Damjan Štrucl

DOI:10.33179/BSV.99.SVI.11.CMC.24.2.6

RUSKA AGRESIJA NA UKRAJINO: KIBERNETSKE OPERACIJE IN VPLIV KIBERNETSKEGA PROSTORA NA SODOBNO BOJEVANJE

RUSSIAN AGGRESSION ON UKRAINE: CYBER OPERATIONS AND THE INFLUENCE OF CYBERSPACE ON MODERN WARFARE

Povzetek Sodobno varnostno okolje je globalno, dinamično in nepredvidljivo, predvsem v smislu zagotavljanja kibernetske varnosti in kibernetske obrambe. Številne analize ruskega hibridnega delovanja so pokazale, da Ruska federacija za doseganje svojih političnostrateških ciljev izvaja veliko kibernetskih operacij. Kljub tovrstnim razpravam pa rusko-ukrajinska vojna pomeni novo prelomnico v globalnem varnostnem okolju, saj so se v konflikt vključili tudi nedržavni subjekti, kibernetski prostor pa je postal orodje za implementacijo sankcij. Cilj članka je analizirati izvajanje kibernetskih operacij Ruske federacije ob njeni vojaški agresiji proti Ukrajini in morebitni globalni vpliv kibernetskega prostora na oborožene spopade v prihodnosti.

Ključne besede ***Hibridne operacije, informacijske operacije, kibernetske operacije, kibernetski napad, kibernetski prostor.***

Abstract The contemporary security environment is global, dynamic, and unpredictable, particularly in terms of providing cyber security and cyber defence. Numerous analyzes of Russian hybrid operations have shown that the Russian Federation is conducting a number of cyber operations to achieve its politically strategic goals. Despite such debates, the Russo-Ukrainian war represents a new turning point in the global security environment, as many non-state actors have become involved in the conflict and cyberspace has become a tool for implementing sanctions. Thus, the article aims to analyze the implementation of cyber operations of the Russian Federation as observed in the case of its military aggression against Ukraine and the potential global impact of cyberspace in armed conflict for the future.

Key words ***Hybrid operations, information operations, cyber operations, cyber attack, cyberspace.***

Introduction

Today's security environment is global, contemporary, and complex, mainly due to its unique characteristics. The processes of globalization and informatization have contributed to changes in the national as well as the international security environment. The global community is inextricably linked, and the fundamental functions of nation-states depend entirely on information and communication technology (ICT). In this regard, the path of thinking of national physical borders as territory has been lost, and as a result, the concept of cyberspace as a global domain has become important for how the international community as a whole understands the current global and contemporary security environment.

Grizold and Bučar note that the contemporary security environment is much more complex, unstable, vulnerable, and endangered than before (Grizold & Bučar, 2011, pp 847-849). Over the last three decades it has been observed, that behaviors in cyberspace by state and non-state actors has changed significantly, while security literature has not (Harknett & Smeets, 2020, p 1). In this regard, it is emphasized that conceptual and doctrinal thinking on military cyber operations and ways of copeing with cyber threats needed to be improved (Brantly & Smeets, 2020, p 2).

In the discourses to date, most academic and political communities have focused on Russian hybrid operations, especially in terms of conducting information and cyber operations, or warfighting in the so-called »gray zone«. In doing so, three main features of Russian hybrid operation were identified: it economizes the use of (miltary) force, is persistent, and is population-centric. In this regard, the three (strategic) objectives of the Russian hybrid warfare have been established: 1. Occupying territory without the use of overt or conventional military force; 2. Creating a pretext for overt, conventional military action; and 3. The use of hybrid measures to influence the politics of countries (Chivvis, 2017, pp 2-3).

The Russian Federation has historically been quite successful in conducting hybrid operations without the direct use of military aggression, but it has had a reversal in the event of an armed attack on Ukraine. Namely, the armed attack on Ukraine and the retaliatory measures of the international community against Russia point to new characteristics of a different mode of global hybrid warfare and cyberspace, the characteristics and dimensions of which have not been known so far. Various actors involved in the »fight« against the Russian Federation have come to the fore, revealing the true dimension of the »power« of cyberspace that affects the global economy and information environment.

As early as August 2008, the Russo-Georgian conflict revealed the importance of controlling the physical components of cyberspace, the information component, the internationalization of cyber conflicts, and the tendency to increase unexpected outcomes in cyber conflicts - a phenomenon called »cyclones in cyberspace« (Deibert, Rohozinski, & Crete-Nishihata, 2012, p 3). However, the Russian-Ukrainian conflict adds another component to the unexpected challenge, and that is the inclusion of sanctions against Russia through cyberspace by states and the commercial sector, as well as the involvement of third parties, i.e. civilian volunteers (a.k.a »cyber partisans«) carrying out cyber attacks on Russian Federation institutions and underground hackers groups. Therefore, the Russo-Ukrainian war represents the most severe geopolitical conflict since World War II that results in vaste global consequences.

In this regard, the article addresses the following research questions: 1. How does Russian Federation conduct military cyber operations and use cyberspace? 2. How does the international community use cyberspace against the Russia Federation? 3. How do non-state actors participate in cyberspace? These research questions are particularly important from a political and strategic point of view, as they will address new challenges to the contemporary security environment, which the international community may not yet have identified.

1 CHARACTERIZATION OF THE TERMINOLOGICAL FRAMEWORK OF BASIC CYBER RELATED CONCEPTS AND PARADIGM OF THE RUSSIAN CYBER OPERATIONS

The accelerated development of digitalization and globalization have greatly changed the contemporary security environment, both in theoretical and factual terms. Many new sources of threats and challenges have arisen, which are also reflected in the conceptual understanding of the contemporary security environment. The EU and NATO are developing defense strategies to protect their member states, and the Russian Federation have been conducting various forms of military and non-military operations for more than a decade to achieve its own political and strategic goals.

1.1 Terminological framework of basic cyber related concepts

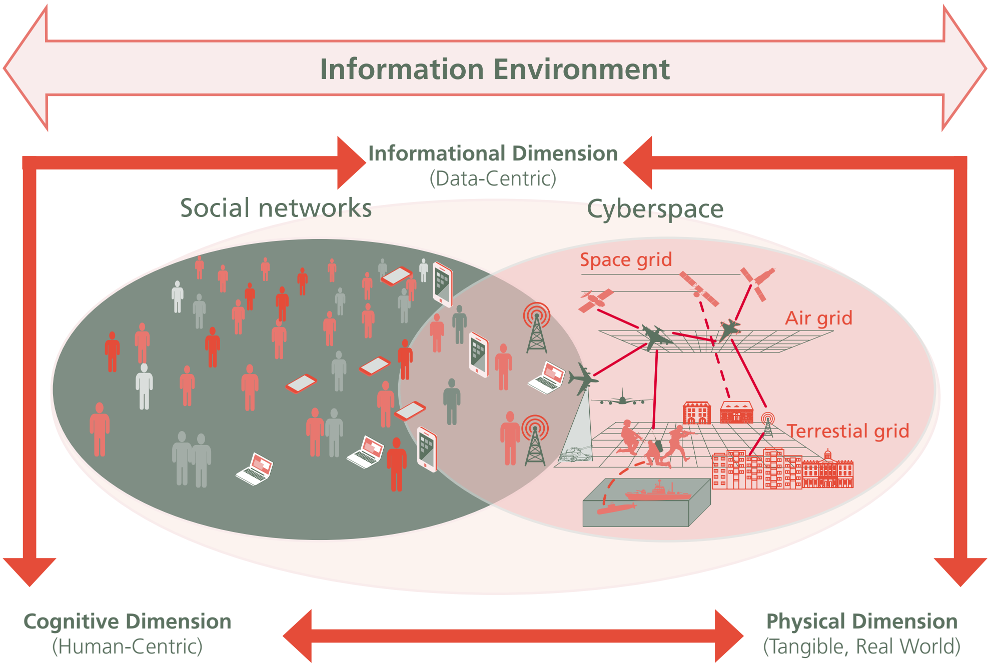
Many political, professional and academic debates today focus mainly on the direct security risks associated with cyberspace, although the contemporary security environment would need to be addressed comprehensively. Namely, cyberspace represents both a source of threat and a subject of threat, or to put it simply, it can be used as a »tool« that has security implications for and in the information environment (IE).

