: collapsed Somalia, the small and resource-scarce Djibouti, drought-prone Ethiopia and its archenemy Eritrea, the Islamist hub of ethnically polarized Sudan, and the youngest, distraught nation of South Sudan. The Sahel belt further encompasses potentially explosive Chad, drought-stricken Niger, Burkina Faso, war-torn Mali, resource-cursed Nigeria, poor Togo and Benin, the religiously tense Cote d'Ivoire, little Gambia, and one relatively stable state, Senegal. The remainder of the states in the belt are Mauritania, a target of anti-slavery campaigners, Liberia, Sierra Leone, and the two Guineas (Bissau and Conakry) (Trayo, 2018).

The Sahel can be defined as an ecozone or as a political zone. As an ecozone, the Sahel is a transnational region between the Sahara Desert in the north and the better-watered savanna in the south. As a political zone, it includes the national territories of the previously stated countries. Although each country of the Sahel region has its own security issues, and it can be analysed country by country, there are multiple and spillover effects of the whole Sahel region which present an additional challenge and a potential threat. Not only the unstable political conditions and historically driven hostilities, but also the geographical and natural characteristics of the regions must be taken into consideration when analysing the security situation of the Sahel region. Multiple factors of influence and drivers of potential conflicts in the Sahel region and their spillover effects can be identified: unstable politics, terrorism, foreign debts, environmental degradation, civil wars, food insecurity, mass displacement, porous borders, illegal migration, and drug trafficking (Trayo, 2018).

Cilliers, in his analysis of violent conflicts in Africa, claims that "Africa will remain turbulent because it is poor, young and badly governed, but also because it

is growing and dynamic", and "In the long term only much more rapid, inclusive economic development combined with good governance and developmentally oriented leadership will make Africa less vulnerable to violence and instability" (Cilliers, 2018, p 2). Although Cilliers has analysed violent conflicts on the entire African continent, his findings concerning the causes of conflicts are particularly important when analysing the Sahel region. According to Cilliers (2018), the following structural drivers can be identified*: high levels of poverty and exclusion,*[2] *regime type and regime dissonance,*[3] *youthful population,*[4] *repeat violence,*[5] *the bad-neighbourhood effect,*[6] *poor governance,*[7] *and climate change*[8].

2 CAUSES OF CONFLICTS

As mentioned above, there has been a major shift in the nature of modern conflict, from traditional symmetrical conflicts (as between armies), to increasing numbers of intra-state conflicts and asymmetric wars (as between states and militias). A similar polarization has afflicted academic debate on the root causes of war, to the extent that some strongly oppose the use of the phrase 'root causes' as they see it as inextricably linked to the idea that there is some justifiable grievance behind every outbreak of conflict (Collier, 2007). Whilst some have traditionally focused on these grievance-related drivers of conflict, such as poverty and inequality, another strand of thinking has suggested that the incidence of war is dependent on material interests instead:

---

[2] *Large portions of poor people in a country often correlates with weak state capacity since limited tax revenues accrue to the government, which means that it has limited capacity and human resource capacity is generally low.*

[3] *The nature of regimes (democratic or autocratic, thin/electoral democracy or thick/liberal democracy) affects conflict vulnerability.*

[4] *Large youth bulges are robustly associated with an increased risk of conflict and high rates of criminal violence in poor countries, particularly when young people lack opportunities in terms of education, training and employment and have no sense of voice and participation. However, youth bulges appear to be more closely related to low-intensity conflict than to civil war.*

[5] *Once a country has experienced large-scale violence, the chances of recurring violence are strong. In recent years, the trend towards conflict recurrence has been more common than the onset of new conflicts in the continent.*

[6] *Being situated in a conflict-ridden region is a major risk factor and countries are more likely to experience the spillover effect of instability. According to the World Development Report 2011, a country making development advances, such as Tanzania, loses an estimated 0.7% of GDP every year for each neighbour in conflict.*

[7] *At low levels of income and development, the nature of the governing elite is more important for economic growth and the achievement of positive development outcomes than the extent to which countries are democratic or authoritarian. Hence, countries that are fortunate enough to produce a developmentally oriented governing elite grow much more rapidly, particularly if this is in the form of a cohesive governing party or coterie of leadership that is clear in its pursuit of development.*

[8] *As climate change alters the nature of resource dependence, it may have consequential effects on states with large natural resource benefits. However, eventually people fight based on the mobilization of perceptions of exclusion and injustice. Africa will experience widely different effects from climate change in the coming decades, which will strain the ability of the environment to support local populations under current developmental conditions. Some areas of the continent are likely to become warmer and drier, and thus experience more frequent and severe droughts close to major population centres (e.g. Cape Town). Other parts of the continent may experience widespread drought and potentially famine without proper government intervention, or experience more extreme rains, which could also adversely affect crops and food security.*

"In other words it is greed rather than grievance which creates armed conflict" (Kett and Rowson, 2007, p 403).

Political science offers an account of conflict in terms of motive: rebellion occurs when grievances are sufficiently acute that people want to engage in violent protests. Hirshleifer (1995) provides an important refinement on the motive-opportunity dichotomy; he classifies the possible causes of conflict into preferences, opportunities, and perceptions. The introduction of perceptions allows for the possibility that both opportunities and grievances may be wrongly perceived. If the perceived opportunity for rebellion is illusory—analogous to the 'winners' curse'—unprofitability will cause collapse. By contrast, when exaggerated grievances trigger rebellion, fighting does not dispel the misperception and indeed may generate genuine grievances.

Goodhand (2003) has argued that it is both greed (opportunity for accumulation) and grievance (generated by poverty and social exclusion) that cause and perpetuate violent conflict. He also raises the important point that notions of social and human vulnerability are transient—and it is this very transience that can be a trigger factor for violent conflict. According to this line of argument, someone who has had access to wealth and who then loses it suddenly is more likely to be aggrieved than someone who never had such access in the first place. What this review and many others have shown is that researchers should resist looking for one particular explanation for the incidence of violent conflict: all wars are produced by multiple confluences of deep underlying causes and sudden triggering events (Kett and Rowson, 2007).

2.1 Economic conditions as a conflict driver in the Sahel region

One of the main questions when analysing the causes of conflict is whether poverty causes violent conflicts. Some of the world's poorest countries are riven by armed conflict, such as Liberia, Sierra Leone, Haiti and the Democratic Republic of Congo. "Cross-country comparisons show that conflict-related humanitarian emergencies are prevalent in those places that have experienced low or negative economic growth" (Kett and Rowson, 2007, p 403). The grind of long-term poverty weakens the ability of the state and communities to redistribute wealth in the face of economic grievance, and provokes the rich to grab the assets of the poor (Nafziger and Auvinen, 2003). Violent conflict impacts on the ability of states to function effectively, and they become trapped in a cycle of poverty, conflict and under-development, each exacerbated by the others, which in turn increases vulnerability and impedes economic growth and development.

However, this does not mean that conflicts afflict only the poorest countries, and many poor countries are not at war; shared poverty may not be a destabilizing influence. Indeed, economic growth itself can be a destabilizing factor, as wars in countries afflicted by an abundance of particular natural resources appear to show.

Furthermore, in economic and developmental terms, the World Bank has designated all the Sahel countries, except Nigeria, as "Heavily Indebted Poor Countries"

(Trayo, 2018). This all-round chronic situation is further compounded by the reality that the Sahel region has most of the continent's refugees and internally displaced people[9]. According to the World Bank Poverty Headcount Ratio (The World Bank, 2023), large parts of the Sahelian populations live below 1.90 US dollars a day. Overall, nearly 50% of the population of the region lives in extreme poverty and, consequentially, most countries in the Sahel rank among the lowest on the Human Development Index (UNHCR Climate Risk Profile: Sahel, 2023).

Moreover, the region has become a fertile breeding ground for the seemingly ever-expanding number of radical Islamist militants[10], as well as being conducive to the proliferation of small arms[11] and international drug trafficking[12]. The Sahel region is also the sole major exporter and traditional exit corridor for the largest percentage of Africa's illegal migrants to Europe. This multi-faceted security crisis facing the Sahel region has already spilled past its boundaries and been felt by the region's neighbours, often in terrorism-related events, especially in Kenya, Uganda, the Central African Republic, Cameroon and Ghana: "It is this intricate mosaic formula that constitutes the metabolism of the Sahel security nexus" (Trayo, 2018, p 6).

