AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 18, No. 2 (2024), pp. 27-37

ELEMENTS OF ANALYSIS CYBERATTACKS AS WAR CRIMES. LEGAL AND PRACTICAL IMPLICATIONS IN MODERN MILITARY CONFLICTS

D. M. BOGDAN

Decebal Manole Bogdan
Faculty of Law and Social Sciences, „1 Decembrie 1918" University of Alba Iulia, România
https://orcid.org/0000-0001-8662-1243, E-mail: decebal.bogdan@uab.ro

Abstract: *Cyber operations have emerged as significant elements of modern warfare, particularly in conflicts like those in Ukraine, where cyberattacks target essential infrastructure alongside physical military actions. This paper examines the potential for cyberattacks to be classified as war crimes under international law, analyzing criteria established by international legal frameworks such as the Rome Statute, Additional Protocol I, and the Tallinn Manual on International Law Applicable to Cyberwarfare. Through case studies and legal analysis, this paper outlines the challenges and implications of prosecuting cyber operations that harm civilians and critical infrastructure in conflict zones.*

Keywords: *cyber warfare; hybrid warfare; cyber-criminal operations; cyber security; critical infrastructure; the potential of digitized actions*

Introduction

Cybersecurity and protection in the Black Sea has become a topic of great importance in the context of the war between Russia and Ukraine. The Black Sea is a region of strategic physical, economic and political geography. The conflicts in the Black Sea area have highlighted the need for robust cybersecurity measures. Cybersecurity involves the security of systems in critical infrastructures from both a military and an economic or social perspective.

In recent military conflicts, cyber operations have been widely used to target critical infrastructure, sometimes in coordination with physical attacks. These attacks raise ethical and legal questions, in particular regarding the possibility of cyber operations being considered war crimes. This paper explores the evolving criteria for war crimes in international law and the challenges of applying these standards to cyber operations, focusing on Ukraine as a primary case study.

Hybrid warfare: **The conflict between Russia and Ukraine is not only taking place on the traditional battlefield, but also in cyberspace**. Cyberattacks and influence operations are used to destabilize critical infrastructure and spread disinformation.

Involvement: The North Atlantic Treaty Organization and its allies have intensified security measures in the Black Sea region, including through military exercises and cooperation in the cyber field. Proximity warfare is an excellent geographical space to test the response capability of the military and military systems and equipment. A military maneuvering range as close as possible to real situations. In this geopolitical and military context, Romania, a

country close to the real conflict, plays an important role in the cyber protection of the region, being involved in NATO initiatives and collaborating with Ukraine to counter cyber threats.

Defining cyber operations in conflict zones. Cyber operations in conflict zones involve actions that disrupt, damage, or manipulate a state's networks and infrastructure, usually for military strategy purposes.

International Humanitarian Law (DIU) traditionally governs physical warfare, but in the case of cyber warfare, establishing thresholds for "attacks" and attributing consequences becomes challenging for justice. The current legal framework with reference to the **Rome Statute, Additional Protocol I** and **The Tallinn Manual**, provides guidance but does not explicitly mention cyber warfare, resulting in a legal gap.

1. **Legal framework in cyber warfare**

Classical warfare has a series of regulations through exceptional legal norms unanimously accepted by International Conventions and Treaties that become part of the sources of law in military conflicts alongside regular legal norms derived from the Constitution, Organic Laws, Emergency Ordinances, Government Decisions, Orders of the Minister of Defense, Military Regulations and Battle Orders. The correct application of legislation during military conflict is carefully supervised by the Military Prosecutor's Offices and Military Courts. In the area of Military Conflicts, we find the authority of the International Criminal Court whose role is to protect states and citizens from non-compliant actions that lead to genocide, crimes against humanity, etc.