Although the term IE is rarely used, it exists in every community or organization. The basic aim of the IE is to connect individuals, information, and processes according to their needs, desires, interests, etc. Today, cyberspace enables states, organizations, and interest groups to exchange information / data and connect processes within and outside a particular community in real time, regardles to their geographical location (Brikše, 2006, pp 375-380).

Given the above, the IE represents two partially intersecting areas, where on the one hand social networks are webs of interaction/relationships between stakeholders, while cyberspace serves as a technical fundation for the implementation of interactions

(Porche III, 2016, p 2). Therefore, IE can be defined as three interrelated dimensions (physical, informational, and cognitive)[1] e.g. information and communication technology (ICT), individuals, and organizations, in which cyberspace (technically) enables their global interaction (Figure 1). In this regard, it can be said that IE is a fundamental environment for Strategic Communications (StratComm) that encompasses information, cyber, and hybrid operations.

Figure 1: Information Environment (Porche III, 2016, pp I-2, Joint Publication 3-13: Information Operations, 2014, pp 1-2)



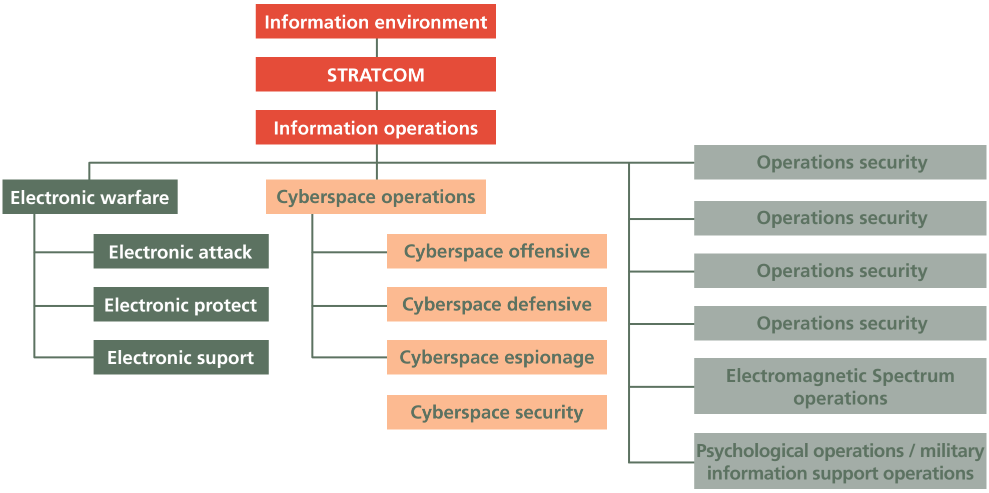
Despite cyberspace not yet having a globally accepted definition, most experts share a common concept of its understanding: it is a collection of information (and communication) technology (I(C)T) devices connected to store, share, and use electronic data over network and the internet (Clark, 2010, p 1, Ottis & Lorents, 2010, p 267). Other experts (and some States) prefer to use a layered approach to define

[1] *JP 3-13, 2014, p IX. Physical Dimension: individuals, organizations, CIS, supporting infrastructure, books, newspapers, or any other objects that are subject to empirical measurement; Information Dimension: the link between the physical and cognitive dimension, actions where information content and flow exist, and the medium by which information is collected, processed, stored, disseminated, and protected; Cognitive Dimension: the minds, perceptions, and decisions of those who use information, or where individual and organizational consciousness exist. (Ibid, pp I-2-I-3)*

cyberspace: it consists physical (ICTcomponents and infrastructure - geographic components), logical (data, software, protocols ect.), and a social layer (real and virtual persona) that are independent and concurrently interconnected (Clark, 2010, pp 1-2; Ministry of Defence Shrivenham, 2016, pp 5-7; Probert, 2021, p 69). Thus, in general, we can conclude that cyberspace consists of tangible and intangible elements, the network and the Internet, which together form the whole of cyberspace within the information environment.

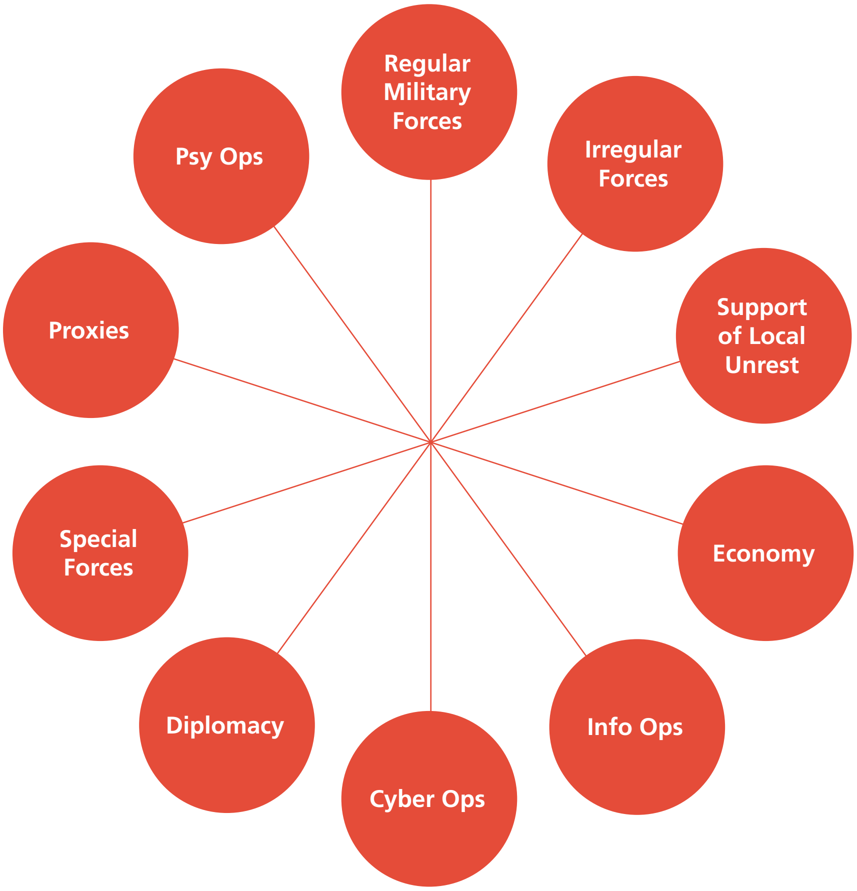
In contemporary IE, almost everything is connected through cyberspace, from critical infrastructure, public administration information systems, society, public and military ICT, to individuals. Thus, the IE and cyberspace serve as sources for many global threats, dangers, risks, and challenges that have implication on the contemporaray security invironment. Information operations, as a superset of other ICT-related operations, serve as a tool of hybrid operations to gain an advantage over the adversary. Hence, we can say that information, including its sub-operations, serves to influence on human, information, and CIS (Orye & Maennel, 2019, p 3).

