Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2463-9575
Junij 2022 – 24/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)
Junij 2022 – 24/št. 2

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Izdajatelj
Publisher
Generalštab Slovenske vojske
General Staff of the Slovenian Armed Forces

Glavni urednik
Executive Editor
generalmajor Roman Urbanč (OF 7)

Odgovorna urednica
Managing Editor
dr. Liliana Brožič

Sekretarka
Secretary
višja praporščakinja Nataša Cankar (OR-9)

Prevajanje
Translation
Iris Žnidarič

Lektoriranje
Proofreading
Justi Carey, Marjetka Brulec, Vesna Vrabič

Oblikovanje
Design & Graphic
Skupina Opus Design

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://dk.mors.si/sodobni-vojaski-izzivi
https://dk.mors.si/sodobni-vojaski-izzivi

E-naslov urednice
Managing Editor
e-mail address
liliana.brozic@mors.si

KIBERNETSKA VARNOST IN OBRAMBNI IZZIVI

»Vojaške razporeditve se oblikujejo kot voda. Voda beži pred višino in hiti v nižino. Vojna se izogiba močnemu in napada šibko.«

Sun Cu, Umetnost vojne

CYBER SECURITY AND DEFENCE CHALLENGES

»Military tactics are like unto water; for water in its natural course runs away from high places and hastens downwards. So in war, the way is to avoid what is strong and to strike at what is weak.«

Sun Tzu, The Art of War

VSEBINA
CONTENTS

Jacob Galbreath
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.0

UVODNIK

KIBERNETSKA VARNOST IN OBRAMBNI IZZIVI

Ferdinand Foch, vrhovni poveljnik zavezniških sil med prvo svetovno vojno, je leta 1910 dejal: »Letalo je zelo dobro za šport, za vojsko pa je neuporabno.« Čeprav je bil strokovnjak v svojem poklicu in je z odliko odslužil štirideset let v vojski ter sodeloval v veliko operacijah na številnih ozemljih in bil priznan ter zelo cenjen intelektualni voditelj in zagovornik napredka v kopenskem bojevanju, ni videl temeljnih tehnoloških sprememb, ki so za vedno spremenile svet. General Foch je tako kot številni drugi v njegovem času verjel, da so domene bojišča stare, kot je staro človeštvo, in absolutne. Ko pogledamo skozi objektiv zgodovine zadnjih osemdesetih let, se nam njegova izjava zdi naivna in arhaična, bežen pogled na neke preprostejše čase. Prav tako, kot so Foch in njegovi sodobniki živeli v času velikih sprememb, bomo tudi mi odslej po 24. februarju 2022 na svoje misli, izjave in pogovore zadnjih dvajsetih let gledali kot na naivne in arhaične. Kibernetski prostor je bil na vrhu Nata leta 2016 v Varšavi priznan kot domena delovanja. Enako pomembno jo je obvladovati kot nebo, morje in kopno. Razprave je konec. Organizirati, upravljati in braniti moramo sebe in svoje zaveznike, ne glede na to, kje se nasprotniki odločijo za boj ali manipulacijo z našo suverenostjo.

Ali bo v prihodnosti obstajal konflikt, ki ne bo vključeval globalnih kibernetskih akterjev? Kako uporabiti haaško in ženevsko konvencijo za globalne kibernetske akterje? Kaj se šteje za kršitev nacionalne suverenosti »v oblaku«? Kakšna je razlika med kibernetskim bojevnikom in kibernetskim vohunom? V kibernetskem prostoru za zdaj še ni dogovorjenih norm, kodeksov ravnanja ali celo skupnega razumevanja po vsem svetu ali celo znotraj držav in organizacij. Zdaj je čas, da se svobodne države dogovorimo o opredelitvah, pravilih in kodeksih ravnanja, da bomo lahko delovali globalno ne le v miru, temveč tudi sodelovali in se povezali z drugimi, da bomo tako ohranili in uveljavili red v času spopadov.

Medtem ko se to novo domeno še vedno trudimo razumeti, je rusko-ukrajinska vojna jasno pokazala, da bodo sodobne države in organizacije to področje uporabljale za delovanje, da bi dosegle svoje cilje in vplivale na rezultate v fizičnem svetu. Čeprav je kibernetski prostor edinstven, ga kljub temu ni mogoče ločiti od fizičnih domen. Nanj je treba gledati ne le kot na orodje, temveč kot na integriran sodoben hibridni aparat, ki je zelo pomemben za odpornost naše infrastrukture in družbe.

Orodja in področja vseh domen se razlikujejo, vendar imajo vsi nekaj skupnega – ljudi. Zamisli Sun Cuja, Jominija, Clausewitza, Mahana in številnih drugih intelektualcev so enako pomembne tudi v kibernetskem prostoru. Njihova spoznanja so še vedno aktualna tudi na tem novem področju. Našim ljudem, organizacijam in narodom ne smemo več dovoliti, da bi na kibernetski prostor gledali kot na sistem, ki obstaja ločeno od njihove opreme in sposobnosti, temveč jih moramo usposobiti, da na kibernetski prostor gledajo kot na integriran del celote, kar v resnici je.

Nato in svobodni narodi po vsem svetu morajo orati ledino na področju varovanja kibernetskega prostora kot globalnega vira, ki omogoča prosto izmenjavo informacij, trgovanje in izmenjavo idej. Kibernetski prostor ne pozna meja, zato moramo združiti moči za ohranitev njegove varnosti.

To lahko storimo. To moramo storiti.

Da bi dosegli postavljeni cilj, smo se odločili za sodelovanje Natovega centra odličnosti za kooperativno kibernetsko obrambo iz Tallina v Estoniji s slovensko publikacijo Sodobni vojaški izzivi, ki jo izdaja Generalštab Slovenske vojske, in pripravili tematsko številko, namenjeno aktualnim temam na področju kibernetske obrambe.

V prispevku **Henrika. P. Beckvarda** z naslovom *Zaščita kritične in informacijske infrastrukture* se najprej seznanimo s terminologijo. Kritična infrastruktura in kritična informacijska infrastruktura sta pojma, ki ju je treba definirati, preden se lahko razvije razprava o njuni zaščiti v domačem in mednarodnem okolju. Šele nato se lahko začnejo resne razprave in oblikovanje sistemskih rešitev ter njihovo poenotenje znotraj mednarodnih varnostnih struktur. Kljub razlikam v definicijah je zaznanih veliko tveganj in načinov, kako kritično informacijsko infrastrukturo zaščititi.

Tveganje za kritično informacijsko infrastrukturo in druga področja kibernetskega prostora in njegove varnosti pomenijo tudi zaposleni. Nato temu namenja veliko pozornosti, o čemer piše **Christopher Young** v prispevku *Načrtovanje za uspeh: poziv k optimizaciji kibernetskega usposabljanja v okviru Nata*. Usposabljanje v tako veliki in razvejeni mednarodni varnostni organizaciji potrebuje ustrezne pristope vrednotenja takega procesa ter njegovo nenehno posodabljanje in aktualizacijo. Kako poteka evalvacijski proces na tem področju in koliko faz vključuje, predstavlja avtor v prispevku.

Vohunstvo v kibernetskem prostoru predstavlja veliko izzivov tako za vohune kot tiste, ki želijo kibernetsko vohunjenje preprečiti ali celo kaznovati. Kaj je podlaga za sankcije, kadar so kršene splošno veljavne norme in etika? Katere pravne norme veljajo, ko se nezaželene dejavnosti dogajajo v škodo neki državi ali družbi na način, ko tega ni mogoče geografsko ali nacionalno uvrstiti glede na nacionalni in mednarodni pravni red? **Davide Giovannelli** se je posvetil tem in nekaterim drugim vprašanjem v prispevku *Zunajozemeljska pristojnost za kibernetsko vohunjenje: nov trend v mednarodnem pravu ali le primer uporabe prava kot orožja*.

Kibernetske operacije spadajo na področje dela oboroženih sil. Kot ugotavlja **Taťána Jančárková** v prispevku *Privajanje psov na povodec v kibernetski vojni,* gre za precej novo vsebino, ki mora biti ustrezno urejena, še posebej glede nadzora. Pri izvajanju kibernetskih operacij lahko pride do zlorab. Da bi to preprečili, morajo biti kibernetske operacije nadzorovane. Civilni nadzor nad oboroženimi silami naj vključuje tudi ta vidik nadzora. Avtorica v prispevku navaja nekaj pristopov k urejanju tega področja.

Kibernetska vojna se zdi logična posledica kibernetskih operacij, vendar pa te potekajo na različnih področjih, ne le v vojaškem, tudi v civilnem okolju. Kje so meje, nadzor, koordinacija in pregled stanja? **Ignacio Pizarro** v prispevku *Učenje na podlagi izkušenj: stare lekcije za novo bojišče* v primerjalni analizi ugotavlja, kakšna je razlika med novimi trendi v kibernetskem prostoru in prvimi naučenimi lekcijami, o katerih je pisal že Sun Cu. Je res vse novo ali gre mogoče za že dolgo znan pojav?

V zadnjem prispevku *Ruska agresija na Ukrajino: kibernetske operacije in vpliv kibernetskega prostora na sodobno bojevanje* **Damjan Štrucl** navaja, da je bila Ukrajina v zadnjih nekaj letih, torej pred ruskim vojaškim napadom februarja 2022, v resnici poligon za preizkušanje različnih ruskih oblik kibernetskega delovanja in kibernetske vojne. Povedano drugače: izvaja se tako imenovana Gerasimova doktrina. Avtor ugotavlja, da Zahod dojema kibernetske operacije drugače od Rusije oziroma jih uporablja za doseganje vojaških ciljev, Rusija pa jih uporablja za doseganje vseh ciljev.

Jacob Galbreath
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.00

EDITORIAL

CYBER SECURITY AND DEFENCE CHALLENGES

Ferdinand Foch, the Supreme Allied Commander during the First World War, famously said in 1910: »The aircraft is all very well for sport - for the army it is useless«. Despite achieving forty years of distinguished service across multiple campaigns and territories, being an acknowledged intellectual leader of the highest regard, and a proponent of advances in land warfare, this expert in his profession was yet completely blind to the fundamental technological shifts that would reshape the world forever. General Foch believed, as did many others in his time, that the domains of the battlefield were as old as human history and absolute. When we look back through the lens of history over the last eighty years, his statement seems naive and archaic, a glimpse of a simpler time. Just as Foch and his contemporaries lived through a time of fundamental change, after 24 February 2022, we shall now look back to our thoughts, statements, and conversations of the last twenty years as naive and archaic. Cyberspace was recognized as a domain of operations at the 2016 NATO Summit in Warsaw. Cyberspace is as critical a domain to be mastered as the skies, the seas, and the land. The debate is over. We must organize, manage, and defend ourselves and our allies wherever our adversaries decide to fight or manipulate our sovereignty.

Will there be a conflict in the future that doesn't involve global cyber actors? How do the Hague and Geneva Conventions apply to these global cyber actors? What is considered a violation of national sovereignty »in the cloud«? What is the difference between a cyber combatant and a cyber spy? Cyberspace does not yet have the agreed upon historic norms, codes of conduct, or even common understanding across the world or even within our own nations and organizations. Now is the time that we must come to an agreement between free nations on those definitions, rules, and codes of conduct so that we may operate in this global domain not just at peace, but

also cooperate and collaborate with others to maintain and enforce order in times of conflict.

While we continue to understand this new domain, what is made clear by the Russo-Ukrainian War is that modern nations and organizations will use this domain to conduct operations in order to achieve their objectives and influence results in the physical world. While cyberspace is unique, it cannot be removed from the physical domains. Cyberspace must be seen as more than a simple tool, but instead as an integrated modern hybrid apparatus fundamental to the resilience of our infrastructure and society.

The tools and terrain of all of the domains are understandably different, however they all have something in common: the people. The ideas of Sun Tzu, Jomini, Clausewitz, Mahan, and many other intellectuals are just as relevant in cyberspace. Their insights are still valid in this »new« realm. We can no longer have our people, organizations, and nations view cyberspace as a separate system to their equipment and abilities, but must instead train them to view cyberspace as the integrated part of the whole that it is.

NATO and free nations around the world must lead the way in securing cyberspace as a global resource that freely allows information exchange, trade, and the sharing of ideas. Cyberspace knows no borders or boundaries and we must act together to maintain its security.

We can do this. We must do this.

In order to achieve this goal, we decided on the cooperation of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, and the publication Slovenian Contemporary Military Challenges, issued by the General Staff of the Slovenian Armed Forces. This cooperation resulted in a thematic issue dedicated to topical issues in the field of cyber defence.

In **Henrik. P. Beckvard's** article entitled *Protecting critical infrastructure and critical information infrastructure*, we first get acquainted with the terminology. Critical infrastructure and critical information infrastructure are the concepts that need to be defined before we open a debate on their protection, both nationally and internationally. The next step is to start serious discussions and the development of systemic solutions and their unification within international security structures. Despite the differences in definitions, there are many perceived risks and ways to protect critical (information) infrastructure.

Those who pose a risk to critical (IT) infrastructure as well as to other areas of cyberspace and its security also include the employees. This topic has received a lot of attention in NATO, which is also discussed by **Christopher Young** in his article *Planning for success: a call to optimise NATO cyber training*. Training in

such a large and diversified international security organization needs appropriate approaches to evaluate such a process and to continuously revise and update it. How the evaluation process in this field is carried out and how many phases it covers is more specifically presented in the paper.

Cyber espionage poses many challenges for both spies and those who wish to prevent or even sanction it. What is the basis for sanctions when generally applicable norms and ethics are violated? What legal norms apply when unwanted activities occur to the detriment of a specific state or society in a way that cannot be geographically or nationally classified in relation to the national and international legal order? **Davide Giovannelli** addressed these and other dilemmas in his article *Extraterritorial jurisdiction over cyber espionage: a new trend in international law or just an example of lawfare*.

Cyber operations fall within the scope of the armed forces. As **Taťána Jančárková** notes in her article *Leashing the dogs of cyber war*, this is a relatively new subject that must be properly regulated, especially from the perspective of oversight. Cyber operations can lead to several types of abuses. To avoid this, they must be properly supervised. Civilian oversight of the armed forces should also include this aspect of supervision. In her paper, the author outlines some approaches to regulate this area.

Cyber war seems to be a logical consequence of cyber operations. However, the latter are not only conducted in a military but also in a civilian setting in various fields. Where are the boundaries, oversight, coordination, and overview? **Ignacio Pizarro's** paper *Learning from experience: old lessons for a new battlefield* benchmarks these new trends in cyberspace against those first lessons learned, which Sun Tzu wrote about. Is it really all new or is it perhaps a long-known »phenomenon«?

In the last article *Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare*, **Damjan Štrucl** argues that Ukraine has been a testing ground for various Russian forms of cyber operations and cyber war in the last few years, i.e. before the Russian military attack in February 2022. In other words, the so-called 'Gerasimov Doctrine' is being implemented to the full. The author notes that the West perceives cyber operations differently than Russia, or rather, it uses them to achieve military objectives, while Russia uses them to achieve all objectives.

Henrik P. Beckvard
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.1

ZAŠČITA KRITIČNE IN KRITIČNE INFORMACIJSKE INFRASTRUKTURE

PROTECTING CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE

Povzetek Ne glede na to, kako sta kritična infrastruktura in kritična informacijska infrastruktura kot njen del opredeljeni, sta obe nujni za delovanje, celovitost in varnost digitalizirane družbe. Opredeljevanje kritične informacijske infrastrukture in ocenjevanje tveganj ter nevarnosti, povezanih z njo, je prvi korak k zaščiti, skupaj z odločitvijo, da se tveganje zmanjša, odpravi ali sprejme. Za zaščito kritične informacijske infrastrukture je treba uskladiti prizadevanja in sodelovanje med resorji, ki so med seboj pogosto odvisni. Pri tem so pomembna javno-zasebna partnerstva in sodelovanje znotraj organizacij, kot sta Nato in EU.

Ključne besede ***Odpornost, kritična infrastruktura, sodelovanje med EU in Natom, javno-zasebna partnerstva, politika kibernetske varnosti.***

Abstract Regardless of how you define critical infrastructure, and critical information infrastructure as part of it, these are elements necessary for the functioning, integrity and security of a digitised society. Mapping what is critical (information) infrastructure and assessing the risks and hazards to it is a first step towards protection, along with a risk decision to either mitigate, remediate or accept the risk. For the protection of critical (information) infrastructure it is necessary to coordinate efforts and collaboration between sectors, which are often interdependent. Public-Private-Partnerships (PPP) and cooperation within organizations such as NATO and the EU are essential.

Key words ***Resilience, critical infrastructure, NATO-EU cooperation, public-private-partnerships, cyber security policy.***

Introduction

It is hardly possible to walk through the ruins of ancient civilisations without noticing the remains of infrastructure such as roads, ports, bridges, canals, aqueducts, dams and so on, all of which formed part of that society's infrastructure. Whenever infrastructure critical for the functioning of a society has been developed, steps to protect it have also been made (Assante, 2009). With the industrial revolution, and later the tech revolution, more layers have been added, but the protection of critical infrastructure is, in itself, nothing new. What sparks the current debate about strengthening the critical infrastructure sectors is, therefore, rather the amount of infrastructure that needs to be defended, the type of threats posed towards it, and the current geopolitical tensions that add to the urgency.

With the growing digitalisation and reliance on information technology (IT), and its linkage with operational technology (OT) devices controlling physical systems, »information« is today an ingrained part of critical infrastructure, and the term Critical Information Infrastructure Protection (CIIP) has become part of our vocabulary and thinking.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) conducts a week-long course in Critical Information Infrastructure Protection (CIIP) together with the Defense Information Systems Agency (DISA)[1], intended for mid-level managers responsible for the protection of critical information infrastructure. The purpose of the course is to provide students with the knowledge necessary to analyse, assess and make decisions relative to CIIP. This article does not substitute the course, but may perhaps serve as an appetiser for delving more into the processes connected with the protection of critical infrastructure (CI) and critical information infrastructure (CII).

As will be discussed, the protection of CI and CII to a large degree depends on coordination and collaboration between agencies and other stakeholders – both civilian and military, private and public. No two countries or societies are quite the same, so how the protection is carried out may vary from country to country. The purpose of this article is therefore to describe the generic aspects of CI and CII protection, and to shed light on how this protection may be carried out.

1 WHAT CONSTITUTES CRITICAL INFRASTRUCTURE AND CRITICAL INFORMATION INFRASTRUCTURE?

Before discussing what is needed for its protection, it may be appropriate to define what constitutes critical infrastructure (CI) and critical information infrastructure (CII). Most nations have their own definitions and, not surprisingly, there is no universally recognised definition of CI or CII. In the United Kingdom, the term critical national infrastructure (CNI) is used to describe *those facilities, systems,*

[1] *The Defense Information Systems Agency (DISA) is a United States Department of Defense (DoD) combat support agency composed of military personnel, federal civilians, and contractors.*

sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example) (CPNI, 2021).

As not everything within a national infrastructure sector is judged to be 'critical', the UK government's official definition of CNI is:

»Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) *Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or*

b) *Significant impact on national security, national defence, or the functioning of the state«* (CPNI, 2021).

Whether or not the critical infrastructure is »national« or simply has a national impact may be a matter of semantics. For instance, undersea cables may today be owned and operated by large companies such as Google, Facebook, Amazon or Microsoft, who have laid thousands of miles of cables along the seafloor, stretching between continents, to carry data around the world (INSIDER, 2021). In other words what is deemed to be critical infrastructure for a nation may not always be nationally owned, or even fully controlled.

Following the 9/11 attacks the United States of America, in its Patriot Act (2001), defined critical infrastructure as those *»systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.«*

According to EU Directive 2008/114/EC, »*'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions«*.

Regardless of the definition, CI may be deemed as the elements essential for the functioning, integrity and security of a society. Equally, there are many definitions of critical information infrastructure (CII). The Estonian Information Systems Agency (RIA) defines CII as *»…information and communications systems whose*

maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure.«

(RIA, 2021).

The European Union Agency for Cybersecurity (ENISA) has a slightly different definition stating that »*the definition of CII is taken from the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection: ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)«* (ENISA, 2021).

In the Critical Information Infrastructure Protection (CIIP) course conducted at the CCDCOE together with DISA, we generally maintain that CII »*includes, but is not limited to:*

– *Terrestrial and undersea cable infrastructure*
– *Internet exchange points and commercial points of presence*
– *Satellite constellations*
– *Multiple disparate networks«* (Ruonavar, 2018)

Even though definitions vary slightly it may be concluded that with the level of digitalisation today CII is an integral part of CI, which is why areas such as power supply, internet exchange points and telecommunications will remain high on the list of CI.

Ultimately, what constitutes CI also varies from country to country depending not only on, for instance, the type of industry and power sources they have, but also on geography (e.g. a land-locked state may not have listed a sea port as CI). Most countries divide their CI into sectors.

As an example the UK has 13 Critical National Infrastructure (CNI) sectors listed: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

In contrast, the US has 16 Critical Infrastructure (CI) sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems and Water and Wastewater Systems.

As there are a great number of mutual interdependencies between sectors, there is obviously also a need for coordination and collaboration between sectors – and

in some cases also between countries[2]. How to facilitate this coordination and collaboration, and who should take the lead in this process, will be dealt with in Section 4 below.

2 WHAT ARE THE RISKS TO CRITICAL INFRASTRUCTURE?

There are different ways of formulating what constitutes a risk to CI, but overall they have always been associated with physical threats and natural disasters. Both natural and human-induced (intentional or unintentional) incidents may pose risks to CI; in addition, as we have become more and more reliant on technology in our CI sectors, the cyber element has been added.

In 2013 the US Department of Homeland Security (DHS) led the process of formulating the National Infrastructure Protection Plan (NIPP) – *Partnering for Critical Infrastructure Security and Resilience*, which serves as a guide to the national (US) effort to manage risks to critical infrastructure. The NIPP (2013) identifies the three elements of critical infrastructure protection as *Physical*, *Cyber*, and *Human.*

The NIPP-process of protecting critical infrastructure focuses on addressing the three elements, *Physical*, *Cyber*, and *Human*, through a continuous and timely sharing of information, as illustrated in Figure 1 below.

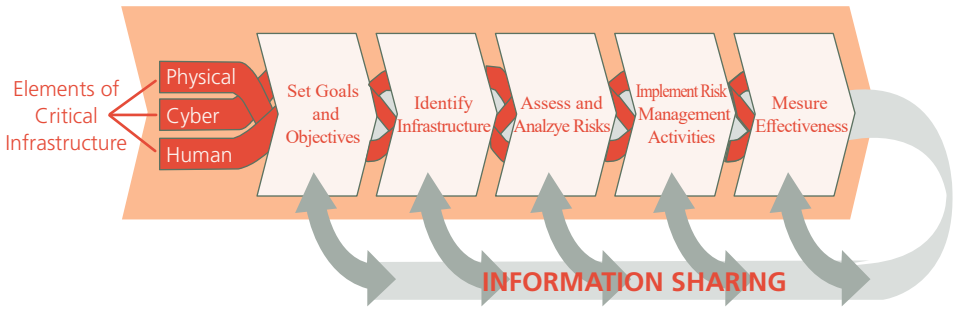


Figure 1: Critical Infrastructure Risk Management Framework (Source: US National Infrastructure Protection Plan (NIPP), Department of Homeland Security (2013))

The process includes setting goals and objectives; identifying infrastructure; assessing and analysing risks; implementing risk management processes, and measuring effectiveness. We will look further into these elements in Section 3 below: Mission Assurance Process.

[2] *Dependencies between countries could, for instance, be within the areas of energy (oil/gas), electric power, or water resources.*

The physical threats described in the NIPP may be either naturally occurring, such as a natural disaster (flooding, heavy snowfall, volcano, earthquake, tsunami etc.) or human-induced. Human-induced threats may be either intentional (a wilful act such as terrorist or other criminal activity) or unintentional (e.g. an accident or security violation). Some threats, such as forest fires, may be either naturally occurring or human-induced.

To mitigate the physical risks and hazards to a CI facility it must not only be located where it is not in direct danger from being destroyed or damaged by natural disasters, but the facility itself must also be well-protected from intentional human-induced activity such as terrorism, and unintentional human-induced activity such as an accident with an impact on the CI facility.

A perimeter fence, 24/7 guarding, CCTV, access control and so on should be in place. A facility such as an Internet Exchange Point (IXP) could also be disguised as just another building in a block, hidden in plain sight.

Just like the physical threats, the threats to CI and CII from cyberspace are human-induced as either intentional (e.g. a cyber-attack) or unintentional (e.g. failing to patch and update an IT system). Although there are other models to consider when focusing on intentional human-induced threats to CI/CII from cyberspace, two models for strengthening cyber-security immediately spring to mind – both with the aim of breaking an intruder's way into the system that is being defended.

The Lockheed Martin Cyber Kill Chain® Model (Lockheed Martin Corporation, 2015) outlines the usual steps in a cyber-attack and includes seven sequential steps for interrupting an attack:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives.

As a variation of the Lockheed Martin Cyber Kill Chain® Model, the two-stage SANS Industrial Control System Cyber Kill Chain model (SANS, 2015) focuses on attacks directed towards the Industrial Control System (ICS) in the CI system that is being targeted, rather than the IT systems.

Stage 1 of this model resembles the Lockheed Martin model (albeit with slightly different wording) and deals with Cyber Intrusion Preparation & Execution.

Stage 2 of the SANS ICS model deals with ICS Attack Development & Execution.

The third element described in the NIPP is the human factor. We have described the physical security that may help protect the CI/CII facility against intruders from outside. Another factor is, of course, the insider threat. Although rare, disgruntled employees who have a desire to harm their own company for an ideological, political or financial motive also pose a threat. To minimize such threats procedures should be in place whereby risks are identified, policies are updated, and control is implemented.

The process outlined in the NIPP (Figure 1) may vary from other processes in other nations, as institutions and responsibilities differ from country to country, but the general principle remains the same. Protection of CI and CII is not purely a question of strengthening cyber security – it is also to a large extent about strengthening physical and human security. The questions must be asked, what are you protecting, and what are you protecting against?

The approach to the protection of CI/CII must be holistic so that it is protected against the most dangerous and most likely threats. As an example, you would not have succeeded in protecting your CI/CII by rigorously updating and constantly patching your IT system if your server room is located in a cellar subject to flooding, or in a building with little or no security, or if your employees do not adhere to the security protocol. Best practices for both physical and human security must also be thought into the process.

3 MISSION ASSURANCE PROCESS

To be sure that CI/CII is protected in the best way possible and that the various sectors can still perform their mission, it is necessary to go through a process to strengthen resilience and minimise the risks.

In the UK the Cabinet Office, the National Cyber Security Centre (NCSC), and the Centre for the Protection of National Infrastructure (CPNI) have made a flyer, *Improving our Understanding of Critical National Infrastructure*, in which a five-step Criticalities Assessment is outlined. The five steps are:

1. Map Essential Functions
2. Determine Systems
3. Assess Sector Impacts
4. Identify supporting Systems, Relationships and Organisations
5. Assess Cross-sector Impacts

Essentially, the purpose of the (US) Mission Assurance Process is the same as the UK model – to be able to make a Risk Decision to either mitigate a risk, remediate it, or accept it, if the risk cannot be dealt with.

I have chosen to present the Mission Assurance Process (Figure 2 below) based on an illustration by DISA showing the process described in the (US) Department of Defense Directive 3020.40 of 2016.

Although focused on the US, the directive has some general aspects and the process seems both elaborate and simple and may be universally applied.

The illustration in Figure 2 has been amended to be more generically applicable to countries outside the US, and hopefully will be broad enough to be of direct value for nations wishing to strengthen the protection of their CI/CII.

