Vol. 8 No. 2, 2022
Baltic Journal of Economic Studies
DOI: https://doi.org/10.30525/2256-0742/2022-8-2-115-120

CYBER DIMENSION OF HYBRID WARS: ESCAPING A 'GREY ZONE' OF INTERNATIONAL LAW TO ADRESS ECONOMIC DAMAGES

Nataliia Mazaraki[1], Yulia Goncharova[2]

Abstract. The subject of the article is the international and national legal aspects of compensation for economic damages caused by cyber attacks. The purpose of the article is to contribute to the ongoing debate on attribution and liability for malicious and destructive cyber activity. Cyber attacks have become a global problem facing the international community, posing enormous risks to the stability of international security, economic and social development, and the safety and well-being of individuals. Cyber attacks have proven to be numerous problems for domestic and international law – international humanitarian law, human rights law, the law of armed conflict – how to counter the actions of hybrid warfare by legal means, what are the remedies for losses due to cyber attacks. This article examines cyber attacks to show how the international community is moving toward responsible behavior by states in cyberspace, protecting civilians and critical infrastructure. The article's methodology is based on doctrinal legal research in this area, as well as international legal instruments, in order to examine how economic damages should be paid to victims of malicious acts in cyberspace. The difficulty of attributing cyber attacks has been analyzed to show that perpetrators evade responsibility, a separate problem for international law. It is concluded that international law, as it currently stands, provides little legal basis for substantive guidance on responsible state behavior in cyberspace, the necessary levels of attribution to establish state or non-state responsibility for cyber attacks. Economic losses from cyber attacks can be covered by insurance schemes, although analysis has shown that they do not work because insurers argue that cyber attacks exclude military risk insurance clauses that exclude coverage, which is reasonable, although it leaves victims of cyber attacks without the ability to recover damages. The paper supplements current research with a comprehensive analysis of legal and economic issues and calls for the development of an appropriate strategic environment, legal and infrastructural framework. The need for a joint international framework is emphasized, as civil liability under national law is hardly possible because cyber attacks are predominantly transnational in nature. A joint structure is also needed to prevent, deter and respond to state-sponsored cyber attacks.

Key words: hybrid war, international law, cyber war, cyber threats, cyber attribution.

JEL Classsification: K10, K30

1. Introduction

Sophisticated aggressors have long since abandoned conventional warfare, but actively engage in the full spectrum of actions directed at the statehood and state security of their adversary. A hybrid threat or war waged by overt or covert action by states, state agents, or non-state actors in peacetime, crisis, or armed conflict will affect the full spectrum of society of the targeted state(s). In particular, it will test the resilience of civil society and citizens, the strength of civilian authorities, agencies, civilian police, and the armed forces of states and alliances, including the strategic political cohesion of alliances (Fogt, 2021).

Both military and civilian researchers have delved deeply into the nature and essence of hybrid warfare, with the aggression of the Russian Federation serving as a major source of examples and evidence. The general approach to hybrid war involves political, military, economic, social, infrastructural and informational elements. The last element, and surely not the last, and one of the most troubling obstacles

[1] State Trade and Economics University, Ukraine *(corresponding author)*
E-mail: n.mazaraki@knute.edu.ua
ORCID: https://orcid.org/0000-0002-1729-7846
[2] State Trade and Economics University, Ukraine
E-mail: y.goncharova@knute.edu.ua
ORCID: https://orcid.org/0000-0003-4679-3715

is cyber attacks. It is a form of sabotage that has far-reaching consequences for international trade and relations. It disables commercial services, including health care, banking and communications, paralyzes industrial operations, defense facilities and educational activities. In addition, cyber attacks drain scarce resources or divert them to unproductive activities and impede research and development (Ali, 2013). Malicious information and communication technology (ICT) activities by persistent threat actors, including states and other actors, can pose significant risks to international security and stability, economic and social development, and human security and well-being (GGE Report, 2021).

Hybrid warfare has raised many problems for domestic and international law – international humanitarian law, human rights law, the law of armed conflict – how to counter the actions of hybrid warfare by legal means, what are the remedies for losses due to cyber attacks. In this article, the authors will address cyber attacks, examining how the international community is moving toward responsible behavior by states in cyberspace, protecting civilians and critical infrastructure. In addition, the authors will address the vital question of how economic damages should be paid to victims of malicious acts in cyberspace.

This paper aims to be a valuable complement to current research with integrated analysis of latest events, including the 2021 Report of the United Nations "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (GGE Report, 2021).

2. Casuistry: cyberwarfare, cyber operations, cyber attacks

Malicious computer or network intrusions are quite common, notorious and destructive.

