FROM CYBER WARFARE TO CYBER PEACE

Colonel (ret.) Professor Gheorghe BOARU, PhD*[*]
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania,
email: secretariat@aosr.ro)

Abstract: *In current peace and security issues, a paradigm shift has occurred in the sense that the role of technological and scientific progress has increased explosively, especially the rapid development of information technology (IT) and artificial intelligence (AI).*

Scientific communication addresses the significance, potential of IT, as well as the challenges it presents in terms of peace and security.

From a military point of view, the rapid pace of technological progress makes it imperative to follow and adapt to the constantly evolving landscape and also to make adjustments in the structure and training of military forces.

The central argument for preventing cyberwarfare and halting the offensive cyber strategies of the military and intelligence services is that cyberweapons are, in many ways, as dangerous and inhumane as biological and chemical weapons, which the international community already considers prohibited.

The issues of cyberwarfare and cyberspace are open to discussion, as disputes over the definitions of crucial terms such as cyberweapons or cyberspace remain unresolved. Consequently, in times of increasing militarization of cyberspace, the application of international law to it remains a challenge.

Keywords: *cyber warfare, cyber peace, cybersecurity, cyber weapons, cyberspace, artificial intelligence, international law.*

DOI 10.56082/annalsarscimilit.2025.3.34

INTRODUCTION

Technological and scientific progress—particularly the rapid development of information technology (IT) and artificial intelligence (AI)—plays a crucial role in matters related to peace and security. The swift advancement of these technologies significantly influences how conflicts emerge, evolve, and are addressed in today's global context.

This scholarly article explores the significance and potential of IT in the realm of peace and security, as well as the challenges it presents. It introduces readers to key research concepts in the fields of peace, conflict, and security studies, with a particular focus on perspectives from the natural sciences, engineering, and computer science. The paper sheds light on topics

[*] Full Member of the Academy of Romanian Scientists; Full Member of the Academy of National Security Sciences, email: boarugheorghe@yahoo.com.

such as cyber conflict, digital warfare and peace, cyber arms control, cyber attribution, critical infrastructures, artificial intelligence, and the role of ICT[1] in both conflict and peacebuilding contexts.

In dynamic domains such as these, major changes can occur within short timeframes—as is the case with information technologies used for peace and security. Recent years have witnessed numerous technological breakthroughs in the areas of cybersecurity and AI.

Political decisions have also impacted the prospects for arms control. For instance, the **I**ntermediate-Range **N**uclear **F**orces (INF) Treaty was formally withdrawn in 2019. In recent years, we have seen numerous wars, including Russia's invasion of Ukraine in 2022, following the annexation of Crimea in 2014, during which semi-autonomous weapons have been increasingly deployed. Additionally, the Israel–Hamas conflict—intensified by the Hamas-led attack on Israel in October 2023—has been accompanied by restrictive content moderation policies implemented by Meta, reportedly aimed at reducing pro-Palestinian narratives on platforms such as Instagram and Facebook.

It is evident that ICTs, including social media, exert a significant influence and play a prominent role in conflict-affected environments.

As a consequence of such violent conflicts worldwide, many individuals are forced to flee their countries, increasingly relying on ICT to coordinate and plan their migration journeys.

Furthermore, we are witnessing a growing trend of disinformation campaigns during electoral processes—as seen in Brazil in 2022—and during armed conflicts, orchestrated by a wide range of actors.

These examples underscore the critical importance of technical research in peace and security studies to comprehensively analyze these relatively new phenomena from an interdisciplinary perspective.

Given the rapid pace of technological advancement, it is imperative to continuously monitor and adapt to the evolving digital landscape.

Closely tied to modern technology are research efforts focused on critical infrastructure, artificial intelligence, and cyber weapons, as well as initiatives for digital peacebuilding and the scientific observation and reflection on these issues in recent years.

In many European countries, such studies are supported by government ministries responsible for education and scientific research, with the goal of deepening and expanding contributions to peace and cybersecurity.

[1] **ICT** refers to *Information and Communication Technology*, a vital field encompassing all technologies used for managing and transmitting information, including hardware, software, the internet, and communication networks. This sector plays a critical role in the development of modern economies, education systems, healthcare, and virtually every other area of society.

1. A MORE RESPONSIBLE, ETHICAL, AND SUSTAINABLE DIGITAL ENVIRONMENT

The widespread trend of digitalization and the growing dependence on IT systems are also triggering adjustments within military forces–both structurally and, more importantly, in terms of equipment and training. In addition to the necessary improvements in IT security and the implementation of defensive measures in cyberspace, an increasing number of states are establishing offensive military capabilities in this domain.

Historical developments and transformations brought about by advances in military technologies–as well as corresponding political progress and the development of appropriate instruments–have contributed to the management of challenges and the mitigation of threats to international security. In this context, it is possible to assess how such efforts might be applied to developments in cyberspace, alongside the obstacles that must be addressed to ensure success.

It is essential to consider ongoing political progress, the role of civic initiatives–such as the Cyber Peace Campaign of the Forum of Computer Scientists for Peace and Social Responsibility (FIfF)[2]–and the potential consequences of the increasing likelihood of cyber warfare in contrast with the prospects for cyber peace.