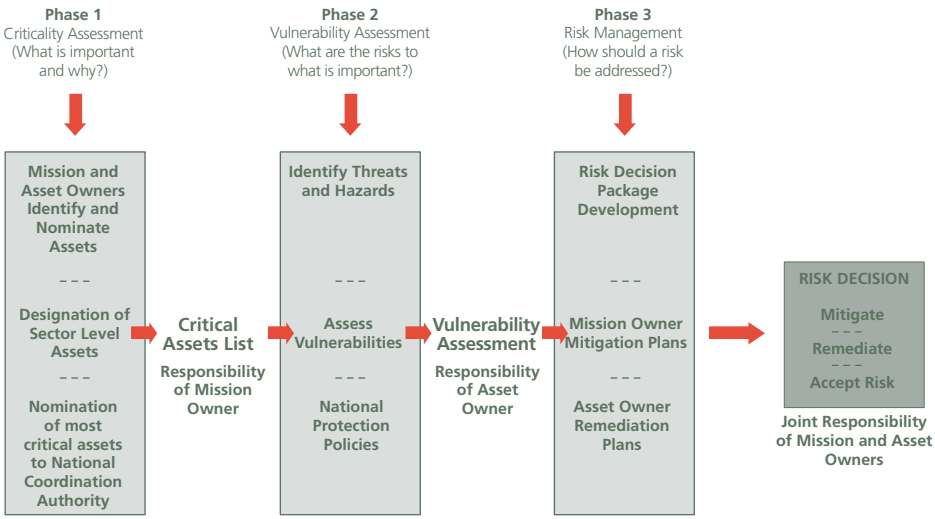


Figure 2: Mission Assurance Process (Source: Based on DISA illustration of US DoD Directive 3020.40 – Mission Assurance)

For much of the CI/CII in our societies, the sector responsible for maintaining a service and those who actually perform it are not the same. The level of privatisation may vary from country to country, but in many cases services have been outsourced to private companies, so the mission owner (sector) and asset owner (company) are not the same.

In **Phase 1** of the Mission Assurance Process, mission owners and asset owners must make a Criticality Assessment determining what is important and why by identifying and nominating assets to a national coordination authority. The mission owner puts these assets on the Critical Assets List.

In **Phase 2** of the process the asset owner will identify threats and hazards by determining what the risks are to what is important and make a Vulnerability Assessment.

In **Phase 3** a plan for Risk Management is formulated by how the risks should be addressed. The mission owner will determine what steps could be taken to mitigate the risk, and the asset owner will plan steps to remediate the hazards.

Based on the outcome of Phases 1-3 a Risk Decision may be formulated to mitigate risks, remediate hazards, or to accept the risk as a condition.

Forming a national coordination authority with all sectors represented and mapping the CI/CII and the interdependencies of different sectors would be a first step (i.e. determining which sectors rely on the services of others).

As illustrated in Figure 3, it would quickly become apparent that most CI sectors have interdependencies with each other and, therefore, there is a great need for cross functional coordination and collaboration. In many instances the sector response to risks are »stovepiped« with not enough coordination between sectors.

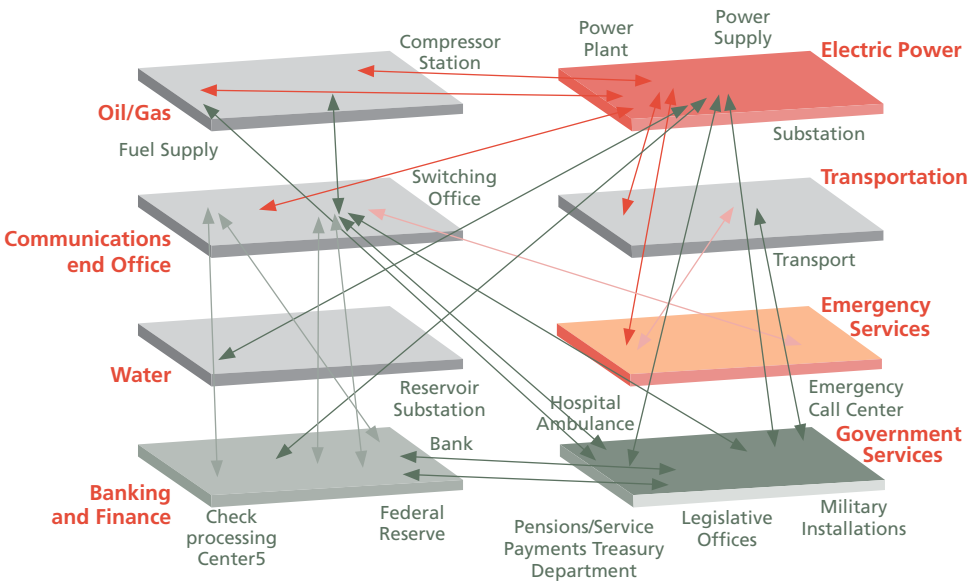


Figure 3: Interdependencies between CI/CII sectors (Source: Ehlen, M. A., Critical Infrastructure Interdependencies, Researchgate.net)

4 COORDINATION, COOPERATION AND PUBLIC PRIVATE PARTNERSHIP

As described in the Mission Assurance Process, CI/CII mission and asset owners need to coordinate their efforts and work closely together. Many of the CI/CII assets and services are today privately owned, whereas the mission owner would normally be a government institution with the responsibility of delivering services within a given sector. For example, a ministry in a country would have overall responsibility for telecommunications, but the services would be provided to the citizens via privately owned and operated telecommunication providers.

In this instance (and examples like it in other CI/CII sectors) there would be a need for close coordination and cooperation between the public and private entities – government agencies and private companies.

According to the European Union Agency for Cybersecurity (ENISA), a »*public-private partnership (PPP) is a long-term agreement/cooperation/collaboration between two or more public and private sectors that has developed through time in many areas*.«

In November 2017 ENISA published *Public Private Partnerships (PPP) Cooperative Models* in which a number of recommendations concerning PPP were brought up:

- Motivation for the private sector to participate should be a priority when establishing a PPP
- The participants should agree to a legal basis when creating a PPP
- Public institutions should lead the PPP or the national action plan for PPP
- PPPs should invest on internal private-private and public-public collaboration
- PPP participants should invest on open communication and a pragmatic approach towards building a PPP
- The representatives of the government should be allowed to participate in the meetings with non-disclosure agreement
- Small and Medium Enterprises (SMEs) should also participate in PPPs

In addition to these points a PPP should form the basis for sharing best practices, as well as actionable information. Furthermore, public entities often have access to information and resources not available to the public, and have the authority to launch criminal investigations and law enforcement actions.

It is also the government which is in a position to regulate areas such as the level of requirement to share information. In many cases private companies would probably be reluctant to publicly state that they have been the victim of, for example, a ransomware attack, as stock prices may be affected. On the other hand sharing such information in a PPP may help to put a stop to such attacks.

A well-functioning PPP is built on trust and dialogue in equal terms, which is why it is important for regulators to base a regulation on, for example, sharing information about cyber-attacks (or other forms of attack) directed against the CI/CII assets (public or private companies), on a shared understanding of the level and speed of information needed to be provided.

An aspect of PPP often overlooked or neglected is exercises. Each year the CCDCOE conducts Locked Shields – a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world. This exercise also makes it possible for the participants to train and exercise PPP within their national teams.

With the goal of enhancing cyber security in the European Union (EU), the European Commission made the first EU-wide legislation, the Network and Information Security (NIS) directive (EU 2016/1148)[3]. As it is an EU directive, EU Member States have begun to adopt national legislation incorporating the content.

The NIS Directive consists of three parts:

National capabilities, whereby EU Member States must have certain national cybersecurity capabilities, e.g. having a national Computer Security Incident Response Team (CSIRT), and carrying out cyber exercises, etc.

Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.

National supervision of critical sectors such as energy, transport, water, health, digital infrastructure and the finance sector.

The European Commission has now proposed a NIS2 Directive to introduce a common higher level of cyber security in the EU. Among other things the NIS2 Directive would *strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU* (European Parliament, 2021).

It follows from Article 3 of the North Atlantic Treaty that *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.*

Even though a (cyber) attack directed against CI/CII in a NATO Member State does not reach the threshold for an armed attack, it still follows the principle of Article 3

[3] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union.*

that each Member Nation should be resilient and take its own precautions to protect its CI/CII.

The NATO Computer Incident Response Capability (NCIRC) is responsible for protecting NATO's own networks and sites (NATO, 2022). In a similar manner the EU Institutions have set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies.

As NATO and the EU face many of the same challenges in cyber security, the two organisations are cooperating by, for instance, increasing their information sharing on cyber incidents. In this context NCIRC and CERT-EU signed a technical arrangement on 10 February 2016.

Ambassador Sorin Ducaru, NATO Assistant Secretary General for Emerging Security Challenges at the time, stated that the *»…agreement facilitates technical information sharing between NCIRC and CERT-EU to improve cyber incident prevention, detection and response in both organisations, in line with their decision-making autonomy and procedures«* (HSD, 2016).

Since then NATO-EU cooperation has increased, and apart from information sharing also covers coordinated planning and concrete cooperation (EU Defence, 2020).

Regardless of whether the cooperation is national in the form of PPP or supranational in the form of NATO-EU cooperation, we, both as individual countries and as NATO and/or EU Member States, stand a better chance of protecting our CI/CII if we coordinate our efforts and cooperate by sharing actionable information.

Conclusion

There is no uniform definition of critical infrastructure (CI) and critical information infrastructure (CII), but CI may be defined as the elements essential for the functioning, integrity and security of a society. Likewise CII may be described as *»…information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure«* (RIA, 2021).

According to the (US) National Infrastructure Protection Plan (NIPP) – *Partnering for Critical Infrastructure Security and Resilience,* the risks to CI/CII may be either *Physical*, *Cyber* or *Human* related, or a combination thereof.

Physical threats may be either natural or human-induced (intentional or unintentional) and protective measures should be implemented to secure the functioning of the CI/CII facility.

The seven-step Lockheed Martin Cyber Kill Chain® Model and the two-stage SANS Industrial Control System (ICS) Cyber Kill Chain may serve to illustrate the cyber threats, and finally, the human threats may take the form of either intentional

or unintentional actions. Although rare, insider threats cannot be discounted and control measures must be implemented and followed by all staff.

No two countries are exactly alike and there is no »one size fits all« solution, but in order to properly protect CI/CII it is necessary to conduct the national variant of the Mission Assurance Process with:

– a Criticality Assessment (what is important and why?);
– a Vulnerability Assessment (what are the risks to what is important?);
– and Risk Management (how should the risk be addressed?)

Based on this, it is possible to make a Risk Decision to either mitigate, remediate, or accept the risk.

Finally, the interdependencies between sectors, as well as the coordination of efforts and cooperation between actors – both nationally in the form of PPP and internationally in organisations such as NATO and the EU – are hugely important. Most countries operate with sector responsibilities, but it will be crucial for success that the interdependencies are well known and efforts are coordinated centrally, with representation from the necessary actors, both public and private.

Bibliography

1. *Assante, M., J., Infrastructure Protection in the Ancient World, 2009, Proceedings of the 42nd Hawaii International Conference on System Sciences. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.7316&rep=rep1&type=pdf, 14 March 2022.*
2. *CERT-EU, RFC 2350, Version 5.2, 2022. https://media.cert.europa.eu/static/RFC2350/RFC2350.pdf, 26 March 2022.*
3. *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, Article 2(a), 2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG&toc=OJ%3AL%3A2008%3A345%3ATOC, 10 March 2022.*
4. *Ehlen, M. A., Critical Infrastructure Interdependencies, Researchgate.net, 2013. https://www.researchgate.net/figure/Critical-Infrastructure-Interdependencies_fig3_257560357, 15 March 2022.*
5. *ENISA, Critical Information Infrastructures, 2021. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii?tab=details, 10 March 2022.*
6. *ENISA, NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, 16 March 2022.*
7. *ENISA, Public Private Partnerships (PPP) Cooperative Models, 2017. https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models, 16 March 2022.*
8. *ENISA, Public-Private-Partnership (PPP). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps, 16 March 2022.*
9. *EU Defence, EU-NATO Cooperation, 2020. https://www.eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf, 26 March 2022.*
10. *EUR-Lex, Document 32016L1148, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 16 March 2022.*

11. *European Commission, NATO and CERT-EU Discuss Cyber Threats ahead of EU Elections, 2019. https://ec.europa.eu/info/news/nato-and-cert-eu-discuss-cyber-threats-ahead-eu-elections-2019-may-06_en, 26 March 2022.*
12. *European Parliament, The NIS2 Directive - A High Common Level of Cybersecurity in the EU, 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, 17 March 2022.*
13. *HSD Securitydelta.nl, NATO and the European Union Enhance Cyber Defence Cooperation, 2016. https://securitydelta.nl/news/newsitem/587-nato-and-the-european-union-enhance-cyber-defence-cooperation, 26 March 2022.*
14. *INSIDER, Photos: How Facebook and Google use sonar ships, gigantic underwater plows, and divers to lay thousands of miles of undersea internet cables around the globe, 2021. https://www.businessinsider.com/google-facebook-giant-undersea-cables-internet-tech-2021-9, 9 March 2022.*
15. *Lockheed Martin Corporation, Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform, 2015. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf, 14 March 2022.*
16. *NATO (The North Atlantic Treaty Organization), Cyber Defence, 2022. https://www.nato.int/cps/en/natohq/topics_78170.htm, 23 March 2022.*
17. *RIA - Republic of Estonia Information System Authority, Critical Information Infrastructure Protection CIIP, 2021.https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html, 10 March 2022.*
18. *Ruonavar, F. P., DISA Task Critical Asset Nomination Process, 2018. https://www.disa.mil/-/media/Files/DISA/News/Events/Symposium/1---Rounavar_DISA-Task-Critical-Asset-Nomination-Process_approved-FINAL.ashx, 10 March 2022.*
19. *SANS, The Industrial Control System Cyber Kill Chain, 2015.https://na-production.s3.amazonaws.com/documents/industrial-control-system-cyber-kill-chain-36297.pdf, 14 March 2022.*
20. *The North Atlantic Treaty, 1949. https://www.nato.int/cps/en/natolive/official_texts_17120.htm, 17 March 2022.*
21. *UK Cabinet Office, the National Cyber Security Centre (NCSC), and the Centre for the Protection of National Infrastructure (CPNI), Improving our Understanding of Critical National Infrastructure, 2020. file:///C:/Users/henrik.beckvard/Downloads/CNI%20Criticalities%20KB%20Flyer%20(2).pdf, 14 March 2022.*
22. *UK Centre for the Protection of National Infrastructure (CPNI), Critical National Infrastructure, 2021. https://www.cpni.gov.uk/critical-national-infrastructure-0, 9 March 2022.*
23. *US Department for Homeland Security, National Infrastructure Protection Plan (NIPP) – Partnering for Critical Infrastructure Security and Resilience, 2013, p 15. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, 11 March 2022.*
24. *US DoD Directive 3020.40, Mission Assurance (MA), 2016. https://irp.fas.org/doddir/dod/d3020_40.pdf, 14 March 2022.*
25. *US Patriot Act, PUBLIC LAW 107–56—OCT. 26, 2001, UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, P.L. 107-56, §1016(e), 2001. https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, 10 March 2022.*

e-mail: henrik.beckvard@ccdcoe.org

Christopher Young
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.2

NAČRTOVANJE ZA USPEH: POZIV K OPTIMIZACIJI KIBERNETSKEGA USPOSABLJANJA V OKVIRU NATA

PLANNING FOR SUCCESS: A CALL TO OPTIMIZE NATO CYBER TRAINING

Povzetek Usposabljanje je naložba v jutrišnji dan, ki jo spodbujajo današnje potrebe in viri. Pravilno oblikovanje usposabljanja je zamudno, še zamudneje pa je, če ga izvedemo slabo. Model, ki ga Nato uporablja za oblikovanje in evalvacijo svojih programov usposabljanja, temelji na sprejetih področnih standardih, vendar pa se v okviru kibernetskega prostora ne uporablja nujno v celoti. Učinkovitost modela je odvisna od objektivne kakovosti rezultatov, ki jih ustvari, vendar so razvojne pobude pogosto prenagljene ali premalo podprte. Tudi sedanje evalvacijske prakse ne potrjujejo dovolj kakovosti pripravljenega usposabljanja. Načrtovanje mora biti skrbnejše in bolj premišljeno, da se oblikujejo dobre rešitve v kibernetskem usposabljanju za zavezništvo in zagotovi doseganje organizacijskih ciljev.

Ključne besede ***Model ADDIE, učinkovitost usposabljanja, vrednotenje, Kirkpatrickov model.***

Abstract Training is an investment in tomorrow fueled by the needs and resources of today. It is time-consuming to build training correctly, but even more so to do it poorly. The model that NATO uses to create and evaluate its training programmes is based on accepted industry standards, but it is not necessarily being used to its full potential in the area of cyberspace. The efficacy of the model is predicated on the objective quality of the deliverables it produces, yet development initiatives are often rushed or under-supported. Current evaluative practices also do not sufficiently confirm the quality of the training produced. More careful and deliberate planning is required, not only to create valid cyber training solutions for the Alliance, but also to ensure that its cyber training achieves organizational goals.

Key words ***ADDIE Model, training efficacy, evaluation, Kirkpatrick Model.***

Introduction

Like any large organization, NATO has at its disposal many options for achieving its strategic goals in cyberspace. Policies can specify tasks and measures of quality, or programs can help simplify workflow, improve communication and manage resources. A tool NATO frequently relies upon to effect changes in human behavior is Education and Individual Training (E&IT). While highly valued by the Alliance, training can be costly to implement and maintain. In 2015, it was estimated that 356 billion was spent globally on corporate E&IT ventures (Beer et al., 2016, p 3). A 2010 Chapman Alliance analysis provides some granularity on the cost, suggesting that, on average, companies spent nearly 6,000 per hour to create instructor-led E&IT and just shy of 10,000 to create one hour of e-Learning E&IT (Chapman, 2010). While somewhat dated, the Chapman study helps to provide an appreciation of the magnitude of the cost behind creating training.

Considering the high cost associated with training, how significant of a return on investment is NATO recognizing for its cyber E&IT ventures? The only way to know for sure is to weigh the known impact of an E&IT solution (i.e. a course) on organizational performance or goals against the cost incurred to create it. Presumably owing to its nature as a unique multinational military defence institution, however, there are limited publications available in the public domain that speak to how NATO builds or revises its training. Accordingly, there is seemingly no publically available research on the potential efficacy or financial cost of any Alliance training. The matter of training efficacy in general is, however, a widely studied topic.

The language throughout NATO's training policy governing the lifecycle of its E&IT initiatives acknowledges the importance of evaluating training efficacy. The structure it uses to guide its training evaluation process is based on the widely accepted Kirkpatrick model, but there appear to be some challenges in how training is constructed and evaluated at the ground level. This article will juxtapose NATO's E&IT policy against relevant research in these fields to identify areas where the Alliance falls short in its efforts to secure a return on its investment in training, and offer suggestions for improvement where possible. Occasionally, arguments will be supported by the empirical observations of the author, who has worked as an E&IT specialist within the NATO cyber community for the last year and a half.

Prior to proceeding, it is prudent to mention that while the experiences referenced within this article occurred during the course of the author's employment with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the opinions expressed within are entirely his own and do not necessarily reflect those of the CCDCOE, NATO, or anyone else.

The author would also like to acknowledge that all personnel working to improve the cyber E&IT portfolio of the Alliance are exceptionally hardworking and dedicated professionals. Every success the Alliance has experienced in creating, managing and revising cyber E&IT is due entirely to their ongoing deliberate efforts and commitment. Any problematic issues referenced within this article occurred despite

the best efforts of these professionals to prevent them. The challenges identified forthwith are largely systemic in nature and cannot justly be attributed to any negligent or malicious activity.

1 CONTEXTUALIZING CYBERSPACE WITHIN NATO

The first step in the discussion is to contextualize several key pieces of information contributing to the current state of affairs in NATO cyberspace E&IT. In particular, the relative immaturity of the domain and its varying national interpretations have helped to create a situation where the necessary subject matter expertise is somewhat scarce[1].

In a relatively short time, NATO had to figure out how to begin incorporating cyberspace into its existing structures. On the heels of a politically motivated cyber attack on Estonia in 2007, NATO adopted its first cyber defence policy in 2008. In 2014, the Alliance proposed that a cyber attack could possibly lead to the invocation of Article 5, NATO's collective defence policy stipulating that an attack on one Alliance member is an attack on all. Finally, in 2016, NATO recognized cyberspace as a domain of operations (Brent, 2019).

To the layman, this would imply that cyberspace is now placed on an equal footing with its other established domains of operation: air, land, sea and space[2]. One key distinction, however, is that while it is possible to exclusively conduct warfare in cyberspace, the ubiquitous global reliance upon technology makes it almost impossible for any modern military to function independently of cyberspace. NATO recognized this connection in its 2018 »NATO Cyberspace Operations Strategic Training Plan« which, as the name aptly suggests, serves as the Alliance's framework guidance to establishing strategic aims for NATO's E&IT efforts in cyberspace[3].

Developing E&IT solutions that achieve the Alliance's cyberspace needs is anything but straightforward. Larger international entities such as NATO or the EU, for example, were only able to attempt to regulate the domain after individual constituent nations had done so first. As cyberspace is a completely human-constructed domain, how it is defined, used and protected within a nation can greatly vary according to that nation's specific needs. National cybersecurity strategies are uniquely tailored to the needs and priorities of individual nations (ITU, 2021, p 13), meaning nations train and employ people to function within cyberspace in a variety of ways. Conceptual discrepancies in and of cyberspace at the national level impede the Alliance's ability to develop cyber E&IT based upon a common body of knowledge. This is a standard requirement of systematic instructional design (Chyung, 2008, pp 81-87), and indeed a component of the Systems Approach to Training (SAT) model NATO uses to create training (NATO, 2015, para 6-5).

---

[1] *Many of these particular issues are worthy of research and exploration in their own right; however, their role within this article will be to set the stage for further discussion of other relevant factors.*

[2] *NATO added space as a domain of operations in 2019, after cyber.*

[3] *This document is not available to those working outside of NATO, and hence, it is not cited.*

Foundational discrepancies in and of cyberspace at the national level can alter the speed at which personnel arriving in NATO billets are able to function as needed. The frustration felt by NATO cyberspace personnel over this discrepancy has led to increased demands for the development of common cyberspace domain foundational training. Individual NATO nations have also expressed a desire to build their own cyber E&IT framework in accordance with common NATO standards. Such initiatives are needed, but often difficult to bring to fruition as nations are often reluctant to discuss capabilities and vulnerabilities within cyberspace (Ertan et al., 2021 p 5, 8).

Despite NATO's recognition of how cyber impacts other domains, the Alliance and many of its member nations still struggle with how to best to integrate cyber into joint functions, battle rhythms and existing collective exercises (Ertan et al., 2021, p 7). For example, an existing NATO operational planning course at one Education and Training Facility (ETF) was unable to incorporate many cyberspace planning considerations owing to an already full curriculum and inflexible schedule. To correct this shortfall, an existing CCDCOE course was approved to train operational planners to incorporate unique cyberspace aspects into the established process. However, not all NATO personnel requiring the original planning course need the cyber »top-up« training, suggesting some reluctance outside the cyber community to acknowledge the cyber domain's impact on established norms and practices.

In recent months, the Alliance has made numerous attempts to develop targeted training that will help cyber gain wider acceptance within the Alliance, but there is a current shortage of available NATO expertise to lean on for input. Expertise takes time to develop and is a critical component for developing effective E&IT solutions (Clark, 2008, pp 5-15). Given the limited availability of subject matter experts to support cyber E&IT development, every effort must be made to ensure the best possible use of any contributions they provide.

2 NATO'S TRAINING GOVERNANCE FRAMEWORK – GLOBAL PROGRAMMING

In order to gain a deeper appreciation of the challenges facing the Alliance's cyber E&IT, one must first understand the environment and structures NATO relies upon to effect its E&IT solutions. NATO employs a governance framework called Global Programming to define and satisfy its E&T requirements through the conduct of individual (i.e. courses) and collective (i.e. exercises) training (NATO, 2016, para 2-5 c(2))[4]. Within this framework, NATO places oversight of individual and collective training on Allied Command Transformation (ACT), to meet the operational requirements identified by Allied Command Operations (ACO).

[4] *Technically, the term E&IT (Education and Individual Training) specifically refers to the courses created to meet NATO training, whereas E&T refers to both E&IT (courses) and collective training (exercises) together. Global Programming manages both E&T and E&IT, yet its SAT policy (discussed in Section 5) applies explicitly to the creation and management of E&IT.*

To streamline the process to map its requirements, NATO categorizes its needs into disciplines which NATO defines as »a NATO approved body of knowledge and skills that outlines an existing or evolving E&T requirement« (NATO, 2015, para 2-2). Cyberspace Operations is one such discipline. Both individual and collective training are integral and complementary components of the operational readiness of any discipline[5].

Broadly speaking, Global Programming outlines the roles and responsibilities of all parties in the process to support NATO's E&T requirements. It outlines NATO's responsibility to define requirements (via ACO) and manage the framework itself (via ACT), but it also requires contributions from entities residing outside of NATO's command and control in order to function. Each discipline requires a Department Head (DH) who is accountable to NATO to ensure that training solutions exist to satisfy the evolving requirements of the Alliance (NATO, 2015, para 2-6). To simplify the process, the DH identifies existing courses that meet NATO needs, or leads the process to create new courses as required. The CCDCOE acts as the DH for the Cyberspace Operations discipline[6]. As a NATO-accredited Centre of Excellence (COE), the CCDCOE operates outside NATO's direct influence, but contributes to the development and delivery of NATO training by conducting NATO training and providing subject matter experts and instructors for other ETFs as needed. Finally, ETFs are required to help create and deliver NATO training. All ETF's supporting NATO cyberspace training also operate outside of NATO's direct sphere of influence.

Global Programming is reliant upon specific deliverables and inputs, the quality of which directly correlate to the efficacy of the framework itself. From a business standpoint, it is far more cost effective for NATO to outsource the coordination and creation of these products than to manage them all internally. This planned flexibility allows the Alliance to focus on end results rather than the process by which they are achieved. Unfortunately, the flexibility required to maintain this framework has occasionally forced the Alliance to make certain compromises in its training.

3 NATO SYSTEMS APPROACH TO TRAINING (SAT)

The SAT model that NATO employs within Global Programming to guide the process by which courses are created and maintained (NATO, 2015) is based on the ADDIE model (see Figure 1). This model is a common industry standard systems model for building training, and NATO's own adaptation is based upon a version of ADDIE used by the Canadian Armed Forces to manage its training.

[5] *The primary focus of this article is on individual training with periodic reference to collective training as required.*

[6] *The author primarily works in support of the DH function at the CCDCOE.*

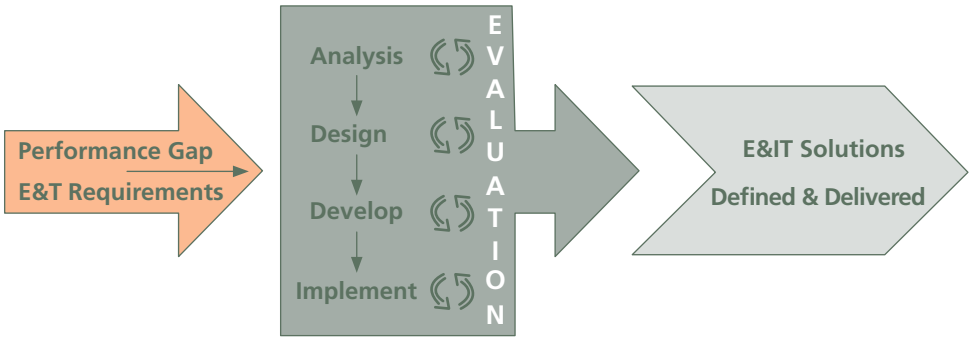


Figure 1: NATO Systems Approach to Training Model (NATO, 2015, para 4-6)

The ADDIE model consists of five phases: analysis, design, development, implementation, and evaluation. These phases are intended to be sequential yet iterative with the success of each phase being largely dependent upon the quality of work produced in the previous phases (Welty, 2008, p 66). The final letter in the acronym, evaluation, has two distinct yet important roles. First, it occurs throughout the process as a measure of periodic quality control. Secondly, it also occurs as a separate and distinct phase after implementation to assess the effectiveness of the solution against the identified problem, and it guides follow-on adjustment activities if required (Chyung 2008, Welty, 2008, p 66). The phases of this model as they pertain to NATO are summarized in Table 1.

