CYBER WARFARE
– THE NEW THEATRE OF WAR AND ITS LEGISLATIVE CLARIFICATIONS –

Marian-Valentin BÎNĂ, PhD
United Nations Support Mission in Libya
DOI: 10.55535/RMT.2024.4.16

This study aims to highlight the growing strategic importance assumed by the field of cybernetics in the dynamics of international politics. Cyberspace, an artificial environment created par excellence by human activity, has become crucial for power in the 21st century. After land, water, air and outer space, cyberspace represents the fifth dimension of new conflicts. In order to overcome these obstacles, I have chosen to clarify, from a legislative point of view, the status of this new dimension of conflict management. For the most part, official documents found in open sources define cyberwarfare as the use of incisive techniques for intrusion or sabotage an actor's information and physical resources, actions carried out in the context of a conflict, through the use of technology and telecommunications networks, which aim to compromise the defence, functioning, as well as the economic and socio-political stability of the adversary.

Keywords: cyberspace; cyberwarfare; information technology; lines of code; Tallinn Manual;

INTRODUCTION

In the modern digital age, every field of activity contains complex and novel technologies, and current combat actions confirm the prominent role of military intelligence and technology in achieving strategic, operational and tactical victory.

Considering traditional conflicts – on land, at sea and in the air –, which involve physical territories and tangible resources, a new front has in fact opened: the so-called *cyberwarfare*, which can be signified by the phrase *cyber theatre of war* (Shultz, 2022). The difference, the most important factor between this war space and traditional conflicts, is its substantially immaterial nature. The weapons used are lines of code, and the battlefield is made up of an infinite cyberspace, which, unfortunately, contributes, on the one hand, to a so-called democratization of information, and on the other hand, facilitates the possibility for malign actors to influence the target audience, through the narratives and information exposed.

EVOLUTION OF REGULATIONS APPLICABLE TO CYBERSPACE

In the international system, the concepts of *jus ad bellum* and *jus in bello* are those that regulate the potential use of force in a conflict. These normative and doctrinal developments, among others, represent the limitation of the behaviour of international actors and the imposition of restrictions, for example on the use of certain weapons, in order to prohibit attacks against specific targets or against the civilian population or to prepare the discipline that regulates the treatment that must be reserved for prisoners of war in addition to the roles, rights and obligations of the combatant. Thus, the provisions of the *Third Geneva Convention relative to the Treatment of Prisoners of War*, adopted in 1949, aim at the protection of prisoners of war, their rights and obligations in prisoner of war camps (Legislative Portal).

The genesis of these regulations is certainly not recent, and over the centuries they have evolved and adapted to the needs of the practical context, ultimately, of cyberspace. One of the first attempts to introduce a binding norm in international law on these issues took place with the establishment of the *Convention on Cybercrime from 2001* (Council of Europe, 2001), promoted by the Council of Europe, which, although it represented a starting point in the field, did not address the issue

of regulating the so-called cyberwarfare or the types of cyberattack inserted in the context of a hybrid war.

Undoubtedly, the legislative regulations made in this regard are found in art. 2 paragraph 4 and art. 51 of the Charter of the United Nations (Statuto delle Nazioni Unite, 1945). From the combination of their provisions, it is clear that states can undertake an act of self-defence when it comes to the use of force and when national security or territorial integrity is endangered. However, cyberspace raises new questions, such as, for example, regarding the existence and possibilities of extending the sovereignty of a country in cyberspace. The answer, although not exactly legal, but of an exclusively doctrinal nature, can be found in the *Tallinn Manual*[1], prepared by leading experts from the international academic world, specialists in international humanitarian law and military law. The manual essentially acts as a framework defining the categories of international law applicable to the cyber domain (Tallinn Manual 2.0). In this regard, the manual prescribes, in the first paragraph, that a country has the authority to exercise control over the entire cyber infrastructure and activities on its territory, with the inevitable consequence that, in the event of a cyber attack being detected, it may qualify it as an armed attack, expressly recognizing the possibility of defending itself (Ib.).