Such forums are typically established to address the ethical and social dilemmas associated with technology and to provide a framework for debating and resolving the issues confronting society in the digital age. Topics of discussion might include:

- **Ethics in technology**: how programmers and engineers can develop software that respects individual rights and freedoms, such as data protection and privacy;
- **The social impact of technologies**: including questions related to automation, artificial intelligence, and what these developments mean for employment, education, and security;
- **Social responsibility**: how to promote fair and inclusive use of technologies, reduce digital exclusion, and ensure universal access;
- **Technologies for peace**: how technologies can be used to resolve conflicts, support peace education, or promote shared values of understanding and cooperation.

[2] The **Forum of Computer Scientists for Peace and Social Responsibility (FIfF)** is an organization or platform dedicated to professionals in the field of computer science who aim to contribute to the development of a more responsible, ethical, and sustainable digital environment. The primary objective of such a forum is to promote the use of information technologies in ways that support peace, human rights, and social responsibility.

2. SOME EXAMPLES OF CYBER ATTACKS

In June 2010, in Iran, malicious software (malware) was discovered on industrial control computers at a uranium enrichment facility. The malware had been used to sabotage the plant by manipulating the centrifuges. Analysis of the program, which had been introduced via an infected USB flash drive and is now known as „Stuxnet", revealed that the sabotage had been ongoing for several years. It also indicated that the attackers possessed exceptional technical skills and detailed knowledge of the facility's design and operation.

Due to the high development costs and complexity involved in creating malware capable of targeting an isolated industrial installation, it was presumed that a state-sponsored agency was behind the Stuxnet operation. This assumption was later confirmed, and Stuxnet is now widely recognized as a joint project of the American and Israeli military and intelligence services[3].

However, Stuxnet was not the first piece of malware believed to have been deployed by a state actor. For instance, in 2007, the Israeli military was accused of sabotaging Syria's air defense systems[4]. In Estonia, a wave of cyberattacks temporarily disabled numerous servers, likely carried out by Kremlin-affiliated Russian activists[5]—incidents that are reported to have occurred during the 2008 Caucasus War in a similar fashion[6].

Since 2010, such events have repeatedly drawn public attention (see Table 1 for an extended list of malicious incidents). One notable case occurred in 2015, when the internal communication system of the German Federal Parliament, Parlakom, was subjected to months-long surveillance. During this time, documents, access credentials, and the personal

[3] Ellen Nakashima and Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say, The* Washington Post, June 2, 2012, available at https://www.-washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, accessed on 10.08.2025.; David E. Sanger, *Syria War Stirs New U.S. Debate on Cyberattacks*, New York Times, 2014; available at https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html, accessed on 10.08.2025.

[4] David A. Fulghum, *Why Syria's Air Defenses Failed to Detect Israelis,* Aviation Week & Space Technology, October 5, 2007; available at https://cyber-peace.org/wp-content/-uploads/2016/11/IMRA-Friday-October-5-2007-Why-Syrias-Air-Defenses-Failed-to-Detect-Israelis.pdf, accessed on 10.08.2025.

[5] Arthur Bright, *Estonia Accuses Russia of „Cyber Attack",* Christian Science Monitor, May 17, 2007, available at https://www.csmonitor.com/2007/0517/p99s01-duts.html, accessed on 11.08.2025.

[6] Dancho Danchev, *Coordinated Russia vs Georgia Cyberattack in Progress*, Zero Day, Aug. 11, 2008, available at https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/, accessed on 11.08.2025.

communications of members of parliament and their staff were likely stolen. The attack severely disrupted parliamentary operations and could not be stopped until the entire system was shut down during the summer recess[7].

Other incidents include phishing attacks targeting members of the German Bundestag in 2021[8]. A video produced by FIfF in 2017 further stimulated discussion on cyber warfare and cyber peace by introducing the concept of "peace informatics," which seeks to link peace and conflict studies with computer science. The organization's core argument for why cyber warfare must be prevented and why offensive cyber strategies by military and intelligence services must be abandoned is based on the assertion that cyber weapons are, in many ways, as dangerous and inhumane as biological and chemical weapons—which have already been banned by the international community.

Cyber weapons, therefore, consist of malicious software (such as viruses, worms, and trojans), which function only by exploiting vulnerabilities in foreign systems. As such, cyber armament primarily involves identifying or even creating potential weaknesses in the networks, institutions, and devices of foreign or adversarial actors. Naturally, since there is a market for everything, access to and knowledge about security vulnerabilities can also be purchased, often through the Darknet[9].

In cyber warfare, attackers use their control over systems to inflict harm or conduct espionage on the adversary. In practice, this means that anything containing a computer can become a target. Every PC, router, phone, and control system—regardless of size—may serve as a potential point of attack.

If our critical infrastructure (e.g., transportation systems, water facilities, hospitals, and power plants) were to be disabled or even turned against us, the consequences—particularly cascading effects—could be as devastating as those caused by conventional weapons, especially if supply chains or transportation networks were disrupted.

Nevertheless, some governments around the world are equipping themselves for offensive cyber warfare. This includes Germany, which has

[7]Thomas Reinhold, *Maßnahmen für den Cyberpeace*, 2018, available at https://cyber-peace.org/cyberpeace-cyberwar/masnahmen-fur-den-cyberpeace/, accessed in 12.08.2025.

[8] Von Frank Jansen, *Cyberattacke auf Bundestagsabgeordnete: Russische Hacker schicken deutschen Politikern Phishing Mails.* Tagesspiegel, 14.07.2021, available at https://www.tagesspiegel.de/politik/russische-hacker-schickendeutschen-politikern-phishing-mails-6858718.html, accessed on 12.08.2025.