Figure 2: Information environment and forms of operation (adopted from Orye & Maennel, 2019, p 4)



Orey and Maennel described the traditional war as *»a violent struggle for domination between nation-states or coalitions and alliances of nation-states«* (Orye & Maennel, 2019, p 4). However, the contemporary security environment is complex, challenging, and dynamic which is reflected in the understanding of its nature. Most of the definitions addressed to the concept of the contemporary security environment have not yet been globally accepted, e.g. the UN has not yet defined its terminology on contemporary security concepts, while NATO and the EU do not have an accepted definition of hybrid operations, nor does the EU have an accepted definition of cyber operations respectively. However, we can agree with many experts on the definition of hybrid warfare[2] as modern warfare or cocktail, intertwined with various forms of war (conventional and irregular, military and non-military) and operations (e.g. information, cyber, psychological, and economical), that must be temporally and spatially coordinated (Popescu, 2015, p 5, Cigler, 2016, p 83, European External Action Service, 2018, pp 1-2).

Figure 3: Elements of hybrid warfare: (adopted from Indian Foreign Affairs, 2022)



[2] *Hybrid warfare can be defined as the activities of state and non-state actors, covering regular and irregular capabilities, tactics and formations, including terrorist acts, indiscriminate violence and coercion, and criminal disorder (Hoffman, 2007, p 14).*

Strategic cyberwar[3] theory is based a strategy whose utility is tied to the likelihood of institutional instability in the targeted nation. In this regard, a cyber attack or cyber operation on an institutional framework will result in destabilization of the attacked nation, which means that it can be subdued to the attacker´s will. However, cyber attacks or cyber operations removes the predictive power of traditional military strategy, as these actions would likely be over before any human leadership understood the strategic landscape based on current understanding of national cyberspace capabilities. (Kallberg, Spring 2016, pp 113-117)

Although the word »operation« has a military connotation, this word needs to be understood more broadly in the context of the modern cyberspace security environment. The IE is complex and organizationally transcendant, so cyber operations (Cyber Ops) cannot and likely could not be linked solely to military capabilitiesbut must also be linked to civilian capabiliities which do not necessarily holistically belong to the State (Andress & Winterfeld, 2014, p 66). In addition, States may also use non-state actors or execute Cyber Ops through proxies (MoD France, September 2019, pp 5-6). Therefore, State actorsor State-sponsored terrorist and criminal organizations, can potentially conduct Cyber Ops on behalf of a sponsoring State. Traditionaly, non-overt State-sponsored actors are used for politically motivated cyber attacks[4] implemented in the form of cyber sabotage, subversion, espionage, blackmail, propaganda, or cyber theft, which does not violate the law of armed conflict (Cyber Ops gray zone) (Kello, 2013, p 19). Constrasted with military Cyber Ops, which aim to achieve strategic, operational, and tactical advantages on the battlefield and divide into offensive and defensive cyber operations, and cyber espionage (Brantly & Smeets, 2020, p 2).

1.2 Defining the paradigm of the Russian cyber operations

In context from a Russian perspective, the Primakov doctrine from 1996 was a defining concept of Russian foreign and defence policy that strives to established a new multipolar world managed by a concert of major powers the favors Russia’s primacy in the post-Soviet geopolitical space (Russia, China, India and USA) (Rumer, 2019, p 3). Additionally, a majority of politicians and security experts associate Russian concepts of hybrid warfare with General Valerij Gerasimov, the author of the so-called Gerasimov doctrine that encompasses a whole-government approach that fuses hard and soft power across all operational domains (Rumer, 2019, p 1). However, the Gerasimov doctrine is not a formal developed doctrine, but a speech Gerasimov gave in 2013. His speech has been understood as an overview of Russia’s modern strategy, a vision of modern warfare or even of total warfare that

[3] *Gray made four statements regarding cyberwarfare: 1. cyber power is primarily enabler of joint military operations, 2. a cyber offensive will not be deadly enough to have major military effects, 3. Cyber power is information and information can be ignored, and 4. the wide-spread fear for a stand-alone »Cybergeddon« (cyber Armageddon) is not logical because it is unlikely to happen (Gray, 2013, pp X-XI).*

[4] *Tallinn Manual defines a cyber attack as cyber defensive and offensive operations (Schmitt, 2017, p 376). Different types and objectives of the cyber attack define the category of cyber actions or threats: Cyber crime, terrorism, espionage, or operations (Rid, 2013, p XIV).*

encompasses all non-military, and the use of military means to achieve political and strategic goals (Galeotti, 2018, McKew, 2017, Giles, 2020). Therefore, we can say that the Gerasimov doctrine is a term evolved by the West by analysing Gerasimov´s speech in regards with the Primakov doctrine.

Geoletti points out that the perception of a hybrid warfare between the West and Russia is different. Russia sees hybrid warfare as the use of subversion to prepare the battlefield before intervention and later to use cyber capabilities to disrupt the chain-of-command, incite local uprisings, and disrupt communications (Galeotti, 2018). According to the West, cyber capabilities are a combination of military and non-military means that allows state and non-state actors to achive strategic objectives that can be political, military, economic, and financial. In this regard, Russia has increasingly used its cyber capabilities since 2007, mainly to support its (global and regional) political goals through information operations, and consequently prepares the environment for possible military intervention.

The former Soviet Republics were the first to serve Russia as a testing ground for the implementation of hybrid warfare with the support of cyber capabilities. Estonia experienced a massive cyber attack in 2007 in the form of a distributed denial of service (DDoS) attack. The cyber attacks targeted Estonia's websites, the financial sector, and communications of Estonian emergency services, and at the same time, an information warfare was conducted calling on the ethic Russian Estonians to riot. Russia used a similar pattern of cyber attacks in Georgia in 2008, where it began preparations for military intervention in July 2008. Russian cyber attacks were also much more organized and coordinated then previously observed, as some Russian-sponsored websites also provided guidance for volunteers on how to attack Georgian websites. However, cyber attacks in the form of support to information operations have not only spread Russian propaganda, but have also prevented the Georgian government from conducting proper strategic communications. Addititonaly, the Russian-Georgian conflict is not only important from the point of view of cyber attacks, but also as the first Russian comprehensive hybrid operation in a conteprorary security environment, as Russia simultaneously used cyber capabilities solely in the cyber domain as well as support conventional forces. Nevertheless, the consequences of the cyber attacks on Estonia and Georgia in 2007 and 2008 were limited and not global due to the relatively low Internet access of both countries. (Ophardt, 2010, pp 1-7; Rumer, 2019, pp 9-10)

The established Russian modus operandi, based on the case of Estonia and Georgia, has shown that Russian cyber operations are mainly conducted in support of StratComm, hybrid operations, and information operations (including cyber espionage). In doing so, Russia, including non-state actors and proxies, is using the former Soviet Republics as a »living« test ground to test its cyber capabilities and to implement the Primakov doctrine.