According to researchers, *"Cyberwarfare is a new type of warfare waged in the cyber environment that can be considered the most developed form of warfare, through which the goal is achieved without human losses and without bloodshed. Cyberwarfare is similar to a classic armed conflict, the difference being the deployment environment, namely the virtual one, as well as the means by which it is carried out. This phenomenon represents the use of digital attacks to attack a nation, causing harm comparable to real war and disrupting vital information systems. There is significant debate among experts regarding the definition of cyberwarfare and even whether such a thing exists* (www.juridice.ro).

The opinion of military specialists (Zavakski, 2018:239-247) is that war in digital space is accessible to every individual who owns digital equipment connected to the Internet or local network and has minimal knowledge of using computers. From this point, structures in social groups "specialized" for cybercrime operations are identified, such as: state actors specialized in special military actions (some act under a foreign flag or under a private identity); military companies acting privately; international corporations; economic agents and organized crime groups.

We note that in the American Doctrine of Information Operations (https://irp.fas.org/doddir/dod/jp3_13.pdf) there are five distinct forms of this type of military operations, but (without limitation) namely:

- OPSEC – Operational Security (operations of operational security);
- MILDEC – Military Deception (operations of military deception),
- PSYOPS - psychological operations,
- EW – Electronic Warfare - operations related to electronic warfare,
- CNA – Computer Network Attack - operations on computer networks.

Most authors consider the actions: research by collecting information; attack determined by the destruction of enemy information and protection for the defense of one's own information as basic elements of information operations. The core of cyber warfare materialized through operations on computer networks (Zavalski, 2018), physical or virtual servers, transmission networks, social networks and elements of social engineering.

1.1 The Rome Statute and the policies of the International Criminal Court (ICC)

The Rome Statute does not contain direct provisions for cyberwarfare. The International Criminal Court has expressed its willingness to investigate cyberattacks on infrastructure that affect civilians, particularly if they align with traditional acts of war crimes. These include attacks that cause harm to civilians or support physical military operations. The Office of the Prosecutor at the International Criminal Court initially declined to comment but has previously stated that it has jurisdiction to investigate cybercrimes as well (Deutsch et al., 2024).

1.2 Additional Protocol I (API) and the Tallinn Manual

Additional Protocol "I" to the Geneva Conventions requires that attacks on civilian objects be prohibited and that methods that cause "unnecessary suffering" be illegal. The Tallinn Manual[i] *extends this concept to cyberwarfare, stipulating that cyberattacks should meet a threshold of physical harm to be considered "attacks." This criterion would exclude nonviolent cyberauction's but complicates cases where cyberoperations indirectly affect civilian well-being without causing immediate physical harm.*

2. Case studies of cyber operations in conflict zones

2.1 Cyberattacks in Ukraine: Power and communications network

Russia's use of cyber operations in Ukraine illustrates the integration of cyber warfare into traditional physical warfare. Notable cases include the attacks on Ukraine's power grid (2015, 2016) and recent operations targeting internet and satellite communications, often coordinated with physical attacks (Popescu et al., 2024). Also in the context of the war between Russia and Ukraine, the Black Sea region has been the target of several recent cyber-attacks. Here are some notable examples:

Attacks on Ukraine: In 2020, a group of hackers from Russia carried out a major cyberattack in Ukraine, affecting approximately 20,000 email accounts (www.forumulsecuritatiimaritime.ro).

GPS signal jamming: Recently, GPS signal jamming in the Black Sea region has become a serious problem, affecting thousands of flights and the movement of commercial ships in the south-eastern area of Romania (Ilie, 2024).

Ransomware attacks: Although not specific to the Black Sea region, ransomware attacks, such as the 2017, Petya malware, have had a significant impact on critical infrastructure around the world, including in this region (Lupescu, 2024a). *A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms* (Prentice, 2017).

These attacks underscore the importance of cybersecurity measures and international cooperation to protect critical infrastructure and ensure stability in the region.

Cyberattacks are deliberate actions designed to compromise the security of computer systems, steal data, disrupt services or gain unauthorized access. Here is how a cyber-attack generally unfolds, divided into stages: a) This type of operation disrupts essential social services. b) The effect of cyber operations is to limit civilians' access to information, energy and healthcare.