[9] The term "Darknet" typically refers to a portion of the internet that is not indexed by traditional search engines and requires special software to access. It is often associated with privacy, anonymity, and at times, illegal activities. However, it also has legitimate uses, such as political activism under oppressive regimes or for individuals concerned with protecting their privacy.

established a dedicated military cyber force known as the *Kommando Cyber- und Informationsraum* (CIR).

A broad societal debate on the legality and ethical implications of turning our own devices into weapons that could be used against us at any moment has yet to emerge. However, FIfF outlines several reasons why cyber weapons should be outlawed, arguing that funds currently used to maintain vulnerabilities in critical infrastructure should instead be invested in closing security gaps.

I conclude with several important considerations regarding the cyber domain:

1. *Cyber weapons can be used anonymously.*

In global virtual networks such as the internet, it is extremely difficult to identify the true perpetrator of a cyberattack, as the attacker typically employs multiple devices to execute the operation, making backtracking nearly impossible. Moreover, attacks are often timed to suggest a different origin. Even if digital traces of the attack are found, they prove nothing with certainty, as such traces may be intentionally or accidentally left. Consequently, cyberattack attribution cannot be established with clarity.

2. *Cyber weapons cannot be controlled.*

Malware is often programmed to operate autonomously. It is difficult to determine whether it was deliberately deployed as a weapon or merely activated by accident. Such weapons can remain latent in systems for years before causing any damage. What distinguishes cyber weapons from conventional weapons—such as small arms—is that they can be easily stolen, endlessly replicated, and spread simply by copying and pasting.

3. *Cyber weapons are costly.*

Military and intelligence agencies spend enormous sums to analyze systems and purchase security vulnerabilities. Since only unpatched vulnerabilities can be weaponized, those who buy this information are motivated to keep them undisclosed and open for as long as possible. As a result, vast amounts of money are being spent globally to deliberately maintain the insecurity and vulnerability of critical infrastructure. Naturally, these maintain the insecurity and vulnerability of critical infrastructure. Naturally, these weaknesses can (and are) discovered and exploited daily by criminals and terrorists[10].

[10] FIfF - Director, 2017, *Cyberpeace statt Cyberwar!,* available at https://peasec.de/paper/-2024/2024_ReinholdReuter_FromCyberWartoCyberPeace_ITforPeaSec.pdf, accessed on 12.08.2025.

3. CYBER INCIDENTS

Over the past 16 years, a number of cyber activities have occurred, from which a list of the most relevant incidents–likely influenced by state or non-state actors-is presented.

The identification of the suspected actor is largely based on information released by intelligence or law enforcement agencies. The underlying evidence for these claims has rarely been made public, and it must be acknowledged that such accusations may also be politically motivated.

It is also important to note that distinguishing between cyber activities conducted by a state and its institutions and those carried out by non-state groups that are not directly affiliated with a state but operate under its indirect control is extremely difficult.

Table 1[11] List of Relevant Cyber Incidents with Presumably State or State-Influenced Actors

Year	Alleged actor	Description
2007	Russia	The cyber attack on the websites of the government and other institutions, banks and ministries of Estonia that prevented access to them is often considered to be the first significant state-driven cyber attack. Russia denied an official involvement, and the attack was attributed to a patriotic Russian youth organisation.
2008	Russia	The cyber attacks against Georgia and South Ossetia websites during the military conflict with Russia prevented public information platforms and media services from working. These incidents are often considered to have been the first attempts to use cyber capabilities as a means in military conflicts.
2010	USA / Israel	The malware Stuxnet was used to sabotage the Iranian nuclear program silently. Its presumably long development and deployment time, which involved specific information on the targeted industrial systems, were an international “eye-opener” on how states use cyberspace attack for foreign policy intentions.

[11] Christian Reuter (editor), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace (Technology, Peace and Security I Technologie, Frieden und Sicherheit),* Publisher: Springer Vieweg; Second Edition 2024, Year: 2024, pp. 145-147.

Year	Alleged actor	Description
2012	Iran	A malware named Shamoon/Wiper was used against industrial oil companies in Saudi Arabia. The malware had been explicitly developed to spread quickly within infected networks and render the targeted computers useless by deleting relevant operating system files. It affected up to 30,000 IT systems.
2012	USA / Israel	The malware Flame was used in the Middle East for espionage and intelligence purposes, especially in Iran, Israel, Palestine, Lebanon and Saudi Arabia. It was considered to be the most versatile malware development so far, with a vast variety of modules to infect different IT systems and perform multiple tasks on them. Therefore, Flame is seen as the first state-developed “cyber attack multi-purpose framework”.
2013	China	A US-based IT security company Mandiant report analysed several long-term cyber attacks and revealed a military cyber force in China, based on IT forensic analysis. The Unit “PLA 61,389” had been accused of espionage attacks with custom-tailored cyber weapons.
2014	Israel	The malware campaign Duqu 2.0 was used for espionage purposes with particularly versatile cloaking mechanisms. It is presumably a further development and extension of earlier versions that had been detected 2011.
2014	Palestine	XtremeRAT was a spear-phishing malware campaign in the context of the Middle East conflicts that a Palestinian activist group had used for espionage and data theft.
2015	USA	The Equation Group is the name of a malware campaign with a highly complex infrastructure and technological basis. The campaign had been active for several years, with the earliest indications from 1996. Its highly developed tools and malware frameworks had been developed and extended over years and share similarities with incidents like Stuxnet and Flame.
2015	Russia	In the context of the Western Ukraine conflict, Russia was accused of attacks against Ukrainian energy companies that stopped the power supply for around 700,000 residents for several hours. The malware BlackEnergy and Killdisk were used to gain access and