2.2 The environment and natural resources as a conflict driver

Some of the drivers of conflict are related to climate shocks that cause disputes over resources, from water rights to territory, and these have become a source of instability. In 2022, hurricanes, floods and tropical storms devastated parts of the Caribbean, North America and South Asia, while drought and desertification pushed thousands

[9] *More than 4.2 million people have been displaced across the region (as of 2023); 3.7 million people are internally displaced in the region (as of 2023); and more than 10 million children in the Sahel are in dire need of humanitarian assistance (as of 2022) (UNHCR Climate Risk Profile: Sahel, 2023).*

[10] *According to Africa Centre for Strategic Studies (2022) we can observe a near doubling in violence linked to militant Islamist groups in the Sahel in 2021 (from 1,180 to 2,005 events), which highlights the rapidly escalating security threat in this region. The 2,005 violent events observed in the Sahel (specifically Burkina Faso, Mali, and western Niger) in 2021 represent a 70% increase over the previous year. This continues an uninterrupted escalation of violence involving militant Islamist groups in the region since 2015. While having originated and still largely centred in Mali, the propensity of this violence has now shifted to Burkina Faso, which accounts for 58% of all events in the Sahel.*

[11] *Weapons trafficking in the region benefits violent extremist groups such as al-Shabaab, Ansaroul Islam, Islamic State Sahel Province, Islamic State in Somalia, and Jama'at Nusrat al-Islam wal Muslimeen. Evidence shows that the diversion of weapons from national armed forces – whether through capture on the battlefield, theft from armouries, or purchase from corrupt elements in the military – is the primary source of firearms in the Sahel countries today. Political instability, disputes between farmers and herders, unemployment, ethnic divisions, and the rise of extremist organizations are among the factors driving the spread of small arms and light weapons in the Sahel and West Africa. The rise of violent extremist groups and other armed groups precipitated the demand for small arms and light weapons in the region. While there is evidence of long-range firearms trafficking to the Sahel, including by air from France and from Turkey via Nigeria, it appears that the vast majority of firearms trafficked in the region are procured within Africa. Since 2019, Libya has become a source of supply for newly manufactured weapons. Apparently, newly produced AK-pattern assault rifles, sourced from Libya, are available on the black market in the Gao, Timbuktu and Ménaka regions of northern Mali (TOCTA Sahel, 2022, and The Africa Defence Forum, 2023a).*

[12] *Crime organizations and terrorist groups have woven a complex trafficking network moving illicit goods such as assault-style rifles, ammunition, explosives, drugs and fake medicine throughout the Sahel region. Once used for legitimate trade, the routes cross porous borders in Burkina Faso, Cameroon, Chad, The Gambia, Guinea, Mali, Mauritania, Niger, Nigeria and Senegal (The Africa Defence Forum, 2023b).*

more towards extreme hunger in the Sahel. From the environmental perspective, the Sahel belt is classified as having cyclically hard-hitting environmental degradation records associated with drought, rapidly encroaching desertification, scarce water, and acute food insecurity. The geographical area of the Sahel is generally considered to be highly sensitive to climate change, as the local population is heavily dependent on agriculture and livestock. Recurrent droughts in the 1970s and 1980s caused severe hunger, malnutrition, disease, loss of life and massive human migration across the region (Trench at al., 2007).

Hammer (2005) defines environmental degradation[13] in the Sahel using three groups of factors: ecological, internal and external. Ecological factors refer to natural processes such as rainfall variability, lowering of watercourses and sea levels, limited vegetation, and strong winds and storms. Other factors represent the internal social structure of society, which degrades the environment through its activities. These are, for example, the traditional usage of land, pastoralism, lack of land, wood as the main source of energy, lack of irrigation, population growth, political structure, and lack of young labour due to migration. The third group relates to the external factors that influence the region: the colonial past, national debt, the global economic system, export-based production, and the increased technological gap between Africa and the North (Hammer, 2005).

Rising temperatures and more extreme weather conditions pose existential challenges to semi-arid regions like the Sahel. In the Sahel, agriculture is the most important sector and provides livelihoods for most of the population (UNHCR Climate Risk Profile: Sahel, 2023). Rain-fed agriculture is vulnerable to climate change. Repeated cycles of droughts, desertification and floods make it increasingly difficult for the local population to sustain subsistence agricultural practices. Extreme weather events can lead to widespread crop failure and a reliance on food assistance programmes. Additionally, the impact of climate change is straining the relationship of herders and pastoralists, and thus also ethnic relations. For centuries, pastoralists crossed the Sahel following seasonal patterns, allowing them to feed their herds. The scarcity of water, pasture and fertile soil force people to migrate. Such displacement can lead to conflicts over land and resources between herders and farmers, which in turn further fuel displacement dynamics. Undoubtedly, in the Sahel region climate variability strongly interacts with other conflict drivers and thus can be difficult to distinguish.

2.3 Political conditions and inequalities as a conflict driver

At the heart of the conflicts in the Sahel region is a governance crisis characterized by elected officials' and some customary authorities' low levels of legitimacy; lack of state presence in rural areas; government shortcomings in delivering essential public

[13] *There are many definitions of degradation in scientific circles, but one of the most accepted remains Rasmussen's (1999), which states that degradation is "a reduction in the biological productivity of ecosystems and an acceleration of certain natural processes". Degradation can be caused by loss of biodiversity, soil erosion by water or wind, nutrient depletion and physical soil change. All these processes are interrelated and may be the result of human or climatic factors, which may be reinforced by the degradation effect.*

goods and services; unequal resource access and distribution; and deeply hierarchical customary structures influencing societal relations. These factors prompt segments of the population to turn to alternative actors, including jihadist groups. The latter expand by building local alliances and exploiting local communal conflicts. Such conflicts can revolve around intercommunal tensions or relate to intra-community disputes. Ansarul Islam built traction in Burkina Faso's Sahel region by capitalizing on local discontent at the prevailing social order in Soum province, taking aim at class hierarchy and corruption among customary authorities. Meanwhile, in Mali, following decades of recurrent conflict between Tuareg populations and central governments, continued delays in the implementation of the 2015 Algiers accord remain a source of discord between signatory armed groups and transitional Malian authorities (Armed Conflict Survey, 2022).

In addition to poverty and food insecurity, there are high levels of corruption, which are reflected in the low scores of most Sahelian countries in the Corruption Perceptions Index by Transparency International (UNHCR Climate Risk Profile: Sahel, 2023). Together, these factors render political instability and lack of state capacity common and, accordingly, all the countries in the region score low on the Fragile States Index (Fragile States Index 2023). Chad is especially vulnerable to conflict, followed by Mali, Niger, Cameroon, Nigeria and the Guinea. Increasingly, this vacuum is being filled by jihadist groups, who represent a threat to civilians and governments and exploit the population´s despair and frustration for recruitment. Jihadist groups also interfere in already existing inter-communal conflicts, for instance between the Fulani and the Dogon in Mali, exacerbating tensions and ethnic disputes. After the Libyan regime fell in 2011, armed uprisings in Mali increased armed conflicts which have spiralled into neighbouring countries. This complex crisis has led to massive internal and cross-border displacement of more than 4 million people in the region (UNHCR Climate Risk Profile: Sahel, 2023).

2.4 History as a conflict driver in the Sahel region

In many conflicts in the Sahel region, historical factors must also be highlighted and analysed as conflict drivers.

A study by Bricman (2018) showed that in Niger, Sudan and Mali resource management has been assigned to local leaders throughout history. These traditional resource management systems have undergone significant changes in political systems over the past fifty years, which have attempted to introduce new policies and ideology. "Traditional systems of resource management are still deeply rooted in people[14], so it is not surprising that changes in social systems and the exercise of control over tribal territories create group cohesion, a sense of marginalization and, in many instances, tension between tribes and state actors" (Bricman, 2018, p 73). In addition, the aforementioned countries have a very violent historical background, so it can be argued that the threshold for entering into conflicts is at a low level.

[14] *Especially in communities where people experience tribe as the broadest form of social organization.*

3 DISCUSSION: AN INTERTWINING OF CAUSES CREATING DEADLY CONDITIONS

Analysis of the security situation in the Sahel region is extremely complex due to the large number of actors, causes and drivers having multiple effects, overlapping and influencing each other. It is therefore impossible to identify single causes of conflicts, as each conflict can be analysed from the historical, political, environmental and several other perspectives.

In the cases of Mauritania and Senegal, large-scale ethnic conflict in 1989 between the two countries was triggered by competition for water and pasture[15] (GSDRC, 2014). Hostilities between different groups reached a critical point when a confrontation between farmers and ranchers resulted in casualties. Strong group cohesion created two strategic groups, which entered ethnic conflict due to entrenched racism in society. Ethnic unrest occurred across large areas of both countries, with the worst fighting occurring in the two state capitals. In this case, a dispute over resources was the catalyst for a large-scale ethnic conflict rooted in discrimination (Bricman, 2018).

In the case of the Lake Chad area, water degradation has fuelled competition between groups of farmers and herders, killing up to 2,000 people annually (Nnamdi et al., 2022). "The root of the conflict lies in the forced southern migration, due to drought, of herdsmen from their traditional grazing grounds, mostly in North-East Nigeria. As the lake shrank, large numbers of herders had to search for alternative pastures and sources of water for their cattle leading to encroachment on settlement and farmlands in the North Central and Southern states of Nigeria" (Nnamdi et al., 2022, p 442). Water and land are merely a catalyst for social effects that ultimately lead to conflicts (Bricman, 2018).