Table 1: NATO SAT Overview (prepared by the author)

Phase	Objective	NATO Input	NATO Output	Lead
Analysis	Define the expected performance standards that E&IT will achieve (CCD II)	Determination that E&IT will correct the problem	CCD I (agreement to conduct training) / CCD II (defined performance standard)	DH[7]
Design	Create a structured plan (program) of instruction (CCD III) to train to the standard in the analysis phase	CCD II	CCD III[8] (programme of instruction)	DH / ETF[9]

[7] *Department Head – the entity accountable to NATO to ensure that training solutions exist to satisfy the evolving requirements of the Alliance (NATO, 2015, para 2-6).*

[8] *Course Control Documents (CCD) refer to specific NATO deliverables produced during the NATO SAT process. The core elements captured within CCD II and CCD III reflect requirements of training created via the ADDIE model in settings beyond that of NATO.*

[9] *Education and Training Facility – an institution where NATO training is delivered.*

Development	Develop and/or procure all resources necessary to conduct the course	CCD III	Lesson plans, presentations, training aids, etc.	ETF
Implementation	Deliver the course (ideally first through a »pilot« trial)	Design and development outputs	Trained students	ETF
Evaluation	Assess course integrity to confirm the degree to which the analysis standard was achieved	Trained students	Validated training solution and/or suggested areas of refinement for any/all earlier phases	ETF (internal) NATO (external)

Of note is that prior to engaging any model to develop a training solution (ADDIE or otherwise) a thorough analysis of the performance problem must be conducted to determine the most appropriate means to correct it (Christensen, 2018, p 38). Unfortunately, this critical step is often inadvertently bypassed, thereby immediately placing a proposed E&IT solution on unsteady ground. Premature selection of E&IT creates the illusion that the problem has been solved when perhaps it has not (Shushan, 2012, p 61, Spitzer, 1984, 6). A decision to develop training to correct a performance problem implies an immediate step toward addressing the issue, whereas the necessary step of analysis can sometimes be incorrectly equated with inaction. Even if training is the correct solution for a performance gap, a proper »needs assessment« will provide valuable insight into the nature of the problem, and will help reinforce the quality of the training solution. At the very least, it will ensure that all future work remains aligned with the scope of the original problem (Christensen, 2018, p 38).

Once training is identified as the correct response to address a performance problem, the analysis phase commences. Here, the DH establishes a team of experts and guides them through the process to define clearly the standard of performance that the training solution will eventually achieve. The results of this process are captured within a document NATO calls a CCD II. From a change management perspective, this also helps to define the scope of the deliverables and outlines the desired result that all follow-on work will achieve (James and Ward, 2001, pp 158-159).

During the design phase, the designated ETF creates a programme of instruction outlining the path of learning for the proposed training solution. Within NATO's framework, this document is called a CCD III. On behalf of NATO, the DH is responsible for verifying that the CCD III fully addresses the standard identified within the CCD II. A quality CCD III outlines topics of instruction as well as methods of instruction and assessment. Ideally, the course and its assessments will

conceptually emulate working conditions as closely as possible (Coscarelli and Shrock, 2007, p 44). The rationale is that this will stimulate learning transfer, that is, to ensure that the candidate will be able to apply that which they learn during the course within the workplace (Burke and Saks, 2012, p 118).

ETFs within the cyber community proficiently conduct the development and implementation phases within the ADDIE model. These two phases essentially involve preparing and executing the plan as laid out within the CCD III, and lend themselves well to the supervision of a project manager. Most problems, however, reside within the details of the CCD III derived from the design phase. Compromises on the structure and granularity of CCD IIIs can expedite the process by which courses are designed, but it can also affect course integrity[10].

NATO's policy governing the SAT process provides guidance on the requirements of a CCD III. In the author's experience, however, the importance of a CCD III document is often underestimated, due to pressure to quickly move on to subsequent phases where more tangible deliverables are produced. Some ETFs proceed into development once broad training topics are defined. This can lead to gaps or overlaps within a course if the problem is not corrected or losses of time if corrections are ultimately made.

Such a decision can result in flaws within a course that lead it to fall short of intended expectations (Bunch, 2007, p 145). Regrettably, acts of this nature have threatened the efficacy of more than one cyber training solution. Of note, one recent cyber E&IT solution prematurely proceeded to the development phase and had the unintended effect of slowing down lesson plan development. Specifically, subject matter experts were asked to create lessons with only broad guidance on topic and lecture duration, and without addressing the assessment standard that their lessons would ultimately prepare students to achieve. This oversight resulted in increased revision time for some subject matter experts based on back and forth communication with the responsible ETF, and eventually slowed down the process by which the lessons were developed.

Even though the CCD III is the responsibility of the ETF to manage, it is within NATO's best interests to encourage more granularity in the document for newly developed training solutions. Formulating a properly detailed plan before attempting to execute it may give the initial impression that a project is moving slowly, but it will pay off in the long run by limiting the need to revisit and correct previous errors based on goals that were initially unclear or unrefined (James and Ward, 2001). As the old adage suggests, it is best to measure twice and cut once.

[10] *These issues are typically observed during the evaluation process.*

4 CUSTOMER FUNDED EDUCATION AND TRAINING FACILITIES (ETF)

All ETFs that deliver NATO cyber training are customer-funded, which is the norm for the Alliance (NATO, 2015, para 2-12). Under this approach, NATO provides funding to design and develop new courses and to conduct major revisions to existing ones. The ETF itself is responsible for funding the delivery and routine maintenance of its NATO courses. Like any business, customer-funded ETFs must generate more revenue than they expend if they are to operate under this model.

ETFs generally rely upon revenue from tuition to maintain their training portfolios, although some ETFs have additional mechanisms in place to minimize tuition fees. It is also important to note that in addition to design and development costs, NATO is still responsible for paying the tuition of personnel that it sends on training courses. ETFs are also typically free to gain revenue by offering their training to entities outside of the Alliance.

ETFs such as the CCDCOE and the NATO School Oberammergau (NSO) partially subsidize the cost of attending training through established national or governing body funding and the staff provided to them by member nations. Their tuition costs are €500 per course (NATO CCDCOE, 2021, p 12) or €550 per week (NATO School Oberammergau, 2021), respectively. The NATO Communications and Information Agency (NCIA) Academy does not have the same supports at its disposal to subsidize its training and, as such, it relies more on tuition and other fees paid by attendees to cover the operating costs. NCIA training is substantially more expensive at an average cost of €1,100 per week (NCI Agency, 2020, p 17).

Keeping in mind the pressures that all organizations face to manage their budgets, the cost of customer-funded training is of concern to both ETFs that deliver training and any organizations that pay tuition. Some institutions which support the development of cyber training have placed pressure on designated ETFs to reduce tuition in exchange for their services. Such practices have slowed down development on occasion. Other institutions have expressed interest in having new courses developed at ETFs with lower tuition and development costs even if they are less suited to conducting the training in question. Even though the NCIA is the most expensive option for cyber E&IT, it is often easier for them to incorporate new courses into their portfolio than it is for most other ETFs. Opposition to their accepted and transparent business model can, however, contribute to delays in their ability to develop training.

Given the approach of many ETFs to establish tuition costs relative to the duration of their courses, there is often a need for NATO and ETFs to compromise on course content to confine training to one or more calendar weeks. This was the case for the previously mentioned operational planning course, which could not be extended to include additional cyber related content. Spitzer (1984, p 6) cites the practice of allowing such constructs to drive training duration rather than the training requirements themselves as one of 39 reasons why training commonly fails. The fact

that most of Spitzer's assertions remain valid nearly 40 years after initial publication speaks volumes about the failure of the education and training community to learn from history.

For one course under development at an ETF, the curriculum identified within the design phase necessitated eight training days; however, the aim was to conclude all training within one week. The increased tuition for an additional week was one factor that contributed to the Alliance's decision to ultimately separate the course into two smaller, sequential ones. In this particular instance, splitting the training was the correct decision. It placed an emphasis on addressing the original identified requirements, and allowed for the development of a desperately needed cyberspace foundational course that is suitable for a much wider audience than the original requirement addressed. This was only feasible, however, because both course projects reside within the same discipline and ETF.

The necessary decision to split this course into two separate ones, however, was not without consequence. The funding provided by NATO to cover design and development costs for the original course was expended. Funding for any additional design and development work for the two new courses could not be obtained. Arguably, any design and development costs for the revised courses would have been minimal, as much of the previously developed resources were still usable, but some work still needed to be done. The absence of funding for this work forced the ETF to find the time and money to make corrections within its existing resources, and was counterintuitive to NATO's SAT process. Specifically, the lack of funding prevented a thorough evaluation of these changes on previous analysis and design assumptions before continuing with development.

5 LACK OF EDUCATION AND TRAINING EXPERTISE

An often overlooked barrier that NATO must contend with in the application of its training model are the assumptions and beliefs held by institutional leadership across all partner entities with regard to E&IT. Most personnel working within the greater NATO training community are unfamiliar with the processes by which courses are created both within NATO, or even in general. There is a widely held misconception that NATO's existing E&IT policy documentation is sufficient in and of itself to help non-experts create and manage efficient training solutions. However, if creating a training solution was as simple and straightforward as reading a book or following a policy, there would likely not be an abundance of research on failed training initiatives.

In practice, individual conflicting interpretations of NATO's E&IT policy documentation, coupled with personal assumptions about training, create more problems than they resolve, and account for the majority of the author's efforts working as an E&IT specialist within the cyber domain. Unfortunately, assumptions made by organizational leadership often prematurely lead to training being identified

as the best means to address a performance problem without any noteworthy analysis of the problem itself (Shushan, 2012, pp 61-62, Spitzer, 1984, pp 6-7). As previously suggested, this bypasses the critical first step upon which NATO's SAT model is based – confirming that training is indeed the solution to the identified requirement.

Worse still, many organizations tend to under-support training development initiatives by searching for solutions that are seen as easier or quicker to implement (Spitzer, 1984, p 6), which often results in »counter intuitive behavior« (Betts and Lu, 2011, p 126). Asynchronous online learning solutions that are essentially screen captures of manuals or policies are excellent examples of rushed solutions, yet careful and deliberate planning is an integral component to building successful online training solutions (Ataizi and Durak, 2016, p 2085). While NATO has made significant effort to weed out poorly planned training solutions, one need not look very far to find examples of such courses within the Alliance.

To compound the problem, training is often a »fire and forget« solution. In much the same way that software requires patching to correct newly discovered vulnerabilities, training also requires maintenance driven by deliberate evaluation activities in order to correct unforeseen design errors and remain relevant over time (Betts and Lu, 2011, pp 126-128; Welty, 2008). Once a training solution has been introduced, however, there is a general reluctance by many organizations to commit to performance improvement initiatives (Spitzer, 1984, p 7), despite calls from training experts to do so. This is particularly true in the case of customer-funded ETFs, where dedicating resources to course revision activities may simply be too costly to justify. Common problems of this nature plague the efficacy of training across the globe, and all are present within NATO cyber E&IT.

Often, ETFs rely on project managers to oversee design, development, implementation and evaluation efforts. Their skillset is well suited to shepherding personnel through complex processes; however, if a project manager lacks experience in course development, they can unknowingly take shortcuts during earlier phases that require costly corrections later in the process. Conversely, some E&IT specialists lack the necessary project management background to mitigate the many challenges in balancing organizational demands and the process to create training. Allan Harris' SPADES model addresses ADDIE requirements by leveraging core project management principles that tend to be more familiar to stakeholders (Harris, 2013). Harris' model shows promise as it seeks to optimize the creation of training by sufficiently informing the influential people within an organization who could ultimately be responsible for success or failure. It is worth noting, however, that in order to apply Harris' model, one must also possess a strong working knowledge of the ADDIE model.

Harris' ideas have merit in other research as well. Bunch suggests that training interventions may fail at least in part due to the fact that more dominant cultures within an organization exclude or undervalue the input from less dominant professionals

within an organization (Bunch, 2007, p 151), such as E&IT specialists. Similarly, Spitzer suggests that training professionals are partly to blame for training failures by not establishing consulting norms and clarifying management's misconceptions on training (Spitzer, 1984, p 7). This is particularly challenging within multinational military structures, such as NATO, where differing assumptions surrounding rank and expertise can heavily influence the means by which input from a subordinate is heard.

In the Canadian model, upon which NATO's version is based, unit leadership relies heavily upon the input of specially trained military E&IT advisors and instructional designers, called Training Development Officers (TDOs)[11] to shepherd their training processes. At Canadian ETFs, TDOs are most often junior officers (Captain or equivalent) whose expertise resides within the realm of E&IT and not the subject matter trained at their ETFs. The underlying principal is that differing perspectives from content and process experts will provide a more well-rounded solution (Clark, 2008, pp 11-12). While the authority to decide and act within the Canadian military also resides within rank, the culture of senior leadership accepting or at least considering advice from a ranking subordinate expert is the norm. In multinational settings, however, there can be differing perceptions with regard to the connection between rank and expertise. Perceptions of this nature can result in the adoption of ill-informed decisions.

The use of an instructional designer in the process to create education and training is a very common practice, but the value of such expertise is often lost to those who normally work outside of the field of E&IT. Despite working within a national structure that relies upon such expertise, a recent commander of Canada's OPERATION UNIFIER was surprised by how well TDOs contributed to the rotation's efforts to effect meaningful and sustainable change in training the Security Forces of Ukraine. He even posited that Ukraine should seek to develop a similar capacity tailored to their own needs to ensure long-term stability within their training system (Leroux, 2019, p 13).

Within the greater NATO community, there is a dearth of E&IT specialist expertise. The Alliance relies upon the DH and expertise within its ETF to provide similar education and training guidance throughout the SAT process, but this does not always work. The breadth of competing strategic responsibilities placed upon a DH makes it very challenging for them to focus on the tactical details within a particular ETF's CCD III. As previously mentioned, ETFs may not have this skillset on hand, either. Some cyber ETFs have even normalized the practice of having a singular content expert or instructor being responsible for the integrity of a CCD III. If this individual is reluctant to accept advice on the structure of their course from a non-content expert, the effectiveness of the CCD III, and even the integrity of the course itself, may suffer.

[11] *The author is one such Training Development Officer (TDO) within the Canadian Armed Forces (CAF).*

The lack of instructional design experience contributes to the production of curriculum documentation lacking sufficient detail to be of any real use to an ETF. If done properly, the CCD III will not only guide the development process, but it will ensure consistent delivery and management of courses over time. Quite often, these documents are populated only to the depth necessary to demonstrate they meet the NATO requirements contained within the CCD II. Regrettably, this proliferates the impression within ETFs that the CCD III is merely an administrative tool required by NATO.

It is also worth noting that some cyber ETFs do not even require a CCD III or equivalent curriculum document for courses they deliver that reside outside the area of NATO's interest. In these instances, lesson plans and PowerPoint presentations exist in lieu of any structured outline of course content. Courses without controlled curriculum documentation (such as a CCD III or equivalent) are subject to frequent unsupervised revision and can easily evolve outside of their intended scope over time. While not an immediate concern for every ETF, this can present an administrative nightmare to any ETF wishing to demonstrate that one of its existing courses meets a NATO requirement.

6 EVALUATION OF TRAINING

A thorough evaluation of a course will confirm the degree to which it contributes to any recognizable performance improvement, and is the basis for assessing return on investment. If a course can be linked to improving organizational objectives, it is viewed as a success. If the results are less conclusive, revision or removal of the training solution may be warranted (Gagné et al., 2005, p 350). In theory, the evaluative results of a course would be more favourable if the training solution were constructed following the guidance and advice of an instructional designer who followed a SAT model, like the one in use by NATO.

NATO's E&IT policy leverages Donald Kirkpatrick's model of evaluating training across four levels: reaction, learning, behavior and results. This model is a common industry standard for evaluating E&IT efficacy, and is summarized and contextualized for NATO's use in Table 2 (Kirkpatrick Partners, 2022). Most instructional designers leverage the requirements of Levels 3 and 4 while creating course curriculum, and focus on Levels 1 and 2 when developing specific course materials (Gagné et al., 2005, p 351).

Table 2: Kirkpatrick's model contextualized for use in NATO (based on information obtained from Kirkpatrick Partners, 2022, with additional NATO contextualization provided by the author)

Level	What it Evaluates	Achieved by	Responsible Entity
Level 1: Reaction	Student perceptions of training value and quality	Student questionnaires, surveys or interviews during training or shortly after training has concluded	ETF
Level 2: Learning	The degree of student learning attributable to the training	Assessing student performance against the objectives of the training solution	ETF
Level 3: Behavior	The degree to which concepts learned during training are applied on the job	Questionnaires, surveys or discussions with supervisors after training has concluded and former student work performance has had the opportunity to normalize (i.e. 6-12 months after training)	ETF
Level 4: Results	How or whether the training solution has affected organizational needs as intended (return on investment)	Observing performance on missions, operations and/or daily work, or by other quantifiable observable means	NATO

6.1 Level 1 Evaluations

The collection and analysis of Level 1 feedback is a component of the quality assurance model ETFs must conduct while delivering NATO training (NATO, 2015, para 9-5, a). At the moment, Level 1 feedback represents the most prevalent source of concrete and tracked data available to cyber ETFs on the efficacy of their training. As such, this information heavily influences the training maintenance activities that ETF leadership will endorse. If data trends suggest a high degree of student satisfaction, then there is little need for improvement. Relying primarily upon student satisfaction as the main measure of training effectiveness will, however, falsely equate training value with entertainment (Spitzer, 1984, p 8).

Reactionary feedback data is insufficient in and of itself to paint a complete picture of training efficacy (Coscarelli and Shrock, 2007, p 7, Kirkpatrick Partners, 2022). Level 1 feedback is intended to be viewed together with data from all other levels in Kirkpatrick's model as part of a systematic and systemic approach to evaluating a training program's efficacy (Chyung 2008, pp 65-66).

6.2 Level 2 Evaluations

Level 2 data is obtained by assessing student performance to confirm the degree of learning attributable to the training solution (Kirkpatrick Partners, 2022). Formative assessments provide feedback to students to guide their learning process and to identify areas where the ETF can improve learning experiences in the future (Gagné et al., 2005, p 349). Summative assessment confirms student achievement of course objectives, and validates the instructional methods employed by the ETF (Gagné et al., 2005, p 350). NATO's training policy acknowledges both forms of assessment (NATO, 2015, para 7-6) and highlights the importance of summative assessment as the means to confirm that performance gaps have been satisfied (NATO, 2015, para 9-5 b.). The use of summative assessments within face-to-face training, cyber or otherwise, appears to be limited[12]. Asynchronous online courses often contain mandatory summative assessments, yet such tests tend to be constructed and/or administered in ways that do not necessarily confirm the achievement of all the intended learning objectives.

Formative assessments occur reasonably well in most cyber courses, but as they are used at present they do not objectively satisfy the second level of Kirkpatrick's model. The general tendency is to collectively assess student performance in small groups or syndicates. The feedback they receive is normally subjective and based on instructor expertise in relation to the course objectives, rather than a clearly established standard. As most NATO personnel work within a team setting, assessments of this nature at least partially emulate working conditions, which is a core component to successful assessment (Coscarelli and Shrock, 2007, p 44). However, group assessments are not always the best tool to evaluate the content mastery of individual learners. Furthermore, effective assessments need to be constructed against a specified criteria or standard (Gagné et al., 2005, p 350) if they are to consistently and objectively evaluate performance over time (Coscarelli and Shrock, 2007, p 190).

The value of assessment extends well beyond determining whether a candidate »passes« or »fails« a particular course. If training is properly constructed, analyzing student assessment results over time will provide statistical relevance on the efficacy of instruction and learning which can guide any corrective measures of an ETF (Gagné et al., 2005, pp 349-350). A lack of objective summative assessments impedes the Alliance's ability to evaluate a training solution against Level 3 or 4 in Kirkpatrick's model (Coscarelli and Shrock, 2007, p 6). Summative assessment establishes the »chain of evidence« between end of course performance and on the job performance (Gagné et al., 2005, p 348). Without it, there is no way to prove that the training actually improved organizational performance.

[12] *Anecdotally, the rationale for avoiding summative assessments seem to be rooted in concerns over how NATO and its individual nation states might react to unsatisfactory student performance.*

6.3 Level 3 and 4 Evaluations

Levels 3 and 4 of Kirkpatrick's model have the greatest correlation to higher rates of training transfer[13], yet organizations are often hesitant to move beyond Level 2 (Burke and Saks, 2012, p 123). To be fair, however, level 1 and 2 evaluations are much easier for an ETF to effect, as the data comes from their students and is relatively easy to collect. Data of this nature is also easier for an ETF to contextualize and analyze.

Within the training policy documentation, levels 3 and 4 are combined under the label »external evaluations« (NATO, 2015, para 9-5 c). The focus of these evaluations is the job-based performance elements identified within the analysis phase of the NATO SAT process (i.e. the performance standards in the CCD II). Job performance is measured against these standards to confirm the degree to which the objectives of training are truly achieved.

The Alliance relies upon ETFs to conduct Level 3 evaluations, typically via survey or questionnaire. A primary data source for both Level 3 and 4 evaluations is former students and/or their supervisors. Their insight is needed to verify whether the training concepts are being employed in the work place (Level 3) and the degree to which this behavior is benefiting the greater organization (Level 4). The strongest correlation between training transfer and such evaluations tends to be within the period of 6 months to a year after the training has concluded (Burke and Saks, 2012, p 123), a sentiment echoed by NATO's E&IT policy (NATO, 2015, para 9-5). Unfortunately, analysis efforts are often mired by a lack of willingness or ability to participate. Also, if a prospective participant is no longer (or never was) employed in a role where the training is used, their input may not be valid. Given the difficulties of collecting Level 3 data, it is hard to say how the results are communicated between the Alliance and the ETF that delivers the training, but both parties have a vested interest in the conversation.

The degree of accountability respondents have to the Alliance may also impact the training transfer and evaluation process, but the process could be improved if NATO appropriately incentivized participation in Level 3 evaluations (Burke and Saks, 2012, p 125). In order to do this, the work that personnel are doing must be connected to the training they receive and it must be both valued and supported by the organization (i.e. NATO) in order to close the gap between training and the workplace (Spitzer, 1984, p 8; Beer et al., 2016, pp 5-7).

The only way that NATO can address the requirements of Kirkpatrick's Level 4 evaluations is by connecting exercise and workplace performance to the individual training delivered via its ETFs. Exercise and workplace performance are both routinely analyzed by the Alliance, but not necessarily in a manner that provides insight on the training one has received. It is important to note that successful

[13] *Again, transfer of training refers to a student's ability to apply that which they learn during the course within the workplace (Burke and Saks, 2012, p 118).*

performance on an exercise or within the workplace is not necessarily a sufficient indicator of training quality – even for carefully and properly constructed courses.

In order to close the loop on Kirkpatrick's model and calculate any real return on investment for its training, NATO needs to collect and analyze data pertaining to how its training solutions contributed to increased operational performance. This information must be shared with ETFs so that they can adjust their training programs accordingly to ensure Alliance requirements are met.

NATO's training documentation clearly highlights the importance of the information it obtains from external evaluations, but it is deliberately written in such a way as to provide ETFs with flexibility in the manner in which they conduct them (NATO, 2015, para 9-5). Unfortunately, the degree or consistency to which external evaluations are done for cyber training is not widely known.

6.4 Why Evaluation Matters

The aim of any NATO training solution is to correct a noted deficiency that is of concern to the Alliance. A Level 4 evaluation under the Kirkpatrick model seeks to confirm whether the training solution has achieved this aim, but such an evaluation is difficult to undertake and relies heavily upon inputs from Levels 2 and 3 (Coscarelli and Shrock, 2007, p 6). Unless summative assessments are used and Level 3 data collection efforts are prioritized, definitively calculating any true return on investment (via Level 4) will be almost impossible.

In their analysis of why process improvement fails, Betts and Lu (2011, pp 126-128) conclude that in order for training to be successful, it must be developed within a supportive framework that actively imposes an honest continuous improvement process. The framework that they suggest aligns with all the requirements within the ADDIE model, but places particular emphasis on open and honest communication throughout the evaluation process.

As it pertains to NATO, the evaluation phase is disjointed and incomplete. As the driver of requirements, NATO is very influential during the onset of the SAT process, but seemingly less so during the later phases. The Alliance clearly has a vested interest in the success of its E&IT solutions; however, NATO's reliance on external entities outside of its command and control to effect its E&IT efforts has somehow created an environment where the existence of training solutions is valued over their quality.

At the moment, NATO can only attempt to gain feedback on the effectiveness of individual training by assessing performance during its collective training efforts and reviewing what little feedback material ETFs are able to gather. The degree of training transfer will never truly be known unless the Alliance takes deliberate steps to ensure the collection, analysis and socialization of data across all the partners involved in the process.

Conclusion

The previously discussed challenges facing NATO in developing meaningful cyber training vary in severity and risk to the Alliance. To those with only a cursory background in E&IT, many of these risks may not seem overly serious. If left dormant, however, these deficiencies can set the conditions for current and future cyber training initiatives to fall short of expectations and waste valuable and already scarce resources.

Most of the subject matter experts required to create NATO cyber training initiatives work within the operational realm of the Alliance. Accordingly, they are only able to support E&IT projects when operational conditions permit, and when their organizations prioritize their support. Even so, many experts who have contributed to recent cyber E&IT development initiatives have at least partially volunteered their personal time to do so. Given the slow rate at which we are able to develop new solutions based on expertise shortages, it is imperative that NATO optimize its E&IT design and development efforts. Using the Chapman Alliance data to contextualize the gravity of the situation, one hour of instructor-led training can take upwards of 43 hours (approximately $5,934 USD) to create. A one week instructor-led course with 36 hours of instruction would, on average, take roughly 1,500 hours to complete (at a cost just over 200K) (Chapman, 2010). The degree of accuracy behind these figures is less important than the message they convey with regard to the magnitude of effort required to create training.

NATO's training solutions need not be perfect to be effective, but currently their effectiveness is largely unverified and there are some obvious holes in how they are managed. Gaining an appreciation of how these problems may collectively affect the efficacy of current E&IT initiatives will help the Alliance to plan for future success.

If an assessment of a performance problem does not occur, then how do we know training will fix the problem? If the training solution is built upon unsteady ground, or participants have too varied experiences within the subject matter, then how can we plan to build a one-size-fits-all training solution for them? If we restrict course content based on the time available to train and not on the content that is required, how are we providing students with the tools they need to succeed in the workplace? If we do not objectively assess learner performance, how can we ensure learning is occurring? If we do not know whether training is causing changes in personnel behavior and improvements in organizational outputs, then how do we know if the training is even correcting the initial problem? If subject matter expert time is perceived to be squandered, how will we get more support in the future when it is needed?

It is proposed that the Alliance's next cyber training intervention should undergo careful and deliberate planning before fully engaging the NATO SAT model. A dedicated project manager and E&IT specialist should collaborate on this endeavour to ensure the requirements of both the SAT model and organizational stakeholders are sufficiently addressed. The plan should clearly identify the level of support required

for all necessary entities at all phases within the NATO SAT model, and prioritize the requirements for deliverables at every step. Once internally approved by the Alliance, the plan will need to be communicated and agreed upon by all stakeholders to ensure project success and enable advanced planning for individual organizational leadership rather than reaction. Only then, should work commence on closing the gap.

At a minimum, this plan should address the following issues:

- Thoroughly assessing a problem before trying to fix it with E&IT;
- A careful analysis of the target audience so as to assess the common starting point and identify potential gap training for some participants as needed;
- A clear emphasis on ensuring quality of SAT deliverables throughout the process;
- Ensuring the necessary content drives training rather than scheduling (minimizing residential training can be offset by leveraging asynchronous online training modules to employ a blended learning approach);
- A requirement to objectively assess student performance (if not to award certification, then to confirm learning at a minimum);
- Identify which entities are required to support the project, and what that support looks like;
- Outline a clear plan to externally evaluate training that is observably endorsed by NATO leadership at the highest appropriate level;
- Ensure that all internal and external evaluation data and analysis is shared between all stakeholders as soon as practicable.

The key to ensuring any change initiative is careful planning and clear and frequent communication. Work of this nature is initially time-consuming, but will ensure higher quality work in the long term. The Alliance need not revise its training policy – yet. Further data is required to assess the existence and magnitude of any perceived holes in their policy before any wide sweeping attempts should be made at correction – this is a clear example of assessing the need before acting.

Piloting and assessing the effectiveness of a slightly revised adaptation to the NATO SAT process would be a more valuable use of time and effort. Specifically, a planned and deliberate attempt to mitigate the known pitfalls coupled with a transparent examination of the results would demonstrate an honest commitment on the part of the Alliance to ensuring training is both efficient and effective. Such a project may uncover more flaws that need to be addressed, or it may even provide a much needed success story.