Attacks on critical infrastructure. A Cook Islands-flagged tanker belonging to Russia's ghost fleet carrying Russian oil has cut the ESTLINK2 power cable between Finland and Estonia (Dumitrache, 2024). In addition to the power cable, four other communication cables were damaged, but the situation could have been much worse if the Finnish Coast Guard had not reacted quickly and boarded the ship. The situation is more complex, as the ship apparently lost its anchor while "dredging" the seabed. "When the authorities asked the EAGLE S to raise the anchor, it was noticed that the anchor was no longer connected to the anchor chain," Finnish media notes (Salon Seudun Sanomat, 2024).

If it is proven that "cyber operations" intentionally affected civilians, legal arguments can be made that the criteria for a war crime are met.

2.2 Global Implications: The Iran-Israel Cyber Conflict

The cyber conflict between the state of Iran and the state of Israel demonstrates the potential of cyber operations to target critical infrastructure beyond "*special operations*" in Ukraine. Notable incidents, such as attacks on water infrastructure, show that cyber operations can create risks to civilians by impacting access to life-essential resources.

These cases support the argument that cyber operations should be subject to standards comparable to physical attacks under *International Humanitarian Law*. (DIU).

2.3 Israel's water infrastructure

A notable example of a cyberattack on Israel is the 2020 attempted attack on Israel's water infrastructure. This incident, attributed to Iranian actors, targeted water and sanitation facilities in Israel, attempting to manipulate control systems and disrupt water supplies. Israeli authorities reported that the attack, if successful, could have had serious consequences, potentially altering chemical levels in the water and endangering public health. This attack sets a worrying precedent for cyberwarfare against civilian infrastructure, with the aim of creating physical harm through digital means.

Given its intent to directly affect civilian assets, this cyberattack highlights the devastating impact of digital actions on civilian society. Cyber-action of this type (affecting the life and integrity of the population) can be classified as a war crime because it threatens the health of civilians and violates humanitarian protection rules under international law.

Protective measures can be achieved and strengthened through: a) International cooperation: States in the region work closely together to share information and develop common cyber defense strategies**. b) Exercises and simulations:** Military exercises, such as those organized by NATO, include cyber warfare components to prepare member states to respond effectively to cyber-attacks**. c) Advanced technologies:** The implementation of

advanced technologies and the development of new cybersecurity solutions are essential for protecting critical infrastructure and communication networks**.**

2.4 Cyber-attack evolution and recognition milestones

2.4.1 Reconnaissance. In this stage, attackers collect information about their target to identify vulnerabilities. This can include scanning networks, analyzing user behavior, and looking for weaknesses in security systems (https://www.dendrio.com/blog/cele-mai-comune-etape-ale-unui-atac-cibernetic/).

2.4.2. Delivery. Attackers use the collected information to deliver a malicious payload. This could be a phishing email, an infected link, or an attachment containing malware.

2.4.3. Exploitation. Once the payload has been delivered and activated, attackers exploit identified vulnerabilities to gain access to the system. This may involve executing malicious code, escalating privileges, or compromising user accounts.

2.4.4. Installation. Once they gain access, attackers install additional software to maintain access and avoid detection. This software can include backdoors, Trojans, or other types of malwares**.**

2.4.5. Command and Control (C2). The attackers establish a line of communication with the compromised systems to control and coordinate the attack. This allows them to extract data, launch additional attacks, or manipulate compromised systems (Lupescu, 2024b).

2.4.6. Action on the objective. In this stage, attackers achieve their final objectives, which may include data theft, information destruction, service disruption, or ransom demands (in the case of ransomware attacks)**.**

Examples of common cyberattacks:

a) Phishing: Sending fraudulent emails that appear to be from trusted sources to obtain sensitive information**.**

b) Malware: Malicious software that can damage or gain unauthorized access to computer systems.

c) Ransomware: Encrypting the victim's data and demanding a ransom to unlock it.

d) DDoS (Distributed Denial of Service): Flooding a server or network with fake traffic to make it unavailable.