2 FROM THEORY TO PRACTICE

Historians have found that almost all wars throughout history were so-called »compound wars« (Hoffman, 2007, pp 17-20) meaning strategically coordinated regular and irregular operations. Throughout human history, many different terms have emerged regarding forms of warfare: »non-Trinitarian« wars, 4th generation warfare, the New War, and in recent years, hybrid warfare (Ibid). The fourth generation and hybrid warfare added an element of a »new environment« which is currently coined as the IE supported by cyberspace.

2.1 Russian´s cyber modus operandi in Ukraine

Based on the Estonia and Georgia case, Russia has »learned« that the international community, apart from sanctions and condemnation of such acts, does not have the right tools to stop Russia from pursuing its foreign and security policy (Giles in Geers, 2015, p 25). Therefore, Russia has continued to use its already tested modus operandi and proceeded with the implementation of Primak's doctrine in cyberspace as is observed by its continued use in the current war in Ukraine. In 2013, Russian strategy for Ukraine included a substantial investment in cyber operations (such as cyber espionage dubbed »Operation Armagedon«), information operations as well as cyber attacks by limited disruption and destruction (Weedon in Geers, 2015). Weedon also discovered that this was not an isolated case, as Russia and its supporters have also used various malicious codes (Snake / Uroburos / Turla) that targeted Ukrainian computer systems.

The escalation of Russian cyber activities began in November 2013, when a DDoS attack was conducted in order to cause destruction of Ukrainian media websites. Such activities were in fact an implementation of new Russian military doctrine[5] in support of Russian hybrid operations in the illegal annexation of Crimea. In February 2014, Russian forces allegedly severed the fiber-optic cables of Ukrainian telecoms and cut off telecommunications between Crimea and the rest of Ukraine. Prior to the entry of Russian military forces into Crimea, a number of cyber attacks were carried out that disabled the ability of Ukrainian government, institutions, and media to function, and at the same time many mobile phones of Ukrainian parliamentarians were hacked (Weedon in Geers, 2015, p 76). Thus, based on the examples above, we can reaffirm that Russia conducted cyber operations primarily in support of political-strategic objectives, and were not directly related to support in the achievement of a commander military goals.

The illegal annexation of Crimea and the possibility of a military conflict as well as the subsequent events in Ukraine have convinced many in the Western world that Russia's foreign and security policy is a reflection of General Gerasimov's speech.

[5] *The 2014 Russian military doctrine warned of »the strengthening of global competition, tensions in various areas of inter-state and interregional interaction, rivalry of proclaimed values and models of development, instability of the processes of economic and political development at the global and regional levels against a background of general complication of international relations.« (Rumer, 2019, p 10)*

After the occupation of Crimea, Russia, with support of pro-Russian hacktivists, continued their cyber activities and in May 2014 executed a sophisticated cyber attack that shut down the computer systems of Ukraine's central election commission. Additionally, in 2015 and 2016, cyber attacks on Ukraine's critical infrastructure (electricity distribution) followed, as well as other cyber operations aimed at destabilizing the political situation in Ukraine (Madnick, 2022). Such targeted cyber attacks have not caused global damage, but have raised many questions about security and international legal dilemmas.

Though the previously mentioned cyber attacks were mainly related to the destabilization of the situation in Ukraine, in 2017, a cyber attack called »NotPetya« did cause global consequences. Namely, the goal of NotPetya was to disrupt the Ukrainian transport and banking sector, but the virus spread globally (Madnick, 2022). In this regard, the question arises as to whether the global expansion of NotPetya was caused by the attacker's ignorance of possible global repercussions or whether Russia was testing a future cyber weapon on a global scale. However, the consequences could be even greater, as a cyber attack on the energy or transportation sector could also result in physical damage, which would also be interepted as use of force under UN Charter Article 2 (4) and armed attack Article 51.

Since 2013, Russia and its supporters have mostly have conducted low-level cyber activities, such as cyber espionage and DDoS attacks (the exception to this trend is a more sophisticated cyber-attack on critical infrastructure) to support information operations and consequently hybrid operations. Therefore, the main topics among politicians and experts have been on the application of current international law as it applied to cyber space, hardening cybersecurity and cyber resilience, and characterizing which cyber operations could lead to armed conflict. In this regard, two different working groups have been established within the UN, and two Joint declarations given on EU-NATO cyber cooperation (including hybrid operations).

Ignoring the aforementioned activities, the »new« Russian invasion of Ukraine began on January 13, 2022, following the same pattern as in the Russian-Georgian Conflict as well as the previous illegal annexation of Crimea. According to Fendorf and Miller, as well as taking into account the volunteer cyber operation tracking databases online, Russian cyber operations initiated with a website defacement in support of Russian information operations. On January 13, 2022, DDoS attacks and cyber attacks on Ukrainian computer systems (WhisperGate wiper-Operation BleedingBear, HermeticWiper and Sandworm / VoodooBear) were launched, aimed at disabling Ukrainian government operations, banks, and some companies. In addition to the aforementioned cyber attacks, the pro-Russian group Gamaredon, (a.k.a. Shuckworm or PrimitiveBear) also has carried out cyber espionage in support of the Russian invasion. (Github, 2022; Fendorf & Miller, 2022).

On the same day of the kinetic milittary attack, Russia lunched a cyber attack dubbed IsaacWiper against Ukrainian government systems and allegedlly a cyber attack on Satellite internet provider Viasat which caused wide-ranging communications outages throughout Ukraine and beyond (Germany, France, Hungary, Greece, Italy, and Poland). The cyber attack on Viasat was, as currently understood, an attack against the satellite ground infrastructure and not the satellite itself. The Viasat satellite system was also used by the Ukrainian defences (Github, 2022; Fendorf & Miller, 2022; Geneva Internet Platform Digiwatch, 2022). It follows that Russia's strategic goal was to disable communication of the Ukrainian defense forces and the Ukrainian people. Concurrently, the Viasat cyber attack seems to be a prominent example of spillover damage like NotPetya, and as such poses a major international threat. By disabling Viasat communications in Ukraine, more than 5,800 wind turbines of Germany energy company Enercon were disconected (Burgess, A mysterious satellite hack has victims far beyond Ukraine, 2022).

Analysis of Russia's further cyber activities have shown that Russia is still using DDoS attacks and malware codes to disrupts operation of Ukrainian government, banks and some prominent private companies without major impact. The only thing that can be pointed out as unique is that Russian cyber operations, in addition to other pro-Russian hackers, are also supported by UNC1151 / Ghostwriter (MOD Belarus), which gained access to Ukrainian military e-mail accounts through mass phishing attack. Notwithstanding above, the majority of international community expected that the Russian Federation, or its supporters, would conduct a global cyber attack or commit a cyber attack that will inadvertently spillover globally (a.k.a. »cyber Armageddon«). However, most currently observed cyber activities from the Russian Federation, or its supporters, target Ukrainian government institutions and media (e.g. UKRNet, fake Telegram account of President Zelensky). In addition, there are cyber attacks on some foreign media sites, such as »Slobodna Dalmacija«, where hackers have replaced content with pro-Russian articles about Ukraine (BalkanInsight). (Github, 2022; Fendorf & Miller, 2022; Geneva Internet Platform Digiwatch, 2022).