Year	Alleged actor	Description
		shut down IT systems.
2016	Russia	In preparations for the US presidential elections 2016, cyber attacks were performed against the Democratic National Committee that led to a severe data breach. Some of the documents were subsequently leaked. The cyber attack is seen as part of severe and long-lasting interference within the democratic election process of the USA. As for the end of 2018, the investigations are still ongoing.
2016	United States / Great Britain	Israel revealed that US and UK intelligence services covertly intercepted real-time video feeds from Israeli military drones and fighter jets. Their surveillance efforts were focused on monitoring military activities in Gaza, anticipating any potential Israeli actions against Iran, and tracking the global export of Israeli drone technology.
2017	Iran	A malware that targeted specific industrial control systems (SCADA) was deployed against Saudi-Arabian petrochemical companies. It had been specifically designed to trigger physical harm and destruction in these facilities, although this never happened due to programming errors.
2017	North Korea	After the leak of the fatal zero-day exploit EternalBlue, which had been stolen from the NSA and affected Microsoft Windows systems, a malware called WannaCry was deployed that used this exploit. It spread massively around the world and held affected users to ransom by encrypting their hard drives.
2018	Russia	In spring 2018, a hacking attack against German governmental IT systems and networks was published. The attack had been active but cloaked for more than a year and had been performed very carefully—without automatic replication or infection of IT systems. Its primary goal presumably had been espionage.
2018	Iran	The US Departments of Justice and Treasury have charged Iran in an indictment, alleging the theft of intellectual property from over 300 universities, in addition to government agencies and financial services firms.

Year	Alleged actor	Description
2019	North Korea	In February 2019, the North Korean Bureau 121 attacked the Bank of Valletta, Malta trying to steal $14.5 Million through phishing attacks.
2019	China	The European aerospace corporation Airbus disclosed that it had been the victim of Chinese cyber attacks that led to the theft of personal and IT identification data belonging to several of its European staff members.
2020	Iran	During the COVID-19 pandemic, hackers supported by the Iranian government made efforts to infiltrate the accounts of personnel working for the World Health Organisation (WHO).
2020	China	US authorities have alleged that hackers associated with the Chinese government made attempts to pilfer American research related to a coronavirus vaccine.
2021	North Korea	North Korean government hackers engaged in a complex social engineering campaign against cybersecurity researchers, utilizing fake Twitter (renamed to X) accounts and a phony blog to lure targets into visiting infected websites or opening compromised email attachments. They approached their targets under the pretense of collaborating on a research project, focusing on individuals associated with the Center for Strategic and International Studies (CSIS, 2023) in Washington, D.C.
2021	China	Norway pointed to China as the source of a cyber attack on its parliamentary email system in March 2021.
2022	Iran	Hackers supported by the Iranian government infiltrated the US Merit Systems Protection Board, exploiting the log4shell vulnerability as early as February 2022. Following the breach, these hackers installed cryptocurrency-mining software and deployed malware to acquire sensitive data.
2023	China	Authorities of the US and Japan have issued warnings, asserting that Chinese state-sponsored hackers have inserted tampering software into routers to target government agencies, industries, and companies in both nations. These hackers employ firmware implants to

Year	Alleged actor	Description
		maintain a covert presence and navigate within the networks of their targets. China has denied these allegations.
2023	Russia	Russia is stepping up cyber attacks against Ukrainian law enforcement agencies, specifically units collecting and analysing evidence of Russian war crimes, according to Ukrainian officials. Russian cyber attacks have primarily targeted Ukrainian infrastructure for most of the war.

4. MILITARIZATION OF CYBERSPACE

Since the discovery of Stuxnet, the term *cyber warfare*—derived from warfare as a military conflict between states and the concept of cyberspace—has been coined in connection with such incidents. However, this term overlooks a crucial distinction that must be considered when managing and interpreting such events: if the initiators of a cyberattack were not directly ordered by a government, the attack in question is a "normal" crime, subject to national and international prosecution and police cooperation.

These multilateral agreements already exist, such as the **Budapest Convention on Cybercrime**, issued in 2001 (Council of Europe, 2001). Only once a government is assumed to be the attacker does the interpretation of the incident shift to the political level and become relevant under international law. At this point, a critical distinction must be made regarding an appropriate response: Are we dealing with intelligence espionage, which primarily targets the confidentiality of a system (the area of "Cyber Espionage and Cyber Defense" should be analyzed), with sabotage intended to destroy a system, or with military activities directed at clear strategic objectives? For this purpose, the damage already inflicted must be analyzed. Depending on the attacker’s intent and the malware used, the consequences can range from simple theft to temporary disruption of an IT service or targeted damage to specific IT and subordinate systems[12].

Questions about cyber warfare go beyond the purely technical aspect of maintaining IT systems or attacking them. In addition to the defensive and offensive aspects and the necessary tools, the **security and strategic military doctrines of states** play a significant role. These doctrines

[12] Gary D. Brown and Owen W. Tullos, *On the Spectrum of Cyberspace Operations,* Small Wars – Journal, Dec 11, 2012; SSRN, available at https://ssrn.com/abstract=2400536, accessed on 13.08.2025 or http:// dx.doi.org/ 10.2139/ssrn.2400536.

determine the extent to which a state identifies cyberspace as a military domain and how it responds to the actions of other states.