It seems appropriate to focus briefly on the *Tallinn Manual* which, as anticipated, does not have coercive effects for states, it only receives a kind of coercive effect through the lens of the main regulated reference notions. The importance of the regulations in question is found in the reinterpretation of existing international law, based on the undeniable dualism between the physical battle space (water, air, land) and the cyberspace. Although the infrastructure of cyberspace exists within territorial states through physical bodies containing data, their flow is only partially controllable by the state, which thus makes cyberspace immune to traditional ways of regulating the conflict context and, above all, although it is true that it is a new dimension, it is equally true that it cannot be considered separately from the three traditional dimensions mentioned earlier.

While the *Tallinn Manual* does not constitute a legislative regulation for states, it is a simple guide. The instruments that have legislative power are essentially international treaties and United Nations Security Council resolutions. For the latter, I believe it is appropriate to focus on the evolution of NATO legislation on the subject of cyberspace.

[1] The *Tallinn Manual* has become an influential resource for legal advisors and policy experts dealing with cyber issues. In many states, emerging state practice and public positions on international cyber law since the publication of the Manual necessitate an update of the 2017 edition. (A.N.)

NATO APPROACHES TO THE EVOLUTION OF CYBERSPACE

Although the North Atlantic Alliance has always protected its communications and information systems, it was not until the 2002 Prague Summit that *cyber defence* was included on the Alliance's political agenda. In 2006, the Riga Summit reiterated the need for additional protection of these information systems. In 2007, the well-known events in Estonia[2], which targeted a series of cyber attacks against public institutions, forced allied defence ministers to agree on the urgent need for intervention in this sector. It led to the approval of NATO's first cyber defence policy in January 2008. In the same year, the conflict between Russia and Georgia (Selene, 2018) demonstrated that cyber attacks can become a significant component of conventional warfare.

It was not until 2010, in Lisbon, that NATO developed a strategic concept in which it recognized that cyber attacks could become so severe that they threatened national and Euro-Atlantic prosperity, security and stability. Since April 2012, *cyber defence* has been introduced into the entire NATO defence planning process. In the following years, cyber warfare continued to be the subject of planning and consolidation on the NATO table, reaching approval at the 2014 summit in Wales (Damiano, Scatto, 2021), where the new cyber defence policy is recognized as an integral part of the defence system, thus allowing the use of force in the case of collective self-defence, according to the regulations of the United Nations Charter.

At the 2016 NATO Summit in Warsaw, Allied Heads of State and Government recognised cyberspace as an operational domain in which NATO must have the capacity to defend and respond (NATO, 2016).

Another crucial moment regarding the legislative regulation of cyberattacks took place at the 2021 NATO Summit in Brussels, where the new Cyber Defence Policy was approved, thus fulfilling NATO's core tasks, as well as its own general deterrence and defence tasks. It was expressly recognised that the impact of a clearly intentional attack in cyberspace must be considered an armed attack in all respects. In fact, it was precisely on that occasion that the 30 member states of the Alliance confirmed that, in the face of cyber attacks, Article 5 of the Treaty can be invoked and a new cyber defence policy was approved for a new approach to any

[2] In 2007, Estonia was the victim of a major cyberattack, affecting government websites, banks and information organizations. The attacker appears to have been Russia, although this cannot be confirmed with certainty. The first real cyberattack that took place in Estonia led to the need to expand the scope of Article 5 of the Atlantic Treaty, with the consequent legitimization of being able to resort to the collective self-defence mechanism. In the same context, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), one of the largest centres of excellence of the Alliance, was established, located right in Tallinn. This centre aims to improve cooperation between member states in the field of cyber defence. (A.N.)

type of cyber threats, even low-level ones (Damiano, Scatto, ib.). At the next NATO summit in Vilnius in 2023, the member states approved a new scheme for improving cyber defence, regarding NATO's global defence and deterrence. The concept will further integrate the three levels of defence, namely:

- information technology defence;
- political, military and technical defence;
- defence regarding civil-military cooperation, in times of peace, crisis and conflict, as well as the commitment to collaboration with the private sector.

OTHER CLARIFICATIONS REGULATING CYBER WARFARE

As we have seen, the laws of war are more likely to be applied in a physical context, which is not as effective in the cyber domain, thus raising issues regarding the difficulty of identifying the attacker and the effectiveness with which this type of attack is characterized.