In any case, the aforementioned activities does not comply with the previous understood expectations of security experts. According to open-source data collected so far and is currentlyl reported, Russian Federation cyber operations are primarily against non-Ukrainian military CIS, nor is it possible to identify military strategic and operational cyber targets, as the activities so far are aimed at achieving Russia's political objectives. In addition, no cyber attacks were launched on civilian critical infrastructure or internet connectivity (except on Viasat), which seems to be Russian practice so far. All Russian cyber operations to date are aimed at disabling the Ukrainian government and supporting Russian information operations. However, the information warfare is not in Russia's favor, as they have blocked all external internet traffic and set up a so-called information iron curtain inside Russia (Sārts, 2022). Nevertheless, it should be noted that the information blockade within Russia has only had a short-term effect, as there are multiple alternative technological solutions that allow people to obtain global data bypassing Russian government information operation efforts.

2.2 Multinational response to Russia

The lack of strong responses by the international community to previous Russian hybrid operations and cyber activities was likely the primary reason for the Russian military invasion was deemed as viable on February 24, 2022, as Russia was not expecting such strong retaliation from the international community. Even before the invasion, the US and UK deployed cyber specialists to help Ukraine defend against an impending strategic cyber attack on critical infrastructure (Maschmeyer & Kostyuk, 2022). In additon, EU Cyber Rapid Resopnse Teams (Lithuania, Netherlands, Poland, Estonia, Romania, and Croatia) as well as Australia cyber team were commited to help defend Ukraine either remotely or on site against Russian-supported cyber attacks and to provide cyber security training for Ukrainian officials (The Conversation, 2022). The latter is confirmed by the fact that the global community has been aware of the possible consequences of large-scale Russian cyber operations, which would have the potential side-effect of spillover damage.

The World is facing a new phenomenon, as Russo-Ukrainian war on the ground war between two sovereign states concurrently with a global cyber warfare[6] that includes underground hackergroups supporting Russia (e.i. Conti, Red Bandits, CyberGhost, and Sandworm) and some that support Ukraine[7] (SOC Radar, 2022). Surprisingly, Ukrainian IT specialists and hacktivists all over the World seemingly »self-mobilized« into Ukraine's voluntary cyber defense. Those entities together form a cyber force, dubbed the »IT Army«, which was created upon the call by the Ukrainian Digital Minister. The main task of the IT Army[8] is the development of cyber weapons and attacks on Russia's critical infrastructure and state-owned media (Cerulus, 2022). Therefore, we can say that the IT Army, together with underground hacker groups supporting Russia, form Ukraine's cyber guerrilla or partisans army, which is a new occurrence in the contemporary security environment.

As currently understood, the IT Army is lead by Ukrainian government, while the Ukrainian´s underground supporters are operating by themselves. The latest is evident by Anonymous »declaration of war« against Russia and their supporters on Twitter (Fendorf & Miller, 2022; Milmo, 2022). However, both the IT Army and Ukrainian supporters are targeting Russia, Belarus, and other Russian supporters in

[6] *Global definition of cyber warfare and cyber war are not yet accepted. Some authors use cyber war and cyber warfare as synonims, while others think of cyberwar in Clausewitzian term that require violence. However, most of authors link the cyber war with the level of violation with the aim to kill, injure, destroy or damage. Therefore, Cyber warfare can be defined as non-violent actions by nation-states and non-state actors employing cyber weapons to penetrate computers or networks. Contrarily, the cyber war is a violent actions by nation-states and non-state actors employing cyber weapons whose intent is to couse significant disruption, damage and destruction. (Krepinevich, F., A., 2012, pp 15-16).*

[7] *Hacker groups supporting Ukraine: Anonymous, AgainstTheWest (AWT), Belarusian Cyber Partisans, GhostSec, IT Army of Ukraine, KelvinSecurity Hacking Team, BlackHawk, Anonymous Liberland & the PWN-BAR Hack Team, Raidforum Admins, GNG, NB65, ECO, Raidforums2, ContiLeaks, SHDWSec, GhostClan, Eye of the Storm, and Netsec. (SOC Radar, 2022)*

[8] *An example of good practice is Estonia, which has a Defense Army in addition to the regular army, which, in addition to other components of the army, also includes IT volunteers (Kaitseliit, 2022). Such a system allows Estonia to be »cyber warriors« part of the Estonian Armed Forces and thus exercises operational command.*

other countries. According to the data collected so far, the IT Army is supposed to use the Telegram application to publish high-valued targets and exchange data, however it has yet to be confirmed that Telegram is also used for operational command of other support groups such as Anonymous. (Burgess, 2022 A). Nonetheless, the Ukrainian government led IT Army and Ukrainian´s supporters have claimed that they are targeting Russian crtitical infrastructure (bank, energetic, and railway sector), Russian oil energy giant Gazprom, Russian state-owned aerospace and defense conglomerate Rostec, Russian state-owned media, Federal Service for Supervision of Communications (Roskomnadzor), Belarusian train systems, and Russian governmental institions (Fendorf & Miller, 2022; Milmo, 2022). In this regard, it is clear that Ukraine's strategic goals are to prevent the normal functioning of Russian institutions, to disable Russian information operations within Russia and to destabilize the Russian government. However, the effects of IT Army and Ukrainian supporter's efforts is difficult to properly assess.

Although, for Ukraine the use of Telegram is a fundamental communication and coordination tool, the question arises on how to check and verify volunteers and avoiding infiltration. Specifically, there is potential that some agent working on behalf of the IT Army could conduct a cyber attack against Russia, which could have a spillover effect, whether intentional or not, that causes damage or injury in the physical domain. Admittedly, this also applies to the Russian side, but Russia is already labeled an aggressor in violation of the principles of international law, but this may trigger other countries to justify the use of national offensive cyber capabilities as well under the guise of the Russo-Ukrainian War.

In addition to widespread support from hackers around the world, Ukraine also has a lot of support from commercial organizations[9], such as Microsoft, PaloAlto, antivuris commercial companies, and various social media such as Google, Youtube, Facebook, Tweeter etc (SOC Radar, 2022). Such sanctions against Russia have made it impossible (e.g. the use of cloud services and software updates/patches or the use of social media for propaganda purposes globally). Cyberspace has also proven to be a »powerful tool« with the exclusion of Russian banks from the Society for Worldwide Interbank Financial Telecommunication system (SWIFT) and in internet payments with Visa, Mastercard, and American Express bank cards, which have ceased business operations in Russia. However, cryptocurrencies can help Russia to evade international sanctions, since there is no central controller who can impose a ban to a business. The importance of the Internet and cyberspace is also evident from official Ukrainian request directly to Elon Musk's via social media to provide the new SpaceX Starlink service to support Ukrainian CIS and evade Russian cyber efforts. Ukraine signed up for this service through its Tweeter account. (Geneva Internet Platform Digiwatch, 2022). Therefore, it is clear that not only the State but also private companies have power in cyberspace as they can influence events in other

[9] *The list of imposed sanctions against Russia is daily updated by Reuters (Funakoshi, Lawson, & Deka, 2022)*

operational environments (Kuehl, 2009, p 10).[10] In this regards, Russia is facing a »mix« of sanctions imposed by States and across the international community, and by independent private companies through the information environment and cyberspace. Admittedly, such sanctions are causing financial damage to all participating entities, however the higher impact on the Russian seems to be much greater as it has pushed Russia into political, financial and technological isolation.