Bibliography

1. *Ataizi, M., and Durak, G., 2016. The ABC's of online course design according to ADDIE model. Universal Journal of Educational Research, 4(9), pp 2084-2091.*
2. *Beer, M., Finnström, M., Schrader, D., 2016. Why leadership training fails—and what to do about it. Harvard Business Review, October, 2016, pp 50-57.*
3. *Betts, A., and Lu, D., 2011. Why process improvement training fails. Journal of Workplace Learning, 23(2), pp 117-132.*

4. *Brent, L., 2019. NATO's Role in Cyberspace. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, 10 February 2022.*
5. *Bunch, K. J., 2007. Training failure as a consequence of organizational culture. Human Resource Development Review, 6(2), pp 142-163.*
6. *Burke, L. A., and Saks, A. M., 2012. An investigation into the relationship between training evaluation and the transfer of training. International Journal of Training and Development, 16(2), pp 118-127.*
7. *Chapman, B., 2010. How long does it take to create learning. http://www.chapmanalliance.com/howlong/ 10 February 2022.*
8. *Christensen, B. D., 2018. From needs assessment to needs analysis. Performance Improvement, 57(7), pp 36-44.*
9. *Chyung, S. Y., 2008. Foundations of Instructional Performance Technology. Amherst: Hrd Press.*
10. *Clark, R. C., 2008. Building Expertise: Cognitive Methods for Training and Performance Improvement. 3rd Ed. San Francisco: Pfeiffer.*
11. *Coscarelli, W. C., and Shrock, S. A., 2007. Criterion-referenced Test Development: Technical and Legal Guidelines for Corporate Training. 3rd Ed. San Francisco: Pfeiffer.*
12. *Ertan, A., Kuprys, A., Lillemets, P., Nordli, G-M., 2021. Cyber Exercises: A Vision for NATO Cycon 2021 Workshop Summary Report. Tallinn: NATO CCDCOE.*
13. *Gagné, R. M., Golas, K. C, Keller, J. M., Wager, W. W., 2005. Principles of Instructional Design. 5th Ed. Belmont, CA: Wadsworth.*
14. *Harris, A., 2013. Training in SPADES. T+D, 67(6), pp 58-62.*
15. *ITU, 2021. Guide to Developing a National Cybersecurity Strategy. 2nd Ed. Geneva: International Telecommunication Union.*
16. *James, M., and Ward, K., 2001. Leading a multinational team of change agents at Glaxo Wellcome (now Glaxo SmithKline). Journal of Change Management, 2(2), pp 148-159.*
17. *Kirkpatrick Partners, 2022. The Kirkpatrick Model. https://kirkpatrickpartners.com/the-kirkpatrick-model/ 10 February 2022.*
18. *Leroux, P., 2019. Security force capability building 2.0: enhancing the structure behind the training. Canadian Military Journal, 19(3), pp 7-14.*
19. *NATO, 2016. Bi-SC Education and Training Directive (E&TD) 075-002.*
20. *NATO, 2015. Bi-SC Education and Training Directive (E&ITD) 075-007.*
21. *NATO CCDCOE, 2021. NATO CCDCOE Training Catalogue, 2022. https://ccdcoe.org/uploads/2022/01/2022_NATO_CCD_COE_Training_Catalogue_FINAL.pdf 15 February 2022.*
22. *NATO School Oberammergau, 2021. Enrolment Instructions. https://www.natoschool.nato.int/Academics/Admin-Info/Enrolment-Instructions, 15 February 2022.*
23. *NCI Agency, 2020. Introducing the NCI Academy. https://www.ncia.nato.int/resources/site1/general/what%20we%20do/nci%20academy/nci_academy_brochure_web_dec20.pdf, 15 February 2022.*
24. *Shushan, E., 2012. Enhance training's worth with learning processes. T+D, 66(2), pp 60-63.*
25. *Spitzer, D. R., 1984. Why training fails. Performance & Instruction Journal, September, 1984, pp 6-10.*
26. *Welty, G., 2008. Formative evaluation in the ADDIE model. Journal of GXP Compliance, 12(4), pp 66-73.*

e-mail: christopher.young@ccdcoe.org

Davide Giovannelli
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.3

ZUNAJOZEMELJSKA PRISTOJNOST ZA KIBERNETSKO VOHUNJENJE: NOV TREND V MEDNARODNEM PRAVU ALI LE PRIMER UPORABE PRAVA KOT OROŽJA

EXTRATERRITORIAL JURISDICTION OVER CYBER ESPIONAGE: A NEW TREND IN INTERNATIONAL LAW OR JUST AN EXAMPLE OF LAWFARE

Povzetek Praksa v državah kaže, da obveščevalne agencije ne izvajajo le vohunjenja, temveč tudi druge, manj plemenite dejavnosti, kot je hibridno vojskovanje. Mednarodno pravo tradicionalno dopušča vohunjenje, domače kazensko pravo pa navadno omogoča njegov pregon. Ne glede na to se nestabilno ravnovesje zaradi rasti kibernetskega vohunjenja, ki omogoča učinkovitejše izvajanje, spreminja. Ni presenetljivo, da se povečuje zanimanje za prakso držav, saj so bili sprejeti novi pravni instrumenti za izvajanje zunajozemeljske pristojnosti nad kibernetskim vohunjenjem. V članku poskušamo oceniti, ali je treba nove pravne instrumente obravnavati kot nov pojav v mednarodnem pravu ali kot občasno uporabo prava kot orožja.

Ključne besede ***Zunajozemeljska pristojnost, kibernetsko vohunjenje, uporabo prava kot orožja , neprimerno tuje vplivanje, ekonomsko vohunjenje.***

Abstract States' practice shows that intelligence agencies have carried out not only espionage, but also other, less noble activities, such as hybrid warfare. Traditionally, international law tolerates espionage, while domestic criminal law generally allows its prosecution. However, this precarious equilibrium is changing due to the growth in cyber espionage, which allows espionage to be carried out more effectively. Not surprisingly, there is increasing interest in States' practice, as new legal instruments for exercising extraterritorial jurisdiction over cyber espionage have been adopted. This article tries to assess whether these new legal instruments should be considered a new trend in international law, or a sporadic exercise of lawfare.

Key words ***Extraterritorial jurisdiction, cyber espionage, lawfare, improper foreign influence, economic espionage.***

Introduction

As shown in this article, »traditional« espionage, as well as hybrid threats[1] and economic espionage, are not new practices. States have carried out such activities for centuries. However, the real game-changer of recent decades has been the impact of Information and Communications Technologies (ICT). ICT, indeed, is allowing more and more States to carry out espionage in all its forms more effectively. As we shall see in this article, this new situation leads to a change in the applicable legal framework in order to react more effectively towards these new threats.

This article aims to analyze this phenomenon, focusing on situations other than an armed conflict. First, the article will analyze what cyber espionage is. It will show that a comprehensive analysis cannot be limited only to what is legally considered espionage, but instead it is vital to also consider other clandestine activities that may be carried out by intelligence agencies from time to time. Secondly, espionage and other clandestine activities will be considered from international and domestic criminal law perspectives. Thus, this article will deepen understanding of how ICT has influenced and modified espionage and other clandestine activities. Finally, the article will address the emerging trends in criminal and administrative law to tackle such cyber threats, and it will try to measure their effectiveness in order to assess whether these are new trends in international law, or just an example of lawfare (i.e. the use of law to achieve national security objectives).

1 WHAT CYBER ESPIONAGE REALLY IS

In order to begin this analysis, it is opportune to define what is traditionally considered as espionage. It is helpful to recall the following passage from Oppenheim's book on International Law of 1905:

»*Spies are secret agents of a State sent abroad for the purpose of obtaining clandestinely information in regard to military or political secrets. Although all States constantly or occasionally send spies abroad, and although it is neither morally nor politically and legally considered wrong to send spies, such agents have, of course, no recognised position whatever according to International Law, since they are not agents of States for their international relations. Every State punishes them severely when they are caught committing an act which is a crime by the law of the land, or expels them if they cannot be punished. And the spy cannot legally excuse himself by pleading that he only executed the orders of his Government. The latter, on the other hand, will never interfere, since it cannot officially confess to having commissioned a spy*« (Oppenheim, 1905, pp 490-491).

Oppenheim's extract clearly shows that espionage is a common practice in international relations, and it gives some valuable features to shape its definition:

[1] *We will consider the following definition of 'hybrid threat': a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.*

1. From a material point of view, this activity is committed abroad (and quite obviously clandestinely);
2. Its purpose/intent is to obtain information with regard to military or political secrets;
3. It is not morally or politically and legally considered wrong by States, but those who carry out such activity (i.e. spies) can be prosecuted or expelled by the State in which the espionage is committed.

However, it would be naive to think that espionage is limited to this legal definition of espionage. States' practice, indeed, shows that intelligence agencies have been constantly used even for other less noble activities, even though States are – quite obviously – reluctant to admit it. It may not be unreasonably denied that sometimes States have been involved in some illegal – or at least regrettable – activities, such as the abduction of people from the territory of another State[2], or disinformation campaigns (Selvage, 2019; Geissler & Sprinkle, 2013).

At the beginning of the Cold War, a US Department of State Policy Planning Staff Memorandum pointed out that »*Political warfare is the logical application of Clausewitz's doctrine in time of peace. In the broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (such as ERP—the Marshall Plan), and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states*« (National Archives and Records Administration, 1948). Looking at the other side of the barricade, already in the 1960s there was a clear awareness among NATO Nations of the threat posed by the clandestine activities of the Soviet Union (NATO-wide co-operation and coordination in the field of psychological warfare – proposal by the Federal Republic of Germany, 1960). It goes without saying that parallel forms of intervention have been carried out by Western States (US *in primis*) also *vis-à-vis* their Allies, as frankly admitted by a reliable former CIA officer[3].

---

[2] *Without considering the most recent US practice of 'extraordinary rendition', it is worth recalliyng the following cases, already quoted by the UN International Law Commission:*

- *The abduction, from Switzerland to Italy, in 1928, of Cesare Rossi, by people probably acting by agreement with the Italian police;*
- *The abduction, from Switzerland to Italy, in 1935, of Berthold Jacob, by people employed for this task by the German Gestapo;*
- *The abduction, from Argentina to Israel, in 1960, of war criminal Adolf Eichmann, by a group of Israeli nationals in a suburb of Buenos Aires;*
- *The abduction, from Germany to France, on 1961, of ex-Colonel Argoud, one of the leaders of the OAS, by unknown individuals.*

Yearbook of the International Law Commission, 1971, Vol. II, Part One, pp 265-266.

[3] *Shane, 2018, where a former CIA officer – referring, among other things, to the CIA's activity in support of Italian candidates – admitted the following: »We've been doing this kind of thing since the CIA was created in 1947,« said Mr. Johnson, now at the University of Georgia. »We've used posters, pamphlets, mailers, banners — you name it. We've planted false information in foreign newspapers. We've used what the British call 'King George's cavalry': suitcases of cash«.*

Thus, it should be clear that not all activities carried out by intelligence agencies can be labelled as espionage. In other words, a clandestine activity carried out by an intelligence agency does not mean that it necessarily falls within the legal definition of espionage.

2 INTERNATIONAL LAW PERSPECTIVE

In essence, scholars' opinion over (traditional) espionage can be divided in the following three ways (A. J. Radsan, 2007, pp 601-607):

a) Espionage is not illegal (Oppenheim's view);

b) Espionage is illegal;

c) Espionage is neither legal nor illegal.

Followers of options A and C give weight to the judgement of the Permanent Court of International Justice in the Lotus case, where it was stated that: »*International law governs relations between independent States. Therefore, the rules of law binding upon States emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed*«.

Therefore, as specified by a scholar: *»According to the principle stated in the Lotus Case it is for those who assert the existence of the rule of law restricting state activity to show that such a restrictive rule exists. Moreover, in any case, it is not a self-evidently sound approach to the newish problems of peacetime espionage to assume that it must be unlawful unless it can be justified on some specific grounds. In the face of such rapid technological, strategic, and psychological change, it seems to be particularly important to approach the matter by asking whether there are any principles manifest in the practice of states that evidence any existing restrictive rules, or any sufficiently close analogies. With the greatest respect, I can at present find none«* (Stone, 1962, p 33).

On the other hand, case law presents cases that support the option that espionage is considered illegal. According to the Canadian Federal Court, *»the intrusive activities … are activities that impinge upon the principles mentioned above of territorial sovereign equality and non-intervention and are likely to violate the jurisdiction's laws where the investigative activities are to occur*« (Federal Court, Blanchard J., Ottawa, April 24, 27, June 14, 2007).

Thus, without wishing to enter into the controversial question of which of the three options should be preferable, even assuming as the most appropriate option B

(i.e. espionage is illegal), the illegality of espionage is sustainable only as far as a violation of territorial sovereignty and non-intervention occurs. Such a conclusion is also consistent with the undisputed practice of passive intelligence reconnaissance towards a foreign State, exercised by another State from its territory, the high seas or even outer space[4].

Additionally, the said conclusion also appears to be corroborated by the most recent case law of the International Court of Justice (ICJ). As convincingly pointed out in a comment to the ICJ order granting provisional measures in the case Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia): »*At present, it seems difficult to argue that a rule of customary international law, based on widespread state practice accepted out of a sense of legal obligation, provides that the interception of a foreign state's communications is either lawful or unlawful. But it can certainly be argued that such activities by an established state (here, one that belongs to an intelligence alliance with other intelligence powers) carried out against a small, newly established state create an unfair and unethical balance in international dispute settlement and negotiations*« (Bettauer, 2014, p 768).

In laymen's terms, the ICJ found that in such a situation (i.e. the Timor Sea International Arbitration between the Democratic Republic of Timor-Leste and Australia), »*a State has a plausible right to the protection of its communications with counsel relating to an arbitration or negotiations, in particular, to the protection of the correspondence between them, as well as to the protection of confidentiality of any documents and data prepared by counsel to advise that State in such a context*« (Timor-Leste v. Australia, Provisional Measures, Order of March 3 2014, ICJ Reports 2014, paragraph 27). Therefore, by a process of *a contrario* reasoning, it seems logical to conclude that ICJ opinion supports the idea that espionage should be considered, *per se*, as unlawful or illegal. Even the ICJ judgement in the case of Jadhav (India v. Pakistan) does not contradict this view. Indeed, the ICJ's recognition that the safeguards provided for in Article 36 of the Vienna Convention on Consular Relations of April 24 1963 are applicable even in the case of allegation of espionage activities can support only the (undisputed) rule that espionage can be punished by domestic criminal law. However, it does not allow the consideration of espionage *per se* as a breach of international law.

In order to analyze hybrid warfare in the light of the principle of foreign intervention, it is essential to recall the ICJ judgement in the case of Contras v. Nicaragua. In short, this judgement emphasized that:

[4] *In the past, the USSR attempted to qualify observation from space to collect intelligence as illegal (see: Soviet Statement in the General Assembly, First Committee, 17th Session, 1298th Meeting, December 3 1962). States' practice, however, has not followed the USSR's point of view.*

– Each State is permitted, by the principle of State sovereignty, to freely decide the choices of a political, economic, social and cultural system and the formulation of foreign policy;
– Foreign intervention is wrongful when it uses methods of coercion with regard to such choices;
– The element of coercion, which defines and indeed forms the very essence of prohibited intervention, is particularly obvious in the case of an intervention which uses force.

The above implies that foreign intervention could be considered wrongful only as far as methods of coercion are used. Thus, it is necessary to understand what coercion means and whether foreign intervention relying on ICT can be considered coercive. In this regard, as pointed out by a scholar: »*although 'coercion' arguably has never been adequately defined and is still an indistinct concept, the Nicaragua dictum remains the leading case on the issue*« (Lahmann, 2020, p 197). Thus, unless the threshold for qualifying a cyber-operation as use of force is met, it would be problematic to qualify a foreign intervention through ICT means as coercive.

Additionally, even the possibility of relying on other international law provisions to qualify a foreign intervention through ICT means as wrongful is hardly disputed. There is no consensus on the possibility of relying on the principle of sovereignty, even within Western countries. In this regard, it is sufficient to recall that »*The United Kingdom does not consider that the general concept of sovereignty provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention«* (UN Official Compendium, 2021). Through an innovative approach, other scholars have tried to rely on the right to self-determination. Ohlin, for example, argued that »*foreign interference is a violation of the membership rules for political decision-making, i.e., the idea that only members of a polity should participate in elections—not only concerning voting but also concerning financial contributions and other forms of electoral participation. Outsiders are free to express their opinions but covertly representing themselves as insiders constitutes a violation of these political norms, which are constitutive of the notion of self-determination, just as much as covertly funnelling foreign money to one candidate«* (Ohlin, 2021). However, even this proposal, to date, seems not to be supported by a significant States' practice and thus lacks the *opinio juris* to rise as a customary rule of international law. To corroborate this conclusion, we refer to and concur with the in-depth survey of States' practice already carried out by Lahmann (2020). Additionally, along the same lines, the UN Official Compendium of Voluntary National Contributions to the subject of how international law applies to the use of information and communications technologies shows that States are worried about foreign influence, mainly for malicious cyber activities targeting foreign elections, but they have maintained a cautious attitude on this topic and avoided considering any form of foreign influence as unlawful *per se*.

Therefore, as already pointed out by the legal doctrine, »*to date, States appear by and large to have maintained a posture of constructive ambiguity when it comes to the international lawfulness of influence operations – via cyber means or otherwise – that do not directly alter votes as they were cast*« (Chimène, 2021, p 193). Even another distinguished author argued that »*beyond the few unequivocally wrongful cases, multiple fault lines in the international law governing cyber activities could hinder definitive characterisation of particular election interference as unlawful*« (Schmitt, 2021, p 764).

3 DOMESTIC CRIMINAL LAW PERSPECTIVE

Concerning criminal law, the possibility of prosecuting espionage and other forms of coercive foreign intervention if the illicit conduct is carried out in the territory of the targeted State is undisputed[5].

States' practice concerning »pure« espionage committed in the territory of the »Victim State« instead shows that expulsion as *persona non grata* is often preferred over criminal prosecution[6]. Municipal law, however, seems not to preclude prosecution, even in the case of espionage committed abroad (i.e. out of the territory of the »Victim State«) by a foreigner, although the *actus reus* is not forbidden by the offender's national law[7].

With regard to improper foreign influence on elections or political systems, almost every legal system has provided regulation on the financing of political parties to prohibit – or at least regulate transparently – contributions from foreigners. The relevant case law on this topic is minimal, although, for example, the Soviet Union's massive transfer of financial resources to the Italian Communist Party (PCI) is documented (Drake, 2004). Finally, concerning economic espionage, it is worth starting from the G7 Declaration (2017) on responsible state behaviour in cyberspace. This document recalled the following non-binding norm of State behaviour during peacetime: »*No country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, to provide competitive advantages to companies or commercial sectors*«. However, as

---

[5] *See the High Court of Auckland judgment of November 22 1985 (concerning the sabotage of a Greenpeace ship – which resulted in the death of a Dutch citizen and the sinking of the ship – carried out in New Zealand by two agents of the French Directorate General of External Security) and the Italian Court of Cassation judgement of March 11 2014, No. 39788 (concerning the abduction and illegal transfer abroad of a person, carried out in Italy by some U.S. CIA officials).*

[6] *US memorandum giving detailed information on the illustrative list of Soviet espionage agents apprehended in the United States since the death of Marshal Stalin, attached to the Letter dated 60/05/24 from the Permanent Representative of the United States of America to the Secretary-General, UN document S/4325.*

[7] *According to the US judgment in the United States v. Zehe, 601 F. Supp. 196 (D. Mass. 1985), »the Court finds that the [Espionage] Act may be applied extraterritorially to both citizens and noncitizens because of the threat to national security that espionage poses«. Even the German Federal Constitutional Court in the Espionage Prosecution Case (Espionage Prosecution Case (Case No 2 BGs 38/91), Bundesgerichtshof [BGH][Federal Court of Justice] Jan. 30, 1991, 94 International Law Reports [ILR] 68, 70, 1994 (Ger.) took this view. For a deep analysis see Krizek, 1988.*

highlighted by some scholars (Hemmings and Swire, 2019), economic espionage is still in the background of the debate on the mechanism allowing law enforcement authorities of different States to request e-evidence directly from a cloud service provider abroad. Regardless of the substance of that concern (and the additional concern over privacy protection in the US), it is to be noted that the negotiation between the EU and the US for an agreement on facilitating access to e-evidence is still ongoing. Thus, absolute mutual trust has not been achieved even between Western States. So it is not surprising that national law in every legal system provides two levels of protection against economic espionage. On the one hand, National Government maintains the right to authorize (or deny) certain transactions involving foreign investment in strategic sectors, whenever the effect of such transactions would undermine the national security of the State concerned. To that end, we can recall Regulation (EU) 2019/452 of the European Parliament and of the Council of March 19 2019, establishing a framework for the screening of foreign direct investments into the Union, as well as the US Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). Additionally, some Nations also have a dedicated legislation on trade secret theft. The US, for example, pursuant to the Economic Espionage Act of 1996 (EEA), has considered two forms of trade secret theft as a criminal offence: (i) theft for the benefit of a foreign entity (economic espionage), and (ii) theft for pecuniary gain (theft of trade secrets).

4 THE IMPACT OF ICT

In order to assess the impact of ICT on the different forms of espionage, we should start by acknowledging that it is not limited to »traditional« espionage, but rather it also affects hybrid warfare and economic espionage. This implies that all these activities, compared with the past, now require a more limited presence of spies in the targeted State's territory and less financial effort. In other words, cyber espionage is dependent mainly on States' availability (directly or by proxy) of ICT technologies; such technologies, however, are not too expensive and so easily obtainable. This new paradigm is not without consequences, as ICT technologies are no longer limited to a few Nations but, on the contrary, they are available to many Nations and criminal groups as well. Additionally, with specific reference to hybrid warfare, social media and new technologies have allowed everyone to deliver their message to a broad target audience. In the past, conversely, mainstream media groups were the only ones able to do that[8]. Not surprisingly, therefore, social media and new technologies have become instruments for foreign influence operations and disinformation. Moreover – even if the question of international lawfulness of influence operations

[8] *The European Court of Auditors pointed out that »disinformation has been present in human communication since the dawn of civilisation and the creation of organised societies. However, what has changed in recent years is its sheer scale and the speed with which false or misleading information can reach its intended and unintended audiences through social media and new technologies. This may cause public harm«. See: Special Report No 09/2021 from the European Court of Auditors »Disinformation Affecting the EU: Tackled but not Tamed«, April 27 2021. Available at: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf.*

has not yet been solved – it is worth noting that nowadays Western democracies seem more vulnerable to foreign influence, while in the past it was East communist regimes that suffered more from such types of influence. This turnaround favouring authoritarian regimes should be considered an unintended consequence of the said ICT technologies.

However, the above alone is not deemed sufficient to explain the increasing threat posed by the impact of ICT. The fact that more States are potentially able to carry out cyber espionage is not sufficient to explain why there is also more willingness to carry out such activities. After all, resorting to cyber espionage could be rewarding, but it could also be dangerous. Therefore, it is a matter of how States perceive the reward-cost calculus. Among the many possible considerations, some elements seem to tip the balance towards a more aggressive posture in applying ICT to carry out cyber espionage. On the one hand, in the case of ICT exploitation, strategic deterrence – i.e. the combination of denial and punishment – does not work correctly. Unlike nuclear weapons, which are not meant to be used due to the mutual assurance of destruction (MAD) of both the attacker and the defender, cyber operations are frequently conducted, since no MAD is applicable. On the other hand, difficulties in determining the attribution to a State of ICT employment for cyber espionage is another incentive for such employment. Moreover, as cyber spies are seldom in the territory of the »victim« State, the latter will have almost no possibility of apprehending and prosecuting those responsible for such crimes. This situation entails an incentive to rely on cyber espionage, since a high sense of impunity is widely perceived. Additionally, the legal understanding of the threshold of cyber-attack for triggering the applicability of the law of armed conflict (LOAC) could also be relevant. To put it simply, the higher the threshold, the more States will be prepared to accept the costs – e.g. possible reputational damage – associated with cyber espionage, since they will not bear the risks of triggering an armed conflict.

Concerning the last point, it is worth noting States' opinions, as expressed in the UN official Compendium of Voluntary National Contributions to this topic[9]. Such opinions are in line with the view expressed in the Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. It means, following the reasoning of the ICJ's Nicaragua judgement, that:

– »*A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force*« (Tallinn Manual – Rule 69);

[9] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established according to General Assembly resolution 73/266. UN document A/76/136 dated July 13 2021. However, it is worth noting that the Netherlands affirmed the following partially nuanced position: »In the view of the government, at this time, it cannot be ruled out that a cyber operation with a severe financial or economic impact may qualify the use of force«.*

– »*A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects*« (Tallinn Manual – Rule 71).

In practice, these rules imply a pretty high threshold. As pointed out by some scholars, »*given that acts of cyber espionage result in the copying of confidential data and do not produce physical damage, they do not contravene the use of force prohibition*« (Buchan, 2018, p 68). Similarly, as the use of ICT for hybrid warfare does not produce any physical damage, it is deemed appropriate to conclude that it will not amount to the use of force. However, from an EU law perspective, it is worth noting that the Member States have a specific measure to apply in each of the two situations (i.e. below or over the threshold). As clarified by the Council: »*Article 42(7) TEU* [*i.e.* the EU collective self-defence clause] *can be invoked by a Member State in case of armed aggression on its territory*«, and cyberattack »*can constitute an armed aggression within the meaning of Article 42(7), under the relevant principles of public international law*«, while »*Article 222 TFEU* [i.e. the EU solidarity clause] *applies to a terrorist attack or a natural or man-made disaster affecting a Member State, which can be triggered by a cyberattack as well*« (Council of the EU – answer to question E-002456/21).

Additionally, some consideration should be given to the argument that the measures in response to cyber operations also comprise retorsion, countermeasures and measures taken based on necessity. A brief analysis of the positions expressed in the UN official Compendium of Voluntary National Contributions may provide some fascinating insight into the nexus between such measures and espionage.

Concerning retorsion, the Netherlands pointed out that *»a state may respond to a cyber operation by another state, for example, by declaring diplomats 'persona non grata', or by taking economic or other measures against individuals or entities involved in the operation. Another retorsion measure a state may consider is limiting or cutting off the other state's access to servers or other digital infrastructure in its territory, provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory*« (UN Official Compendium, 2021, p 62). Therefore, it seems reasonable to conclude that retorsion could not be a valid excuse for extraterritorial espionage activity violating international law.

Concerning countermeasures, instead, according to Germany: »*Due to the multifold and close interlinkage of cyberinfrastructures not only across different States but also across different institutions and segments of society within States, cyber countermeasures are specifically prone to generating unwanted or even unlawful side effects. Against this background, States must be extensive and prudent in examining whether or not the applicable limitation criteria to cyber countermeasures are met. A State may – a maiore ad minus – engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of*

side effects if such measures fulfil the requirements for countermeasures« (UN Official Compendium, 2021, p 42). Then, as sharply observed by another author, »*by suggesting this precautionary step, Germany necessarily acknowledges that espionage as such is not a violation of international law*« (Schmitt, 2021).

However, an extensive interpretation of the requirements allowing measures taken based on necessity might create an unexpected deterrence effect. In order to clarify this point, it is helpful to follow the German position expressed in the UN Official Compendium of Voluntary National Contributions. According to Germany, »*the wrongfulness of a State's cyber operation that contravenes its international obligations may be precluded by exception if that State acted out of necessity. It entails that a State may – under certain narrow circumstances – act against malicious cyber operations by resorting, for its part, to active counter-operations even in certain situations in which the prerequisites for countermeasures or self-defence are not met*« (UN Official Compendium, 2021, p 42). An extensive interpretation of the requirements for the measures taken based on necessity will somehow allow the circumvention of the limits that characterize countermeasures (it goes without saying, however, that the measures taken based on necessity will, in any event, have to comply with other requirements, including proportionality). It means that the interpretation of the concepts of *essential interest* and *grave and imminent peril* will be essential[10]. The margin for interpretation, however, seems to be narrow. Indeed, as convincingly pointed out by Schmitt, *»the critical point is that the mere fact that a hostile cyber operation has targeted a vital interest does not alone justify acting based on necessity; the peril must be grave. An example of failure to satisfy this element would be pure espionage involving critical infrastructure«* (Ibid.).

5 CRIMINAL AND ADMINISTRATIVE RESPONSE TO CYBER ESPIONAGE

The recent responses of the US and EU to cyber espionage will be now analyzed. As previous paragraphs have discussed, the analysis of cyber espionage phenomena will cover hybrid warfare, economic theft, and »traditional« espionage.