The classification of attackers is only one of the many problems in this field. In 2000, McConnell International produced a very interesting report examining crimes and attacks committed in cyberspace and the related penalties. Analysing the current state of the laws in 52 states, they found that only a small number of them had changed their legislation to address the various cyber attacks, but the main problem was represented by transnational cyberspace, since there can be major problems when a criminal cyber attack involves several nations (Cyber Crime Treaty, 2024; Soafer, Goodman, 2001, pp. 1-34).

In order to determine whether military intervention is needed, it is necessary to correctly identify the aggressor, because depending on who the attacker is, where the attack comes from and what is being attacked, different rules will be applied. In today's society, in cyberspace, criminals are becoming increasingly expert in the use of computer technology. Hacking tools, with video tutorials on how to use them, are freely available. So-called *"script kiddies"*[3] or people with little technical knowledge can already find the code written to carry out the desired actions. These attacks can range from simple, vandalistic attacks to well-thought-out operations against critical infrastructure. In this context, identifying the source of a cyberattack requires identifying the physical location of the attacking system, for example, tracing the attack and attributing it to a specific IP address, identifying the system or systems used, identifying the people responsible for the attack,

[3] A *script kiddie*, by definition, is a person without technical expertise who uses pre-existing automated tools or scripts to launch attacks on computer systems or networks, https://www.sangfor.com/glossary/cybersecurity/what-are-script-kiddies. (A.N.).

and possibly identifying the organization sponsoring it. In rare cases, all of these elements can be concentrated in a single subject.

Due to the need to integrate information from the commercial and government sides, intelligence and military agencies thus complicate identification and can lead to a significant delay in the investigation of the attack. In an environment where attacks can take place in less than a second and, especially, at zero cost, when you already have the appropriate electronic equipment, the placement of such attacks facilitates the spread and exponential growth of the number of subjects who can resort to such measures (Strouble, Carroll, 2008).

CONCLUSIONS: CHALLENGES AND PROSPECTS

Currently, there is still no complete set of regulations, thus raising a number of implementation problems for international law, first of all, identifying the moment when a state is allowed to resort to self-defence and, therefore, to the possible use of force, if it were the victim of a cyber attack.

The current legislative regulations regarding cyber warfare are lacking in the unfortunate situation of overcoming a crisis that, even tomorrow, unfortunately, could lead to dramatic events. The absence of predetermined standards for the assessment and reaction to cyber attacks, which are validly adopted by the member states of the European Union or by the member countries of NATO, could constitute the fundamental element of a possible defeat in cyberspace. We must hope that, perhaps, as soon as possible, Western governments, NATO, as well as other commercial entities can have homogeneous and timely resources and criteria to achieve uniform, adequate and sufficient defensive standards to counter any attack of a cyber nature.

As history has taught us, decisions that in some way limit national sovereignty can be difficult to implement, especially since any form of integration inevitably leads to an erosion of state sovereignty. Cyberspace should, however, be managed much more effectively if it is shared with other states or members of international organizations.

Perhaps we could go so far as to say that national integration, rather than a possibility, should be considered an inevitable and mandatory requirement for defensive validity, precisely because cyberattacks could produce harmful effects comparable to physical attacks, with widespread consequences. It is necessary and indispensable that possible conduct should be identified and codified without delay by states and international actors, implemented at the level of cyberspace and reinterpreted on the basis of the legislation in force.

Therefore, it is now clear that cyberspace represents the opening of a new front, which must be taken into account. Despite the fact that NATO has declared the possibility of invoking Article 5 in the event of a cyber attack against any member of the Alliance, this situation requires a precise and concise assessment, carried out by relevant, unambiguous methods. The lack of predetermined standards for assessing cyber attacks could pose problems for NATO member countries, which have different internal methods to counter them. To overcome this ambiguity, it would be desirable for NATO to adopt uniform standards to assess individual cyber attacks and to determine whether they have reached a level of increased severity that would make it an armed attack.

According to what is presented in this article, we can say that the laws of war are applied rather in a physical context, not being as effective in the cyber domain, raising, as such, problems regarding the difficulty of identifying the attacker and the efficiency that characterizes such type of attack.