In the late 1980s, a diplomatic conflict arose between Niger and Nigeria in the Komadugu-Yobe region. The use of water in the upper watercourses originating from Lake Chad created shortages in the lower reaches of the rivers. The most likely reason why water shortages fuelled violence in one case, and a diplomatic dispute in the other, is the drastic reduction of water in Lake Chad (Hall, 2009). The perception of countries that there is not enough water for their needs is most likely to have created conflict rather than cooperation. In the lake region, the lack of water, land and jobs has also contributed to the spread of Islamic extremists in the south of the lake, who have claimed up to 10,000 lives since 2005. The lack of resources and livelihoods most likely encouraged residents to organize and join violent strategic groups in order to ensure their survival (Bricman, 2018).

Burkina Faso's state institutions estimate that up to 4,000 cases of conflict between farmers and herders have occurred in the country. In Burkina Faso the degradation

[15] *Due to the degradation of both resources by climate change combined with human factors.*

of natural resources, combined with state agrarian policies (which sought to legislate and distribute resource scarcity), created conflicts between herders and pastoralists. Due to the clumsily created agrarian and pastoral zones, the two groups began to compete for the same land, leading to conflicts. In addition to these factors, conflicts also arise between migrants (from urban centres) and indigenous populations (from marginalized zones), who have different views on natural resources (FAO, 2021). Here too, social factors rather than resources directly were responsible for the conflicts (Bricman, 2018).

In Mali, water degradation in the Niger Delta has created conflicts between farmers and pastoralists. According to Malian institutions, 820 cases of conflict between farmers, livestock breeders and fishermen have been recorded in the delta area. The conflicts are the result of competition between different groups for the same land and water. Here, the conflicts arose due to the use of pastoral lands by farmers, which were traditionally owned by livestock farmers. In this case, too, there was group cohesion and the formation of strategic actors, but the situation is complicated by other factors, such as an ill-considered agrarian policy that increasingly marginalizes groups (giving priority to farmers) and a political vacuum that allows the inhabitants of the region to resolve disputes independently. Here, too, the lack of resources fuelled tension between different subsistence groups, which were fundamentally rooted in traditional livelihoods (Bricman, 2018).

Cases in Sudan also testify to the effects of a lack of resources in the emergence of conflicts. Sudan represents the most devastated area in the Sahel, so resources play a significant role in creating conflicts. In Sudan, especially in the Darfur area, up to 51 large-scale conflicts between different ethnic groups related to natural resources have developed in the past (UCDP, 2023). Competition for limited resources and different livelihoods create a sense of marginalization and promote group cohesion. This leads to the formation of strategic actors who are ready to use violence. The causes of marginalization are rooted mainly in the traditional management of resources (some groups dominate and manage the resources of other groups) and different livelihoods (farmers and livestock breeders). In addition to the direct competition for limited resources (degraded by droughts, war and other factors), it is also necessary to mention the Sudanese agrarian policy, which, due to the privileging of certain groups (mainly stationary farmers), has further triggered the marginalization of groups. Farmers in some areas of Sudan enjoy privileges, so other groups feel marginalized, which causes tension and conflict. Thus, since 1988, nearly 15,000 people have been killed in Sudan (including Darfur and South Sudan) due to conflicts that have an environmental dimension. In addition, for many years Sudan has been involved in an interstate conflict with South Sudan, and in conflicts taking place for power in the country. These conflicts do not have an environmental dimension, yet they create a socio-political environment that multiplies the effects of conflicts at the local level (degradation of the environment, weak political institutions, quantity of weapons) (Bricman, 2018).

In Niger, too, conflicts are linked to a lack of water and arable land, and to two ways of making a living. In Niger, conflicts arise due to the expansion of farmers into the pastoral areas of livestock farmers. This creates tensions between the two livelihood groups, fosters group cohesion, forms strategic actors, and triggers conflict. Another type of conflict occurs between migrants and the indigenous population of Niger. The indigenous population blames the migrants for the degradation of resources, and this creates intergroup tensions leading to conflict (Bricman, 2018).

In addition to internal causes and conflicts, external factors influencing the security situation in the Sahel region also appear. The Sahel region is greatly dependent on food imports and is disproportionately affected by the global food crisis triggered by Russia's invasion of Ukraine. Heightened food insecurity could prompt further displacement, raise poverty rates, and aggravate competition for resources, leading to worsening intercommunal conflict and social unrest. Besides this, the Sahel region has become a playground for world powers. "At the beginning of 2022 the Sahel (and Mali in particular) increasingly became a battlefield for informational warfare waged on social media, with France and Russia "fighting" for political influence in the region. In February 2022, reports emerged that a network of Facebook pages in Mali promoting pro-Russian and anti-French narratives had coordinated support for the Wagner Group and the junta's postponement of elections" (Armed Conflict Survey, 2022). In April 2022, France accused Russian private military contractors of staging a war crime in Mali in an attempt to frame French forces. As a consequence, France has decided to pull French troops out of Mali after nine years, leaving open space for others to step in and take over, adding more tensions and complexities to already a very difficult and complex security situation in the region.

Conclusion

In conclusion, it can be seen that the Sahel region is facing a complex security situation fuelled by several different causes and conflict drivers. These drivers are interwoven, creating multiple and spillover effects and making conflict resolution extremely difficult. The internationalization of internal armed conflicts, including civil wars, has only added to the complexity of the situation. It is crucial to identify the root causes of conflicts in the Sahel region and take effective measures to resolve them. The spillover effects of the Sahel's security puzzle not only pose a real security threat to Africa, but also affect the whole world, making it a global security nuisance. The Sahel region is the spinal cord of the African continent's geopolitical body, and its stability and security are essential for the overall security of Africa and the world.

References

1. *Africa Centre for Strategic Studies, 2022. Surge in Militant Islamist Violence in the Sahel Dominates Africa's Fight against Extremists. Available at: https://africacenter.org/spotlight/mig2022-01-surge-militant-islamist-violence-sahel-dominates-africa-fight-extremists/ (Accessed: 10 November 2023).*
2. *Africa Defence Forum, 2023a. Instability Drives Proliferation of Small Arms, Light Weapons in Sahel Region. Available at: https://adf-magazine.com/2023/11/instability-drives-proliferation-of-small-arms-light-weapons-in-sahel-region/ (Accessed: 10 November 2023).*
3. *Africa Defence Forum, 2023b. Ancient Sahel Trade Routes Used to Traffic Illegal Weapons, Drugs. Available at: https://adf-magazine.com/2023/06/ancient-sahel-trade-routes--used-to-traffic-illegal-weapons-drugs/ (Accessed: 10 November 2023).*
4. *Avis, W. R., 2019. Current Trends in Violent Conflict. K4D Helpdesk Reports. Available at: https://assets.publishing.service.gov.uk/media/5cf669ace5274a07692466db/565_Trends_in_Violent_Conflict.pdf (Accessed: 12 November 2023).*
5. *Armed Conflict Survey, 2022. Sub-Saharan Africa. Armed Conflict Survey, 8(1), pp 200-321, DOI: 10.1080/23740973.2022.2135793.*
6. *Bricman, U., 2018. Podnebne spremembe, degradacija okolja in konflikti v Sahelu (Climate change, environmental degradation and conflicts in the Sahel), Fakulteta za družbene vede.*
7. *Cilliers, J., 2018. Violence in Africa: Trends, Drivers and Prospects to 2023. Africa Report 12, 30 August 2018, Available at SSRN: https://ssrn.com/abstract=3254122 (Accessed: 5 November 2023).*
8. *Collier, P., 2007. Ethnic Civil Wars: Securing the Post-Conflict Peace. Harvard International Review 28, pp 56-60*
9. *Collier, P., and Hoeffler, A., 2004. Greed and Grievance in Civil War. Oxford Economic Papers 56, pp 563-95.*
10. *FAO, 2021. Burkina Faso: Analysis of Conflicts over the Exploitation of Natural Resources. Available at: https://www.fao.org/3/cb6023en/cb6023en.pdf (Accessed: 5 November 2023).*
11. *Fragile States Index, 2023. Fragile States Index. Available at: https://fragilestatesindex.org/ (Accessed: 10 November 2023).*
12. *GSDRC, 2014. Conflict Analysis of Mauritania. Available at: https://gsdrc.org/wp-content/uploads/2015/07/GSDRC_ConflAnal_Mauritania.pdf (Accessed: 5 November 2023).*
13. *Goodhand, J., 2003. Enduring disorder and persistent poverty: a review of the linkages between war and chronic poverty. World Dev 31, pp 629-646.*
14. *Hammer, T., 2005. Sahel – Geographische Strukturen, Entwicklungen, Probleme. Stuttgart: Klett-Perthes Verlag.*
15. *Hall, E. L., 2009. Conflict for Resources: Water in the Lake Chad Basin. Available at: https://apps.dtic.mil/sti/pdfs/ADA505231.pdf (Accessed: 15 November 2023).*
16. *Hirshleifer, J., 1995. Theorizing about Conflict. In K. Hartley and T. Sandler (Eds),*
17. *Handbook of Defense Economics, Vol. 1, Elsevier Science, Amsterdam, pp 165-89.*
18. *Kett, M., and Rowson, M., 2007. Drivers of Violent Conflict. Journal of the Royal Society of Medicine, 100(9), pp 403-406, DOI: 10.1177/014107680710000912.*
19. *Nafziger, E. W., and Auvinen, J., 2003. Economic Development, Inequality and War: Humanitarian Emergencies in Developing Countries. Basingstoke, UK: Palgrave Macmillan.*
20. *Nnamdi, K. D., Duhu, J. O., and Ngwu, E. C. 2022. Rethinking the Lake Chad Herder--Farmer Conflicts and Food Security in Nigeria. University of Nigeria Journal of Political Economy, 12(2), pp 439-451.*
21. *Rasmussen, K., 1999. Land degradation in the Sahel-Sudan: the conceptual basis. In Geografisk Tidsskrift, Bind si02. Available at: https://tidsskrift.dk/geografisktidsskrift/article/view/42468/49399 (Accessed: 15 November 2023).*