In cyber warfare, targets can be grouped into several critical categories:

1. **Critical Infrastructure**: Energy networks (electricity, gas); Water supply systems; Transportation (airports, ports, railways); Telecommunications (radio, analog or digital, encrypted, satellite); Systems regarding public health and financial-banking systems;
2. **Government Systems**: National databases; Military communication systems; Diplomatic networks; Emergency systems (112); Digital public services; Inter-institutional communication and public communication;
3. **Mass-Media Systems**: Televisions; Radio; News sites; Online social communication networks; Mass communication systems;
4. **Sensitive Data**: Military information; Government and diplomatic information; Medical information; Financial data; Classified documents; Economic and intellectual property data and Personal information of citizens

2.4.7 Protection against cyber-attacks:

Protection against cyberattacks involves using advanced security solutions, constantly updating software, and educating users to recognize and avoid threats in cyberspace.

The security situation in the Black Sea region is complex and strategic from several perspectives. The strategic importance of the Black Sea is given by the fact that it is a vital trade route for Ukrainian grain exports. World trade between ASIA and EUROPE via the Black Sea route reduces the route of goods compared to the Mediterranean Sea option and the Atlantic Ocean area in Western Europe by 2,429 nautical miles.

Figure 1. The navigable artery of the Danube

Source: https://acn.ro/images/PDF/Site_2019/comercial/Nota_conceptuala_v1.pdf

The Black Sea is a crucial access point between Europe and Asia for the transport of oil and methane gas from Central Asia. Thus, the region has major strategic importance for NATO as an area to counter Russian influence

Romania's role: The Port of Constanta has become a crucial hub for Ukrainian grain exports but also for the entry of energy products into the European Union market. Romania hosts important NATO military facilities, including the Mihail Kogălniceanu base, and actively participates in surveillance and air defense missions in the region.

2.4.8 Threats and challenges in the geographical space of the Black Sea:

- Russia's frequent attacks on Ukrainian Black Sea ports with potential failures turn us into collateral victims;
- The presence of sea mines, which pose a high risk to navigation in the Black Sea area, constitutes challenges to freedom of navigation;
- Attempts at destabilization through hybrid warfare (cyber attacks, disinformation) affect the entire society.

2.5 Some security measures: Increasing NATO presence in the region; Strengthening air defense capabilities; Intensifying multinational military exercises and Developing surveillance and early warning systems. Specific mechanisms for protection against cyber attacks through active structures specialized in Cyber Security.

2.5.1 Regional cooperation:

- Close collaboration between Romania, Bulgaria and Turkey within NATO;
- Inclusion of the Republic of Georgia in the invisible front of cyber security on the geographical, political and military side of the West;
- Support for Ukraine by facilitating exports/imports, as well as cargo transit through Romania's infrastructure;
- Coordination with NATO partners to ensure maritime security in the Black Sea geographical area;

From the perspective of cyber security in the Black Sea area, the situation is quite complex:
Strengths:

- Romania has CERT-RO (National Cyber Security Incident Response Center) which monitors and responds to threats from the digitalized/informatized space.
- Within the Romanian army there is a complex military structure in cyber warfare within the Cyber Defense Command;
- Collaboration with NATO through the Tallinn Cyber Defense Center of Excellence
- Partnerships with private cybersecurity companies provide added value to cybersecurity with real-time action, countering cybercrime attacks and limiting potential damage.