Perhaps the most common and well-known cases involving cyber-attacks against a State include the large-scale cyber operations against Estonia in 2007, the Stuxnet cyber-attack on Iran's nuclear program in 2010, and the 2017 cyber-attack on the United Kingdom's National Health Service, the Wanna Cry attack that affected 300,000 computers across 150 countries, NotPetya, that brought losses of USD 300 million. The COVID-19 pandemic has been marked by a significant increase in malicious cyber operations against states' health infrastructure. These include operations against hospitals treating COVID-19 patients, intelligence-gathering operations against research centers developing COVID-19 vaccines, and operations against public health services dealing with COVID-19 (Interpol, 2020).

Causing great losses – both tangible and intangible – and being too problematic to investigate and prosecute, cyber attacks have become a center of research and analysis for military and civilian experts and academics.

Before turning to the central part of this article, a brief review of terminology is in order, since there are a number of terms used in various sources to define malicious intrusions into a computer or network.

According to the U.S. position, "cyberwarfare" is the action of a state against a state, equivalent to an armed attack or use of force in cyberspace, that could trigger a military response with a proportionate kinetic use of force (Cyberwarfare and Cyberterrorism, 2015).

Russian military theorists generally do not use the terms cyber or cyber warfare. Instead, they view cyber operations within the broader framework of information warfare, a holistic concept that includes computer network operations, electronic warfare, psychological operations and information operations (Russia's Approach to Cyber Warfare, 2016).

EU law defines cyber attacks as actions involving any of the following:
(a) access to information systems;
(b) information system interference;
(c) data interference; or
(d) data interception,

if such actions are not duly authorized by the owner or other right holder of the system or data or part thereof, or are not permitted by Union law or the Member State concerned (Council Regulation (EC) 2019/796).

The concise definition of cyber attacks has been laid down in the Tallinn Manual 2.0: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to result in injury or death, damage or destruction of facilities" (Tallinn Manual 2.0).

Another view of the definition of a cyber attack focuses on its implications for vital state information, then "cyber attack" refers to cases involving international cyber operations where deliberate actions are taken against state interests to "disrupt, deceive, degrade, manipulate or destroy information residing in the target information system or computer networks of the systems or networks themselves" (National Research Council, 2009).

Along with questions of definition come aspects of categorization of cyber attacks: Should malicious intrusion be considered a crime, an act of vandalism, an act of terrorism, or the use of force from the perspective of international humanitarian law? The Report "Cyberwarfare and Cyberterrorism: In Brief" provides a detailed picture of the cyberwarfare ecosystem distinguishing cyberterrorists, cyberspies, cyberthieves, cyberwarriors and cyberactivists. This broad range of actors points to the need for certain criteria to determine whether a cyber attack is criminal, an act of hacktivism, terrorism, or a use of

state force equivalent to an armed attack (Cyberwarfare and Cyberterrorism, 2015).

The authors believe that correct classification leads to correct answers about proportionate and lawful response, as well as responsibility for cyber attacks. In the course of this article, the authors will consider a cyber attack as an element of hybrid warfare, hence as a deliberate act against state security using ICTs.

3. Hybrid wars, cyber attacks and international law

Hybrid warfare is never officially declared and so far, has not ended with conventional warfare. It implies a permanent state, similar to war, with variable intensity. Hybrid warfare is often a covert and concealed activity (Radin, 2017). These features of hybrid wars presume they lay in a "grey zone" of international law, that is entitled to borderline peace and war. Analyzing the relevance on international law instruments to hybrid wars, O. Korhonen points out three main difficulties:

1) sustainment of distinguishing feature of the law in the context of a hybrid war, e.g., "distinguish public from private, state officials from non-state actors, combatants from civilians, and military from non-military engagement";

2) recognizing compliance with international law in particular cases. "Certain incidents in the Russian-Ukrainian relations over the past decade, such as cyber attacks, espionage, hostile corporate takeovers, or wintertime gas-cuts, can be interpreted either as systematic acts of hybrid war or as merely unsavory, but nonetheless legal, incidents in the interaction among sovereign states. Different interpretations place them under different legal regimes and render different outcomes when it comes to judging compliance with international law";

3) the shortcomings of the doctrine of international law, which cannot promote the interests of the international community as a whole, but only the interests of the heavyweight states of the world (Korhonen, 2015).

With regard to cyber attacks, these difficulties become even more complex because of the rapid development of cyber warfare, the problematic attribution of cyber attacks, their covert nature, the intensive involvement of nonstate actors, etc. The latter aspect underscores the limited effectiveness of international law in cyber age, when international institutions have no authority to regulate nonstate actors. Schmitt and Watts stress that "while cyber operations by a state may violate the sovereignty of the state where the non-state actors are located, cyber operations by non-state actors that are not attributable to a state as described below do not constitute a violation of sovereignty" (Watts, 2016).

The huge academic debate on the application of international law to cyberspace has led to profound and well-reasoned conclusions that international law, and especially the UN Charter, should apply fully to cyberspace, and that international humanitarian law should apply in cases of armed conflict. The GGE Report admits "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment" (GGE Report, 2021).