3 EXECUTIVE SUMMARY OF RUSSO-UKRAINIAN WAR

Over the last decade, security experts have increasingly paid attention on the application of international law to hybrid warfare and related cyber-hostile activities. In this regard, most security studies focus on current legal framework of military and intelligence operations, as well as strategic concepts such as cyber deterrence, coercion, and offense-defense balance (Liebetrau, 2022, p 3). The reason behind this is mainly due to the fact that apart from the war in Georgia, no cyber conflict escalated or took place as a part of a full-scale operation, but was limited to a cyber conflict short of war (cyber operations in »gray zone«).

In the case of Ukraine in 2022, most (cyber) security experts expected mass use of cyber weapons and an »open salvo« of Russian devastating cyber attacks, or some experts even predicted that Russia may not need to use military force at all. Many of these experts also predicted that Russia will gain a strategic advantage through cyber operations and that escalating cyber warfare will conjure a recurring specter of a »cyber Pearl Harbor« strategic surprise attack (Maschmeyer & Kostyuk, 2022; Sherman, 2022). These assumptions were most likely based on an analysis of the escalation of Russian cyber operations in the light of recent events in Georgia and, since 2013, in Ukraine. With the occupation of Crimea in 2015, Russia even temporarily and partially disabled communications in Ukraine, but surprisingly this did not happen in February 2022.

Based on our research we found that Ukraine has become a test environment for Gerasimov doctrine/Hybrid warfare as is called in West or a New Generation Warfare (NWG) as is called by Russian strategic thinkers, describing the doctrine as one that involves everybody and everything (Rácz, 2015, p 37). In this regards, Russian cyber activities in Ukraine are fully in line with the NWG, which is divided into three phases (Murphy, 2016):

1. First phase: Weakening the target and preparing the battlefield through information operations and using political, diplomatic, media, and other covert means to promote dissatisfaction with the central government.
2. Second phase: Attack. Exploiting the tensions created to overthrow the legitimate government and establish its own alternative regime.
3. Third phase: Consolidation of strength. Change of power in the attacked country.

[10] *Kuehl defines a cyber power as »the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.« (Ibid.)*

Although Russia was expected to carry out large-scale cyber attacks with the support of its supporters, this has not (yet) happened. Russia's cyber operations to date of the current ongoing armed conflict have shown no deviation from the onset of this conflict, as no analysis of cyber attacks has shown the utilization of cyber capabilities to achieve military strategic objectives, but only political-strategic goals related to support StratComm and information operations. Namely, Russia continues to conduct cyber operations in support of information warfare and the realization of Russia's strategic goals: undermining the Ukrainian government, forcing Ukraine to abandon pro-European Union and pro-NATO foreign policy, demoralizing Ukrainians, and misleading domestic and global public by spreading disinformation.

The Russo-Ukrainian war also showed that the actual cyber capabilities of the country are not only military or government capabilities, but also the capabilities of the commercial sector as well as with supporters all over the world. As the case of Ukraine shows, private cybersecurity companies (Hacken and Cyber Unit Technology) have joined the ongoing global cyber warfare, in addition to individual hackers from Ukraine (Ukraine's hacktivists) and beyond (Cerulus, 2022). In this regard, businesses IT companies and civilian volunteers have de facto become Ukraine's offensive cyber capabilities as they conduct cyber operations against Russia in line with the guidelines established by the Ukrainian government. The combination of underground hackers groups on both sites, cyber volunteers over the world, and the IT Army is causing new concerns regarding attribution and escalation of (cyber) warfigting as this could potentially trigger Russia to use its own global affecting cyber capabilities and further gain pro-Russian supporters for cyber attacks/operations at the global scale of cyberspace. In this regard, this occurrence raises an additional question on a State´s responsibilities concerning International law, and the priciples of Jus ad bellum and Jus in bello. Furthermore, according to Politico, with Hacken registered in Estonia, and is carrying out cyber attacks from Spain (Cerulus, 2022). In this regard, we can ask two questions: 1. Is Russia at cyber war with Spain and consequently with the EU and NATO? 2. Does such extensive international involvment in the Russian-Ukrainian army indicate traditional signs of a World War? The answers to these questions are far from simple, but they certainly depend on the state's perception of the application of international law.

Yet, common definition of cyber warfare and cyber war are not accepted Libicki advocates that act of (cyber) war may be defined on one of three ways: universally, multilaterally, and unilaterally. Additionally, cyberwar is base on how States or international organization have defined a cyberattack (Libicki, 2009, p 179), or how they perceive the violence or treshold associated with the term of war. Rid defines a cyberwar based on the following criteria: violent by using force; instrumental in seeking to force an enemy to change; and with political aims (Rid, 2013, p 10). However, based on the UN Charter, States must refrain from using force against the territorial integrity or political independence of another State and respect the principle of due diligence (United Nations Charter, 1945). Nevertheless, cyber activities in Russo-Ukrainian War do not only involve States or armed forces, so it is necessary to take into account the component of civilian non-state actors and determine whether the tasks are delegated by States or acts by parties of their own initiative. In this regard, based on International Humanitarian Law, the IT Army can be considered as one of the following 1. civilians indirectly supporting hostilities 2. civilians directly participating in hostilities or in some circumstances hypothetically also 3. levée en mass; an underground group considered to be civilians directly participating in hostilities or cyber criminals. At first glance, the current malicious cyber activities on both sidies could be defined as an international armed conflict (none of the countries are involved in a war, except Russia and Ukraine) or non-international armed conflicts. As a last point, under Article 3 common to the Geneva Conventions of 12 August 1949, non-international armed conflicts are armed conflicts in which one or more non-State armed groups are involved. Furthermore, two requirements are necessary for such situations to be classified as non-international armed conflicts: 1. minimum level of intensity, and 2. non states actor should be considered »parties to the conflict«.

Concurrently, global cyber »warfighting« raises a question on what is the difference between peacetime and wartime. In this regard, international law is rather clear as civilians, critical infrastructure, critical communication, and information infrastructure should not be subject of any attack. Therefore, Heli Tiirmaa-Klaar has argued that, »we have to differentiate between peacetime and wartime really clearly,« and »There are different tools that apply to wartime ... as long as they are strictly limited to military purposes and do not harm civilian infrastructure (Cerulus, 2022).« However, activities to date on both sides have not shown a distinction between cyber operations in peace and war. Both countries, with their supporters, are carrying out cyber attacks on critical infrastructure as well as government institutions. From the existing data collected, it cannot be established that any special cyber weapons have been used or that the principle of choosing military strategic objectives to achieve the commander's objectives, as understood by the Alliance, was followed. On the Russian side, it has been observed that Russian Federation decided to destroy critical infrastructure with kinetic weapons, rather than using cyber. There may be several reasons for such a decision by Russia; faster and more efficient achievement of targets using kinetic weapons, high cyber resilience of Ukraine, the EU, and NATO, or too much risk of a spillover effect that could further affect Russia. In addition, both sides with their supportes are using cyber operations to reduce public confidence in State institutions and the military.