2.5.2 Significant vulnerabilities of critical infrastructures:

- Critical infrastructure (ports, airports, bridges, road or rail tunnels, energy systems, communications) may still be vulnerable. Not all systems are up to date with the latest technologies. The high cost of modern equipment and the dependence on foreign technologies in some areas make defense vulnerable. Many industrial systems still use a series of outdated technologies that do not have the capability to stop attacks from cyberspace with devastating effects on the geographical, economic and social reality.
- Lack of specialized personnel. Lack of training of personnel operating computer systems, but also the lack of education of the population who, through involuntary, innocent actions, allow attackers to penetrate the digital space from where to launch attacks.
- Sometimes insufficient coordination between institutions. The arrogance of some institution leaders allows a lack of coordination between institutions and provides open spaces for attackers to penetrate databases.
- Attacks on port/airport infrastructure can disrupt specific activities. Critical infrastructure is connected to various support companies (which provide software and protection for this software), as well as partner companies that provide related services in marketing, sales, service, etc. Example: tourism or aviation ticketing companies that have access to airport infrastructure and specific commercial activities can also be cyber-attacked with the ultimate goal of reaching their partners, the airport structures.
- Maritime traffic control systems can be targets of cyber-attacks to block traffic or generate asset losses.
- Energy networks connected to the internet are vulnerable due to the relatively simple way to access computer systems and hijack dispatchers' actions.
- The potential for manipulation of maritime navigation and communications data

Conclusions

Proximity conflicts that combine classic warfare with elements of cyber attacks constitute a basis for a new military doctrine and effective strategies to combat potential risks at the population level. **A first step is to educate** the population about cybersecurity because through awareness you reduce risks. The more people we have who understand the basics of cybersecurity, the harder they can be manipulated or exploited, increasing the "digital immunity" of the entire society.

The next step can be to demystify the field. Everyone must understand that **Cybersecurity is not "black magic" and is not just for "*experts in black suits*".** Cybersecurity is a shared responsibility, like locking the door to your house. Irresponsible or unconscious use of the internet opens the door for cybercriminals who attack everything in the online environment. It is the context in which they have access to digital commands for the critical infrastructure area, so essential for the existence of the state, social peace and public health. Educating the population also brings social benefits in that parents will encourage their children towards this career and increase the reporting of suspicious incidents.

An educated population is the first line of defense against cyberattacks and substantially reduces the attack surface. In fact, a culture of security is created. We must start with basic education and then build specializations. We can assimilate the procedure as in medicine - when the population understands the importance of hygiene and prevention, the medical system works more efficiently.

In cybersecurity this means:

a. At the population level:

- Understanding the importance of "cyber hygiene" and paying attention to system access passwords, unwanted software updates or phishing.
- Awareness of the importance of data protection
- Ability to identify simple threats
- Development of natural preventive behavior

b. Construction of a digital technical system:

- Specialists will be able to focus on complex threats
- Resources are not wasted on basic cybersecurity problems
- Defense systems will be much more efficient, and a long-term strategy can be developed

c. Benefits:

- Simple attacks fail from the start!!!
- Specialists no longer "put out fires" continuously by acting reactively.
- Increases the efficiency of investments in social security and forms a sustainable security ecosystem

Opinion: The situation is similar to an immune system - the better the population has *"digital antibodies*", the more the specialized defense system can focus on truly dangerous threats. Right? If we look at it as a whole, the system of protection against cyber actions looks like an inverted pyramid: The wide base at the top of the pyramid. The educated population knows how to protect itself and understands the threats coming from the digital sphere, from the ground up. In this way, the population can avoid simple traps and pass on basic knowledge or potential cyber-attacks.

The middle portion of the pyramid system, thus imagined, will consist of specialists with training in information technology who understand the importance of security, implement preventive measures correctly to identify more complex problems.

The bottom of the pyramid where we imagine the top is made up of security experts who deal with advanced threats, develop complex strategies to prevent attacks or eradicate them, and manage major crises. The result will be real-time solution innovation.

By applying the principles presented, we no longer waste top resources on "I clicked on a suspicious link". Specialists can focus on the real defense of critical infrastructure. It's like building a house - you need a solid foundation (the educated population) before you put on the roof (the experts).