At first, the different approaches adopted by the US and EU on the question of attribution need to be mentioned. On the one hand, the US does not hesitate to

[10] *In this regard, according to the said position, »Germany holds the view that, in the cyber context, the affectedness of an 'essential interest' may, among other things, be explained by reference to the type of infrastructure actually or potentially targeted by a malicious cyber operation and an analysis of that infrastructure's relevance for the State as a whole. For example, the protection of certain critical infrastructures may constitute an 'essential interest'. It might likewise be determined by reference to the type of harm actually or potentially caused due to a foreign State's cyber operation. For example, protecting its citizens against serious physical harm will be an 'essential interest' of each State – regardless of whether critical infrastructure is targeted or not. Nevertheless, given the exceptional character of the necessity argument, an 'essential interest' must not be assumed prematurely«. Additionally, Germany pointed out also that »a case-by-case assessment is necessary to determine whether a peril is 'grave'. The more important an 'essential interest' is for the basic functioning of a State, the lower the threshold of the 'gravity' criterion should be. Germany agrees that a 'grave peril' does not presuppose physical injury but may also be caused by large-scale functional impairments«.*

attribute malicious cyber activities and irresponsible State behaviour to the People's Republic of China (White House, 2021), while the EU limits its assertion only to a lack of due diligence for allowing Chinese territory to be used for malicious cyber activities (Declaration by the High Representative, 2021).

On the contrary, concerning Russia's improper influence activities, we can find only a low-profile posture from the US (Statement by the President, 2016), notwithstanding the well-known Mueller Report has shown that »*in sum, the investigation established that Russia interfered in the 2016 presidential election through the »active measures« social media campaign carried out by the IRA, an organization funded by Prigozhin and companies that he controlled*« (Mueller Report, 2019, p 35). Apart from the sanctions regime concerning hybrid warfare which will be analyzed shortly, the US reacted against Russia's improper influence on the US election by the expulsion of some Russian diplomatic staff. This measure of retorsion, however, as already pointed out by Schmitt, »*involves acts that international law does not prohibit*« (Schmitt, 2021, p 762). Thus »*a State may engage in it without establishing that the underlying activities violate its international legal rights*«. Instead, the European Council did not miss the opportunity to »*condemn the illegal, provocative and disruptive Russian activities against the EU, its Member States and beyond«* (European Council 2021). Such European Council conclusions, moreover, should be read in conjunction with the subsequent Joint Communication (EU Commission and High Representative for Foreign Affairs and Security Policy) to the European Parliament, the European Council and the Council on EU-Russia relations, issued on June 16 2021, where it is clearly stated that »*the Russian leadership uses a variety of instruments to influence, interfere in, weaken or even seek to destabilise the EU and its Member States, as well as the Western Balkans and Eastern Partnership countries. As part of these efforts, it invests heavily in its ability to control and influence the information space inside and outside its borders«* (Joint Communication, 2021, p 1). In this regard, it is also relevant to highlight that the European Council had already invited the »*EU's High Representative for Foreign Affairs and Security Policy, in cooperation with the Member States and EU institutions, 'to develop an action plan on strategic communication to address Russia's ongoing disinformation campaigns'«* (European Council Conclusions, 2015)[11]. Therefore, the European External Action Service set up (Joint Communication, 2018, p 1)[12]:

– Specific strategic communication task forces to address disinformation and develop response strategies. In this regard, the flagship project named *EUvsDisinfo,* with the aims of providing a better forecast, address, and response to ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood, is of note;

[11] *European Council meeting (19 and 20 March 2015) – Conclusions – EUCO 11/15 (https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf).*

[12] *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation, 5 December 2018 JOIN(2018) 36 final (https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf).*

– A Rapid Alert System (RAS) to provide warnings on disinformation campaigns in real time through dedicated technological infrastructure.

Additionally, the EU Commission has issued a European democracy action plan (Communication from the Commission, 2020) which, *inter alia*, strengthens the fight against disinformation. Among the EU's different activities against disinformation, it is also essential to mention Special Report No. 09/2021 from the European Court of Auditors, »Disinformation Affecting the EU: Tackled but not Tamed«. The European Court of Auditors found that *»the EU action plan against disinformation was relevant but incomplete, and even though its implementation is broadly on track and there is evidence of positive developments, some results have not been delivered as intended«* (European Court of Auditors, 2021, p 4).

The US Department of Defence (DoD), instead, recently recalled that »*a core part of the DoD's mission to defend the US elections consists of defending against covert foreign government malign influence operations; targeting the US electorate*« (Ney, Jr., 2020). To that end, the DoD supported the idea of responding to malicious cyber activities carried out against the United States, including carrying out military cyber operations. According to the DoD, compliance with the right of free expression under the First Amendment of such cyber operations against covert foreign government malign influence is ensured »…*whether the operation is targeting the foreign actors seeking to influence US elections covertly rather than the information itself; the extent to which the operation may be conducted in a »content-neutral« manner; and, the foreign location and foreign government affiliation of the targeted entity … Accordingly, in assessing proposed operations related to elections, DoD lawyers pay particular attention to whether the proposed operation may be conducted consistent with legal and regulatory limits on the use of official positions to influence or affect the results of US elections or to engage in, or create the appearance of engaging in, partisan politics«* (Ibid.). However, of note is the fact that the DoD speaks only of the First Amendment, without mentioning international law on this topic. The absence of clear and manifest blame from the US for improper foreign influence is consistent with US jurisprudence. The Ninth Circuit Court of Appeals, among other things, affirmed that the Foreign Sovereign Immunities Act (FSIA) bars plaintiffs' claims against Qatar for allegedly hacking into their computer servers, stealing their confidential information, and leaking it to the media in a retaliatory effort to embarrass the plaintiff and thereby to neutralize their ability to continue to effectively criticize the Qatari regime and its alleged support of terrorism[13].

[13] *Broidy Capital Management v. the State of Qatar, No. 18-56256 (9th Cir. 2020). According to this judgement: »The alleged actions that Qatar took here have not been shown to violate either Qatari law or applicable international law. The parties do not dispute that, under Qatari law, the various criminal prohibitions against hacking, theft, or disclosure of trade secrets do not bind government agents acting following official orders. Indeed, it would perhaps be surprising if the domestic law of any country prohibited its government agents from engaging in covert cyber espionage and public relations activities aimed at foreign nationals in other countries. Nor have the specific forms of cyber espionage alleged here been shown to violate international law's judicially enforceable principles. The status of peacetime espionage under international law is a subject of vigorous debate. The parties have not pointed us to any sufficiently clear rule of international law that would impose a mandatory and judicially enforceable duty on Qatar not to do what it allegedly did here.«*

The US and EU have also developed a dedicated sanctions regime concerning hybrid warfare and economic theft.

In the US, Executive Order (EO) 13694, issued on April 1, 2015 authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities which result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. This EO was amended to allow for the imposition of sanctions on individuals and entities responsible for tampering, altering, or causing the misappropriation of information to interfere with or undermine election processes or institutions. Moreover, EO 13757, issued on December 28, 2016, allowed the Secretary of the Treasury (in consultation with the Attorney General and the Secretary of State) to impose sanctions on those determined to be responsible for or complicit in cyber-enabled activities under EO 13694. The US Department of State and other US government agencies work to identify individuals and entities whose conduct meets the criteria outlined in EO 13694, and designate them for sanction under the delegated authority of the Treasury's Office of Foreign Assets Control (OFAC). Those designated under this authority are added to OFACS's Specially Designated Nationals and Blocked Persons list. Of note, US-designated Russia-linked individuals have been included in OFACS's list for attempting to influence the US electoral process, while a debate is ongoing within the US Administration on whether and how to sanction China for ransomware attacks (Bertrand, Liptak and Fung, 2021). Additionally, OFAC recently resorts to EO 13694 in order to designate a Russia-based virtual currency exchange for its part in facilitating financial transactions for ransomware actors.

The EU, on the other hand, adopted the Council Decision (CFSP) 2019/797 and the Council Regulation (EU) 2019/796 on May 17 2019, concerning restrictive measures (such as travel bans, asset and funds freezes) against cyber-attacks threatening the Union or its Member States. Subsequently, these Acts have been amended to designate individuals and entities. Looking at the last consolidated version of the Acts, we can see the designation of both Chinese individuals and entities (neither of which, however, belong to the Chinese People's Liberation Army) and individuals and entities belonging to the Armed Forces of the Russian Federation. The designations of Russian individuals and entities are related to acts of hybrid warfare. In contrast, for the Chinese individuals and entities, the designation is related to cyber-attacks that had targeted multinational companies' information systems, including companies located in the Union, and had gained unauthorized access to commercially sensitive data, resulting in significant economic loss.

As already pointed out by Chachko, a significant difference between the US and EU sanction regimes is the standard of judicial review applied for delisting. The US judiciary shows a deferential attitude towards OFAC designations, and non-resident aliens without substantial connections to the United States are not entitled

to Fifth Amendment protections. On the other hand, the European Court of Justice (ECJ), under Kadi jurisprudence, shows a minor degree of deference towards EU designation and requests well-founded reasons supported by evidence. This means that disclosure of classified information could be necessary in the case of a request for judicial review of a designation. However, the ECJ jurisprudence also allows the disclosure of a summary outlining the information's content or that of the evidence in question (Chachko, 2019). Additionally, Article 105.8 of the General Court Rules of Procedure, in the case of information or material about the security of the Union or that of one or more of its Member States, even allows – after an assessment of strict necessity – the judgment to be delivered based on closed evidence not disclosed to the applicant even as a non-confidential summary[14]. Finally, concerning the EU's sanction regime, it is worth noting that Recital 9 of the Council Decision (CFSP) 2019/797 of May 17 2019 explicitly clarified that »*targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State«*. The latter understanding is consistent with that expressed by Germany[15] and it is in line with the US point of view. According to the US, *»It is crucial, however, to distinguish legal attribution from attribution in the technical and political senses* » (UN Official Compendium, 2021, p 142).

In addition to the sanctions regime, the US – but not the EU or any of its Member States – is fighting relentlessly against economic espionage through means belonging to criminal law. To that end, we can mention the Department of Justice's (DoJ) China Initiative, which aims to identify and prosecute those engaged in trade secret theft, hacking, and economic espionage, as well as protecting US critical infrastructure against external threats through foreign direct investment and supply chain compromises, and combating covert efforts to influence the American public and policymakers without proper transparency. This initiative, of course, is not limited to the cyber threat, but the latter was clearly included. Within the framework of this initiative, the DoJ has also obtained several indictments against Chinese cyber spies, including some belonging to the Chinese People's Liberation Army (Department of Justice, February 10, 2020). This type of judicial activism of the DoJ, however, has not been limited to Chinese PLA personnel, as other indictments have been issued against personnel belonging to the Russian Federal Security Service (Department of Justice, 2017). Moreover, the DoJ issued a criminal complaint charging North Korean citizens for their involvement in a conspiracy to conduct multiple destructive cyberattacks around the world, and alleging the DPRK government's support in those malicious cyber actions (Department of Justice, 2018). Additionally, to pull the rug

[14] *For more details on the EU General Court Rules of Procedure, see Abazi, V., & Eckes, C., 2018.*

[15] *See: UN Official Compendium, 2021. According to the German view, »attribution in the context of State responsibility must be distinguished from politically assigning responsibility for an incident to States or non-State actors: generally, such statements are made at the discretion of each State and constitute a manifestation of state sovereignty«.*

from under the cybercriminals' feet (including but not limited to those potentially hired for cyber espionage), the DoJ obtained an indictment against a darknet-based cryptocurrency laundering service for the charge of conducting money transmission without a licence (Department of Justice, February 13, 2020).

As already pointed out by Chimène (2019), this attribution through criminal indictment had at least three audiences: (i) Chinese (or Russian) authorities and potential hackers; (ii) the US domestic audience; and (iii) an international audience comprised of other foreign states and individuals. Concerning the latter, however, it seems opportune to draw a distinction. On the one hand, such indictments are an occasion to encourage law enforcement cooperation, mainly with like-minded States. On the other hand, however, if we look to States dissenting from the US, the indictments are essential to assert that cyber espionage should be considered unlawful even when carried out by State officials. The latter consideration is not of small importance, as the legal framework on cyber espionage is far from clear (Chimène, 2019).

Finally, concerning »traditional« espionage, it is worth recalling Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016, concerning measures for a typically high level of security of network and information systems across the Union. Although public administration entities that carry out activities in public security, law enforcement, defence or national security are explicitly excluded from the scope of its application, this legislation sets significant and detailed standards of cyber security measures. Consequently, *de facto*, Directive (EU) 2016/1148 produced a spill-over effect implying the application of its standard (at least as a minimum standard) even to other areas, including defence or national security. With regard to EU Member States' practice in the case of »traditional« espionage, it is only worth noting that after the 2014 expulsion of US personnel from Germany due to allegations of spying, no prosecution of US personnel was attempted by Germany (Patrick, 2015). Instead, Germany asked the US to reach a comprehensive intelligence agreement. The US, however, declined the request (Daugirdas, 2014).

6 US MILITARY RESPONSE TO CYBER ESPIONAGE: CLANDESTINE MILITARY ACTIVITY OR OPERATION IN CYBERSPACE

While the US diplomatic response to improper influence activities by Russia has been limited, US legislation has been significantly modified.

First, it should be mentioned that the provision allows active cyber defence operations against attacks in cyberspace by the Russian Federation, the People's Republic of

China, the Democratic People's Republic of Korea, and the Islamic Republic of Iran[16]. Moreover, US Congress also affirmed the authority of the Secretary of Defense to »*conduct military operations, including clandestine operations, in the information environment to defend the United States, allies of the United States, and interests of the United States, including in response to malicious influence activities carried out against the United States or a United States person by a foreign power*«[17].

Additionally, Title 10 of the USC (United States Code) § 394 was amended to allow the Armed Forces to conduct cyber activities or operations in cyberspace, including clandestine military activities. The latter authority includes »*the conduct of military activities or operations in cyberspace short of hostilities or in areas in which hostilities are not occurring, including for the preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States*«. Of note is the fact that the Title 10 authority to carry out clandestine military activities or operations in cyberspace is additional to Title 50 of the US Code statutory authority for intelligence activities. In other words, even before the new Title 10 authority, Armed Forces could carry out clandestine activities, including in cyberspace, under Title 50 of the US Code statutory authority. The new USC § 394 has not created an additional category of permissible secret cyberspace operations, but rather it has established a dedicated Congressional oversight of clandestine cyber activities.

Conclusion

Espionage is commonly symbolized by the Roman god Janus, represented by a double-faced head. It is related to the root ambivalence that characterizes espionage, where no foreign State, even the tightest Ally, can be deemed an absolute friend. From the legal point of view this ambivalence is also confirmed, as espionage is not illegal *per se* for international law, but it can be prosecuted as a crime by domestic law.

The impact of ICT on espionage is significant since, today, more and more States can carry out espionage in all its facets more effectively. This new situation is creating a circle that keeps turning since more and more States, echoing the German position on the application of international law in cyberspace, may *»engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of side effects if such measures fulfil the requirements for countermeasures*« (UN Official Compendium, 2021, p 42). The new Title 10

---

[16] *According to the fiscal year (FY) 2019, the National Defense Authorization Act (NDAA): »In the event that the National Command Authority determines that the Russian Federation, the People's Republic of China, the Democratic People's Republic of Korea, or the Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense from conducting cyber operations and information operations as traditional military activities« (John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 1642(a), 132 Stat. 1636, 2132 (2018).*

[17] *Section 1631 of the National Defense Authorization Act for Fiscal Year 2020, amending USC (United States Code) § 391.*

authority allowing Armed Forces to conduct clandestine cyber military activities is one example that confirms this conclusion.

It implies that espionage should not be accepted whenever it aims at foreign influence or economic theft. On the contrary, »pure« cyber-espionage committed by a foreigner abroad through ITC means should not be punishable by the criminal law of the »Victim State«, as the intelligence-gathering activities were legal by the law of the country where they took place, as well as »tolerable« for the international community.

A high threshold for triggering the Law of Armed Conflict (LOAC) in the case of cyber operations resulted in the proliferation of cyber espionage, particularly in hybrid warfare and economic theft. This suggests an opportunity for radical change in the appraisal of traditional espionage. The latter, in some ways, should be seen as a measure aimed at preventing and reacting to the use of ICT means for hybrid warfare and economic theft. »Traditional« espionage should indeed be seen as the lesser evil, to avoid a possible uncontrolled escalation in the case of cyber operations. Failing to do so could sooner or later open Pandora's Box, i.e. accept the risk of triggering a full-scale armed conflict in reaction to cyber operations; a situation that is not desirable because not all the possible consequences and effects can be predicted.

With regard to foreign influence, it is hoped that hybrid confrontation will drop in intensity. To reach this goal, Western countries, which are currently those more affected by this type of warfare, might not exclude *a priori* the possibility of having a frank and open discussion with China and other non-Western countries. Such negotiation should increase transparency rather than limit human rights. A fair balance on this sensitive issue is opportune. One should keep in mind that the fight against disinformation should not lead to the creation of a sort of Orwellian Ministry of Truth[18].

Concerning economic espionage, a clear understanding of this topic has not been reached so far; US and EU activism on this side is critical. Even though some criticism can be reasonable[19], it is vital to seize every opportunity to hamper

---

[18] *It is worth mentioning the following extract from the remarks of EU Vice-President Vera Jourová: »I am thrilled that our response to disinformation is maturing with every step we take. I need to say one thing from the outset. We will not regulate the removal of disputed content. We do not want to create a Ministry of Truth. Freedom of speech is essential, and I will not support any solution that undermines it«.*

European Democracy Action Plan: Remarks by Vice-President Vera Jourová, December 3 2020 (https://ec.europa.eu/commission/presscorner/detail/en/speech_20_2308).

[19] *For example, Stefan Soesanto (2020) argued that »as far as tangible evidence goes, there is no proof that sanctions deter anyone, shame anyone, nor impose costs or restrict an adversary's ability to conduct their malicious campaigns. The very notion that cyber sanctions (for example, travel bans) might work because Russian military intelligence officials are longing for a house on the French Riviera and want to visit the Colosseum in Rome is built on fragile ice. Similarly, it is highly doubtful that any intelligence front companies nor individual cyber operatives own any funds subject to EU jurisdiction. It is not known whether the EU has frozen any assets of individuals and entities listed under the EU cyber sanctions regime so far. Given this discrepancy, EU cyber sanctions are largely symbolic, and their prime utility seems to signal red lines, political intent and EU unity«.*

those who may have the idea to carry out cyber-attacks for economic theft. In the same vein, as the DoJ has done, it seems even more helpful to chase and block virtual currency exchange providers involved in facilitating financial transactions for ransomware actors. To that end, even domestic criminal law could be helpful. While cybercriminals – even more so when belonging to the armed forces of foreign countries – will rarely be prosecuted for extraterritorial offences, domestic criminal law offences can still be helpful. Taking into account that each sanctions regime can be applied only to a limited number of situations (due to the need for specific and robust evidence), in order to achieve a significant deterrent effect, domestic criminal law could fill the gap by indicting virtual currency exchange providers of conducting money transmission without a licence. Indeed, this *modus operandi* could break the business model of those involved in economic theft by seizing assets that otherwise would have been available to the cybercriminals. Although it may be true that in the case of State-led theft of confidential information this kind of criminal approach is not enough, it could play an essential role in dissuading criminal gangs from acting as a proxy for States' intelligence agencies.

Above all, however, within the ongoing strategic competition between Western and non-Western countries, the actual match is the ongoing development of international law applicable to cyber operations. Western countries' attempt to shape international law to effectively tackle hybrid warfare and economic theft. On the contrary, other actors are exploiting the loopholes of the actual contradictory legal regime on these matters.

As highlighted in this article, different forms of cyber espionage are currently in grey areas of international law. Consequently, on the current stage, it appears not to be possible to conclude whether the new legal measures adopted by the US and EU will become a new trend in international law. Nevertheless, these legal measures still play an essential part in reaching that desired trend.

Bibliography

1. *Abazi, V., and Eckes, C., 2018. Closed evidence in EU courts: Security, secrets and access to justice. Common Market Law Review, 55(3), 753-782. http://www.kluwerlawonline.com/abstract.php?area=Journals&id=COLA2018069.*
2. *Bertrand, N., Liptak, K., Fung, B., 2021. Biden administration debating whether and how to sanction China for ransomware attacks, www.cnn.com 20 July 2021. https://edition.cnn.com/2021/07/19/politics/china-biden-ransomware/index.html.*
3. *Bettauer, R. J., 2014. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). Provisional Measures Order, The American Journal of International Law, Vol. 108, No. 4 (October 2014), pp 763-769.*
4. *Buchan, R., 2018. Cyber Espionage and International Law, Hart Publishing.*
5. *Chachko, E., 2019. Due Process Is in the Details: US Targeted Economic Sanctions and International Human Rights Law, 113 AJIL Unbound 157-162.*

6. *Cheng, B., Properly Speaking, Only Celestial Bodies Have Been Reserved for Use Exclusively for Peaceful (Non-Military) Purposes, but Not Outer Void Space, International Law Studies – Volume 75 (2000) – International Law Across the Spectrum of Conflict: Essays in Honour of Professor L.C. Green On the Occasion of His Eightieth Birthday. Michael N. Schmitt (Ed.).*
7. *Chimène, K., 2021. Foreign Election Interference and International Law In: Duncan B. Hollis and Jens David Ohlin (Eds.), Defending Democracies. Oxford University Press.*
8. *Chimène, K., 2019. Attribution by Indictment. UC Hastings Research Paper No. 316. https://ssrn.com/abstract=3322943, 9 January 2019.*
9. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – On the European Democracy Action Plan, 3 December 2020 COM (2020) 790 Final.*
10. *Council of the EU, Parliamentary Question, Answer to Question E-002456/21, 22 September 2021. https://www.europarl.europa.eu/doceo/document/E-9-2021-002456-ASW_EN.html.*
11. *Daugirdas, K., and Mortenson, D. J., 2014. Contemporary practice of the United States relating to international law. The American Journal of International Law, Vol. 108, No. 4, [American Society of International Law, Cambridge University Press], 2014, pp 783-842. https://doi.org/10.5305/amerjintelaw.108.4.0783.*
12. *Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory, 19 July 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/.*
13. *Department of Justice – Office of Public Affairs, Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax, 10 February 2020. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.*
14. *Department of Justice – Office of Public Affairs, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, 6 September 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.*
15. *Department of Justice – Office of Public Affairs, Ohio Resident Charged with Operating Darknet-Based Bitcoin »Mixer,« which Laundered Over $300 Million, 13 February 2020, https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.*
16. *Department of Justice – Office of Public Affairs, US Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts, 15 March 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.*
17. *Drake, R., 2004. The Soviet Dimension of Italian Communism [Review of Oro da Mosca: I Finanziamenti Sovietici al PCI dalla Rivoluzione d'Ottobre al Crollo dell'URSS; L'Oro di Mosca: La Verità sui Finanziamenti Sovietici al PCI Raccontata dal Diretto Protagonista. 2nd Ed., by V. Riva & G. Cervetti. Journal of Cold War Studies, 6(3), 115-119. https://www.jstor.org/stable/26925390.*
18. *European Council (19 and 20 March 2015) – Conclusions.*
19. *European Council (24 and 25 May 2021) – Conclusions.*
20. *European Court of Auditors Special Report No 09/2021, Disinformation Affecting the EU: Tackled but not Tamed.*
21. *Fiore, P., 1837-1914; Borchard, E. M., 1884-1951, International Law Codified and its Legal Sanction: Or, The Legal Organization of the Society of States.*

22. *Geissler, E., and Hunt Sprinkle, R., 2013. Disinformation Squared: Was the HIV-from-Fort-Detrick Myth a Stasi Success? Politics and the Life Sciences, Vol. 32, No. 2, Association for Politics and the Life Sciences, pp. 2-99. http://www.jstor.org/stable/43287281.*
23. *Hemmings, J., Swire, N., 2019. The Cloud Act Is Not a Tool for Theft of Trade Secrets, 23 April 2019, https://www.lawfareblog.com/cloud-act-not-tool-theft-trade-secrets.*
24. *Joint Communication to the European Parliament, the European Council and the Council on EU-Russia relations – Push Back, Constrain and Engage, dated 16. June 2021 – JOIN (2021) 20 Final.*
25. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation, 5. December 2018 JOIN (2018) 36 Final.*
26. *Krizek, M. B., 1988. The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal 6, No. 2 (Fall 1988): pp 337-360.*
27. *Lahmann, H., 2020. Information Operations and the Question of Illegitimate Interference under International Law (June 2020). Israel Law Review, Volume 53, Issue 2, pp 189-224 36, June 2020.*
28. *Lotrionte, C., 2014. Countering State-Sponsored Cyber Economic Espionage under International Law, 40 – NC. J. INT'L L. 443.*
29. *Lubin, A., 2018. Cyber Law and Espionage Law as Communicating Vessels (March 17, 2018). Proceedings of the 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2018), Available at SSRN: https://ssrn.com/abstract=3099769.*
30. *Mueller Report – US Dep't of Justice, Report On The Investigation Into Russian Interference In The 2016 Election Vol. I, 1-5 (2019), p 35.*
31. *National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2. Top Secret. No drafting information appears in the source text. An earlier, similar version, 30 April, in Ibid., RG 59, Records of the Department of State, Policy Planning Staff Files 1944-47: Lot 64 D 563, Box 11.*
32. *NATO-wide co-operation and coordination in the field of psychological warfare – proposal by the Federal Republic of Germany, 1960. Available at: https://archives.nato.int/nato-wide-co-operation-and-co-ordination-in-field-of-psychological-warfare-proposal-by-federal-republic-of-germany.*
33. *Navarrete, I., and Buchan, R., 2019. Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions, Cornell International Law Journal: Vol. 51: No. 4, Article 4.*
34. *Ney, Hon. P. C. Jr., 2020. DOD General Counsel Remarks at US Cyber Command Legal Conference – 2 March 2020. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.*
35. *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established according to General Assembly resolution 73/266. UN document A/76/136 dated 13 July 2021.*
36. *Ohlin, J. D., 2021. Election Interference: A Unique Harm Requiring Unique Solutions, 1 November 2018. Defending Democracies: Combating Foreign Election Interference in a Digital Age (Oxford University Press, 2021), Cornell Legal Studies Research Paper No. 18-50. https://ssrn.com/abstract=3276940 or http://dx.doi.org/10.2139/ssrn.3276940.*
37. *Oppenheim, L., 1905. International Law Vol. 1, 1905. https://archive.org/details/in.ernet.dli.2015.24439/page/n529/mode/2up?q=spy.*

38. *Orde F. K., 2016. Lawfare – Law as a Weapon of War, Oxford University Press 2016.*
39. *Patrick, T. C. R., 2015. »Absolute Friends«: US Espionage against Germany and Public International Law. In: Revue Québécoise de Droit International, Volume 28-2, 2015. pp 173-203. https://www.persee.fr/doc/rqdi_0828-9999_2015_num_28_2_2188.*
40. *Pompeo, M. R., 2019. U. S. Secretary of State, Why Diplomacy Matters (Questions and Answers), 15 April, 2019. From the official US State Department transcript. https://2017-2021.state.gov/remarks-at-texas-am-wiley-lecture-series/index.html.*
41. *Quint, P. E., 1997. The Imperfect Union: Constitutional Structures of German Unification. Princeton University Press, 1997, pp 213-214.*
42. *Radsan, A. J., 2007. The Unresolved Equation of Espionage and International Law, 28 MICH. J. INT'L L. 595.*
43. *Schmitt, M., 2021. Foreign Cyber Interference in Elections. Vol. 97, International Law Studies 2021.*
44. *Schmitt, M., 2021. Germany's Positions on International Law in Cyberspace Part I. https://www.justsecurity.org/, 9 March 2021.*
45. *Selvage, D., 2019. Operation »Denver«: The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985-1986 (Part 1). Journal of Cold War Studies 2019; 21 (4): 71-123. https://doi.org/10.1162/jcws_a_00907.*
46. *Shane, S., 2018. NEWS ANALYSIS – Russia Is not the Only One Meddling in Elections. We Do It, Too, The New York Times, 17 February 2018.*
47. *Soesanto, S., 2020. Europe Has No Strategy on Cyber Sanctions, November 20, 2020. https://www.lawfareblog.com/, https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions.*
48. *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 29 December 2016. In that statement, President Obama attributed to Russia (only) the violation of »established international norms of behaviour«, but not the violation of international law. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.*
49. *Stone, J.,1962. Legal Problems of Espionage in Conditions of Modern Conflict, Essays on Espionage and International Law. OHIO State University Press 1962.*
50. *Strawbridge, J., 2016. The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation, 47 GEO. J. INT'l L. 833.*
51. *Tondini, M., 2019. Espionage and International Law in the Age of Permanent Competition. Military Law and the Law of War Review Vol. 57, No. 1, 2018-2019.*
52. *Van Wie Davis, E., 2021. Shadow Warfare: Cyberwar Policy in the United States, Russia and China, Rowman & Littlefield Publishers.*
53. *Whitehouse Statements and Releases – The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, 19 July 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.*
54. *Yearbook of the International Law Commission, 1971, Vol. II, Part One, pp 265-266.*

e-mail: davide.giovannelli@ccdcoe.org

Taťána Jančárková

DOI:10.33179/BSV.99.SVI.11.CMC.24.2.4

PRIVAJANJE PSOV NA POVODEC V KIBERNETSKI VOJNI

LEASHING THE DOGS OF CYBER WAR

Povzetek Države se vse bolj ukvarjajo z razvojem kibernetskih zmogljivosti, ki lahko delujejo v celotnem spektru učinkov. Strukture, pristojne za doseganje teh učinkov, so navadno institucionalno povezane z oboroženimi silami ali obveščevalnimi službami oziroma so sestavljene iz obeh. Zaradi narave njihovih dejavnosti in možnosti vpliva na ustavne temelje demokratične države za obe vrsti organizacij navadno veljajo strogi mehanizmi nadzora in kontrole. Kljub temu je na voljo le malo raziskav o ustreznih nacionalnih okvirih, ki urejajo ofenzivne kibernetske zmogljivosti, in malo informacij o veljavnih nadzornih mehanizmih. V članku so predstavljeni pregled področij nadzora in izzivi, povezani s kibernetskimi zmogljivostmi, ter nakazane možnosti za prihodnje raziskave.