22. *Schafer, H., 2018. The drivers of conflict: where climate, gender and infrastructure intersect. Available at: https://blogs.worldbank.org/dev4peace/drivers-conflict-where-climate--gender-and-infrastructure-intersect (Accessed: 20 October 2023).*
23. *Trayo, A., 2018. Mitigating the Sahel Security Conundrum: The Need for a Strategic Paradigm Shift. Africa Policy Journal, 13, pp 3-13.*
24. *Trench, P., Rowley, J., Diarra, M., Sano, F., and Keita, B., 2007. Beyond any drought: root causes of chronic vulnerability in the Sahel. The Sahel Working Group. Available at: https://www.iied.org/sites/default/files/pdfs/migrate/G02317.pdf (Accessed: 20 October 2023).*
25. *TOCTA Sahel, 2022. Firearms Trafficking in the Sahel. Transnational Organized Crime Threat Assessment — Sahe. Available at: https://www.unodc.org/documents/data-and-analysis/tocta_sahel/TOCTA_Sahel_firearms_2023.pdf (Accessed: 20 October 2023).*
26. *The World Bank, 2023. Poverty Headcount Ratio. Available at: https://data.worldbank.org/indicator/SI.POV.DDAY (Accessed: 15 November 2023).*
27. *UNHCR Climate Risk Profile: Sahel, 2023. Available at: https://www.unhcr.org/fr-fr/en/media/representative-concentration-pathways-climate-risk-profile-sahel-region (Accessed: 20 October 2023).*
28. *UCDP, 2023. Uppsala Conflict Data Program. Available at: https://ucdp.uu.se/ (Accessed: 15 October 2023).*
29. *World Bank and United Nations, 2018. Pathways for Peace: Inclusive Approaches to Preventing Violent Conflict, Main Messages and Emerging Policy Directions. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/28337/211162mm.pdf?-sequence=2&isAllowed=y (Accessed: 3 November 2023).*

email: jelena.juvan@fdv.uni-lj.si

ORCID: 0000-0002-1479-1566

sciendo

Sodobni vojaški izzivi, 2024 – 26/št. 2
Contemporary Military Challenges, 2024 – 26/No. 2

Klemen Kocjančič

DOI: 10.2478/cmc-2024-0014

RECENZIJA

O POTREBI DELITVE BREMENA V NATU

Leta 2022 je mednarodna založba Palgrave Macmillan izdala monografijo dveh finskih raziskovalcev (Tommija Koivule in Helje Ossa) s Finske nacionalne obrambne univerze z naslovom *NATO's Burden-Sharing Disputes. Past, Present and Future Prospects* (Spori o delitvi bremena v Natu. Zgodovinske, trenutne in bodoče priložnosti).

V prvem poglavju avtorja uvodoma izpostavita pomen 3. člena Washingtonske (Severnoatlantske) pogodbe iz leta 1949: »Za učinkovitejše doseganje ciljev te pogodbe bodo pogodbenice z nenehno in učinkovito samopomočjo ter vzajemno pomočjo vsaka zase in skupaj vzdrževale in razvijale svojo individualno in kolektivno sposobnost upreti se oboroženemu napadu.« Prav različno razumevanje fraz »z nenehno in učinkovito samopomočjo« ter »vzajemno pomočjo« povzroča probleme pri razumevanju potreb po delitvi bremena znotraj severnoatlantskega zavezništva (str. 2).

Drugo poglavje navaja, da so se članice zavezništva že leta 2006 (in ponovno leta 2014) dogovorile o potrebi po zagotovitvi najmanj dvoodstotnega deleža bruto državnega proizvoda (BDP) za potrebe obrambe, pri čemer bo dvajset odstotkov obrambnega proračuna namenjenih za večje nakupe opreme oz. oborožitve. Glede tega pa se znotraj zavezništva uporabljajo različni pristopi: od racionalističnega in post-pozitivističnega do kombinacije pozitivističnega in post-pozitivističnega pristopa. Avtorja ugotavljata, da so javne (politične) razprave glede finančnega vložka za potrebe Nata ciklične narave in se po navadi nanašajo na štiri dejavnike: geopolitične spremembe glede Rusije, ameriško zunanjo politiko (intervencionizem ali izolacionizem), evropsko dejavnost (aktivnost ali pasivnost) ter večje operacije zveze Nato zunaj držav članic (str. 28).

Tretje poglavje se ukvarja z zgodovinskim vprašanjem delitve bremen znotraj zavezništva, in sicer vse od ustanovitve v času hladne vojne. Neposredno po ustanovitvi so se države članice dogovorile, da se »vsaka država članica mora specializirati v silah in orožju, ki jim bodo najbolj koristili in ki bodo lahko vključeni v integrirane obrambne načrte« (str. 37). Med korejsko vojno so ZDA povečale obrambni proračun, čemur so sledile tudi nekatere evropske države članice. A kmalu se je izkazalo, da lahko Sovjetska zveza mobilizira večje konvencionalne sile kot celotna zveza Nato, zato so se odločili za strategijo prožnega odziva, kar se je pokazalo predvsem v razvoju jedrskega orožja. V 60. letih 20. stoletja so evropske države članice dosegle stopnjo razvoja, ki je označevala dokončno izboljšanje gospodarskega stanja po koncu druge svetovne vojne, kar je pomenilo, da bi lahko povečale lastne obrambne proračune. Kljub temu se je izkazalo, da evropske države članice ne morejo vzpostaviti prave protiuteži pomenu in vlogi ameriškega hegemona; eno od spornih vprašanj je bilo tudi (ponovno) nemško oboroževanje.

Konec hladne vojne je odprl novo poglavje v zgodovini zveze, saj sta primarna vojaška in ideološka nasprotnika – Varšavski pakt in Sovjetska zveza – prenehala obstajati. Zaradi tega so se pojavili pozivi k ukinitvi Nata (kot nepotrebnega relikta končane hladne vojne) oz. preusmeritvi pozornosti, kar se je dejansko zgodilo, saj je zveza Nato postala krizni upravitelj sveta. Posledično so začeli izvajati operacije zunaj teritorialnih področij držav članic, kar se je pokazalo predvsem po terorističnih napadih septembra 2001, ko so oborožene sile zveze Nato začele delovati na Bližnjem vzhodu, v Aziji in Afriki. Sočasno je Ruska federacija preživljala obdobja zmanjševanja in povečanja obrambnega proračuna, hkrati pa je pomembno zunanjepolitično vprašanje postalo približevanje nekdanjih držav članic Varšavskega pakta svojemu nekdanjemu nasprotniku – zvezi Nato. To se je dejansko zgodilo leta 1999, ko so Češka, Poljska in Madžarska postale nove članice. Že pred tem– med vojnami v nekdanji Jugoslaviji – se je izkazalo, da bodo morale evropske države članice Nata izboljšati lastne vojaške zmogljivosti za posredovanje v lastni soseščini: »Novo varnostno okolje v 90. letih 20. stoletja je prineslo priložnost za razvoj skupnih evropskih obrambnih politik in sodelovanja ter za premislek o evropski in transatlantski varnostni arhitekturi« (str. 89). Kljub temu so evropske države začele zmanjševati obrambne proračune, kar je vodilo k že omenjeni deklaraciji iz Rige leta 2006, s katero naj bi se zmanjšal razkorak v zmogljivostih med Evropo in ZDA.