Proposals and Suggestions to improve security capacity for cyber risks:

1. Greater investments in modern security technologies
2. Training more specialists in the field
3. Cyberattack simulation exercises
4. Closer public-private cooperation

2. Training programs through specialized institutions: Military Technical Academy, NATO specialized courses, Joint exercises with allies and optional course programs included in youth education

Major challenges:

1. Personnel and expertise:

- Shortage of military specialists in the cyber field
- "Competition" with the private sector that offers higher salaries
- Difficulty in retaining experts in the system
- Increase in salaries in the military cyber field
- Partnerships with technical universities
- Mentoring program between experts and newcomers
- Regular practical exercises

2. Technology:

- Acquisition of modern detection and response systems
- Infrastructure upgrades
- Development of solutions own (not to be totally dependent on others)
- Increasing the role of private industry

Opinion: Maybe we should take the example of Israel or Estonia, which have developed integrated programs - they prepare young people from high school for cyber-security and then integrate them into military structures.

3. Operational vulnerabilities:

- Legacy systems that cannot be easily updated
- Interconnection with less secure civilian systems
- Challenges in coordination between different military structures

We are developing, but we are not yet at the optimal level necessary for current threats. We have the basic structures, but we lack the resources and expertise to deal with sophisticated attacks

4. A possible model for Romania could look like this:

1. Specialized high schools that have classes with a cyber and security profile. Partnerships between computer science high schools and military structures.
2. Specialized laboratories with real equipment
3. Practical programs with "Capture the Flag" type exercises; Attack and defense simulations;
- Ethical learning of hacking methods and real case studies (anonymized)
4. Benefits for students: Special scholarships; Guaranteed job after studies; Access to advanced technologies and possible internship programs during the summer.
5. Continuity: the possibility for young people to have a direct transition to military academies and "early binding" contracts with benefits.

Specifically:

1. Structure of the collaboration:
- Specialist officers teaching special modules in high schools
- Secure access to military testing infrastructure
- Shadowing programs where students observe specialists at work
- Military-IT summer camps

2. Advantages for military structures:
- Identify talents early
- Build loyalty and interest in the military field
- Develop their own specialist nursery
- Can influence the curriculum for their specific needs

3. Benefits for high schools:
- Access to specialized expertise
- Advanced equipment and technologies
- Real opportunities for students
- Increased prestige and attractiveness

4. Challenges to be solved:
- Security checks for access to information
- Balance between secrecy and educational needs
- Coordination between the civilian and military systems

REFERENCES

1. Deutsch Anthony, van den Berg Stephanie, Pearson James (2024). *Exclusive: ICC probes cyberattacks in Ukraine as possible war crimes, sources say*. Reuters [online] https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/ [accessed on 30.11.2024]
2. Dumitrache Ciprian (2024). *Finlandezii au arătat cum trebuie să lupți împotriva sabotajului: În maxim o oră, petrolierul secționa gazoductul Balticconnector și un alt cablu electric Estlink* [The Finns showed how to fight sabotage: Within an hour, the tanker was cutting the Balticconnector gas pipeline and another Estlink power cable]. Defense Romania [online] https://www.defenseromania.ro/finlandezii-au-aratat-cum-trebuie-sa-lupti-impotriva-sabotajului-in-maxim-o-ora-petrolierul-sectiona-gazoductul-balticconnector-si-un-alt-cablu-electric-estlink_631858.html [accessed on 30.11.2024]