Conclusion

The Russo-Ukrainian war is a watershed moment forthe future of national and international security policy, and in international law. The global security environment is inheretnly asymmetric, and global threats are predominantly non-military in nature. The asymmetry of the modern security environment is reflected in the different approach to respecting the values and rights of the State to its own identity, and the non-military aspects of endangerment in the choice of »tools« to achieve political and strategic goals. Russia's way of conducting cyber operations has »improved« since 2007 to the extent we see it today. Perhaps the reason is that

Russia perceives hybrid operation and cyber operations completely differently from the West. For Russia, hybrid operations are a tool to change the global geopolitical situation, which justifies using cyber operations to manipulate information (cognitive domain). Contrarily, the West perceives hybrid operations and cyber operations mainly from a military point of view and too little from a political-strategic point of view. This stems mainly from the fact that Western terminology regarding cyber operations focuses on achieving military strategic objectives, while Russian cyber operations in practice and seen so far represent a tool to influence the geopolitical distribution of power.

This Russo-Ukrainian War is a military conflict between two sovereign States on a full scale, and concurrently a »world war«, including commercial sector imposing economic and technical sanctions against Russia using cyberspace. Furthermore, we are witnessing a cyber and information warfare involving non-state actors and underground groups from foreign territories outside of direct kinetic conflict in the form of crowdsourced warfighting, distributed warfare, and protest war. A special characteristic of this war is the self-mobilization of »cyber« people around the world to a cause and the use of the information environment as a tool for strategic and operational action. Thus, the conflict in practice has shown that the cyber capabilities of the State are potentially not the only the capabilities of the State, but also the capabilities of the commercial sector, as the cyber capabilities of Ukraine consisting of the IT Army, which includes ICT experts and volunteer hackers.

A unique characteristic of this conflict is also the participation of underground hacktivist groups, which are criminal groups by nature. In this regard, questions are raised about their responsibilities and the principles of legitimacy of their participation, and what goals they pursue. Although underground hacker groups hold to the reputation of justice fighters, caution is needed, as they are not by nature subordinate to the state apparatus. Thus, it also raises the question of operational command and targeting, and how to effectively curb and stop their cyber activities once peace is achieved. However, currently, the Russo-Ukrainian War does not clearly distinguish between war and peace cyber operations. Even during the armed conflict, we are witnessing cyber operations in the so-called »gray zone« on both sides, which seems to be a continuation of the Cold War. In any case, it is necessary to ask whether the supporters of the Ukrainian side, including underground hacker groups, are conducting military actions or humanitarian actions.

Security experts also agree that hybrid threats are difficult to detect as they are constantly changing and difficult to attribute. The analysis of the Russian-Ukrainian War shows the full dimension of the parties involved, as well as a different understanding of current cyberspace terminology. In this regard, we need to re-examine strategic and doctrinal policy as well as the applicability of currently understood international law. The fact is that current cyber operations as seen and understand in the Russo-Ukrainian War are not well understood by modern democratic societies and that the Western way of conducting military cyber operations do not currently exist in a

Russian doctrinal concept. Therefore, it is even more important to reach a consensus on terminology regarding contemporary security threats, including violence and the threshold of aggression, which will allow the principles of jus ad bellum and jus in bello to be implemented and the limit cyber operations in the gray area preceeding an act of war.

Bibliography

1. *Andress, J., and Winterfeld, S., 2014. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2nd Edition). Waltham: Elsevier.*
2. *Brantly, A., and Smeets, M., 2020. Military Cyber Operations. In A. McD Sookermany, Handbook of Military Sciences (pp 1-13). Cham: Springer.*
3. *Brikše, I., 2006. The information environment: theoretical approaches and explanations, Informācijas vide Latvijā: 21. gadsimta sākums.: 2006. Retrieved from University of Latvia: https://www.szf.lu.lv/fileadmin/user_upload/szf_faili/Petnieciba/sppi/mediji/inta-brikse_anglu.pdf, 10 February 2022.*
4. *Burgess, M., 2022, 24 March. A mysterious satellite hack has victims far beyond Ukraine. Retrieved from Wired: https://www.wired.com/story/viasat-internet-hack-ukraine-russia/, 24 March 2022.*
5. *Burgess, M., 2022 A, 27 February. Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. Retrieved from Wired: https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/, 2 March 2022.*
6. *Cerulus, L., 2022, 10 March. Kyiv's hackers seize their wartime moment. Retrieved from Politico: https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/, 10 March 2022.*
7. *Chivvis, C. S., 2017. Understanding Russian »Hybrid Warfare« and What Can be Done About It. Santa Monica: RAND.*
8. *Cigler, M., 2016. Hibridna varnost in M. Malešič, Konvencionalna in hibridna varnost: vzorci (dis)kontiuitete (pp 75-95). Ljubljana: Fakulteta za družbene vede.*
9. *Clark, D., 2010. Characterizing cyberspace: past, present and future. ECIR Working Paper, Massachusetts Institute of Technology. Massachusetts: Cambridge.*
10. *Clausewitz, V. C., 1989. On War. New Yersey: Princeton.*
11. *Deibert, R. J., Rohozinski, R., Crete-Nishihata, M., 2012, February. Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War. Security Dialogue Vol. 43, No. 1, pp 3-24.*
12. *European External Action Service, 2018. A Europe That Protects: Countering Hybrid Threats. Brussels: European External Action Service.*
13. *Fendorf, K., and Miller, J., 2022, 24 March. Tracking Cyber Operations and Actors in the Russia-Ukraine War. Retrieved from Council on Foreign Affairs: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war, 26 March 2022.*
14. *Funakoshi, M., Lawson, H., Deka, K., 2022, 28 March. Tracking sanctions against Russia. Retrieved from Reuters: https://graphics.reuters.com/UKRAINE-CRISIS/SANCTIONS/byvrjenzmve/, 30 March 2022.*
15. *Galeotti, M., 2018, 5 March. I'm Sorry for Creating the 'Gerasimov Doctrine'. Retrieved from Foreign Policy: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/, 10 March 2022.*
16. *Geneva Internet Platform Digiwatch, 2022, 27 March. Ukraine conflict: Digital and cyber aspects. Retrieved from Geneva Internet Platform Digiwatch: https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects, 29 March 2022.*