Peto poglavje obravnava prelomno leto 2014; tega leta se je končala Natova misija v Afganistanu, hkrati pa je Rusija zasedla Krim in donbaško regijo v vzhodni Ukrajini: »Aneksija je bila na splošno razumljena kot prelomna točka v evropski varnosti, ki je ustvarila globok prelom med Rusijo in Zahodom ter ogrozila varnostni red, ki je bil ustvarjen v več kot dvajset letih« (str. 115). Posledično je bilo na zasedanju zveze Nato v Walesu ponovno odprto vprašanje o potrebi po zagotovitvi dvoodstotnega deleža BDP za obrambne proračune. K temu so se takrat zavezale vse evropske članice, prav tako k vlaganju dvajsetih odstotkov obrambnega proračuna v raziskave in razvoj. Medtem ko so večje države (npr. Nemčija) takim zavezam nasprotovale (v smislu, da je kakovost sil pomembnejša od številčnosti oz. obsega

obrambnega proračuna), so predvsem vzhodno- in srednjeevropske države članice začele povečevati vlaganja v lastno obrambo. Poleg ukrajinske krize (ter vzpona Rusije na njihovih mejah) je bilo povečanje obrambnih proračunov tudi posledica izboljšanja splošne gospodarske klime po svetovni gospodarski krizi. V tem času se je pokazala tudi potreba po izboljšanju vojaških (in nevojaških) zmogljivosti na področjih nekinetičnega delovanja – predvsem zaradi grožnje elementov hibridnega delovanja (npr. kibernetičnih napadov). Znotraj Evrope so se sočasno razvili trije različni pristopi: krepitev lastnih sil (vzhodni blok), prizadevanje k oblikovanju skupne varnostne politike (Francija) in izolacionistični pristop (Združeno kraljestvo, Danska).

Naslednje poglavje prinaša pregled zgodovinskih dinamik deljenja bremen znotraj Nata. V času hladne vojne so se evropske države primarno integrirale na gospodarskem področju, medtem ko na obrambnem področju niso dosegle večjega napredka. Odhod Francije iz Natove vojaške strukture leta 1967 je ta prizadevanja še dodatno zavrl. Pokazalo se je tudi različno razumevanje zagotavljanja varnosti: ZDA so nanj gledale globalno, medtem ko so evropske države varnostno politiko razumele kot nacionalno vprašanje. ZDA so nenehno večale obrambni proračun zaradi globalnega konflikta proti komunizmu, medtem ko so evropske države to storile le v primerih kriznih razmer v Evropi (npr. po praški pomladi leta 1968). Hkrati so hotele ZDA zapustiti evropsko celino in prepustiti obrambo evropskim zaveznicam, pri tem pa še vedno ohraniti svoj (vojaški in politični) vpliv. Po koncu hladne vojne so se odnosi med Natom in Rusijo sprva izboljšali, nato pa znova ohladili, ko so se Natu začele približevati nekdanje članice Varšavskega pakta. Odnosi so se ponovno izboljšali po septembrskih napadih leta 2001, ko so ZDA preusmerile pozornost z Evrope na Bližnji vzhod in Azijo. Tudi vzpon Kitajske je spremenil geopolitične usmeritve ameriške zunanje politike. Vendar je to izkoristila tudi Rusija, ko se je leta 2014 odločila zasesti vzhod Ukrajine, pri čemer je računala na mlačen odgovor Zahoda (predvsem v obliki gospodarskih sankcij), kar se je dejansko zgodilo. Kljub temu je ruska agresija predvsem vzhodnoevropske države spodbudila k povečanju obrambnih vlaganj, hkrati pa je zveza Nato okrepila svojo (mednarodno) prisotnost na vzhodu z mednarodno operacijo Okrepljena prednja prisotnost (Enhanced Forward Presence oz. EFP). Avtorja na koncu izpostavljata, da se zveza Nato nenehno sooča s kompleksno problematiko pri razumevanju pristopa k nacionalnim in mednarodnim varnostnim zavezam.

Zadnje, sedmo poglavje je usmerjeno v prihodnost. Pri tem avtorja ugotavljata, da bodo v prihodnosti na problematiko delitve bremen znotraj zveze Nato vplivali naslednji elementi: dejavnosti Rusije v mednarodnem okolju (še posebej glede (ne) posrednega ogrožanja vzhodnoevropskih članic zveze Nato, ki jih razume kot lastno interesno območje); geopolitično ravnanje ZDA (ali se bo nadaljevalo zmanjševanje ameriške navzočnosti na evropski celini ali bo prišlo do zasuka); evropski odziv na ameriško ravnanje (če pride do umika, bo nedvomno sledilo povečanje vlaganj v lastne zmogljivosti); ter skupno delovanje zveze Nato v drugih državah. Pri zadnji točki se je že zdaj pokazalo, da so nekatere države zagotovile neprimerno večji obseg sil za

operacije EFP kot druge, ki so ponudile malo ali dejansko nič za okrepitev Natove prisotnosti na vzhodu Evrope. Pomemben vpliv bo nedvomno imel tudi tehnološki napredek, tako na vojaškem kot na civilnem področju. Nadalje avtorja ponudita štiri možne scenarije: onesposobljeni Nato (države bodo zavračale povečanje sredstev za Nato ter izpolnjevanje skupnih zavez, kar bo na koncu pripeljalo do zmanjšanja vojaške moči zavezništva); transatlantsko pogajanje (države bodo zagotavljale določeno stopnjo sredstev, a večjega napredka pri povečanju zmogljivosti ne bo); države članice, ki zasledujejo lastne interese (države bodo povečale obrambne proračune, vendar bodo skrbele predvsem za izboljšanje lastnih zmogljivosti); in transatlantska solidarnost (države bodo poskrbele za izboljšanje zmogljivosti tako lastnih oboroženih sil kot tudi celotnega zavezništva). Avtorja sta se odzvala tudi na možnost razpada Nata zaradi problematike delitve bremen: »Razprava je tesno povezana z drugimi težavami, kot so težave z zaupanjem med zavezniki in različno dojemanje groženj, kar lahko resno ogrozi Natovo sposobnost, da preživi prihodnje krize« (str. 190).

Avtorja v obravnavanem delu z opisom zgodovinskih, političnih in varnostnih dogodkov nazorno prikažeta razvoj problematike finančnega vlaganja držav članic zveze Nato v izgradnjo lastnih zmogljivosti in za potrebe delovanje celotne zveze. Pri tem pokažeta na razkol predvsem med ZDA in evropskimi članicami, ki je posledica več različnih dejavnikov, od notranjepolitičnih in gospodarskih do dejavnosti tretjih držav ali nedržavnih akterjev. Dotična monografija je priporočeno branje za vse raziskovalce zveze Nato, mednarodnih odnosov in (mednarodne) varnosti.

Klemen Kocjančič

DOI: 10.2478/cmc-2024-0015

REVIEW

ON THE NEED FOR BURDEN SHARING IN NATO

In 2022, Palgrave Macmillan published a monograph by two Finnish researchers (Tommi Koivula and Heljä Ossa) from the Finnish National Defence University, entitled "NATO's Burden-Sharing Disputes: Past, Present and Future Prospects".

The authors begin the first chapter by highlighting the importance of Article 3 of the 1949 Washington (North Atlantic) Treaty: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." It is the different interpretations of the phrases "continuous and effective self-help" and "mutual aid" which create problems in understanding the burden-sharing needs within the North Atlantic Alliance (p 2).

The second chapter states that the members of the Alliance agreed in 2006 (and again in 2014) on the need to allocate at least 2% of Gross Domestic Product (GDP) to defence, with 20% of the defence budget to be allocated to major equipment or armaments purchases. In this respect, however, different approaches have been taken within the Alliance, ranging from the rationalist and the post-positivist to a combination of positivist and post-positivist approaches. The authors note that public (political) debates about the financial input for NATO purposes are cyclical in nature, usually referring to four factors: the geopolitical changes with regard to Russia; US foreign policy (interventionism or isolationism); European activity (activism or passivity); and major NATO operations outside its member states (p 28).

The third chapter deals with the historical issue of burden-sharing within the Alliance, starting with its creation during the Cold War. Immediately after its establishment, the member states agreed that "each member state should specialise in the forces and weapons that served them best and could also be included in the integrated defence patterns" (p 37). During the Korean War, the US increased its defence budget, and

some European member states followed suit. But it soon became clear that the Soviet Union could mobilize a larger conventional force than the entire NATO Alliance, leading to a decision to adopt a strategy of flexible response, as seen in particular in the development of nuclear weapons. In the 1960s, the European member states reached a stage of development which marked a definitive improvement in their economic situation since the end of the Second World War, which meant that they could increase their own defence budgets. Nevertheless, European member states proved unable to establish a real counterweight to the importance and role of the American hegemon; one of the contentious issues was the (re)armament of Germany.

The end of the Cold War opened a new chapter in the history of the Alliance, as the primary military as well as ideological opponents – the Warsaw Pact and the Soviet Union – ceased to exist. This led to calls for the abolition of NATO (as an unnecessary relic of the end of the Cold War) or a refocusing of attention, which indeed happened, as NATO became the world's crisis manager. As a consequence, operations began to be carried out outside member states' territories, as was particularly evident after the terrorist attacks of September 2001, when NATO forces began to operate in the Middle East, Asia and Africa. At the same time as the Russian Federation was going through periods of cuts and increases in its defence budget, the possibility of rapprochement of the former Warsaw Pact member states with their former adversary, NATO, became an important foreign policy issue. This actually happened in 1999, when the Czech Republic, Poland and Hungary became new members. It had already become clear – during the wars in the former Yugoslavia – that European NATO member states would have to improve their own military capabilities to intervene in their own neighbourhood. The new security environment in Europe in the 1990s was among the most dangerous in the world at the time. Nevertheless, European countries began to cut their defence budgets, leading to the Riga Declaration of 2006, which was supposed to narrow the capabilities gap between Europe and the US.