BIBLIOGRAPHY:

1. Brown, G., Poellet, K. *The Customary International Law of Cyberspace.* In *Strategic Studies Quarterly*, http://www.jstor.org/stable/26267265, retrieved on 2 August 2024.
2. *UN Charter* (1945), https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf., retrieved on 12 June 2024.
3. *Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021*, Brussels Summit, https://www.nato.int/cps/en/natohq/news_185000.htm, Press Release (2021) 086, published on 14 June 2021, updated on 1 July 2022, retrieved on 22 August 2024.
4. *Council of Europe* (2001). *Convention on Cybercrime*, https://www.coe.int/it/web/portal/home (STE no. 185), https://rm.coe.int/1680081561, retrieved on 27 May 2024.
5. *Council of Europe action against Cybercrime*, https://www.coe.int/it/web/portal/coe-action-against-cybercrime#:~:text=La%20Convenzione%20sulla%20criminalit%C3%A0%20informatica%20(2001)%20%C3%A8%20l'unico,tra%20i%20suoi%20Stati%20parti, retrieved on 22 June 2024.
6. *Cyber Crime Treaty*. Global Information Assurance Certification Paper, https://www.giac.org/paper/gsec/839/cybercrime-treaty/101761, retrieved on 22 June 2024.
7. *Cyber defence*. *NATO*, https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 2 August 2024.
8. Damiano, L., Scatto, E. *Nato, la nuova "Cyber Defence Policy": ecco le priorità dell'Alleanza nella difesa dello spazio cibernetico*, https://www.agendadigitale.eu/sicurezza/nato-la-nuova-cyber-defence-policy-ecco-le-priorita-dellalleanza-nella-difesa-dello-spazio-cibernetico/, retrieved on 12 June 2024.
9. *Manualul Tallinn* 2.0. CyberLaws, https://www.cyberlaws.it/2019/manuale-tallinn/, retrieved on 22 August 2024.
10. NATO (2016). *Cyber defence,* https://www.nato.int/cps/en/natohq/topics_78170.htm., retrieved on 22 August 2024.

11. Pool, P. (2013). *War of the Cyber World: The Law of Cyber Warfare. The International Lawyer*, source: http://www.jstor.org/stable/43923953, retrieved on 22 August 2024.
12. Portal legislativ/Legislative Portal, https://legislatie.just.ro/Public/DetaliiDocument/255597, retrieved on 12 August 2024.
13. Sironi de Gregorio, F. (2019). *Il Manuale di Tallinn 2.0.*, CyberLaws, https://www.cyberlaws.it/2019/manuale-tallinn/, retrieved on 12 July 2024.
14. Shultz, N. (2022), https://www.fordhamilj.org/iljonline/cyber-warfare-the-newest-theater-of-war, retrieved on 22 July 2024.
15. Soafer, A., Goodman, S. (2021). *Cyber Crime and Security. The Transnational Dimension.* In *The Transnational Dimension of Cyber Crime and Terrorism*, vol. Hoover Institution's National Security Forum Series, pp. 1-34, California: Hoover Institution Press, https://www.hoover.org/sites/default/files/uploads/documents/0817999825_1.pdf, retrieved on 22 August 2024.
16. *Statuto delle Nazioni Unite* (1945), https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf; Organizzazione delle Nazioni Unite, https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf, retrieved on 27 May 2024.
17. Strouble, D., Carroll, M. (2008). *Law and Cyber War*, SAIS 2008 Proceedings, http://aisel.aisnet.org/sais2008/37, retrieved on 12 July 2024.
18. *The North Atlantic Treaty* (4 April 1949. Washington D.C., https://www.nato.int/cps/en/natohq/official_texts_17120.htm, retrieved on 22 June 2024.
19. Verri, S. (8 August 2018). *La guerra dimenticata: sintesi e analisi del conflitto russo-georgiano 10 anni dopo.* Euronews, https://it.euronews.com/2018/08/08/la-guerra-dimenticata-sintesi-eanalisi-del-conflitto-russo-georgiano-10-anni-dopo, retrieved on 12 July 2024.
20. https://www.sangfor.com/glossary/cybersecurity/what-are-script-kiddies, retrieved on 22 August 2024.