For several years—at the latest since the discovery of Stuxnet—governments have increasingly perceived cyberspace as a military domain. According to a study conducted by the **United Nations Institute for Disarmament Research (UNIDIR)**, at least **47 states operated military cyber programs in 2013**, ten of which had nominal offensive intent—a situation that has likely evolved since then. It is known that in 2012, then-President **Barack Obama instructed his military and intelligence leaders** to compile a list of the most critical potential military targets in cyberspace and to develop solutions for disrupting or even destroying them[13].

In October 2012, President **Barack Obama issued a Presidential Policy Directive** known by the acronym **PPD-20** (*Presidential Policy Directive 20*). The document, formally titled *"U.S. Cyber Operations Policy,"* was classified, but some information was made public in 2013 through **Edward Snowden's revelations[14]**. This directive was issued in the context of increasingly sophisticated cyber threats facing the U.S., including attacks attributed to state actors such as China.

PPD-20 emphasized the importance of integrating cyber operations into the national security strategy, alongside traditional diplomatic and military options. However, the authorizations granted for **offensive cyberattacks without the consent of other states** raised questions regarding the **legality and ethics** of such actions.

The consequences of this presidential directive became evident through the opportunities for **cyber espionage and manipulation** revealed in 2013, which the **National Security Agency (NSA)** had been developing in the U.S. This included the deployment of **digital agents embedded in commercial products**. Traditionally, the NSA is subordinate to the head of the **U.S. Cyber Command**, which controls the **offensive cyber forces** of the U.S. military, and therefore has direct access to NSA technologies.

In the **Warsaw Summit Communiqué of 2016**, **NATO** integrated cyber defense into its **collective defense** framework, in accordance with **Article 5 of the North Atlantic Treaty**. This means that NATO now assesses cyberattacks within the broader scope of military aggression.

[13] For further details, see the original article from The Guardian: Obama orders US to draw up overseas target list for cyber-attacks, available at https://www.theguardian.com/-world/2013/jun/07/obama-china-targets-cyber-overseas, accessed on 14.08.2025.

[14] Edward Snowden did not publish a "work" in the academic sense, but the information we referred to comes from classified US government documents that he revealed in 2013, notably through journalists Glenn Greenwald, Laura Poitras, and publications like The Guardian and The Washington Post.

CNO[15] **forces** (Computer Network Operations) are assigned to the organizational unit of the strategic reconnaissance command. The task of this unit is **offensive access to foreign IT systems**.

In a military or cybersecurity context, **CNO** refers to the entire set of activities conducted within information networks, divided into three main categories:

1. CNA (Computer Network Attack) – Attacks on information systems intended to disrupt, degrade, destroy, or manipulate data and the functioning of target systems;

2. CND (Computer Network Defense) – Active or passive defense of one's own networks against attacks or intrusions;

3. CNE (Computer Network Exploitation) – Exploitation of foreign systems for intelligence collection, often without altering the targeted systems.

Thus, in the context of the earlier statement, the **CNO forces** assigned to the **strategic reconnaissance command** primarily focus on **offensive access to foreign IT systems**, which corresponds to the **CNE (Computer Network Exploitation)** component but may also include **CNA**, depending on the mission.

A notable example is **Germany**. However, these forces are currently being trained in **closed training networks** and have **not yet been deployed**, according to official statements (German Federal Parliament Defense Committee, 2016). At the end of 2017, the **Federal Ministry of Defense** officially integrated the organizational units of the **German Armed Forces (Bundeswehr)** responsible for IT and cyberspace into a separate organizational unit.

The "***Cyber and Information Space"*** comprises **16,000 employees** and holds an organizational level equal to the traditional military branches of the Army, Navy, Air Force, and Medical Service, according to information from the Federal Ministry of Defense of Germany.

Germany's Ministry of Defense announced in April 2016 the plans to establish a new military branch called "Cyber and Information Space" (*Cyber- und Informationsraum – CIR*) to strengthen the Bundeswehr's cyber defense. This structure became operational on April 1, 2017, and was given **equal standing with the other traditional branches** of the military. Initially, the CIR comprised **13,500 positions**, transferred from other branches of the armed forces, and was led by an inspector with the rank of lieutenant general. The development plans aimed to reach a force of **16,000 personnel by 2021**. By **2022**, the unit had approximately **15,000 military and civilian personnel**[16].

[15] CNO - Computer Network Operations.

[16] Available at en.wikipedia.org, Defense News, Deutsche Welle.

Additionally, the **CNO unit** was transformed into a **Network Operations Center** and expanded by **20 positions**. Given the need for information about relevant targets in cyberspace, it is assumed that this center works more closely with the **federal intelligence service**.

The **strategic directions of the White Paper** indicate that these restructuring measures are related not only to improved defensive capabilities but also to an **imposed strategic offensive orientation** of the German Armed Forces in cyberspace:

"The joint operational capability of the Bundeswehr across all dimensions is the supreme benchmark,"and "Superiority of effect must be achieved at all levels of intensity".

To achieve this goal, the **Federal Ministry of Defense**, in cooperation with the **Federal Ministry of the Interior, Building, and Community**, founded a **new agency for innovations in IT security**, modeled after the **U.S. Defense Advanced Research Projects Agency (DARPA).**

The task of this agency is to **initiate, promote, and fund research and innovation projects** in the field of **cybersecurity**, particularly focusing on the "**IT security solutions of tomorrow**," according to the **Federal Ministry of Defense of Germany, 2016**. For the period **2019–2022**, the agency may have spent a total of approximately **200 million euros**.