Chapter 5 deals with the watershed year of 2014, which saw the end of the NATO mission in Afghanistan, and Russia's occupation of Crimea and the Donbas region in eastern Ukraine: "The annexation has been viewed widely as a tipping point in European security, creating a deep rift between Russia and the West and upending the security order that had been built for more than 20 years" (p 115). As a result, the NATO summit in Wales reopened the issue of the need to secure a 2% share of GDP for defence budgets. All the European member states committed to this at the time, as well as to investing 20% of their defence budgets in research and development. While the larger states (e.g. Germany) were opposed to such commitments (claiming that the quality of the forces was more important than the quantity or size of the defence budget), the Eastern and Central European member states, in particular, began to increase investment in their own defence. In addition to the Ukraine crisis (and the rise of Russia on their borders), the increase in defence budgets was also a consequence of the improvement in the general economic climate following the global economic crisis. At the same time, the need to improve military (and non-military) capabilities in non-kinetic areas of action – particularly in the face of hybrid

threats (e.g. cyber-attacks) – also emerged. Three different approaches developed simultaneously within Europe: the strengthening of own forces (the Eastern bloc), the pursuit of a common security policy (France), and an isolationist approach (UK, Denmark).

The next chapter provides an overview of the historical dynamics of burden-sharing within NATO. During the Cold War, European countries primarily integrated in the economic sphere, while they did not make much progress in the field of defence. France's departure from the NATO military structure in 1967 was a further setback to such efforts. In addition, different perceptions of security provision emerged: while the US took a global view, European countries considered security policy a national issue. The US continuously increased its defence budget in the face of the global conflict against communism, while European countries did so only in the event of a crisis in Europe (e.g. after the Prague Spring of 1968). At the same time, the US wanted to leave the European continent, abandoning its defence to the European allies, while still maintaining its (military and political) influence. After the end of the Cold War, relations between NATO and Russia initially improved, only to be cooled again as former Warsaw Pact members began to move closer to NATO. Relations improved again after the September 2001 attacks, when the US turned its attention away from Europe to the Middle East and Asia. The rise of China also changed the geopolitical orientations of US foreign policy. However, Russia also took advantage of this, deciding to occupy eastern Ukraine in 2014 while counting on a lukewarm response from the West (mainly in the form of economic sanctions), which indeed came about. Nevertheless, this Russian aggression brought Eastern European countries, in particular, to increase their defence investments, while NATO strengthened its (international) presence in the East through the international operation Enhanced Forward Presence (EFP). The authors conclude by pointing out that NATO is constantly confronted with a complex problem in interpreting the approach to national and international security commitments.

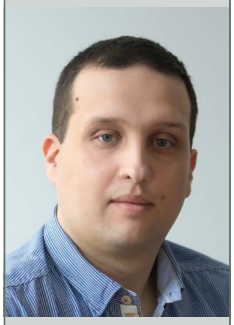
The final, seventh chapter is forward-looking. In it, the authors conclude that the following elements will influence the future of burden-sharing within NATO: Russia's activities in the international environment (especially with regard to (in) indirectly threatening Eastern European NATO members, which it considers its own area of interest); the geopolitical behaviour of the US (whether the reduction of the US presence on the European continent will continue or reverse); the European response to US behaviour (a withdrawal would undoubtedly cause an increase in investment in its own capabilities); and NATO's collective action in other countries. With regard to the latter, it has already become clear that some countries have provided a disproportionately larger force for EFP operations than others, which have offered little or nothing to reinforce NATO's presence in Eastern Europe. Technological advances, both military and civilian, will undoubtedly also have an important impact. The authors go on to offer four possible scenarios: a disempowered NATO (countries will refuse to increase funding for NATO and to meet common commitments, ultimately leading to a reduction in the military strength

of the Alliance); a transatlantic negotiation (countries will provide a certain level of funding, but there will be no significant progress towards increasing capabilities); self-interested member states (countries will increase their defence budgets but will primarily focus on improving their own capabilities); and transatlantic solidarity (countries will focus on improving the capabilities of their own armed forces as well as those of the Alliance as a whole). The authors also respond to the possibility of NATO's disintegration due to burden-sharing issues: "The debate is closely linked to other problems, such as trust issues among allies and diverse threat perceptions, which can severely damage NATO's ability to survive future crisis." (p 190)

In this work, the authors illustrate the evolution of the issue of financial investment by NATO member states in building their own capabilities, as well as the capabilities of the Alliance as a whole, by presenting historical, political and security developments. In doing so, they illustrate the divide between the US and the European members, in particular, which is the result of a number of factors ranging from domestic policy and the economy to the activities of third countries or non-state actors. This book is recommended reading for all scholars of NATO, international relations and (international) security.

Avtorji

Authors



Klemen Kocjančič

Dr. Klemen Kocjančič je po izobrazbi univerzitetni diplomirani teolog, magister obramboslovja in doktor zgodovine. Zaposlen je kot podsekretar za vojaško tehnologijo, raziskave in razvoj na Ministrstvu za obrambo RS in je habilitiran kot znanstveni sodelavec na Obramboslovnem raziskovalnem centru (Fakulteta za družbene vede, Univerza v Ljubljani). Njegovi raziskovalni interesi so s področij vojaške zgodovine, ekstremizma in terorizma, vojaške sociologije in kritične infrastrukture.

Klemen Kocjančič, PhD, *holds a bachelor's degree in theology, MA in defence studies, and a PhD in history. He works as undersecretary for military technology, research and development at the Ministry of Defence of the Republic of Slovenia and is habilitated as a research fellow at the Defence Research Centre (Faculty of Social Sciences, University of Ljubljana). His research interests are in the fields of military history, extremism and terrorism, military sociology, and critical infrastructure.*

Lawrence E. Cline

Dr. Lawrence E. Cline je magistriral iz mednarodnih odnosov in doktoriral iz političnih ved. Je urednik recenzij knjig pri reviji Small Wars & Insurgencies, pred tem pa je poučeval obveščevalno analitiko na Državni univerzi v Buffalu. Je upokojen vojaški obveščevalni častnik ameriške kopenske vojske in častnik za bližnjevzhodno območje, ki je deloval v Libanonu, Salvadorju, operaciji Puščavski vihar, Somaliji in Iraku. Raziskovalno se ukvarja z neregularnim vojskovanjem, terorizmom in obveščevalno dejavnostjo.

Lawrence E. Cline, PhD, *holds an MA in international relations and a PhD in political science. He is the Book Review Editor at the journal Small Wars & Insurgencies and previously taught intelligence analysis at Buffalo State University. He is a retired US Army Military Intelligence officer and Middle East Foreign Area Officer, with operational service in Lebanon, El Salvador, Desert Storm, Somalia, and Iraq. His research interests are in irregular warfare, terrorism, and intelligence.*

Urban Praprotnik

Urban Praprotnik je po izobrazbi magister prava. Tekom študija je uspešno zastopal Univerzo v Ljubljani na tekmovanjih v poznavanju mednarodnega prava, pripravništvo pa je opravil na Stalnem predstavništvu Republike Slovenije pri OZN, OVSE in drugih mednarodnih organizacijah na Dunaju. Zaposlen je kot pravni svetovalec v Slovenski vojski, ki jo predstavlja tudi v slovenski Stalni koordinacijski skupini za mednarodno humanitarno pravo. Njegovi interesi vključujejo zlasti poučevanje mednarodnega prava z inovativnimi metodami ter kibernetsko pravo.

Urban Praprotnik *holds a Master's degree in Law. During his studies, he successfully represented the University of Ljubljana in international legal competitions and completed an internship at the Slovenian Permanent Representation to the UN, OSCE and other International Organisations in Vienna. He is a legal advisor to the Slovenian Armed Forces, which he also represents in Slovenian Permanent Coordination Group for International Humanitarian Law. His particular interests include teaching international law using innovative methods, as well as cyber law.*

Guillermo López-Rodríguez

Dr. Guillermo López-Rodríguez je zaposlen kot profesor političnih znanosti na Univerzi v Granadi (Španija). Doktoriral je iz političnih ved s specializacijo iz vojaških študij (2023), diplomiral iz političnih ved (2017) in magistriral iz javnega upravljanja (2018). Leta 2018 je delal kot raziskovalec za Poveljstvo za usposabljanje in doktrino Španske vojske pri pripravi doktrinarnega dokumenta »Prihodnje kopensko operativno okolje 2035«.

Guillermo López-Rodríguez, PhD, *works as a Professor in Political Science in the University of Granada (Spain). He holds a PhD in Political Science specializing in Military Studies (2023), a BA in Political Science (2017) and an MA in Public Management (2018). In 2018 he worked as a researcher for the Training and Doctrine Command of the Spanish Army to develop the doctrinal document »Future Land Operating Environment 2035«.*

Daniel Montoya-Roldan

Daniel Montoya-Roldan ima srednjo tehnično izobrazbo iz mikroinformatike in omrežij (2019). Na Univerzi v Granadi je študent dodiplomskega študija političnih ved in javne uprave. Njegove raziskave so osredotočene na mednarodno varnost in obrambne politike s poudarkom na uporabi brezpilotnih zrakoplovov in vojaških inovacijah.