17. *Giles, A., 2020. Valery Gerasimov's Doctrine: From Soviet armor officer to strategic mastermind? Potsdam: Universität Potsdam.*
18. *Giles, K., 2015. Russia and its Neighbours: Old attitudes, New capabilities. In K. Geers, Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine (pp 67-77). Tallin: CCDCOE.*
19. *Github, 2022, 27 March. Ukraine-Cyber-Operations. Retrieved from Github: https://github.com/curated-intel/Ukraine-Cyber-Operations, 20 March 2022.*
20. *Gray, C. S., 2013. Making strategic sense of cyber power: Why the sky is not falling. Carlisle: Strategic Studies Institute and U.S. Army War College Press, Army War College.*
21. *Grizold, A., and Bučar, B., 2011. Knjižna zbirka Teorija in praksa: Izzivi sodobne varnosti: od nacionalne in mednarodne do človekove varnosti. Teorija in praksa, 827-851.*
22. *Harknett, J. R., and Smeets, M., 2020, 4 March. Cyber campaigns and strategic outcomes. Journal of Strategic Studies, pp 1-34.*
23. *Hoffman, G. F., 2007. Conflict in the 21st century: The rise of Hybrid wars. Arlington: Potomac Institute for Policy Studies Arlington.*
24. *Indian Foreign Affairs, 2022, 6 March. Hybrid Warfare : A New Face of Warfare. Retrieved from Indian Foreign Affairs: https://indianforeignaffairs.com/hybrid-warfare-a-new-face-of-war-in-the-modern-world/, 10 March 2022.*
25. *Joint Chief of Staff, 2014. Joint Publication 3-13: Information Operations. Chairman of the Joint Chief of Staff.*
26. *Kaitseliit., 2022, 20 March. Estonian Defence League. Retrieved from Kaitseliit: https://www.kaitseliit.ee/en/edl, 20 March 2022.*
27. *Kallberg, J., Spring 2016. Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber. The Cyber Defense Review , Vol. 1, No. 1, 113-128.*
28. *Kello, L., 2013. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, Vol. 38, No. 2, pp 4-40.*
29. *Krepinevich, F., A., 2012. Cyber Warfare A »Nuclear Option "?. Washington: Center for Strategic and Budgetary Assessments.*
30. *Kuehl, T. D., 2009. From Cyberspace to Cyberpower: Defining the Problem. In D. F. Kramer, H. S. Starr, and K. l. Wentz, Cyberpower and National Security (pp 3-24). Washington DC: National Defense University Press.*
31. *Libicki, C. M., 2009. Cyberdeterrence and Cyberwar. Santa Monica: RAND.*
32. *Liebetrau, T., 2022. Cyber conflict short of war: a European strategic vacuum. European Security, 1-21.*
33. *Madnick, S., 2022, 7 March. What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare. Retrieved from Harvard Business Review: https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare, 8 March 2022.*
34. *Maschmeyer, L., & Kostyuk, N., 2022, 8 February. There Is No Cyber 'Shock And Awe': Plausible Threats In The Ukrainian Conflict. Retrieved from War on the rocks: https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/, 13 March 2022.*
35. *McKew, K. M., 2017, 5 September. The Gerasimov Doctrine. Retrieved from Politico: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/, 20 March 2022.*
36. *Milmo, D., 2022, 27 February. Anonymous: the hacker collective that has declared cyberwar on Russia. Retrieved from The Guardian: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia, 4 March 2022.*
37. *Ministry of Defence Shrivenham, July 2016. Cyber Primer, (2nd Edition). Ministry of Defence Shrivenham.*

38. *MoD France, September 2019. International Law Applied to Operations in Cyberspace. MoD France.*
39. *Murphy, M., 2016. Understanding Russia's Concept for Total War in Europe. Washington DC: The heritage Fundation.*
40. *Ophardt, A. J., 2010. Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. Duke Law & Technology Review, No. 3, 1-27.*
41. *Orye, E., and Maennel, M. O., 2019. Recommendations for Enhancing the Results of Cyber Effects. 11th International Conference on Cyber Conflict: Silent Battle (pp 1-19). Tallinn: CCDCOE.*
42. *Porche III, R. I., 2016. Emerging Cyber Threats and Implications. Santa Monica: RAND.*
43. *Probert, E., 2021, 25 August. Organisational Structures & Incident Management for Cybersecurity in the America. Retrieved from ITU: SlideShare: https://www.slideshare.net/DrDavidProbert/saltaworkshop1v12, 10 March 2022.*
44. *Rácz, A., 2015. Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist, FIIA Report 43. Helsinki: The Finnish Institute of International Affairs.*
45. *Rid, T., 2013. Cyber War Will Not Take Place. New York: Oxford.*
46. *Rumer, E., 2019, 5 June. The Primakov (Not Gerasimov) Doctrine in Action. Carnegie Endowment for International Peace, 1-30. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254, 10 March 2022.*
47. *Sārts, J., 2022, 8 March. #StratComPodcast/S2E2:#StratCom and Modern Warfare. Retrieved from NATO Strategic Communications Centre of Excellenc: https://open.spotify.com/episode/54w6pDaUemFp6je4iPJehr, 10 March 2022.*
48. *Schmitt, N. M., 2017. Tallinn manual 2.0 on the international law applicable to cyber operations, Second edition. Cambridge: Cambridge.*
49. *Sherman, J., 2022, 24 February. Russia's Cyber Threat to Ukraine Is Vast—and Underestimated. Retrieved from Wired: https://www.wired.com/story/russias-cyber-threat-to-ukraine-is-vast-and-underestimated/, 20 March 2022.*
50. *SOC Radar, 2022, 28 February. What You Need to Know About Russian Cyber Escalation in Ukraine. Retrieved from SOC Radar: https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/, 20 March 2022.*
51. *The Conversation, 2022, 24 February. Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities. Retrieved from The Conversation: https://theconversation.com/russia-is-using-an-onslaught-of-cyber-attacks-to-undermine-ukraines-defence-capabilities-177638, 20 March 2022.*
52. *UN General Assembly (A/RES/70/237), 2015. Developments in the field of information and telecommunications in the context of international security. United Nations General Assembly.*
53. *UN General Assembly (A/RES/73/266), 2019. Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. UN General Assembly.*
54. *UN General Assembly (A/RES/73/27), 2018. Developments in the field of information and telecommunications in the context of international security. UN General Assembly.*
55. *UN General Assembly, 1974, 14 December. United Nations General Assembly Resolution 3314 (XXIX), A/RES/3314. UN General Assembly. Retrieved from United Nations: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement.*
56. *UN GGE (A/70/174), 2015. Report of the Group of Governmental Experts on Report of the Group of Governmental Experts on Telecommunications in the Context of International Security. United Nations General Assebly.*

57. *UN GGE (A/76/135), 2021. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN General Assembly.*
58. *UN OEWG (A/AC.290/2021/CRP.2), 2021. Open-ended working group on developments in the field of information and telecommunications in the context of international security. UN General Assembly.*
59. *United Nations, 1945, 27 March. United Nations Charter. United Nations. Retrieved from United Nations: https://www.un.org/en/about-us/un-charter/full-text, 22 March 2022.*
60. *Weedon, J., 2015. Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine. In K. Geers, Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine (pp 67-77). Tallin: CCDCOE.*
61. *Wolff, J., 2022, 2 March. Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine. Retrieved from Time: https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/, 25 March 2022.*

e-mail: strucl.damjan@siol.net

e-mail: strucl.damjan@siol.net

Podpolkovnik dr. Damjan Štrucl je doktoriral s temo Pravni in institucionalni vidiki ureditve kibernetske varnosti in obrambe Republike Slovenije. V Slovenski vojski je zaposlen od leta 2000. Opravljal je različne poveljniške in štabne dolžnosti. Od leta 2007 do 2015 je opravljal naloge častnika za informacijsko varnost. Leta 2015 je bil prerazporejen v Odsek za kibernetsko varnost Slovenske vojske, ki ga je nekaj časa tudi vodil. Trenutno opravlja dela in naloge raziskovalca v Natovem centru za kibernetsko obrambo v Talinu.

Lieutenant Colonel Damjan Štrucl, PhD, wrote a PhD thesis on legal and institutional aspects of cyber security and defence regulation in the Republic of Slovenia. He joined the Slovenian Armed Forces in 2000, and has since then performed various command and staff duties. Between 2007 and 2015, he was an Information Security Officer. In 2015, he was assigned to the Cyber Security Detachment of the Slovenian Armed Forces, which he also headed for some time. He is currently working as a researcher at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.

*Prispevki, objavljeni v Sodobnih vojaških izzivih, niso uradno stališče Slovenske vojske niti organov, iz katerih so avtorji prispevkov.

*Articles, published in the Contemporary Military Challenges do not reflect the official viewpoint of the Slovenian Armed Forces nor the bodies in which the authors of articles are employed.