Ključne besede ***Ofenzivne kibernetske operacije, človekove pravice, pravna država, ustavni red, nadzor.***

Abstract States have increasingly been engaged in the development of cyber capabilities which can act across the full spectrum of effects. The structures competent to deliver these effects are usually institutionally tied to armed forces or intelligence services, or represent a mixture of the two. Both types of organizations are typically subject to strict oversight and control mechanisms due to the nature of their activities and their potential to impact on the constitutional foundations of a democratic state. Yet, there is limited research available on the respective national frameworks governing offensive cyber capabilities, and similarly little information on the applicable control mechanisms. This article provides an overview of the areas of oversight, explores the challenges related to cyber capabilities, and offers possible avenues for future research.

Key words ***Offensive cyber operations, human rights, rule of law, constitutional order, oversight.***

Introduction

When the US Cyber Command was established in 2009, it was a trailblazer in the field of institutionalizing cyber capabilities. Ten years later, several countries, including NATO and EU Member States, had established or were openly planning to develop cyber capabilities spanning the full spectrum of effects. In recent years »offensive cyber« has lost its somewhat negative legal and political connotations, and has been on the way to becoming a regular component of a modern state's national security and defence toolkit. Nevertheless, in spite of being a part of a broader general framework, cyber operations and cyberspace effects also have a novel character and potentially constitute a challenge from the perspective of constitutional and administrative law, including the respect and protection of fundamental rights and freedoms. This article contemplates the oversight and control mechanisms traditionally implemented in democratic states in respect of security and military elements, and assesses the applicability of executive control, parliamentary oversight and judicial review to cyber operations, with a particular focus on offensive cyber capabilities.

1 »OFFENSIVE CYBER« REVISITED

1.1 Institutionalization and frameworks

Offensive cyber capabilities can be understood as those that can deliver the full range of effects, that is, from securing to destroying or »completely and irreparably deny[ing] access to, or operation of, an asset« (NATO, 2020). They can also be understood as those that do not limit themselves to defence of one's own perimeter, but produce 'noticeable denial effects (i.e. degradation, disruption or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains' (DoD, 2018).

Unlike cyber security, which is primarily concerned with the protection of one's own information infrastructure and dependent services, cyber defence which includes offensive capabilities has the purpose of supporting multiple lines of a nation's efforts. Besides complementing the protection of critical information infrastructure, such capabilities also form part of the national defence system against terrorists, criminal and state actors, enable conventional defence operations, and help further the foreign policy agenda (UK, n.d.). While cyber security is often entrusted to civilian authorities or entities outside the military, cyber defence is an area of responsibility of structures directly belonging to or affiliated with armed forces and ministries of defence. The two concepts are, however, closely linked, feed into each other and at times overlap.

As mentioned in the introduction, there has been a clear and growing trend in openly developing offensive cyber capabilities, or active cyber defence, and institutionalizing them, including in NATO and EU countries (Pernik, 2018). According to Blessing (2021), cyber forces defined as 'active-duty military organizations with the capability and authority to direct and control strategic cyberspace operations to influence

strategic diplomatic and/or military interactions' had, by 2018, been established in as many as 61 UN Member States.

It has been repeatedly confirmed in national statements (Cyber Law Toolkit, 2021) and academic literature that offensive cyber operations can deliver effects which qualify as use of force. Even cyber operations that do not inflict physical harm or injury, i.e. lack the effect of kinetic force, can qualify as use of force under certain circumstances (Netherlands, 2019; Schmitt, 2019). Use of force has traditionally been reserved for armed forces and subjected to stringent control nationally and internationally, given the consensus of the international community on the general prohibition of the threat or use of force, enshrined in Article 2(4) of the UN Charter.

In parallel, active cyber defence involves a number of activities usually associated with intelligence services and espionage. Reconnaissance, exploitation, infiltration and information gathering are necessary preparatory activities for offensive cyber operations, which are undertaken both abroad and on domestic soil. The entities entrusted with these activities must therefore be authorized to act internally on home territory and infrastructure. However, deployment of armed forces at home is always subject to exceptions provided by law and often limited to assistance in civilian crisis management such as cases of natural disasters or internal security (including the recent Covid-19 pandemic, for instance). It should not come as a surprise, then, if cyber defence structures including offensive capabilities are often built within military intelligence or as joint structures involving both traditional military and intelligence components (Pernik, 2018).

Given the growth in the number of countries investing in these capabilities, research interest must inevitably turn to examining the underlying regulatory frameworks. The applicable frameworks span from those governing crisis management, to intelligence services, to those regulating deployment of the military and use of force.

1.2 What are the stakes?

The activities of both military and intelligence services are subject to scrutiny and control because of their potential to interfere with fundamental rights and freedoms and the values democratic states are based on. Most states will have civilian control of the armed forces inscribed into their constitutional law, along with professed respect and promotion of human rights and fundamental freedoms. Depending on historical experience, some states apply more restrictive governance concepts to intelligence services than others; when it comes to military intelligence, the record is however, almost universally mixed (Jasutis et al., 2020).

Should we be particularly wary about oversight measures for cyber capabilities? How can they be controlled? Is it at all possible?

Cyber effects can have major negative implications for a state's performance in human rights and fundamental freedoms. The range of potential interferences is

broad, from right to privacy, freedom of speech, freedom of assembly and peaceful enjoyment of property, all the way to right to life, if we consider cyber operations that lead to destructive effects comparable to conventional acts of violence.

To some extent, cyber operations have a specific character which warrants a specific approach. Due to the borderless nature of cyberspace and the ease with which unintended effects can propagate and bleed over to other systems and infrastructure, cyberspace operations should be carefully used and well controlled. In parallel, there is need for speed, flexibility and secrecy if the desired effects are to be delivered, which might caution against too heavy a supervisory mechanism.

Considering the above, it can be expected that cyber operations will rarely be executed under declared states of emergency; most of them require quite the opposite in order to maintain the advantage of surprise over the adversary. While human rights law can be derogated under certain circumstances, in most instances of cyber operations states would be unlikely to be able to rely on such a derogation.

Admittedly, the stakes are high. Firstly, there is the constitutional principle of civilian control over armed forces, and constraints on their deployment at home and abroad. Secondly, if cyber operations can constitute use of force, states must be very careful not to trespass their commitments under international law. Thirdly, the public in NATO and EU Member States are very sensitive to interference with their rights and freedoms by excessive intelligence work. The revelations of Edward Snowden and other whistle-blowers dealt a severe blow to confidence in intelligence services in the past, and only the ensuing judicial decisions have forced states to change the applicable legislation. At the same time, armed forces usually benefit from a positive public reputation, and should strive to maintain it.

2 THREE PRONGS OF OVERSIGHT

There are three areas in which control and supervision can typically be exercised in respect of state activities: control mechanisms within the executive branch itself, parliamentary oversight, and judicial review (at the national and international levels). All three contain measures which have been applicable to intelligence activities and/or the deployment of armed forces. Can they be applied to cyber operations? What are the challenges?

The parliament and government or president are the two most important tools in restraining war or »leashing the dogs of war« (Rudesill, 2021). We might add that independent judicial review, either *ex ante* or *ex post facto*, complements the guarantees and protection against excesses of security measures. Existing case-law of the European Court of Human Rights and the European Court of Justice bears witness to that.

Nevertheless, existing research says very little on the topic of oversight of cyber operations. As a matter of fact, literature explaining the institutional and legal frameworks applicable to offensive cyber capabilities in individual states appears rather limited, and information is often scattered over various sources, while comprehensive accounts of the likes of Pernik's study (2018) are few.

One notable exception is the US literature and research on the US framework. This is understandable to a large extent, given that the US framework may be the most developed one, if simply on the account of their head start in institutionalizing cyber capabilities and regulating military operations abroad. The system of constitutional checks and balances applicable to cyber operations begins with the War Powers Resolution of 1973. Even in the US, however, the Title 10/Title 50 debate related to whether cyber operations should be considered, and therefore regulated, as traditional military activities or as intelligence covert actions, suggests that dilemmas accompanying the authorization and oversight of US cyber operations persist (Waxmann, 2020; West, 2021). The uncertainty became even more obvious with the signing into law of the 2019 National Defence Authorization Act by President Trump, which broadened the authorizations given to the Department of Defense and the Cyber Command (Bailey, 2020).

Admittedly, much of this regulatory framework is classified (albeit sometimes leaked) and thus difficult to analyze, beginning with the Obama administration's Presidential Policy Directive 20 (PPD-20) which laid out, in 2012, guidelines for more assertive actions of the US in cyberspace, all the way to the Trump administration's 2018 amendments to PDD-20 or new national strategic documents. Nonetheless, there is a rich body of academic literature on the Title 10/Title 50 debate and congressional oversight of US cyber operations.

When it comes to European states and offensive cyber capabilities, less information is available in the literature, and even less again when it comes to constitutional protections. There are some studies presenting the existing or envisaged national structures (Pernik, 2018; Ducheine et al. 2021); there are posts on dedicated blogs (Schulze, 2020); and there are limited explanations offered by the governments themselves (UK, n.d.).

A project currently implemented by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, aims to partially fill the gap with a comparative study providing an overview of national governance frameworks of cyber defence forces, with a particular focus on constitutional foundations and oversight provisions.[1]

[1] *NATO CCDCOE, Governing Cyber Defence Forces, Project No. 22-L2-01P (POW 2022). The outcome of the project should be publicly available in early 2023.*

2.1 Executive control – autoregulation mechanisms

The first of the areas outlined in this paper pertains to the self-regulatory mechanisms within the executive branch that deploys cyber capabilities and, more broadly, the government.

The decision-making process should be set in such a way that the decision to use offensive cyber capabilities, or the competence to effectively review and change it, should lie at the highest possible, yet reasonably practical, level of the executive, with someone with political accountability. This means a minister or even the government, not merely the head of the cyber force concerned. The minister, government and other relevant parts of the executive structures should also be informed without delay of the executed cyber operation and its effects.

There should also be the possibility within the executive branch to inspect the cyber operations. The inspection function is a well-established concept and tool of control against administrative abuses or excesses available across various areas of public activity, including the national security and defence sectors, in many countries. They serve as watchdogs within the executive branch (Gaudion, 2021), their independence being guaranteed by the manner of appointment, competences granted by law, and sources of funding.

The Czech Republic, for instance, has incorporated the position of inspector of cyber defence into its cyber defence legislation (CZ, 2021). They are appointed by the government following a hearing in the relevant parliamentary committee, and have a mandate to inspect activities of military intelligence related to cyber defence, on which they report to parliament.

Inspectors, nevertheless, can hardly have enforcement power; their main contribution is to report their findings to the leadership of a ministry and/or the parliament or specialized bodies established by the latter. On the other hand, inspectors working within or close to the structures responsible for cyber operations can alleviate some of the concerns related to the risk of leaks of information, and can develop appropriate expertise that will enable them to understand and evaluate cyber operations.

2.2 Parliamentary oversight – by the will of the people

This leads us to the second, and possibly the most important, area where oversight of state activities is exercised: parliament.

The legislature is the representative of the people as the supreme source of power and legitimacy in a state. Obligations can only be imposed by law. Parliament thus already fulfils its oversight role by adopting legislation which respects the state's constitutional commitments and protects fundamental rights and freedoms.

Parliaments also have the power to call the executive branch to accountability by way of requesting information or reporting to specialized committees or the plenary. They can establish fact-finding or investigatory bodies and, not without importance, they approve the budget.

It is a fact that intelligence services oversight has met with mixed results across many jurisdictions. On the one hand, the secretive nature of the work causes the legislature to adamantly insist on supervision, and leads some to a default suspicion of abuse of powers. In countries with a history of autocratic regimes, the regulation of intelligence services tends to be more restrictive, and individual services can even have their own legislation (such as in the Czech Republic, where apart from the general law on intelligence services, each of the services active on domestic soil has its own law further regulating its activities).

On the other hand, research reveals that military intelligence oversight, which is of particular importance to offensive cyber operations, specifically lags behind in many aspects in numerous states (Jasutis et al., 2020). For a long time, many states have had only a very rudimentary regulatory framework concerning military intelligence, considering it only an element of the armed forces and therefore not necessitating a specific normative approach (Jasutis et al., 2020).

In addition, parliaments are not known to be the most efficient controlling bodies. Their procedures are lengthy and formalistic. Their elected members, who form the core of the specialized bodies, lack expertise (or there is a serious imbalance in technical understanding of the controlled and the controlling) or do not have time to develop it due to the election cycle. They can also be overburdened by other agendas.

There is also a legitimate and substantiated concern about the politicization of the oversight process, and of information leaks. In intelligence operations in particular, the risk of misinterpretation taking a wrong turn is very high, leading to unwanted escalations, nationally and internationally.

Nevertheless, along with the executive branch's self-regulatory mechanisms, challenged by uncertain transparency and independence, parliamentary oversight is probably the most promising form of oversight of offensive cyber capabilities. By way of an example, Czech public and parliamentary debate led, between 2017 and 2020, to a complete overhaul of cyber defence legislation, and although the latter still leaves things to be desired, the amendments to the Act on Military Intelligence and related law adopted in early 2021 marked a substantive and substantial improvement to the original draft tabled in 2016, particularly where transparency and legal guarantees were concerned.

Last but not least, it is parliaments that control the deployment of armed forces. In some countries, parliamentary consent is already required *ex ante* (Denmark or Germany). While arguably posing administrative difficulties, the character of cyber

operations and specifically their potential effects do not automatically provide grounds for absolving the military and the executive branch of this obligation. However, more work is admittedly needed to make the process efficient and effective in respect of cyber operations.

2.3 Judicial review – powerful tool or irrelevant concept?

The third available tool of oversight, judiciary review, is potentially powerful in its impact, yet particularly challenging to resort to.

In recent years, it has been thanks to the binding decisions by the European Court of Human Rights (ECtHR) and the European Court of Justice (ECJ) that national surveillance frameworks have had to change, including bulk interception systems using similar technologies to those deployed within cyber defence capabilities.

Beginning with Klass v. Germany, courts ruled as early as the 1970s that surveillance legislation itself was susceptible to the violation of human rights, even if there was no ascertained and actual interference with the rights of the applicant (ECtHR, 1979). Rulings in cases such as Privacy International (UKSC, 2019; ECJ, 2020) or Big Brother Watch v. the UK (ECtHR, 2021) ascertained judicial review of decisions by bodies authorizing hacking, found flaws in bulk interception regimes, and brought about changes in the regulatory frameworks pertaining to the work of the same intelligence organizations that today deal with or participate in the development and deployment of offensive cyber capabilities.

At the same time, it cannot be ignored that several of those decisions hinged on procedural issues, and in principle did not oppose the legitimacy of national security concerns and the state's need to pursue it effectively. Furthermore, the courts have been criticized for not having gone all the way to establish principles more adequate for the technologies and modern digital mass surveillance systems used today, or even to declare the latter incompatible with international human rights law (O'Donoghue, 2018; Zalnieriute, 2021).

The existing case law has also shown that any change in the system is likely to have to come from within. Be that as it may, relying on the civic duty of individuals to report unconstitutional behaviour is clearly not a sustainable, systemic solution to the requirements of a democratic cyber power.

Over the past few decades, we have also seen a growing number of proceedings brought against states with regard to the conduct of their armed forces during military operations. Several court judgments by both national courts and the ECtHR are available on the application of human rights law and IHL in cases concerning the killing of foreign nationals abroad. The rulings in these cases have raised questions as to the primary source of legal authority – whether it was IHL or human rights law – and the scholarly debate on this issue is equally rich. Nevertheless, it is not disputed that states are responsible for human rights violations committed abroad.

It is also widely accepted by states that human rights apply online just as they do offline (OHCHR, n.d.). If cyber means can bring about the same effects as kinetic force, it is then easy to imagine a future case-law on the effects brought about by cyber operations.

When it comes to *ex ante* judicial control, in most countries intelligence services are obliged to seek a court's permission, an independent authorization, if their operations are to interfere with fundamental rights. While cyber defence structures may not be entirely equated with intelligence services, and the threat scanning will usually not touch upon individuals, it does appear plausible that the execution of a cyber operation should be vetted by an independent authority, be that a secret tribunal or another independent body. Yet at present there is no indication that any European or other country would incorporate a court's permission into the decision-making process applicable to offensive cyber operations, be it for any partial component of the operation.

Conclusion

Our modern values-based society model dictates mostly a defensive posture. However, the dilemma of whether to build offensive cyber capabilities appears to have been largely solved in the affirmative, and the states have been moving from advocating strictly passive defence in cyberspace to openly admitting offensive capabilities and building corresponding institutional frameworks.

Yet, resorting to 'active cyber defence' brings implicit regulatory challenges that democratic, rule-of-law abiding societies cannot ignore. Offensive cyber operations oscillate on the borderline of intelligence and military actions and are usually executed by either one, or by another type of structure within a state's security/defence apparatus. Some states have created capabilities combining the two.

Both types of structures are subject to cautious national regulation given the potential impact of their actions on rights and freedoms, on political stability and on the state's international standing.

The challenge therefore lies in crafting a democratic and responsible cyber power. Respect for the constitution, protection of fundamental rights and freedoms, and effective oversight of cyber capabilities should be an integral part of the solution. In fact, the new regulatory frameworks should address these concerns by design, learning from and avoiding the mistakes of their predecessors in cyber security or other avenues of national security business.

While there are differences between states in regulatory approaches, as well as varying levels of sensitization towards potential human rights violations, the 'right to security' advocated by states and to a growing extent accepted by courts and international organizations should be approached with caution, lest we risk its over-securitization and compromise the values we profess to defend.

Future research should therefore take a closer interest in states' approaches to national cyber defence and their constitutional foundations, and should be able to alert states should they get too close to falling into a chasm of 'unconstitutionalism', in these turbulent times of 'unpeace'.[2]

Bibliography

1. *Bailey, C. E., 2020. Offensive Cyber Operations: A Gray Area in Congressional Oversight, Boston University International Law Journal, 38-2, pp 240-85.*
2. *Big Brother Watch and Others v. the United Kingdom (2021), European Court of Human Rights, Applications Nos. 58170/13, 62322/14 and 24960/15. https://hudoc.echr.coe.int/eng?i=001-210077.*
3. *Blessing, J., 2021. The Global Spread of Cyber Forces, 2000-2018, 14th International Conference on Cyber Conflict: Going Viral, T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.), NATO CCDCOE Publications, Tallinn, Estonia, pp 233-55.*
4. *Czech Republic, 2021. Act No. 289/2005 Coll, on Military Intelligence, as amended by Act No. 150/2021 Coll, Article 16k. https://www.zakonyprolidi.cz/cs/2005-289, [CZ, 2021].*
5. *Ducheine, P. A. L., Arnold, K. L., Pijpers, B. M. J., 2021. Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces, in Military Operations and the Notion of Control under International Law. https://doi.org/10.2139/ssrn.3540732.*
6. *Gaudion, A. C., 2021. Answering the Cyber Oversight Call, work in progress. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904732.*
7. *Jasutis, G., Fuior, T., Vashakmadze, M., 2020. Parliamentary Oversight of Military Intelligence, DCAF – Geneva Centre for Security Sector Governance, Geneva. https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf.*
8. *Klass and Other v. Germany, 1979. European Court of Human Rights, No. 5029/71. https://hudoc.echr.coe.int/fre?i=001-57510.*
9. *Ministry of Foreign Affairs, 2019. Letter to Parliament on the International Legal Order in Cyberspace, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace. [Netherlands, 2019]. Not available online.*
10. *NATO, 2020. AJP-3.20: Allied Joint Doctrine of Cyberspace Operations, Allied Joint Publication, January 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.*
11. *O'Donoghue C., Keyhani N., 2018. ECtHR Rules on UK Mass Surveillance under RIPA, Technology Law Dispatch, 25 October 2018. https://www.technologylawdispatch.com/2018/10/in-the-courts/ecthr-rules-on-uk-mass-surveillance-under-ripa/.*
12. *OHCHR (n. d.) International Standards. OHCHR and Privacy in the Digital Age. https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards.*
13. *Pernik P., 2018. Preparing for Cyber Conflict: Case Studies of Cyber Command, ICDS, Tallinn. https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018.pdf.*
14. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (2020), European Court of Justice, C-623/17. https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-623/17 [ECJ, 2020].*

[2] *The notion of 'unpeace' has been borrowed from Lucas Kello and his keynote speech delivered at the 2022 US Cyber Command Legal Conference, on 10 March 2022.*

15. *R (Privacy International) v Investigatory Powers Tribunal, 2019. United Kingdom Supreme Court, UKSC 22, Judgment of 15 May 2019. https://www.supremecourt.uk/cases/uksc-2018-0004.html [UKSC, 2019].*
16. *Rudesill, D. S., 2021. Cyber Operations, Legal Secrecy, and Civil-Military Relations, in Beehner L., Brooks R., Maurer D., Reconsidering American Civil-Military Relations: The Military, Society, Politics, and Modern War, Oxford University Press, as published on 16 December 2020 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745263.*
17. *Schmitt, M., 2019. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis, Just Security, 14 October 2019. https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.*
18. *Schulze, M., 2020. German Military Cyber Operations are in a Legal Gray Zone, Lawfare Blog, 8 April 2020. https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone.*
19. *United Kingdom Government (n.d.), National Cyber Force Explainer, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041113/Force_Explainer_20211213_FINAL__1_.pdf [UK, n. d.].*
20. *US Department of Defense, Joint Chiefs of Staff 2018, JOINT PUB. 3-12, CYBERSPACE OPERATIONS II-7 (2018). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.*
21. *Use of Force. National Positions, 2021. International Cyber Law in Practice – Interactive Toolkit, NATO CCDCOE, viewed 2 April 2022. https://cyberlaw.ccdcoe.org/wiki/Use_of_force.*
22. *Waxmann, M. C., 2020. Cyberattacks and the Constitution, The Hoover Institution Working Group on National Security, Technology and Law, Aegis Series Paper No. 2007, Columbia Public Law Research Paper No. 14-675. https://scholarship.law.columbia.edu/faculty_scholarship/2725.*
23. *West, L.B., 2021. The Rise of the »Fifth Fight« in Cyberspace: A New Legal Framework and Implications for Great Power Competition, Military Law Review, 229-3, pp 273-347.*
24. *Zalnieriute, M., 2021. Procedural Fetishism and Mass Surveillance under the ECHR: Big Brother Watch v. UK, Verfassungs Blog on Matters Constitutional, 2 June 2021, https://verfassungsblog.de/big-b-v-uk/, DOI: 10.17176/20210602-123858-0.*

e-mail: tatana.jancarkova@ccdcoe.org

Ignacio Pizarro
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.5

UČENJE NA PODLAGI IZKUŠENJ: STARE LEKCIJE ZA NOVO BOJIŠČE

LEARNING FROM EXPERIENCE: OLD LESSONS FOR A NEW BATTLEFIELD

Povzetek Uvajanje kibernetske domene in zmogljivosti v večdomenske operacije so zaznamovale težave, od katerih so mnoge posledica napačnega razumevanja narave te domene kot tehničnega področja, ločeno od običajnega razumevanja bojnega delovanja. Voditelji so zato domeno previdno naslavljali, kar je povzročilo zamudo pri prilagajanju vojaškega razmišljanja novemu okolju. V prispevku poskušamo opozoriti na pomanjkljivosti in morebitne vzroke za zapozneli pristop ter izpostaviti področja, na katerih je uveljavljeno vojaško znanje, in veljavno doktrino. Za spoprijemanje z izzivom, kako kibernetske zmogljivosti kar najbolje uporabiti v vojaških operacijah, je mogoče uporabiti celo stara načela.

Ključne besede ***Kibernetski prostor, operacije, vojska, doktrina.***

Abstract The implementation of the cyberspace domain and capabilities into multi-domain operations has been plagued with difficulties, many of which come from a misperception of the nature of this domain as a technical field, detached from the usual understanding of combat operations. This has made leaders wary of addressing this domain, which has caused a delay in the adaptation of our military thinking to this new environment. In the article, we seek to point out the shortcomings and possible reasons for this delayed approach, and highlight areas in which established military knowledge, existing doctrine and even ancient principles can be used to meet the challenge of bringing cyber capabilities to their full potential in military operations.

Key words ***Cyberspace, operations, military, doctrine.***

Introduction

Military operations in cyberspace, even after more than a full decade since they first made their way into the mainstream media headlines, do not seem to have yet made their way so successfully into the mindset of military planners, decision-makers and commanders. Although cyberspace has been recognized as a separate domain of operations (NATO, 2016), it is still treated as a kind of private realm of technical experts, constrained somehow within the field of communications and information systems, and handled, and possibly understood, only by Information Technologies (IT) specialists. This creates a gap in our military understanding that needs to be addressed at all levels and during all phases of conception and planning of military operations. It is understood by many experts that military cyberspace operations, and addressing the cyber threat, still require an improvement in our conceptual and doctrinal thinking (Brantly & Smeets, 2020, p 2).

This initial understanding of cyberspace as a somehow separate and fundamentally different field, which may not even merit equal footing with all other areas of military thought, has made our response to this new environment slower than it has been in the past to other emerging threats and opportunities. Even though much has been said and written about cyberspace operations, both conceptually and practically, on their military applications, parts of this field are still considered by many to be in their infancy (Brantly & Smeets, 2020, pp 12-13).

In modern times the threat cycle for any emerging form of warfare has been consistently shown to take about a decade. This means the time between the appearance of a new kind of military threat, its understanding, its implementation into military doctrine, organization, materials and procedures and the subsequent appearance of the next emerging threat requiring a new change, has taken approximately a decade every time. For many reasons, which we will not attempt to unveil in this article, it takes military planners, organizers, and decision-makers about ten years to become aware of a new problem, understand it, devise ways to address it, and implement the solutions into military thinking, doctrine, organization, and materials. This is usually the point at which adversaries, having lost the advantage provided by the novel approach, move on to a new way of fighting to exploit different weaknesses, whether new or old.

The 1970s were the age of indirect strategy, with the main power blocks unable to confront each other directly for fear of apocalyptic consequences (Van Creveld, 1991), and resorting to battles in proxy conflicts through proxy nations to achieve their political goals. The 1980s were dominated by a revival of conventional warfare theory (Van Creveld, 2000, p 171), with the global bipolar landscape and the nuclear threat still as its backdrop, and a covert economic battle defining its final strategic outcome. The 1990s were the decade of large-scale tactical operations, of the overwhelming dominance of air power as the decisive factor of conventional battles, once the fear of nuclear escalation no longer put a stop to the deployment of a large

military force. The 2000s brought the rise of Asymmetric Warfare[1] to the forefront, with armies rushing to adapt their organization, tactics and materials to this way of fighting which exploited their weaknesses and negated the strengths (Field, 2009, p 4) of the massive military forces of the previous decade. Finally, the 2010s saw the appearance of Cyber Warfare (Denning, 2012), with all its new challenges and opportunities, as well as threats of a nature and scope that we struggled to fully comprehend.

We find ourselves now in the 2020s already fully under the shadow of the Hybrid Warfare threat (Gvineria, 2017). We are addressing the new challenge of waging a war that takes place at the same time in the field of battle and in the information and cognitive landscape of the general population, and we may yet even see a return to the power dynamics and polarities reminiscent of the Cold War.