The growing **militarization of cyberspace** presents several challenges in the fields of **international law** and **security policy** for both the international community and individual states, which will be addressed in the following sections.

The Russian war against Ukraine, which began in February 2022, showed for the first time an open military conflict that was also accompanied by strong activities in cyberspace. In addition, as shown earlier in Table 1, there have been quite a few malicious incidents—with different objectives and magnitudes. This suggests the potential areas of application and consequences of future cyber warfare and, therefore, the (growing) relevance of the topic.

5. INTERNATIONAL LAW IN CYBERSPACE

With regard to the established rules of international operation, the question arises as to how they can be applied in cyberspace. The difficulty of clarifying this issue becomes apparent even in discussions about a common definition of cyberspace: while technical standards guide the understanding of the U.S. and Western Europe and cover the number of IT systems and their network infrastructure–so that security refers primarily to the integrity of these systems–other countries such as Russia or China consider the information that is stored, transmitted, and published through them as part of cyberspace. As a result, security, especially at the national level, goes beyond the integrity of technical systems and becomes a matter of control and access to this information–a perspective that is difficult to reconcile with the principles of human rights.

5.1. The Tallinn Manual

Experts convened by NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE) tried for the first time to address this issue in 2013 with the so-called Tallinn Manual, a guide that includes 95 guidelines for nations in the event of cyber warfare. Although not binding, it highlights the specific features of cyberspace where international law applies (NATO CCDCOE, 2013) and shows how international law can be interpreted for military conflicts in this new domain. In 2017, the CCDCOE published a second version of the manual, entitled *"The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"* (NATO CCDCOE, 2017), which continues this assessment—particularly regarding the behavior of states, as well as rules and norms in times of peace.

5.2. Virtual nature of cyberspace

The central challenge lies in the virtual nature of cyberspace, which undermines approaches and regulations based on territorial borders or the physical location of military assets. Equally problematic are the immateriality of malware programs and the unlimited possibility of reproducing them. In addition, due to the structure of cyberspace and the principles of data transmission, it is easy to act covertly or hide the true origin of an attack using proxy servers or other hijacked and exploited foreign IT systems—leading to the problem of attribution. Furthermore, IT systems are often highly interconnected and directly or indirectly control the processes of so-called critical infrastructures, such as electricity or water supply, communications, or transportation.

Therefore, damaging a nation's IT system can have potentially incalculable consequences, with serious impacts on initially unintended targets. Because covert access to IT systems for the purpose of espionage or military situational assessment is often linked to the application of malware and the manipulation of IT system functions, the threshold for such threats is superficial.

In relation to the core concepts of international law, these features of cyberspace raise a number of issues. For example, this refers to the international agreement on nonviolence and the right to self-defense according to Article 2, paragraph 4, and Article 51 of the UN Charter, as well as the principles of necessity and proportionality of military responses: What does "use of force" mean in cyberspace? When are malware programs and various cyberattack tools and methods considered "weapons"? When are we speaking about an "armed attack"?

Previous approaches to applying these concepts in cyberspace usually refer to the consequences of conventional, kinetic weapons to evaluate specific cyber incidents and possible reactions legitimized by international law. Thus, the Tallinn Manual defines armed attacks in cyberspace as “cyber activities that directly result in death, injury, or significant destruction” (NATO CCDCOE, 2013).

5.3. Characteristics of the Application of Malware

Such an approach, however, is insufficient, as it does not adequately take into account that the scope, timing, and form of damage caused by cyberattacks are in many ways not comparable to conventional weapons:

- Firstly, malware programs can spread uncontrollably beyond the target IT networks and affect external systems that were not the target of the attack and may belong to an uninvolved nation. For example, inactive versions of Stuxnet were discovered on tens of thousands of systems around the world. The use of malware that operates covertly over a longer period of time or uses indirect methods to manipulate subsystems—and therefore does not cause directly visible and attributable damage—is equally problematic.
- Furthermore, the current trend toward cloud technologies makes it even more difficult to geographically locate IT systems, since electronic data is processed and stored not on a single computer, but possibly on various such systems that are often distributed globally.

Related to this is the so-called problem of attribution ("Attribution of Cyberattacks"): A nation’s right to self-defense implies that the origin of an attack that requires prompt reaction must be clearly identified. In cyberspace, however, as mentioned above, it is common practice to carry out attacks from external systems hijacked specifically for this purpose in order to mask the source. Consequently, tracing these attacks through multiple stages cannot be conducted promptly or reliably from a forensic point of view.

The specific limitation of the permissible military use of malware also proves to be difficult. The tools, methods, and IT software used by criminals, IT security experts, and military forces to access IT systems are usually barely distinguishable. However, depending on the intention, their use can have very different results: for example, revealing, analyzing, and fixing vulnerabilities (IT security expert); stealing credit card data (criminals); or disrupting or destroying a military system such as an air surveillance program (military).

In addition to tools, identifying state or military agents, the concept of combatants in cyberspace, and distinguishing them from civilians is difficult to achieve with current technologies. Nevertheless, such labels are essential for managing agents in crisis and wartime situations.

Expert groups are debating these issues within the **United Nations** and the **Organization for Security and Co-operation in Europe (OSCE)**. However, we are still not seeing specific approaches to binding international regulations in cyberspace, particularly concerning the "right to war" (*jus ad bellum*) and the "laws of war" (*jus in bello*).