Daniel Montoya-Roldan *holds a technical medium-degree in Micro-informatics and Networks (2019). He is studying for a Bachelor's degree in Political Science and Public Administration in the University of Granada. His research is focused on international security and defence policies, specializing in the use of unmanned aerial vehicles and military innovation.*

Jelena Juvan

Doc. dr. Jelena Juvan je predavateljica in raziskovalka na Katedri za obramboslovje in Obramboslovnem raziskovalne centru Fakultete za družbene vede Univerze v Ljubljani. Je predavateljica pri predmetih Varnostna in obrambna politika EU, Strokovna praksa, Varnost v informacijski družbi, Obrambni in varnostni sistem in Kibernetska varnost. Je predstojnica Katedre za obramboslovje in Oddelka za politologijo in podpredsednica Evroatlantskega sveta Slovenije.

Asis. Prof. Jelena Juvan, PhD, *is a lecturer and senior research fellow at the Chair of Defence Studies and Defence Research Centre at the Faculty of Social Sciences, University of Ljubljana. She is a lecturer in courses EU Security and Defence Policy, Professional Practice, Security in the Information Society, Defence and Security System and Cyber Security. She is the head of the Chair of Defence Studies and Department of Political Science and the vice-president of the Euro Atlantic Council of Slovenia.*

Navodila za avtorje

Instructions to authors

NAVODILA ZA AVTORJE

Vsebinska navodila

Splošno

Sodobni vojaški izzivi je interdisciplinarna znanstveno-strokovna publikacija, ki objavlja prispevke o aktualnih temah, raziskavah, znanstvenih in strokovnih razpravah, tehničnih ali družboslovnih analizah z varnostnega, obrambnega in vojaškega področja ter recenzije znanstvenih in strokovnih monografij (prikaz knjige).

Vsebina

Objavljamo prispevke v slovenskem jeziku s povzetki, prevedenimi v angleški jezik, in po odločitvi uredniškega odbora prispevke v angleškem jeziku s povzetki, prevedenimi v slovenski jezik.
Objavljamo prispevke, ki še niso bili objavljeni ali poslani v objavo drugi reviji. Pisec je odgovoren za vse morebitne kršitve avtorskih pravic. Če je bil prispevek že natisnjen drugje, poslan v objavo ali predstavljen na strokovni konferenci, naj to avtor sporoči uredniku in pridobi soglasje založnika (če je treba) ter navede razloge za ponovno objavo.
Objava prispevka je brezplačna.

Tehnična navodila

Omejitve dolžine prispevkov

Prispevki naj obsegajo 16 strani oziroma 30.000 znakov s presledki (avtorska pola), izjemoma najmanj 8 strani oziroma 15.000 znakov ali največ 24 strani oziroma 45.000 znakov.
Recenzija znanstvene in strokovne monografije (prikaz knjige) naj obsega največ 3.000 znakov s presledki.

Recenzije

Prispevki se recenzirajo. Recenzija je anonimna. Glede na oceno recenzentov uredniški odbor ali urednik prispevek sprejme, če je treba, zahteva popravke ali ga zavrne. Pripombe recenzentov avtor vnese v prispevek.
Zaradi anonimnega recenzentskega postopka je treba prvo stran in vsebino oblikovati tako, da identiteta avtorja ni prepoznavna.
Avtor ob naslovu prispevka napiše, v katero kategorijo po njegovem mnenju in glede na klasifikacijo v COBISS, spada njegov prispevek. Klasifikacija je dostopna na spletni strani revije in pri odgovornem uredniku. Končno klasifikacijo določi uredniški odbor.

Lektoriranje

Lektoriranje besedil zagotavlja OE, pristojna za založniško dejavnost. Lektorirana besedila se avtorizirajo.

Navajanje avtorjev prispevka

Navajanje avtorjev je skrajno zgoraj, levo poravnano.
Primer:
Ime 1 Priimek 1,
Ime 2 Priimek 2

Naslov prispevka

Navedbi avtorjev sledi naslov prispevka. Črke v naslovu so velike 16 pik, natisnjene krepko, besedilo naslova pa poravnano na sredini.

Povzetek

Prispevku mora biti dodan povzetek, ki obsega največ 800 znakov (10 vrstic). Povzetek naj na kratko opredeli temo prispevka, predvsem naj povzame rezultate in ugotovitve. Splošne ugotovitve in misli ne spadajo v povzetek, temveč v uvod.

Povzetek v angleščini

Avtorji morajo oddati tudi prevod povzetka v angleščino. Tudi za prevod povzetka velja omejitev do 800 znakov (10 vrstic).

Ključne besede

Ključne besede (3–5, tudi v angleškem jeziku) naj bodo natisnjene krepko in z obojestransko poravnavo besedila.

Besedilo

Avtorji naj oddajo svoje prispevke na papirju formata A4, s presledkom med vrsticami 1,5 in velikostjo črk 12 pik Arial. Na zgornjem in spodnjem robu naj bo do besedila približno 3 cm, levi rob naj bo širok 2 cm, desni pa 4 cm. Na vsaki strani je tako približno 30 vrstic s približno 62 znaki. Besedilo naj bo obojestransko poravnano, brez umikov na začetku odstavka.

Kratka predstavitev avtorjev

Avtorji morajo pripraviti kratko predstavitev svojega strokovnega oziroma znanstvenega dela. Predstavitev naj ne presega 600 znakov s presledki (10 vrstic, 80 besed). Avtorji naj besedilo umestijo na konec prispevka po navedeni literaturi.

Strukturiranje besedila

Posamezna poglavja v besedilu naj bodo ločena s samostojnimi podnaslovi in ustrezno oštevilčena (členitev največ na 4 ravni).
Primer:
1 Uvod
2 Naslov poglavja (1. raven)
2.1 Podnaslov (2. raven)
2.1.1 Podnaslov (3. raven)
2.1.1.1 Podnaslov (4. raven)

Oblikovanje seznama literature

V seznamu literature je treba po abecednem redu navesti le avtorje, na katere se sklicujete v prispevku, celotna oznaka vira pa mora biti skladna s **harvardskim načinom navajanja**. Če je avtorjev več, navedemo vse, kot so navedeni na izvirnem delu.

Primeri:

a) knjiga:

Priimek, ime (začetnica imena), letnica. *Naslov dela*. Kraj: Založba.

Na primer: Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press.

b) zbornik:

Samson, C., 1970. Problems of information studies in history. S. Stone, ur. *Humanities information research*. Sheffield: CRUS, 1980, str. 44–68. Pri posameznih člankih v zbornikih na koncu posameznega vira navedemo strani, na katerih je članek, na primer:

c) članek v reviji

Kolega, N., 2006. Slovenian coast sea flood risk. Acta geographica Slovenica. 46-2, str. 143–167.

Navajanje virov z interneta

Vse reference se začenjajo enako kot pri natisnjenih virih, le da običajnemu delu sledi še podatek o tem, kje na internetu je bil dokument dobljen in kdaj. Podatek o tem, kdaj je bil dokument dobljen, je pomemben zaradi pogostega spreminjanja www okolja.

Primer:

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press, str. 45–100. http://www.mors.si/index.php?id=213, 17. 10. 2008.

Pri navajanju zanimivih internetnih naslovov v besedilu (ne gre za navajanje posebnega dokumenta) zadošča navedba naslova (http://www.vpvs.uni-lj.si). Posebna referenca na koncu besedila v tem primeru ni potrebna.

Sklicevanje na vire

Pri sklicevanju na vire med besedilom navedite priimek avtorja, letnico izdaje in stran. *Primer:* … (Smith, 1997, str. 12) …

Če dobesedno navajate del besedila, ga ustrezno označite z narekovaji, v oklepaju pa poleg avtorja in letnice navedite stran besedila, iz katerega ste navajali.

Primer: … (Smith, 1997, str. 15) …

Pri povzemanju drugega avtorja napišemo besedilo brez narekovajev, v oklepaju pa napišemo, da gre za povzeto besedilo. *Primer*: (po Smith, 1997, str. 15). Če avtorja navajamo v besedilu, v oklepaju navedemo samo letnico izida in stran (1997, str. 15).

Slike, diagrami in tabele

Slike, diagrami in tabele v prispevku naj bodo v posebej pripravljenih datotekah, ki omogočajo lektorske popravke. V besedilu mora biti jasno označeno mesto, kamor je treba vnesti sliko. Skupna dolžina prispevka ne sme preseči dane omejitve.

Če avtor iz tehničnih razlogov grafičnih dodatkov ne more oddati v elektronski obliki, je izjemoma sprejemljivo, da slike priloži besedilu. Avtor mora v tem primeru na zadnjo stran slike napisati zaporedno številko in naslov, v besedilu pa pustiti dovolj prostora zanjo. Prav tako mora biti besedilo opremljeno z naslovom in številčenjem slike. Diagrami se štejejo kot slike.