We might say we have already begun the next threat cycle, and yet we still have not fully implemented and addressed the decade-old cyber threat, which should by now be part of the last successful cycle of change in military thinking. We are late in our implementation of solutions, while our dependence on this domain has only grown.

Part of the reason for our delayed response to the cyber threat is that cyberspace seems to be a fundamentally different theatre of operations, requiring a fundamentally different way of thinking. It is not just a new way to fight, but a new space to fight in. In this sense we could equate it with the emergence of air power a century ago (Van Creveld, 2011). Military leaders of the past had as much trouble understanding air operations, and the challenges and opportunities they could bring, as modern planners have with cyberspace operations. It is a new space, with new rules, and our intuition does not always appear to give us the right answers.

However, we would be wise to notice that the same has been said before of many new weapons and methods. Many technological advances have been hailed as fundamental changes in war, and yet we find that war does not change that much in its essence. Technology brings new ways to fight the same battles, for roughly the same motives. Technology may advance but human nature remains, and the nature and purpose of armed conflict is no different now from what it has been in the past. As Carl Von Clausewitz said *»The need to fight quickly led man to invent appropriate devices to gain advantages in combat, and these brought about great changes in the forms of fighting. Still, no matter how it is constituted, the concept of fighting remains unchanged. That is what we mean by war«* (Clausewitz, 2007). Therefore, when confronted with a new problem, it would be wise to look back to the brilliant military minds who preceded us and take counsel from their experience.

---

[1] *Asymmetric warfare is a form of warfare between opposing forces which differ greatly in military power and that typically involves the use of unconventional weapons and tactics (such as those associated with guerrilla warfare and terrorist attacks) (Merriam-Webster Inc., n.d.).*

This is why we can look into this challenge from the perspective of many well-established and even ancient principles and lessons that may help to dispel the image of cyberspace as a mysterious domain, in which everything must be learned again. By rejecting the assumption that the problem is completely new we may find ways in which our current military knowledge applies to the threat at hand, and solutions that could have been implemented by now and would probably have been implemented if cyberspace did not have an aura of mystery. We will attempt to point out some classic approaches that may be taken to help to close those gaps in our doctrine and move on to the next threat.

1 THE SCOPE OF THE CHALLENGE

First, let us define the scope of what we will be addressing. For the purposes of this article, we will be discussing the role of cyberspace in the context of military operations. That is, we will be discussing cyberspace as a domain of operations, with military forces in cyberspace deploying and operating alongside conventional forces. We will discuss cyberspace as an integral part of military operations (CCDCOE, 2020, p 12) in a theatre that may encompass many and possibly all domains, from land, sea, and air forces to every potential instrument of military power.

The most frequently discussed form of the cyberspace threat in public forums tends to be, instead of multi-domain military operations, cyber warfare. This usually also means the hostile use of cyberspace, but it tends to refer to actions taken outside a conventional battlefield. Cyber warfare can happen, and often does, below the threshold of armed conflict. It exploits grey areas in legislation and often takes advantage of the difficulties of attribution (CCDCOE, 2020, p 21). This use of cyberspace is, of course, a constant concern, since it happens during peacetime and is not limited to an active armed conflict. Nevertheless, since the scope of this form of cyber threat is addressed by institutions far beyond the military, and it does not necessarily relate to military operations, it will not be the subject of our study this time. We, as military experts, are concerned mainly with the needs of military organizations that are still struggling with the challenge of incorporating cyberspace into their operations.

The first challenge of incorporating cyberspace into classic military thinking is that its nature, and the nature of actions within it, are fundamentally different from any other classic military action. Even the most technical disciplines employed in warfare share fewer similarities with the kind of actions carried out in this domain than one may think at first glance. Even though cyberspace operations overlap in many ways with other operational domains, the weapons and procedures used in cyberspace are unlike anything that has been used in the past. They are tailored, after all, to affect an environment that did not even exist not so long ago.

Cyberspace operations take place in a completely artificial domain (NATO, 2020, p 13), unlike any other operation in military history, and it would appear at first that

this makes them different from any other kind of operation ever conceived in all aspects. As we will see, this may not be the most realistic approach. Our analysis should start, nevertheless, by addressing the fundamental differences between cyber warfare and conventional operations, and how these differences condition the way in which modern nations address the building of capabilities and the incorporation of this domain into their planning.

Cyberspace has many noticeable and frequently pointed out differences from the traditional domains of operations, although not all of them are equally relevant to the problem at hand. It would be redundant at this point to highlight the anonymity cyberspace allows its actors (NATO, 2020, p 13), the proportion of non-state actors (NATO, 2020, p 5; CCDCOE, 2020, p 22) operating in it, or the legal void that tends to accompany the reaction to the threats and the conduction of operations in this domain. All these characteristics were already present in Asymmetric Warfare, and they hardly constitute new challenges. Nations are already experienced in dealing with these aspects of the problem, and these lessons are recent enough not to have been forgotten (NATO, 2017, p 2-13).

One fundamental challenge of cyberspace which may help us understand our own slow response to the threat in this domain is the subtle nature of its effects. The threats our military forces have addressed in the past have all been highly visible, if not in practice at least potentially. Even nuclear weapons, whose use was always uncertain to the point it never materialized into a nuclear attack during the Cold War, had potential catastrophic effects that were painfully understood by all the actors involved (Van Creveld, 1991, p 16).

The cyber threat, in contrast, presents us with levels of uncertainty comparable to the Cold War, while at the same time remaining unclear and covert in its effects. The possible consequences of a cyberattack range all the way from a mere nuisance to a full collapse of command and control or critical infrastructure, and the perception of this threat suffers from this undefined magnitude of the consequences. In the last decade, military forces have known about the cyber threat at an intellectual level but have not felt vulnerable to it at the emotional level that drives truly world-changing efforts. A cyberattack may well neutralize a military operation, but it may do so in a way that is not immediately visible (CCDCOE, 2020, p 20), and that does not cause direct loss of life.

This signals the first problem of addressing cyberspace as a domain of operations. It is not a visible enough threat to be frightening, except to the experts. It places cyberspace operations, once again, only in the minds of technicians, who are rarely the ones defining policy or doctrine. The decision-makers do not feel the urgency of a threat that is not visible, and whose consequences cannot be clearly assessed, for all the efforts of the experts to warn them. It is a threat that thrives in the shadows and takes full advantage of its obscurity to remain seen as a potential threat, more than an actual one, until it is too late.

The second fundamental difference that makes cyberspace operations difficult to conceive in classic military thinking is the nature of time and space in these operations. Military commanders throughout history have understood space and time clearly. Time is a critical resource in military operations. Space is where these operations take place. All actions in a battlefield have a defined place in space as well as a known cost in time (Clausewitz, 2007, p 52). Commanders understand how long it takes for a force to move, for an attack to take place, for a weapon to reach its target depending on distance and speed. In classic warfare space and time are inextricably linked. Distance needs time to cover it. Space can even be exchanged for time when the need arises (US Army, 2012, p 13).

Cyberspace changes this known nature of space and time in the battlefield. In cyberspace, actions that used to take significant time are executed instantaneously, and distances may become meaningless (CCDCOE, 2020, pp 16-17). Distances in cyberspace are not measured in length, and are sometimes not measurable in any tangible way. Defensive lines deployed in physical space are mostly inconsequential, and enemy actions avoid classic defences and seek the least defended points from which to reach key terrain. This makes the proximity of the threat much harder to assess, and it forces commanders to think about risk in an unfamiliar way. It is easy for the threat to be perceived as closer, or far more distant, than it is. A threat whose proximity cannot be easily established is uncomfortable to any military mind. A good commander will notice this discomfort and never look away from it. Discomfort is an instinctive indicator that our position is vulnerable, and that is where a commander's attention should focus. Unfortunately, human nature tends to do the opposite, and look away from that which causes discomfort. Looking away from a threat may provide some momentary emotional relief, but it certainly does not make it go away.

Still dealing with the subject of time, and specifically the tempo of cyberspace operations, another peculiarity arises. As quick as the execution of an action in cyberspace can be, its preparation is often the very opposite (CCDCOE, 2020, p 17). Once again, the nature of time in this domain veers away from the familiar and into uncharted territory. Preparing an action in cyberspace may require weeks, months or even years of manoeuvring. It often requires massive amounts of information that needs to be gathered, processed, and employed to drive the next steps. It requires layers in defences to be peeled away, lateral movements to be completed and assets prepositioned. The moment when, at the press of a button, a cyberattack commences, is the final step of a complex campaign that has been running in the shadows and has crossed vast distances to reach its objective, however virtual and indefinable those distances may be. In this respect, cyberspace operations resemble guerrilla warfare (US. Marine Corps, 1990), in which preparation and even most of the actions are covert if executed properly, and only the final step is detectable by the opponent. In fact, its very success depends on this.

Now that we have examined the nature of the cyberspace battlefield in some detail, and looked past the technical details that often obfuscate its understanding, we

cannot possibly think these concepts of uncertainty, subterfuge, covert manoeuvring seeking the weakest defences, and long preparations before the fight breaks out are new. Once stated in these terms we cannot help noticing they take a very familiar shape. There is a long-established school of military thought in which action is swift, preparation is meticulous, covert manoeuvring is the norm, the enemy may be close or far without our knowledge, and attacks avoid the strong and well defended points to focus on the weaknesses. A school of military thought based on deception, subterfuge, calculation, and patience. This school of thought dates back 25 centuries and its most known proponent, who in fairness we must point out may or may not have been a real historical figure, was Sun Tzu[2].

This is a character, and a school of thought, that need no introduction. He is by no means the only voice of wisdom we will quote, but his work has the advantage of being particularly well suited to cyberspace operations, as well as an easy read and an accessible way of thinking despite its antiquity. His school of thought is well known, based on timeless principles, and taught even outside the military. That is why we can easily refer to his teachings, so far back in time, to explore the solutions to the problems of such a modern concept as cyberspace operations. We will look at the ways in which many of the problems we face today are no different from the challenges others faced in the past, and how we can look at the past to solve them.

2 BEFORE THE BATTLE: PLANNING FOR WAR

Sun Tzu said: *»Now the general who wins a battle makes many calculations in his temple before the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose.«* (Sun Tzu, 1910, p 5)

This old principle of meticulous planning and preparation before battle is not only still valid today, but even more prominent than ever in the battle over the cyberspace domain.

No one can deny that cyberspace operations are complex and require long preparation times, and yet current planning methods for military operations contend with time constraints that clash with this requirement, and often make it impractical for an operation to be supported in a timely manner from the cyberspace domain.

In the classic battlefields of the European theatre during the Cold War, detailed military planning was carried out meticulously during peacetime (Ambrose, et al., 2006). Scenarios were considered and forces were allocated for a confrontation in which the potential adversary was known, and the terrain in which the battle would

[2] *Sun Tzu (孫子) was a Chinese general who allegedly lived between 544 BCE and 496 BCE. He is traditionally credited for the influential work of military strategy »The Art of War«.*

be fought could be predicted. Whether these plans were realistic or not, and even if the battle would be fought, turned out to be secondary to whether the plans were in place, since none of these plans were ever carried out, to the relief of the entire planet. The calculations ensured, however, that all elements of the combat forces would be prepared, equipped, and trained for their task, and this in turn constituted a deterrent against aggression. No doubt the plans would be leaked, and enemies would know each other's script. This planning and positioning of forces were as much posturing as they were preparation, but had the battle been fought, these preparations would have allowed operations of a complexity and magnitude that a reactive approach could not have achieved in time.

This principle of meticulous preparation in a known battlefield became mostly obsolete in Western military thinking after the fall of the Soviet Union. Forces have become expeditionary, expected to respond to situations at short notice, in uncertain and distant battlefields, and against unpredictable enemies. To their credit, Western military planners have successfully adapted to this requirement and changed their methods for planning military operations (NATO, 2021) and the materials used to conduct them. In doing so they have gained new capabilities, but they also may have lost sight of some of the lessons of the past.

Dazzled by our own success in this war of projection and flexibility, we may have failed to realize that cyberspace is not necessarily an expeditionary battlefield. It is not an unknown place that requires distant deployment or long logistic tethers, even if the rest of our forces are still in that situation. Distances in cyberspace are irrelevant, and most of our deployment does not take place in a physical space, as we pointed out before. The battlefield in which this conflict is going to be fought may be dynamic and constantly changing, but its location is not undetermined. This could allow us to return to some of the quasi-deterministic military thought of the past, when generals studied a battlefield and started planning around it before war broke out. No matter where our forces may be deployed, the cyberspace domain for the battle is bound to be almost identical in many aspects. The systems deployed will be the same regardless of location, their connections will follow the same protocols, and even our enemy is unlikely to use technologies or methods that are fundamentally different from anything we have encountered, or even from the technologies we use ourselves. In the cyberspace domain our generals know where the battle will be fought, and they can plan for it long before the war begins. The calculations for battle can begin today, and they probably should have begun yesterday.

Since much of the planning can be undertaken in advance, we should ask ourselves if the same is true of the deployment. Unlike land, sea, or air forces, which cannot plan their operations, much less deploy their forces, until they know which war they will be fighting (NATO, 2021), cyber forces can and should already be deploying in peacetime. Cyber soldiers know where they will fight, and for the most part they also know what kind of enemy they will be fighting and with what weapons. They are ready to take positions for battle, but they often do not. They may fail to deploy

to their full potential because they are being held back by a shackle of doctrine and procedures that ties them to conventional forces. No force can begin deployment until an operation is declared, which is valid for conventional forces, but not necessarily so for cyber forces. The sooner we realize that restriction has no reason to exist besides tradition, the sooner we can begin our deployment in a way, it must be said, that our enemies are already doing.

Let it be said this does not mean deploying cyber forces in enemy territory during peacetime. As tempting as this may be, and even convenient from an operational point of view, it is not a freedom of action any law-abiding state can enjoy (CCDCOE, 2017). We have already learned, in the decade of adaptation to asymmetric warfare, that there are methods and practices available to our adversaries that will never be available to us, and that should not be imitated without risking the compromise of the very society we intend to defend. Imitation of the adversary is a natural but dangerous consequence of any prolonged human conflict. »War is an imitative and reciprocal activity. In order to defeat an enemy in a long war one becomes more and more like him, and both sides end up feeding off the other« (Smith, 2005, p 60). Since this limitation is a legal and sociological matter, we should leave it to the legal experts to study in detail. For the moment it should suffice to say that our military deployment will probably be limited to the areas of cyberspace we already control, and any deployment within enemy territory must be planned but cannot be executed in the context of a military operation until the Rules of Engagement allow it. This will be necessarily late in crisis response planning, and not before the operational planning process has already been initiated.

This restriction places a constraint on our preparations that, once again, can make any commander feel uncomfortable. We must listen to this discomfort, as it indicates a weakness in our position that needs to be addressed, not by looking away from the discomfort and abandoning this preparation, but by realizing how much more exhaustive it must be, so that deployment, when finally authorized, can be swift.

This is no different in essence from the way a battlefield is prepared when battle lines have been drawn and positions defined, but the order to advance has not yet been given. In this respect cyberspace operations resemble the battlefield preparations common in World War II. We can, then, draw lessons from this conflict and realize that, although the battlefield is determined and the weapons are known, the actions of the enemy cannot be predicted. The only predictable action from an enemy is that they will attack – *»The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him«* (Sun Tzu, 1910, p 29) – but not where or when this attack will come. In cyberspace, just as in the physical battlefield, we do not want to establish a Maginot line only to see it outflanked by a clever enemy[3].

[3] *The Maginot Line was a series of heavy defensive fortifications established by France with the purpose of stopping a potential German offensive into French territory. It was outflanked and avoided altogether by the German Army by advancing through the Ardennes Forest on May 10th 1940.*

So, if World War II taught us that static defensive lines are unreliable, even when the battlefield is already determined, the preparation of this battlefield must follow a different pattern. This pattern can also come from past experience and established doctrine. When the battlefield is known, but a static operation is unwise or unfeasible, the response is a mobile defence and a flexible offensive force. In cyberspace this translates into the ability to react, to respond and to counter. Our battlespace must be prepared, not to be unassailable, but to allow swift defence in depth. Our friendly cyberspace battlefield must be tailored to allow our cyberspace operations full and rapid access to it, rather than on putting our trust in a single perimeter defence that any clever enemy will seek to outflank. »Military tactics are like unto water; for water in its natural course runs away from high places and hastens downwards. So in war, the way is to avoid what is strong and to strike at what is weak« (Sun Tzu, 1910, p 21).

Sun Tzu also said: *»Whether the object be to crush an army, to storm a city, or to assassinate an individual, it is always necessary to begin by finding out the names of the attendants, the aides-de-camp, and door-keepers and sentries of the general in command«* (Sun Tzu, 1910, p 55).

If preparations can be made during peacetime for defensive operations, the same can be said for Cyberspace Intelligence, Surveillance and Reconnaissance (ISR) operations. Non-intrusive collection[4] can and should be employed during peacetime to gather not only threat information, but also potential target information, vulnerabilities, user profiles and identities required to breach potential objectives, system specifications and attack surfaces. This information requires a substantial time to collect and process, which means that the deployment of this capability will follow the same principles of peacetime deployment and peacetime full activity, parallel to Cold War defensive doctrine, as Defensive Cyberspace Operations. As for Intrusive Collection[5], it will follow an approach not unlike Offensive Cyberspace Operations, which we will deal with next.

Our offensive cyber forces, as much as we wish they could follow the same principle of early deployment, will probably not be able to preposition forces inside enemy space. As we have already pointed out, these methods are at best questionable and at worst illegal for a law-abiding state. This means the slow and elaborate pattern of infiltration followed frequently by Advanced Persistent Threats (APT)[6] to

[4] *Collection methods that draw from own networks or open source intelligence on adversary and third-party networks (CCDCOE, 2020, p 33).*

[5] *Collection methods that draw from non-available, third party networks including adversary networks (CCDCOE, 2020, p 33).*

[6] *An APT, or Advanced Persistent Threat, is an adversary which possesses sophisticated levels of expertise and significant resources, allowing it to create opportunities to achieve its objectives by using multiple attack vectors (e.g. cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The Advanced Persistent Threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives (U.S. Department of Commerce, 2011).*

devastating effect may not be available to our forces, even though it is favoured by our adversaries.

Instead, our forces in cyberspace may not need to prioritize their offensive preparations to be overwhelming, but to be fast and able to occupy enemy space and make advances as the opportunity presents itself. In this, Sun Tzu's statement *»If the enemy leaves a door open, you must rush in«* (Sun Tzu, 1910, p 48) fully applies, but can only be implemented if your forces are built and capable to fulfil this very task in time. In cyberspace, as a law-abiding nation, we cannot count on an early deployment in enemy cyberspace, so we must be capable instead of a rapid one. In this operational domain, this means having the ability to compromise, carry out infiltration and perform lateral movement in enemy systems at relatively short notice. Since this will not always be feasible, a military force in cyberspace also needs to be prepared to carry out faster and less target-specific offensive actions in cyberspace, such as Denial of Service attacks. All these capabilities, even the least specific ones, will require extensive preparations long before an operation is declared. Just like in the days of the Cold War, attack plans must be drawn, and potential targets designated and reviewed periodically to keep them current, as a peacetime task.

3 PREPARING FOR BATTLE: DEPLOYING FORCES IN CYBERSPACE

Sun Tzu said: *»Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight; whoever is second in the field and has to hasten to battle will arrive exhausted«* (Sun Tzu, 1910, p 18).

Once a military operation has been declared, an arduous process begins in order to constitute a suitable force, integrate that force, deploy it, and sustain it to carry out the operation. This is a process that becomes more time-consuming and costly the longer the distance is to the area of operations. As we have pointed out before, space equals time in conventional operations. This factor behaves quite differently in cyberspace, where distance to the area of operations is a virtual metric, often independent of geography.

This drives us to an immediate conclusion, which we have already hinted at when discussing preparation of the battlefield in friendly territory. Since cyber forces are not constrained by some of the limitations of conventional forces, this alters the tempo of their deployment to the point that it will not match the tempo of the rest of the components of a Joint Force. Cyberspace offensive forces may take a long time to seize an objective and gain control of it (McGhee, 2016, p 61), but they can commence deployment immediately, without waiting for other forces to be in place. Whether this is an advantage or a challenge to be addressed depends on how we think about it.

As new as this situation may seem when we label it as »cyber«, it is most certainly not a new concept. Armies have dealt with the challenge of different deployment times and different speeds of manoeuvring since the tribes of Asia began training horses to pull war chariots – an innovation with consequences that would reach, we could even say, biblical proportions[7]. If the situation is as old as civilization, it stands to reason that the procedure to address it does not need to be new. Where should we look in time for a force that can begin deploying ahead of the main force, must do so covertly, takes time to be in position to gather information or strike a target, and keeps a low profile until a visible effect on a high-value objective is required from it? Stated in these terms, the answer is obvious. This is exactly what Special Operations elements have always done (NATO, 2013, p 1.5.1), and even if their formal existence under this name in military doctrine is recent, the concept of small agile elements deploying ahead of the main force and even behind enemy lines is ancient. Thus, we can look at our own Special Operations doctrine (NATO, 2013) to understand how the preparation of our Offensive and Intrusive Collection cyberspace operations must be carried out. Instead of looking at this capability as a purely technical element, we may want to draw parallels with the Special Operations capability it resembles. Once this is understood, the deployment requirements, already detailed in this doctrine, become much more familiar to the Commander. These commonalities also explain why offensive cyberspace operations and special operations training sometimes converge to the point of sharing exercises[8] in which no other deployed forces participate.

Defensive cyber forces deploy in a different manner, since they do not share the need to position themselves behind enemy lines, but they are not completely detached from this concept of forward deployment. As we have stated before, defensive forces and Non-Intrusive Collection capabilities must already be deployed and prepared for action in the Joint Force's own cyberspace even during peacetime. Not only deployed, but actively engaged in defensive cyberspace operations[9] and in Cyberspace ISR activities. Nevertheless, defensive and ISR cyberspace operations often need to encompass systems that are beyond the military area of responsibility. Conventional forces need to secure the critical infrastructure employed for a military operation, whether this infrastructure is military or not. Airports, port facilities, railways and water supply systems may not be military forces, but no modern military force will deploy and sustain an operation without them. If these assets can be attacked through cyberspace, cyberspace operations are needed to secure them as well. That this is

---

[7] *»And the Lord was with Judah; and he drave out the inhabitants of the mountain; but could not drive out the inhabitants of the valley, because they had chariots of iron« (King James Bible, 1796/2022, Judges 1:19).*

[8] *An excellent example of this is Exercise Crossed Swords, carried out every year by the NATO Cooperative Cyber Defence Centre of Excellence, in which special operations elements train together with offensive cyberspace teams.*

[9] *In this respect we are using a general concept of Defensive Cyberspace Operations (NATO, 2020, p 16), which includes all defensive actions and preventive measures even in the absence of an adversary Offensive Cyberspace Operation. We will not be referring to allied military doctrines in which a defensive operation in cyberspace is specific in time and scope and declared in response to a specific enemy offensive operation (U.S. Army War College, 2020). These can be considered a subset of the operations we refer to.*

the case is not in question. Cyberspace can indeed reach many places and be used to strike at many major assets. It is not just a space, but also a space that allows access to other key spaces. In this respect, cyberspace is what Sun Tzu called the »Ground of Intersecting Highways«[10], so once again we can look at his writings for how to occupy such ground.

Sun Tzu said: *»On ground of intersecting highways, I would consolidate my alliances«* (Sun Tzu, 1910, p 46).

Many of the critical assets an operation requires, which do not fall under the commander's authority, will belong to a host nation that may be undetermined until a crisis breaks out. This precludes the deployment of defensive forces in this vital cyberspace during peacetime, but it hopefully does not prevent the preparation and planning of this movement. Agreements and liaison with friendly nations can be established during peacetime, and a potential deployment of cyberspace defensive and ISR capabilities can be part of any defensive agreement. Building trust and mutual knowledge with potential allies is a slow process, but it will be the key to rapid deployment once operations begin. The preparation of this deployment, thus, begins in peacetime even if the deployment will not take place until the crisis begins.

There is one notable exception to this constraint when allied nations share a strong enough mutual interest to allow the deployment of friendly forces in their own cyberspace, providing mutual support and a close observation of the activities of potential adversaries. This is nowadays known as the Defence Forward concept, a conceptual descendant of the Cold War »Forward Defence« strategy (Chourchoulis, 2015), and its potential for gaining an early foothold in this domain prior to military operations cannot be stressed enough. Any deployment of defensive and intelligence assets made during peacetime, before any open opposition exists, will be far less taxing on our forces and far more efficient[11]. It is not unlike the classic concept of prepositioning forces in friendly territory, but it takes full advantage of the low profile of cyberspace activities. Positioning conventional forces in the vicinity of a potential adversary almost always risks escalation, which is why this is usually done with the greatest caution and is the subject of serious diplomacy. Cyberspace defensive forces, on the other hand, lack the visibility and threatening presence that would contribute to escalation, and can be deployed with no other requirement than the consent of the allied partner. Whenever this consent can be gained, this early deployment merits serious consideration.

If we respect these ancient principles, and translate them into our doctrine, we will find our forces at the beginning of an operation in three different stages of deployment. In the cyberspace composed of military systems under the control of the Force

[10] *»Ground which forms the key to three contiguous states, so that he who occupies it first has most of the Empire at his command, is a ground of intersecting highways« (Sun Tzu, 1910, p 41).*

[11] *»An army may march great distances without distress, if it marches through country where the enemy is not« (Sun Tzu, 1910).*

Commander, all defensive and intelligence collection cyberspace assets should have been deployed almost fully during peacetime. Any final preparations in this terrain should be mostly concerned with the coordination of efforts from different nations, their liaison, and the building of situational awareness.

Deployment of defensive and ISR forces in the areas of cyberspace which, however friendly and necessary for the conduction of Operations, are not areas under the authority of the Force Commander, should have been planned and prepared as much as possible in peacetime. This deployment may even have commenced before operations if the nation where this deployment takes place is a close ally. This deployment, unconstrained by the needs of conventional assets, can and should take place once a military intervention is authorized, and may begin before any conventional forces deploy.

Of all the cyber forces, offensive forces and intrusive ISR capabilities will probably be in the least complete state of deployment, despite a commander's wishes. Preparations will have been made, and capabilities should be ready, but deployment may not commence until the authorization is received and the Rules of Engagement are in place. As we have mentioned, this would put them on par with Special Operations elements but, unlike these elements, offensive capabilities may be less constrained by distance and support. Our cyber forces should be prepared to be the first elements of our force to enter enemy territory.

5 THE CYBERSPACE BATTLE: INTEGRATING MILITARY OPERATIONS

Sun Tzu said: *»The clever combatant looks to the effect of combined energy, and does not require too much from individuals. Hence his ability to pick out the right men and utilize combined energy«* (Sun Tzu, 1910, p 17).

With deployment underway at whatever pace the circumstances allow, and operations commencing, the commander now faces one of the most difficult challenges of cyberspace operations: integrating this space into the battlefield and translating its capabilities into an operational advantage. Let us remember we are not discussing the kind of cyber warfare that happens below the threshold of armed conflict. We are framing cyberspace in the context of the full complexity, chaos, and violence of a conventional military operation. It has been our experience that commanders lack the familiarity to integrate cyberspace capabilities once they share the battlefield with more conventional means, with which they are far better acquainted. How, then, can we find the right place for a capability that even the experts sometimes struggle to grasp?

We shall be fair and point out that defensive capabilities do not appear to be particularly challenging in this regard. They often overlap with common security and protection measures, which commanders are already accustomed to. Even

when these defensive capabilities are mistaken for communications and information security measures, they are not unfamiliar.

The difficulties of integrating cyberspace operations of any kind into the flow of the battle come mainly from the obscure and often poorly understood technical nature of their actions, their effects and their requirements. To dispel this veil of mystery we will once again attempt to find similarities with established doctrine and familiar capabilities, to find the doctrinal space that fits cyberspace operations, if not perfectly, at least in ways that make the leap from the old way of thinking into the new easier.

As it turns out, this place is not so hard to find once we outline the capabilities and constraints of our force. Cyberspace operations have the capability of reaching targets covertly, striking unexpectedly, and causing minimum or no physical effects, limiting collateral damage. These capabilities also constitute their own limitations. Cyberspace effects in the physical space are often reduced, and their covert nature is as much a requirement as it is an ability. These two characteristics also make battle damage assessment challenging, both for the attacker and for the target (CCDCOE, 2020, p 20).