6. THE „CYBER PEACE" CAMPAIGN

In its campaign for cyber peace, "Cyberpeace," the Forum of Computer Scientists for Peace and Societal Responsibility (2014) uses an interesting symbol – see Fig. 1. The Forum calls for the cessation of all military operations on the internet by raising awareness about such dangers to, among others, individual privacy and human rights.

According to the Forum, the greatest threat lies in (unreported) flaws and vulnerabilities within IT systems used for cyberattacks. Since such attacks are hardly controllable, they could affect civilian sectors and critical infrastructures that provide electricity, water, communications, and healthcare, as well as other IT systems with possible security gaps. Especially government-led cyberattacks, which can deploy the most resources and influence, can weaken these systems and threaten the functioning of society and even human lives.

The Forum calls for the abolition of all cyber weapons through the creation of binding international agreements on arms control, disarmament, and the renunciation of the development and use of cyber weapons for offensive government-level actions. At the same time, the internet should serve as a civilian and peaceful resource, not abused for spying on civilians. Related to this, the concept of generalized suspicion should be abandoned and replaced with the pursuit of reliable evidence.

The threshold for military activities is lower in the cyber domain, as it does not give the impression of a real war, which makes the elimination of all cyber weapons necessary. This involves extending existing agreements, such as the Geneva Convention, into cyberspace.

Especially when it comes to critical infrastructures that ensure the provision of essential goods and services, whose failure can endanger human lives, their disruption from outside should be treated as a war crime. All operators of critical infrastructure should be obligated to secure and protect their systems independently and transparently from attacks and, where possible, disconnect them from the internet to prevent criminal access. At the same time, governments should establish a binding international initiative in cyberspace to protect the internet as critical infrastructure and to support research and development of peace strategies.

Figure 1. Logo of the Cyberpeace campaign

The use of conventional weapons in response to a cyberattack equally contradicts the Forum's peaceful policy. Due to the attribution problem, the source of a cyberattack cannot be clearly identified. Therefore, conventional weapons could lead to military escalation without a solid set of evidence.

Nevertheless, nations are urged to pursue a defensive strategy to protect their IT systems against cyberattacks and thus be allowed to use (hacker) tools for defense and for exposing existing security vulnerabilities.

Such security gaps, once identified, should be officially reported—especially for public and corporate IT systems—and closed before they can be exploited, instead of being left open for intelligence services or the military. Consequently, public awareness and trust in defensive cyber strategies will increase. In addition, to prevent such weaknesses from arising in the first place, security should be a central aspect of computer architecture, operating systems, infrastructures, and networks. Education systems should promote learning around IT competencies and their importance to society in order to increase the number of qualified experts, improve the security and quality of IT systems, and reinvigorate discussions on ethical and political issues related to technology.

Transparency and democracy are other core aspects of the campaign. By officially promoting independent and transparent development, review, and risk analysis of software, vulnerabilities can be identified and prevented openly, increasing security—especially for critical infrastructures.

Furthermore, instead of being the domain of intelligence services and military consulting firms, cybersecurity strategies and attacks should be officially confirmed and openly discussed in order to be part of the democratic decision-making process. Since freedom of speech and assembly are fundamental human rights, they should be equally respected in cyberspace and not serve as justification for criminal prosecution or military actions. To further contribute to the protection of human rights, independent and democratically regulated cybersecurity centers should be established to prevent cyberattacks and promote cyber peace.

As an essential tool for shaping public opinion, discussions about cyberspace in the media and politics should follow defined terms and not be used to mislead or fuel conflict. Therefore, the Forum also provides definitions to promote a better understanding of terms related to cyberspace.

7. CYBER WARFARE AND CYBER PEACE – MEASURES AT THE ROMANIAN LEVEL

Cyber warfare refers to the use of coordinated computer attacks to disrupt, damage, or destroy essential IT infrastructures and networks for military, political, or economic purposes. Romania, as a member state of the European Union and NATO, is aware of the growing risks in cyberspace and has adopted a series of measures to protect its national security and promote cyber peace.

7.1. Legislative and Institutional Framework

Romania has developed a legislative and institutional framework to prevent and manage cyber threats:

- **The Cybersecurity Law** (currently being updated): regulates the protection of national-interest networks and IT systems.
- **CERT-RO (National Computer Security Incident Response Team)**: monitors, analyzes, and responds to cyber incidents.
- **National Cybersecurity Directorate (DNSC)**: established in 2021, it is responsible for strategic and operational coordination in the field of cybersecurity.
- **Romanian Intelligence Service (SRI) – Cyberint National Center**: responsible for countering cyber threats to national security.

7.2. International Collaboration

Romania actively participates in NATO’s cyber defense initiatives, including exercises such as **Locked Shields** and **Cyber Coalition**.

It contributes to the development of cyber diplomacy policies within the EU and supports the **UN-**promoted Code of Responsible Conduct in Cyberspace.

7.3. Cyber Defense Capabilities

The **Romanian Army** is developing dedicated cyber warfare components, including within the **Cyber Defense Command**.

The establishment of a **European Cybersecurity Competence Centre in Bucharest** (EU Cyber Centre) gives Romania a key role in shaping European cyber defense policies.

7.4. Education and Awareness

Initiatives like **CyberSmart**, partnerships between universities, DNSC, and the private sector promote cyber literacy.

Development of cybersecurity educational programs in high schools and technical universities (e.g., **Politehnica University of Bucharest**, **Babeș-Bolyai University**).

7.5. Public-Private Partnerships

Collaboration between authorities and private IT&C companies is essential for the rapid detection of threats and information sharing.

Initiatives like **Cyberintelligence4Gov** or **DNSC Forums** help unite a common front against cyber threats.