Vse slike in tabele se številčijo. Številčenje poteka enotno in ni povezano s številčenjem poglavij. Naslov slike je naveden pod sliko, naslov tabele pa nad tabelo. Navadno je v besedilu navedeno vsaj eno sklicevanje na sliko ali tabelo. Sklic na sliko ali tabelo je: ... (slika 5) ... (tabela 2) ...

Primer slike:

Slika 5: Naslov slike

Primer tabele:

Tabela 2: Naslov tabele

Opombe pod črto

Številčenje opomb pod črto je neodvisno od strukture besedila in se v vsakem prispevku začne s številko 1. Posebej opozarjamo avtorje, da so opombe pod črto namenjene pojasnjevanju misli, zapisanih v besedilu, in ne navajanju literature.

Kratice

Kratice naj bodo dodane v oklepaju, ko se okrajšana beseda prvič uporabi, zato posebnih seznamov kratic ne dodajamo. Za kratico ali izraz v angleškem jeziku napišemo najprej slovensko ustreznico, v oklepaju pa angleški izvirnik in morebitno angleško kratico.

Format zapisa prispevka

Uredniški odbor sprejema prispevke, napisane z urejevalnikom besedil MS Word, izjemoma tudi v besedilnem zapisu (text only).

Naslov avtorja

Prispevkom naj bosta dodana avtorjeva naslov in internetni naslov ali telefonska številka, na katerih bo dosegljiv uredniškemu odboru.

Kako poslati prispevek

Na naslov uredništva ali članov uredniškega odbora je treba poslati elektronsko različico prispevka.

Potrjevanje prejetja prispevka

Uredniški odbor avtorju pisno potrdi prejetje prispevka.

Korekture

Avtor opravi korekture svojega prispevka v treh dneh.

Naslov uredniškega odbora

Ministrstvo za obrambo
Generalštab Slovenske vojske
Sodobni vojaški izzivi
Uredniški odbor
Vojkova cesta 55
1000 Ljubljana
Slovenija

Elektronski naslov uredništva:
svi-cmc@mors.si

Prispevkov, ki ne bodo urejeni skladno s tem navodilom, uredniški odbor ne bo sprejemal.

INSTRUCTIONS FOR THE AUTHORS OF PAPERS FOR THE CONTEMPORARY MILITARY CHALLENGES

Content-related instructions

General

The Contemporary Military Challenges is an interdisciplinary scientific expert magazine, which publishes papers on current topics, researches, scientific and expert discussions, technical or social sciences analysis from the security, defence and military field, as well as overviews of professional and science monographs (book reviews).

What do we publish?

We publish papers, which have not been previously published or sent to another magazine for publication. The author is held responsible for all eventual copyright violations. If the paper has already been printed elsewhere, sent for publication or presented at an expert conference, the author must notify the editor, obtain the publisher's consent (if necessary) and indicate the reasons for republishing.

Publishing an article is free of charge.

Technical instructions

Limitations regarding the length of the papers

The papers should consist of 16 typewritten pages or 30,000 characters with spaces, at a minimum they should have 8 pages or 15,000 characters and at a maximum 24 pages or 45,000 characters.

Overviews of science or professional monograph (book presentation) shoud not have more than 3.000 characters with spaces.

Reviews

The papers are reviewed. The review is anonymous. With regard to the reviewer's assessment, the editorial board or the editor either accepts the paper, demands modifications if necessary or rejects it. After the reception of the reviewers' remarks the author inserts them into the paper.

Due to an anonymous review process the first page must be designed in the way that the author's identity cannot be recognized.

Next to the title the author indicated the category the paper. The classification is available on the magazine's internet page and at the responsible editor. The editorial board determines the final classification.

Proofreading

The organizational unit responsible for publishing provides the proofreading of the papers. The proofread papers have to be approved.

Translating

The translation of the papers or abstracts is provided by the organizational unit competent for translation or the School of Foreign Languages, DDETC.

Indicating the authors of the paper

The authors' name should be written in the upper left corner, aligned left.
Example:
Name 1 Surname 1,
Name 2 Surname 2,

Title of the paper

The title of the paper is written below the listed authors. The letters in the address are bold with font size 16. The text of the address is centrally aligned.

Abstract

The paper should have an abstract of a maximum 800 characters with spaces. The abstract should present the topic of the paper in short, particularly the results and the findings. General findings and reflections do not belong in the abstract, but rather in the introduction.

Abstract in English

The authors must also submit the translation of the abstract into English. The translation of the abstract is likewise limited to a maximum of 900 characters with spaces (12 lines).

Key words

Key words (3-5 also in the English language) should be bold with a justified text alignment.

Text

The authors should submit their papers on a A4 paper format, with a 1,5 line spacing written in Arial and with font size 12. At the upper and the bottom edge, there should be approx. 3 cm of space, the left margin should be 2 cm wide and the right margin 4 cm. Each page consists of approx. 30 lines with 62 characters. The text should have a justified alignment, without indents at the beginning of the paragraphs.

A brief presentation of the authors

The authors must prepare a brief presentation of their expert or scientific work. The presentation should not exceed 600 characters (10 lines, 80 words). These texts should be placed at the end of the paper, after the cited literature.
The author's photo should be at least 600 kb or 200 dpi in size.

Text structuring

Individual chapters should be separated with independent subtitles and adequately numbered.
Example:
1 Introduction
2 Title of the chapter (1st level)
2.1 Subtitle (2nd level)
2.1.1 Subtitle (3rd level)
2.1.1.1 Subtitle (4th level)

Referencing

In the bibliography only the authors of the references you refer to in the paper have to be listed alphabetically. The entire reference has to be in compliance with the **Harvard referencing style**.

Example:

Surname, name (can also be the initial of the name), year. *Title of the work.* Place. Publishing House.

Example A:

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press.

At certain papers published in a collection of papers, at the end of each reference a page on which the paper can be found is indicated.

Example B:

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press. pp. 45-100.

Referencing internet sources

All references start the same way as the references for the printed sources, only that the usual part is followed by the information about the internet page on which the document was found as well as the date on which it was found. The information on the time the document was taken off the internet is important because the WWW environment constantly changes.

Example C:

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press. p. 45-100. http://www.mors.si/index.php?id=213, 17 October 2008.

When referencing interesting WWW pages in the text (not citing an individual document) it is enough to state only the internet address (http://www.vpvs.uni-lj.si). A separate reference at the end of the text is therefore not necessary.

More on the Harvard referencing style in the A Guide to the Harvard System of Referencing, 2007; http://libweb.anglia.ac.uk/referencing/harvard.thm#1.3, 16 May 2007.

Citing

When citing sources in the text, indicate only the surname of the author and the year of publication. *Example*: ..... (Smith, 1997) …

If you cite the text literary, that part should be adequately marked »text«…after which you state the exact page of the text in which the cited text is written.

Example: …(Smith, 1997, p 15) …

Figures, diagrams, tables

Figures, diagrams and tables in the paper should be prepared in separate files that allow proofreading corrections. The place in the text where the picture should be inserted must be clearly indicated. The total length of the paper must not surpass the given limitation.

If the author cannot submit the graphical supplements in the electronic form due to technical reasons, it is exceptionally acceptable to enclose the figures to the text. In this case the author must write a sequence number and a title on the back of each picture and leave enough space in the text for it. The text must likewise contain the title and the sequence number of the figure. Diagrams are considered figures.

All figures and tables are numbered. The numbering is not uniform and not linked with the numbering of the chapters. The title of the figure is listed beneath it and the title of the table is listed above it.

As a rule at least one reference to a figure or a table must be in the paper.

Reference to a figure or a table is: … (figure 5) …… (table 2) ……

Example of a figure:

Figure 5: Title of the figure

Example of a table:

Table 2: Title of the table

Footnotes

Numbering footnotes is individual form the structure of the text and starts with the number 1 in each paper. We want to stress that the footnotes are intended for explaining thoughts written in the text and not for referencing literature.

Abbreviations

When used for the first time, the abbreviations in the text must be explained in parenthesis, for which reason non additional list of abbreviations is needed. If the abbreviations or terms are written in English, we have to write the appropriate Slovenian term with the English original and possibly the English abbreviation in the parenthesis.

Format type of the paper

The editorial board accepts only the texts written with a MS Word text editor and only exceptionally texts in the text only format.

Title of the author

Each paper should include the author's ORCID, address, e-mail and a telephone number, so the editorial board could reach him or her.

An ORCID number is preferred.

Sending the paper

An electronic version of the paper should be submitted via the ScholarOne website available through the journal's website.

Confirmation of the reception of the paper

All the information and procedures related to the author's submission of articles are available on the ScholarOne website.

Corrections

The author makes corrections to the paper in seven days.

Editorial Board address

Ministrstvo za obrambo
Generalštab Slovenske vojske
Sodobni vojaški izzivi
Uredniški odbor
Vojkova cesta 55
1000 Ljubljana
Slovenia

E-mail address:
svi-cmc@mors.si

The editorial board will not accept papers, which will not be in compliance with the above instructions.

Vsebina