With regard to defensive operations, we find that the security of friendly cyberspace often depends as much on the end user and the implementation of proper procedures than on technological solutions and centralized action. Centralized monitoring of the space is key to its security, but decentralized execution of preventive measures is the norm (CCDCOE, 2020, pp 32-33).

Cyberspace ISR also works on distant targets and has access to information not available through other means. This information can be of high value and provide deep insights into the enemy's situation, plans and intentions, as long as the sources and methods of collection are kept as closely guarded as possible[12].

As we keep listing the characteristics of this capability, they begin to take another familiar shape. In our operations we already find ourselves trying to employ a capability with few or no physical destructive effects, that can act at a distance and whose effects on the target are sometimes uncertain, often hard to evaluate and may not be permanent. A capability that, when planned defensively, depends heavily on procedure and decentralized execution, and that has the potential to obtain reliable information from sources not available to other means. A capability that, interestingly, often also gets confused or mixed with Communications and Information Systems (CIS) (CCDCOE, 2020, p 19).

This capability may not be as ancient as most examples we have used so far, but it is no less familiar. All these traits, limitations and even mistakes in its implementation closely resemble the characteristics of Electronic Warfare (EW) (NATO, 2020).

---

[12] *»O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence we can hold the enemy's fate in our hands« (Sun Tzu, 1910).*

Note that we say it *resembles* Electronic Warfare, not that the capabilities are equivalent. This is a source of confusion that we should dispel before we go any further. Electronic Warfare deals with the use of electromagnetic energy (US Joint Chiefs of Staff, 2020, pp I-5), and its methods and equipment are fundamentally different from cyberspace operations, which deal with the logical layer of systems (CCDCOE, 2020, p 13), regardless of whether they employ electromagnetic energy or not. The procedures, equipment and skills used to carry out their actions are completely different from each other, even if the targets sometimes overlap.

Their similarities, nevertheless, will help us understand the role of cyberspace operations in the battlefield and how to employ them to maximum effect. Like Electronic Warfare measures, the greatest value of cyberspace operations comes from their ability to cause and prevent effects in support of the Joint Operation and the forces in it.

Like an EW action on a critical system, a cyberspace effect in isolation can be damaging, but it could amount to no more than a disruption, and possibly a nuisance. Military forces are trained, equipped and ready to handle temporary failures in their critical systems as a matter of routine business continuity. It is when these effects are combined with manoeuvre and kinetic effects that they will reach their full potential.

The main principle for employing offensive cyberspace capabilities will be, then, the combination and synchronization of efforts. Every offensive action must have a specific effect to create in the battlefield, a specific time at which to create this effect, and a specific operational purpose for it, linked to the other operational activities and coordinated. Just like Electronic Countermeasures, the use of cyberspace effects loses much of its effectiveness after the first use (McGhee, 2016, p 57), and also risks the loss of information from the target system from that point on if it was under surveillance. This means the employment of these capabilities, even in cases where it may seem safe and of low cost, must always have a clear and coordinated operational purpose. The ancient principle »Do not do anything for which there is no purpose« (Musashi, 2011) applies.

This might lead us to believe that cyberspace offensive capabilities are a tool to be held back, kept in reserve, and employed only in rare occasions. Although it is true that the culmination of an offensive action must necessarily be infrequent due to the nature of cyber weapons, we cannot forget that cyberspace offensive forces are military forces, and they must always be active. When a cyberspace offensive capability is not being employed to cause an effect, the force must be manoeuvring, prepositioning, and preparing to cause such effects when required. Inactivity cannot be the position of any military force. »When the time for action comes, the first requirement should be that all parts must act« (Clausewitz, 2007).

Conclusion

Sun Tzu said: *»The general that hearkens to my counsel and acts upon it, will conquer: let such a one be retained in command! The general that hearkens not to my counsel nor acts upon it, will suffer defeat: let such a one be dismissed!«* (Sun Tzu, 1910, p 4).

We have attempted to bring cyberspace out of the obscurity of its technical nature, and under the scope of well-established military knowledge, which is understood by all military thinkers, and which all domains in the battlefield share.

The purpose of this analysis has not been to state that all principles of ancient doctrine should be followed in cyberspace, or any other domain. Rather, we have pointed out that many such principles apply, and that the fight in the cyberspace domain is not of such a different nature that we can ignore the knowledge of war gained from centuries of human conflict. This helps us bring this new domain of operations to a level where it can be understood, framed in a familiar context, and hopefully allows it to be better addressed without having to learn from the experience of our own mistakes. It allows us to see past the differences of this new domain and focus on the similarities with other domains, which we can use to better implement the changes in our forces this new environment requires.

Cyberspace defensive forces can borrow concepts from the Cold War to plan and secure an early deployment in a battlefield that is determined, with allies that are known, and against an enemy that is familiar. They can learn from the lessons of ancient China when gathering the information to infiltrate an enemy position, whether the gates are made of wood or guarded by layers of encryption. They can learn from Von Clausewitz about the uneconomical perils of inactivity, from Miyamoto Musashi about the need for purpose in every action, and from Sun Tzu about the power of combined energy, the need for agility and the wisdom of seeking the least defended points in an enemy's defence. We can borrow procedures from Special Operations and from Electronic Warfare doctrines without mistaking our force for either one of them, and without losing sight of the unique identity of the forces that borrow these principles.

The purpose of this indirect intellectual approach to cyberspace is not to understand it in its most minute detail, but to help guide the implementation of general changes in doctrine, procedures and organization that will allow us to take full advantage of its capabilities and address the threats it contains in a timely manner. Knowledge alone will not be sufficient, if it is not translated into action. As Sun Tzu said, »One may KNOW how to conquer without being able to DO it« (Sun Tzu, 1910, p 12).

No doubt new principles and lessons are waiting to be learned in a battleground of such an unfamiliar nature: »While heeding the profit of my counsel, avail yourself also of any helpful circumstances over and beyond the ordinary rules« (Sun Tzu, 1910, p 4). However, in the same way that military experts have borrowed from the knowledge of their predecessors even when the weapons at their disposal were

vastly different, we should not let our pride make us believe we have grown beyond benefiting from the inheritance of the brilliant minds of the past.

Cyberspace may be a new battlefield but war, as an act of force to compel our enemy to do our will (Clausewitz, 2007, p 13), is one of the oldest human activities. Human nature has remained constant for thousands of years, and it would be hubris to think it has suddenly changed in our generation. For as long as the nature of the commanders, the soldiers, and the purpose of warfare itself remain the same, the ancient principles will continue to apply.

Bibliography

1. *Ambrose, E. S. et al., 2006. The Cold War: A Military History. New York: Random House Trade Paperbacks.*
2. *Brantly, A., and Smeets, M., 2020. Military Operations in Cyberspace. In: Handbook of Military Sciences. s.l.: s.n.*
3. *CCDCOE, 2017. Tallinn Manual 2.0 on the international Law Applicable to Cyber Operations. 2nd Ed. Cambridge: Cambridge University Press.*
4. *CCDCOE, 2020. Cyber Commanders' Handbook. 1st Ed. Tallinn: NATO CCDCOE Publications.*
5. *Chourchoulis, D., 2015. A secondary front? NATO's forward defence strategy and its application in the southeastern region, 1966-1974. In: B. Lemke, (Ed.) Periphery or Contact Zone? The NATO Flanks 1961 to 2013. Berlin: Bundeswehr Centre of Military History and Social Sciences.*
6. *Clausewitz, C. V., 2007. On War. Oxford: Oxford University Press.*
7. *Denning, D. E., 2012. Stuxnet: What Has Changed? Future Internet, Issue 4.*
8. *Field, C., 2009. Asymmetric Warfare and Australian National Tactical Advantages: Taking the Fight to the Enemy. Sydney: Land Warfare Stdies Centre (Australia).*
9. *Gvineria, S., 2017. Information Warfare: New Security Challenge for Europe. 1st Ed. Bratislava: Centre For European and North Atlantic Affairs (CENAA).*
10. *McGhee, J., 2016. Liberating Cyber Offense. Strategic Studies Quarterly, 10(4), pp 46-63.*
11. *Merriam-Webster Inc., s.f. Merriam Webster Dictionary. https://www.merriam-webster.com/dictionary/, February 2022.*
12. *Musashi, M., 2011. The Book of Five Rings. 1 Ed. Boston: Shambhala Publications Inc..*
13. *NATO, 2013. AJP 3.5 Allied Joint Doctrine for Special Operations. A1 Ed. s.l.:NATO Standardization Office (NSO).*
14. *NATO, 2016. Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm, February 2022.*
15. *NATO, 2017. AJP-01 Allied Joint Doctrine. E Version 1 Ed. s.l.: NATO Standardization Office (NSO).*
16. *NATO, 2020. AJP 3.20 Allied Joint Doctrine for Cyberspace Operations. A Ed. s.l.: NATO Standardization Office (NSO).*
17. *NATO, 2020. AJP-3.6 Allied Joint Doctrine for Electronic Warfare. Brussels: NATO Standardization Office (NSO).*
18. *NATO, 2021. Allied Command Operations Comprehensive Operations Planning Guide COPD. 3rd Ed. Brussels: NATO Standardization Office.*
19. *Smith, R., 2005. The Utility of Force: The Art of War in the Modern World. s.l.: Allen Lane.*
20. *Sun Tzu, 1910. The Art of War. s.l.: Project Gutenberg.*

21. *U.S. Army War College, 2020. Strategic Cyberspace Operations Guide. 1st Ed. Carlisle: Center for Strategic Leadership.*
22. *U.S. Department of Commerce, 2011. Managing Information Security Risk: Organization, Mission and Information System View. Gaithersburg (Maryland): National institute of Standards and technology, U. S. Department of Commerce.*
23. *Unknown, 2022 (original work published 1769). King James Bible. https://www.kingjamesbibleonline.org/ [Last accessed: February 2022].*
24. *US Army, 2012. ADP 3-90 Offense and Defense. 1st Ed. Washington D.C.: Department of the Army.*
25. *US Joint Chiefs of Staff, 2020. JP 3-85 Electromagnetic Spectrum Operations. 1st Ed. Washington D.C.: US Joint Chiefs of Staff.*
26. *US. Marine Corps, 1990. The Guerrilla and How to Fight Him. 1st Ed. Washington D.C.: Department of the Navy.*
27. *Van Creveld, M., 1991. The Transformation of War. New York: Simon & Schuster Inc.*
28. *Van Creveld, M., 2000. A History of Strategy: From Sun Tzu to William S. Lind. 2nd Ed. Kouvola: Castalia House.*
29. *Van Creveld, M., 2011. The Age of Air Power. Digital Ed. New York: Simon & Schuster Inc.*

e-mail: ignacio.pizarro@ccdcoe.org

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.

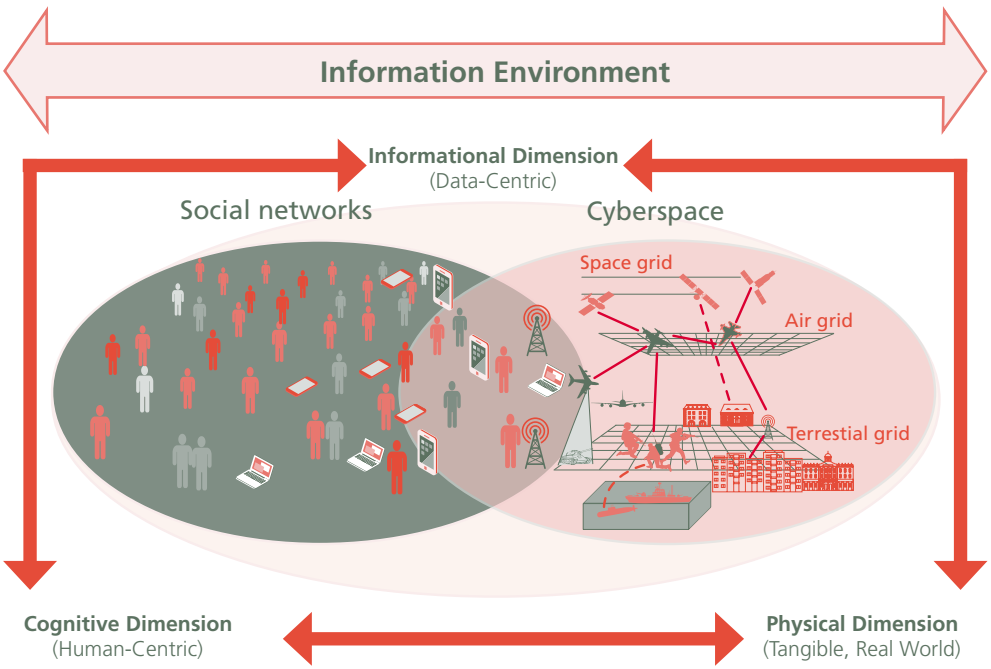


Figure 1: Information Environment (Porche III, 2016, pp I-2, Joint Publication 3-13: Information Operations, 2014, pp 1-2)

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).

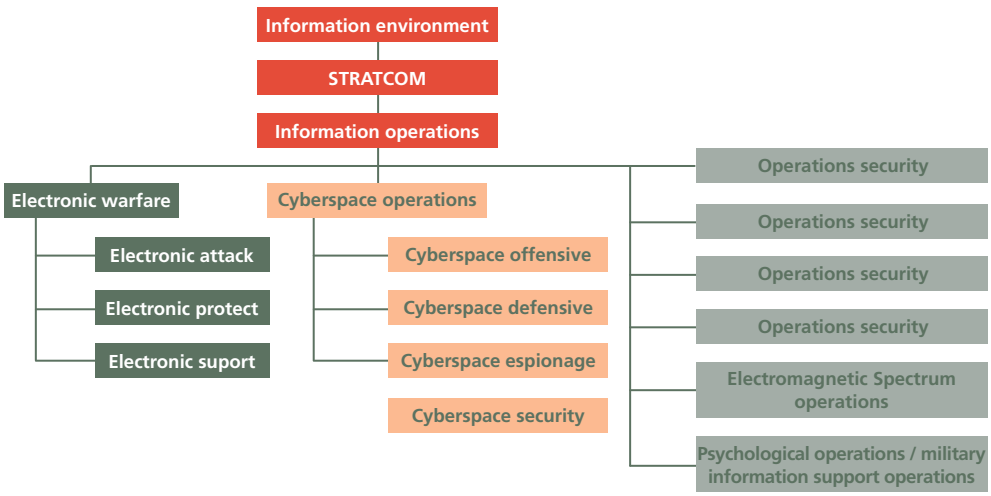


Figure 2: Information environment and forms of operation (adopted from Orye & Maennel, 2019, p 4)

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

Avtorji

Authors

Henrik P. Beckvard

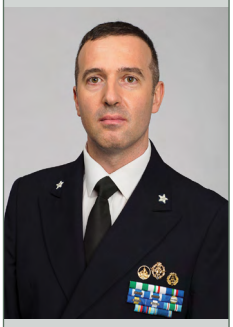
Henrik P. Beckvard je diplomiral iz prava na univerzi v Københavnu in končal šolanje na štabni šoli Canadian Forces College v Torontu. Opravljal je številne štabne funkcije doma in v tujini, leta 2018 pa ga je dansko ministrstvo za obrambo napotilo kot raziskovalca v Sektor za strategijo Natovega Centra odličnosti za kibernetsko obrambo v Talinu v Estoniji. Je vodja skupine v strateški komponenti vaje kibernetske obrambe Locked Shields in vodja tečajev za zaščito kritične informacijske infrastrukture v tem centru odličnosti.

Henrik P. Beckvard *holds a Law degree from the University of Copenhagen and is a Staff College graduate from the Canadian Forces College, Toronto. He has served in various staff positions both domestically and abroad, and since 2018 has been seconded from the Danish Ministry of Defence to the Strategy Branch of the NATO CCDCOE in Tallinn, Estonia, where he serves as a researcher. He is a Team Leader for the Strategic Track for Cyber Defence Exercise Locked Shields and serves as the CCDCOE Course Director for Critical Information Infrastructure Protection.*

Christopher Young

Stotnik Christopher Young je magistriral iz upravljanja in pedagoškega vodenja na Univerzi Saint Francis Xavier v Novi Škotski v Kanadi. V kanadskih oboroženih silah se je zaposlil leta 1995. Kot kanadski častnik za razvoj usposabljanja trenutno dela v Natovem centru odličnosti za kibernetsko obrambo (CCDCOE) v Talinu v Estoniji. Deluje v okviru Sektorja za izobraževanje in usposabljanje v CCDCOE kot član vodstvene skupine Oddelka za kibernetske operacije. Podpira vodjo oddelka pri analizi in obravnavi Natovih potreb glede usposabljanj v kibernetskih operacijah.

Captain Christopher Young *holds a Masters of Education in Administration and Educational Leadership from Saint Francis Xavier University in Nova Scotia, Canada. He joined the Canadian Armed Forces in 1995. He is a Canadian Training Development Officer (TDO) working at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Captain Young works within the Education and Training Branch at the CCDCOE, as a member of the Cyberspace Operations (CO) Department Head (DH) team. He supports the DH in analyzing and addressing NATO's training needs within the Cyber Operations domain.*



Davide Giovannelli

Davide Giovannelli je magistriral iz prava na univerzi v Pisi in na univerzi LUISS. Končal je italijansko mornariško akademijo v Livornu in leta 2004 pridobil čin poročnika korvete. Trenutno je kapitan fregate. Avgusta 2021 je začel delati v Natovem Centru odličnosti za kibernetsko obrambo kot raziskovalec v Sektorju za pravne zadeve. Pred tem je služboval na številnih vojaškopravnih funkcijah, med drugim kot pravni svetovalec v mednarodnih operacijah (Nato Allied Provider in Unified Protector, Unifil v Libanonu ter EU Atalanta in Sophia), v italijanski mornarici in na generalštabu obrambnih sil.

Davide Giovannelli *has a master's degree in Law from Pisa University and a LLM from LUISS University. He attended the Italian Naval Academy in Livorno and was commissioned to the rank of Ensign in 2004. Currently, he is a Commander (OF-4). He joined the CCDCOE in August 2021 as Researcher in the Law Branch. Prior to assuming his current position, he served in many areas of military legal counselling, including Legal Advisor in several operations (NATO Allied Provider and Unified Protector, United Nations Interim Force in Lebanon, EU Naval Operations ATALANTA and SOPHIA), the Navy and the Defence General Staff.*

Taťána Jančárková

Taťána Jančárková je magistrirala iz prava in ruskih ter vzhodnoevropskih študij na Karlovi univerzi v Pragi in iz mednarodnega javnega prava na Univerzi Leiden. Je raziskovalka v Sektorju za pravne zadeve CCDCOE v Talinu v Estoniji. Zanima jo uporaba mednarodnega prava v kibernetskih operacijah (projekt Interactive Cyber Law Toolkit), regulativni vidiki zaščite kritične informacijske infrastrukture in nacionalni okviri kibernetske obrambe. Pred tem je bila pravna svetovalka in vodja Oddelka za mednarodne organizacije in pravo pri Nacionalni agenciji za kibernetsko in informacijsko varnost Češke republike.

Taťána Jančárková *holods master's degrees in law and in Russian and East European studies from Charles University in Prague and an LL.M. in public international law from Leiden University. She is a researcher at the Law Branch of NATO CCDCOE in Tallinn, Estonia. She is interested in application of international law to cyberspace operations (Interactive Cyber Law Toolkit project), regulatory aspects of critical information infrastructure protection and national cyber defence frameworks. She has previously served as legal adviser and led the International Organisations and Law Unit at the National Cyber and Information Security Agency of the Czech Republic.*

Ignacio Pizarro

Podpolkovnik Ignazio Pizarro je štabni častnik za zveze španske kopenske vojske. Šolal se je na vojaški častniški akademiji v Zaragozi v Španiji, usposabljanje s področja zvez pa je opravil v Madridu in leta 2000 pridobil čin poročnika. Končal je generalštabno šolanje na španski vojni akademiji. Opravil je različne specializirane tečaje in usposabljanja španskih oboroženih sil, ameriške vojske in Nata iz vojaških komunikacij, operativnega načrtovanja in kibernetske obrambe. Je vodja Sektorja za operacije v Natovem centru odličnosti za kibernetsko obrambo.

Lieutenant Colonel Ignacio Pizarro *is a Spanish Army Signal Corps Staff Officer. He received training at the Army Officer's Academy in Zaragoza (Spain), and his Signal Corps Officer training and education in Madrid, graduating as an Army Lieutenant in 2000. He graduated as a General Staff Officer from the Spanish War College. He has received specialized courses and training by the Spanish Armed Forces, the U.S. Army and NATO in the areas of Military Communications, Operational Planning and Cyber Defence. He holds the position of head of the Operations Branch, at the NATO Cooperative Cyber Defence Center of Excellence.*

Damjan Štrucl

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.

Liutenent 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.*

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).
Vojaškošolski zbornik je vojaškostrokovna in informativna publikacija, namenjena izobraževanju in obveščanju o dosežkih ter izkušnjah na področju vojaškega izobraževanja, usposabljanja in izpopolnjevanja.

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
Odgovorna urednica:
liliana.brozic@mors.si

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

INSTRUCTIONS TO AUTHORS

Content-related guidelines

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 monograps (book review).
The Military Education Journal is a military professional and an informative publication intended for education and informing on achievements and experiences in the field of military education, training and improvement.

What do we publish?

We publish papers in Slovene with abstracts translated into English and, based on the decision of the editorial board; we also publish papers in English with abstracts translated in Slovene.
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 guidelines

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 reviewers 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 belongs to according to him and according the classification in the COBISS . 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 (10 lines). 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 text should be placed at the end of the paper, after the cited literature.

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 address, e-mail or a telephone number, so the editorial board could reach him or her.

Sending the paper

An electronic version of the paper should be sent to the address of the editorial board or the members of the editorial board.

Confirmation of the reception of the paper

The editorial board sends the author a written confirmation regarding the reception of the paper via e-mail.

Corrections

The author makes corrections to the paper in three days.

Editorial Board address

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

Executive editor address:
liliana.brozic@mors.si

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

https://dk.mors.si/sodobni-vojaski-izzivi/

Vsebina

Henrik P. Beckvard

Henrik P. Beckvard je diplomiral iz prava na univerzi v Københavnu in končal šolanje na štabni šoli Canadian Forces College v Torontu. Opravljal je številne štabne funkcije doma in v tujini, leta 2018 pa ga je dansko ministrstvo za obrambo napotilo kot raziskovalca v Sektor za strategijo Natovega Centra odličnosti za kibernetsko obrambo v Talinu v Estoniji. Je vodja skupine v strateški komponenti vaje kibernetske obrambe Locked Shields in vodja tečajev za zaščito kritične informacijske infrastrukture v tem centru odličnosti.

Henrik P. Beckvard holds a Law degree from the University of Copenhagen and is a Staff College graduate from the Canadian Forces College, Toronto. He has served in various staff positions both domestically and abroad, and since 2018 has been seconded from the Danish Ministry of Defence to the Strategy Branch of the NATO CCDCOE in Tallinn, Estonia, where he serves as a researcher. He is a Team Leader for the Strategic Track for Cyber Defence Exercise Locked Shields and serves as the CCDCOE Course Director for Critical Information Infrastructure Protection.

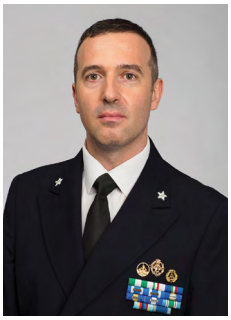
e-mail: henrik.beckvard@ccdcoe.org

Christopher Young

Stotnik Christopher Young je magistriral iz upravljanja in pedagoškega vodenja na Univerzi Saint Francis Xavier v Novi Škotski v Kanadi. V kanadskih oboroženih silah se je zaposlil leta 1995. Kot kanadski častnik za razvoj usposabljanja trenutno dela v Natovem centru odličnosti za kibernetsko obrambo (CCDCOE) v Talinu v Estoniji. Deluje v okviru Sektorja za izobraževanje in usposabljanje v CCDCOE kot član vodstvene skupine Oddelka za kibernetske operacije. Podpira vodjo oddelka pri analizi in obravnavi Natovih potreb glede usposabljanj v kibernetskih operacijah.

Captain Christopher Young holds a Masters of Education in Administration and Educational Leadership from Saint Francis Xavier University in Nova Scotia, Canada. He joined the Canadian Armed Forces in 1995. He is a Canadian Training Development Officer (TDO) working at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Captain Young works within the Education and Training Branch at the CCDCOE, as a member of the Cyberspace Operations (CO) Department Head (DH) team. He supports the DH in analyzing and addressing NATO's training needs within the Cyber Operations domain.

e-mail: christopher.young@ccdcoe.org



Davide Giovannelli

Davide Giovannelli je magistriral iz prava na univerzi v Pisi in na univerzi LUISS. Končal je italijansko mornariško akademijo v Livornu in leta 2004 pridobil čin poročnika korvete. Trenutno je kapitan fregate. Avgusta 2021 je začel delati v Natovem centru odličnosti za kibernetsko obrambo kot raziskovalec v Sektorju za pravne zadeve. Pred tem je služboval na številnih vojaškopravnih funkcijah, med drugim kot pravni svetovalec v mednarodnih operacijah (NATO Allied Provider in Unified Protector, Unifil v Libanonu ter EU Atalanta in Sophia), v italijanski mornarici in na generalštabu obrambnih sil.

Davide Giovannelli has a master's degree in Law from Pisa University and a LLM from LUISS University. He attended the Italian Naval Academy in Livorno and was commissioned to the rank of Ensign in 2004. Currently, he is a Commander (OF-4). He joined the CCDCOE in August 2021 as Researcher in the Law Branch. Prior to assuming his current position, he served in many areas of military legal counselling, including Legal Advisor in several operations (NATO Allied Provider and Unified Protector, United Nations Interim Force in Lebanon, EU Naval Operations ATALANTA and SOPHIA), the Navy and the Defence General Staff.

e-mail: davide.giovannelli@ccdcoe.org

Taťána Jančárková

Taťána Jančárková je magistrirala iz prava in ruskih ter vzhodnoevropskih študij na Karlovi univerzi v Pragi in iz mednarodnega javnega prava na Univerzi Leiden. Je raziskovalka v Sektorju za pravne zadeve Natovega Centra odličnosti za kibernetsko obrambo v Talinu v Estoniji. Kot raziskovalko jo trenutno zanimajo uporaba mednarodnega prava v kibernetskih operacijah (projekt Interactive Cyber Law Toolkit), regulativni vidiki zaščite kritične informacijske infrastrukture in nacionalni okviri kibernetske obrambe. Pred tem je bila pravna svetovalka in vodja Oddelka za mednarodne organizacije in pravo pri Nacionalni agenciji za kibernetsko in informacijsko varnost Češke republike.

Taťána Jančárková holds master's degrees in law and in Russian and East European studies from Charles University in Prague and an LL.M. in public international law from Leiden University. She is a researcher at the Law Branch of NATO CCDCOE in Tallinn, Estonia. Her current research interests include application of international law to cyberspace operations (Interactive Cyber Law Toolkit project), regulatory aspects of critical information infrastructure protection and national cyber defence frameworks. She has previously served as legal adviser and led the International Organisations and Law Unit at the National Cyber and Information Security Agency of the Czech Republic.

e-mail: tatana.jancarkova@ccdcoe.org

Ignacio Pizarro

Podpolkovnik Ignazio Pizarro je štabni častnik za zveze španske kopenske vojske. Šolal se je na vojaški častniški akademiji v Zaragozi v Španiji, usposabljanje s področja zvez pa je opravil v Madridu in leta 2000 pridobil čin poročnika. Končal je generalštabno šolanje na španski vojni akademiji. Opravil je različne specializirane tečaje in usposabljanja španskih oboroženih sil, ameriške vojske in Nata iz vojaških komunikacij, operativnega načrtovanja in kibernetske obrambe. Je vodja Sektorja za operacije v Natovem centru odličnosti za kibernetsko obrambo.

Lieutenant Colonel Ignazio Pizarro is a Spanish Army Signal Corps Staff Officer. He received training at the Army Officer's Academy in Zaragoza (Spain), and his Signal Corps Officer training and education in Madrid, graduating as an Army Lieutenant in 2000. He graduated as a General Staff Officer from the Spanish War College. He has received specialized courses and training by the Spanish Armed Forces, the U.S. Army and NATO in the areas of Military Communications, Operational Planning and Cyber Defence. He holds the position of head of the Operations Branch, at the NATO Cooperative Cyber Defence Center of Excellence.

e-mail: ignacio.pizarro@ccdcoe.org

Damjan Štrucl

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.

e-mail: strucl.damjan@siol.net