7.6. Conclusion

Romania is actively involved in combating cyber warfare and promoting cyber peace through strong domestic policies, international collaboration, and investments in education and technology. Continuing these efforts is essential to protecting national interests and maintaining regional stability.

CONCLUSIONS

The answer to the initial question essentially depends on the underlying concepts of cyber warfare and cyber peace. These concepts remain open to debate, as disagreements over the definitions of crucial terms–such as *cyber weapons* or *cyberspace*–are still unresolved. Consequently, in times of increasing militarization of cyberspace, the application of international law to this domain remains a challenge.

At the same time, an increasing number of activists are attempting to shape the concept of cyber peace. Among them is the **Forum of Computer Scientists for Peace and Societal Responsibility**, which advocates for international disarmament, purely defensive cyber military capabilities, and the growing formalization of organizations and international law in cyberspace.

To summarize, the key challenges posed by cyber weapons are:

- The **militarization of cyberspace**;
- The **application of international law** to cyberspace, as necessitated by its militarization;
- Difficulties arise due to the nature of cyberspace and malware (which lead to attribution issues, and thus difficulties distinguishing cybercrime from cyberattacks), as well as the **lack of international norms and definitions**;
- Arms control in cyberspace is further complicated by the above issues. The offensive utility of defensive cyber capabilities and the dual-use nature of civilian IT systems also hinder efforts.

Measures to overcome these problems and achieve cyber peace include:

- Cooperative and declarative approaches, i.e., promoting interaction and information exchange on the one hand, and unilateral commitments to arms control on the other;
- Informational approaches, i.e., increasing cooperation in intelligence gathering;
- **Technical approaches**, i.e., strengthening cybersecurity through technical means, particularly by intensifying research.

Or, more concisely, the measures to achieve cyber peace would be:

- **Allowing only purely defensive cyber policies**. The focus should be on protecting IT systems; all other capabilities should be disarmed;
- **Outlawing conventional responses to cyberattacks**. Since the source of a cyberattack cannot be clearly identified, conventional weapons should not be used as a response;
- **Extending the Geneva Convention to cyberspace** in order to hold states legally accountable for their actions in this domain.

BIBLIOGRAPHY

BRIGHT A., *Estonia Accuses Russia of „Cyber Attack“*, Christian Science Monitor, May 17, 2007, available at https://www.csmonitor.com/2007/0517/p99s01-duts.html;

BROWN G.D., TULLOS O., *On the Spectrum of Cyberspace Operations*, Small Wars – Journal, Dec 11, 2012; SSRN, available at https://ssrn.com/abstract=2400536 or http://dx.doi.org/10.2139/ssrn.2400536;

CHIEN, E., FALLIERE, N., MURCHU L.O, available at https://symantec-enterprise-blogs.security.com/threatintelligence/stuxnet-dossier-espionage.

DANCHEV D., *Coordinated Russia vs Georgia Cyberattack in Progress, Zero Day*, Aug. 11, 2008, available at https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.

FULGHUM D., *Why Syria's Air Defenses Failed to Detect Israelis, Aviation Week & Space Technology*, October 5, 2007, available at https://cyber-peace.org/wp-content/uploads/2016/11/IMRA-Friday-October-5-2007-Why-Syrias-Air-Defenses-Failed-to-Detect-Israelis.pdf;

JANSEN VF., *Cyberattacke auf Bundestagsabgeordnete: Russische Hacker schicken deutschen Politikern Phishing Mails*, Tagesspiegel, 14.07.2021, available at https://www.tagesspiegel.de/politik/-russische-hacker-schickendeutschen-politikern-phishing-mails-6858718.html;

NAKASHIMA E., WARRICK J., *Stuxnet was work of U.S. and Israeli experts, officials say*, The Washington Post, June 2, 2012, available at https://www.washingtonpost.com/world/national-security/-stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/-01/ gJQAlnEy6U_story.html;

REINHOLD T., *Maßnahmen für den Cyberpeace*, 2018, available at https:-//cyber-peace.org/cyberpeace-cyberwar/masnahmen-fur-den-cyberpeace/;

REINHOLD T., REUTER C., Zur Debatte über die Einhegung eines Cyberwars: Analyse militärischer Cyberaktivitäten im Krieg Russlands gegen die Ukraine, Zeitschrift für Friedens- und Konfliktforschung, 2023, 12 (1), pp. 135–149, available at https://doi.org/10.1007/s42597-023-00094-y;

REUTER C. (editor), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace (Technology, Peace and Security I Technologie, Frieden und Sicherheit)*, Publisher: Springer Vieweg; Second Edition 2024, Year: 2024;

SANGER D., *Syria War Stirs New U.S. Debate on Cyberattacks*, New York Times, 2014 available at https://www.nytimes.com/2014/02/25/-world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html;

FIfF - Director, 2017 Cyberpeace stat Cyberwar!, available at https://-peasec.de/paper/2024/2024_ReinholdReuter_FromCyberWartoCyberPeace_ITforPeaSec.pdf;

The Guardian, Obama orders US to draw up overseas target list for cyber-attacks, available at https://www.theguardian.com/world/2013/-jun/07/obama-china-targets-cyber-overseas.

en.wikipedia.org, Defense News, Deutsche Welle;

https://www.darpa.mil/about-us/buget;

„United Nations General Assembly Resolution 66/24, adopted on 3 November 2011, entitled "Promotion and protection of human rights in the context of national security", (A/RES/66/24).