3. Federation of American Scientists (2024). *American Doctrine of Information Operations* [online] https://irp.fas.org/doddir/dod/jp3_13.pdf [accessed on 30.11.2024]
4. Ilie Sandrina (2024). Rusia, atacuri cibernetice asupra României. Risc pentru siguranța zborurilor. Care sunt județele vizate [Russia, cyber attacks on Romania. Risk to flight safety. Which are the counties concerned] [online] https://www.capital.ro/rusia-atacuri-cibernetice-asupra-romaniei-risc-pentru-siguranta-zborurilor-care-sunt-judetele-vizate.html [accessed on 30.11.2024]
5. Lupescu Anca (2024a). Cele mai mari atacuri cibernetice ransomware din lume: De la întârzierea avioanelor, la salarii și răscumpărări colosale [The World's Biggest Ransomware Cyberattacks: From Plane Delays, to Colossal Paychecks and Ransoms] [online] https://stirileprotv.ro/divers/cele-mai-mari-atacuri-cibernetice-ransomware-din-lume-de-la-intarzierea-avioanelor-la-salarii-si-rascumparari-colosale.html [accessed on 30.11.2024]
6. Lupescu Anca (2024b). Ce este un atac cibernetic ransomware și cum funcționează [What is a ransomware cyberattack and how does it work] [online] https://stirileprotv.ro/divers/ce-este-un-atac-cibernetic-ransomware-si-cum-functioneaza.html [accessed on 30.11.2024]
7. National Company Administration of Navigable Channels S.A (2019). Nota conceptuala privind modelarea tarifelor de tranzitare a navelor fluviale pe canalele Dunăre-Marea Neagră și Poarta Albă- Midia Năvodari, raportat la tona marfă tranzitată [online] https://acn.ro/images/PDF/Site_2019/comercial/Nota_conceptuala_v1.pdf [accessed on 30.11.2024]
8. Prentice Alessandra (2017). "*Ukrainian banks, electricity firm hit by fresh cyber attack*". Reuters. Archived from the original on 16 July 2019. Retrieved 10.10.2024.
9. Popescu Felix-Angel, Petrila Laurențiu, Coatu Ana-Maria (2024). Securing EU Democracy and Citizenship at what Costs? Reflections on Defence Spendings between North-South and West-East Divergens in *Analele Universităţii din Oradea, Seria Relaţii Internaţionale şi Studii Europene*, TOM XVI, pp. 61-73 [online] https://analerise.igri.ro/resurse/reviste/2024/Felix-Angel%20POPESCU%20-%20Laurentiu%20PETRILA%20-%20Ana-Maria%20COATU.pdf [accessed on 30.11.2024]
10. Salon Seudun Sanomat (2024). Poliisi: Eagle S -tankkeri olisi voinut matkaa jatkaessaan vaurioittaa myös toista sähkökaapelia sekä kaasuputkea [Police: The Eagle S tanker could have damaged another power cable and gas pipeline as it continued its journey] [online]https://www.sss.fi/2024/12/poliisi-eagle-s-tankkeri-olisi-voinut-matkaa-jatkaessaan-vaurioittaa-myos-toista-sahkokaapelia-seka-kaasuputkea/ [accessed on 30.11.2024]
11. Statute of the International Criminal Court of 17 July 1998 in Rome [online] https://legal.un.org/icc/statute/99_corr/cstatute.htm [accessed on 30.11.2024]
12. The Tallinn Manual on International Law Applicable to Cyber Warfare (2013) [online] https://www.penncerl.org/wp-content/uploads/2021/12/6481-tallinn-manual-on-the-international-law-applicable.pdf [accessed on 30.11.2024]
13. Zavalski Igor (2018). "Războiul Cibernetic: Forțe și Procedee Necesare pentru Acțiunile Militare de Tip Nou", *Mediul Strategic de Securitate: Tendințe și Provocări*, Centrul de Studii Strategice de Apărare și Securitate al Academiei Militare a Forțelor Armate "Alexandru cel Bun", Chișinău. [online] Mediul strategic de securitate_tendinţe şi provocări_2017.pdf [accessed on 30.11.2024]
14. https://www.dendrio.com/blog/cele-mai-comune-etape-ale-unui-atac-cibernetic/ [accessed on 30.11.2024]
15. www.forumulsecuritatiimaritime.ro [accessed on 30.11.2024]
16. www.juridice.ro [accessed on 30.11.2024]