The focus of much scholarly debate has been to highlight the criteria when a cyber attack constitutes a use of force or an act of war, giving rise to a right of self-defense under international law. Experts in international humanitarian law are now convinced that cyber attacks fall under this body of law in times of armed conflict, and we cite the latest position of the International Committee of the Red Cross: "Certainly, international humanitarian law applies to and therefore limits cyber operations during armed conflict – just as it regulates the use of any other weapons, means and methods of warfare in armed conflict, whether new or old. This is true regardless of whether cyberspace is viewed as a new domain of warfare, similar to air, land, sea, and space; as a different type of domain because it is man-made, while the former is natural; or as not a domain as such" (ICRC Position Paper, 2020).

The assumption that international law applies to cyberspace directs the debate to questions of state jurisdiction and state responsibility for cyber activities, attribution of cyber attacks, and the legality of countermeasures.

4. Cyber attack attribution

One of the problems encountered in cyber attacks is attribution, as it is extremely difficult to clearly identify the perpetrators and determine whether their actions are attributable to a particular state. Although technical attribution capabilities have improved considerably in recent years, the political and legal issues surrounding ultimate attribution to state actors remain unsettled and contentious (Eichensehr, 2020), and common approaches and understandings have not been established. Attribution of a cyber attack, which establishes the source, facts, and circumstances of a cyber attack, is the basis for proper enforcement of the rights and responsibilities of victim states.

Art. 51 of the UN Charter lists two requirements for the attribution of the use of force falling within Art. 2(4) in order for the exercise of self-defense:

1) the attributed attack imposes an "imminent threat" to the attacked state:

2) the attack is attributed to a state actor (the individuals, groups, or organizations related to state government.

The Tallinn Manuals 1.0 and 2.0 broaden the interpretations of both the "imminent threat" and the "state actor" underlying the U.N. Charter Art. 51.

The GGE report points out that attribution is a complex undertaking and that a broad range of factors should be considered before establishing the source of an ICT incident (GGE Report).

International law does not preclude the standards, forms, and amount of evidence needed to attribute cyber attacks, although national practice is sparse, limited to the United States, and the International Court of Justice's position remains debatable.

Public attributions by the U.S. government take one of four forms:
(1) criminal indictments;
(2) economic sanctions;
(3) technical alerts; and
(4) official statements or press releases with a range of state bodies are involved (Eichensehr, 2020)

Eichensehr also provides examples of combination of abovementioned methods: "The U.S government frequently deploys more than one mechanism to attribute a particular cyber attack, including rolling out different attribution methods over the course of months or even years. For the Sony hack, the U.S. government first attributed the attack to North Korea in the FBI statement, and followed with attribution-by-sanctions a few weeks later. Nearly four years later in September 2018, the United States also engaged in attribution by-indictment, unveiling criminal charges against a North Korean citizen, Park Jin Hyok, for allegedly participating in a 'government-sponsored hacking team' responsible for the Sony hack, among others." (Eichensehr, 2020)

The international community has made a collective effort to establish certain standards for attributing cyber attacks. The GGE report also spells out the elements of cyber attack attribution, namely: "the technical characteristics of the incident; its scale, scope, and impact; the broader context, including the impact of the incident on international peace and security; and the results of consultations among the states involved."

Due to the aforementioned difficulties in attributing cyber attacks, it can be assumed that the process of creating some kind of framework can be quite lengthy, nevertheless, the victim states must resort to legal remedies, eliminate economic losses. Aravindakshan acknowledges, "On the other hand, the use of remedies in an international legal forum can lead to tangible benefits, such as injunctions and damages, as well as serve as a strong reminder to states that cyber abuse has real consequences" (Aravindakshan, 2021).

5. Remedies

The victim State may resort to non-judicial measures such as retorsion, countermeasures, and sanctions. By taking retorsion measures, the State expresses its disagreement with the activities of another State within the limits of the law. Such measures can take a variety of forms, including: severing or interrupting diplomatic relations or other forms of contact; expelling diplomats, journalists, or other nationals of target states; travel restrictions; restrictive monitoring of foreigners; reducing or interrupting economic assistance programs; various forms of economic and commercial restrictions; and embargoes (Delerue, 2020).

Countermeasures as an extrajudicial response to a cyber attack seem a rather appropriate response, aimed at forcing the accused state to comply with its obligations under the law of state responsibility. The doctrine of countermeasures was set forth in the Tallinn Manual 2.0, and its Rule Nine prescribes the principle of proportionality for countermeasures against cyber attacks: "a state affected by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state" (Tallin Manual 2.0.).

Self-defense in the case of cyber attacks may be available when it amounts to an armed attack, although states' reluctance to recognize and attribute, as discussed above, would diminish the ability to use such a defense.

GGE report encompass that States may engage in full range of diplomatic, legal and other consultative options as a response to cyber attacks (GGE Report, 2021).

Economic losses, often measured in enormous sums of money, are one of the most problematic consequences of cyber attacks because they are often irreversible. Victims of cyber attacks suffer the destruction of cyber infrastructure and data, incur remediation costs, and suffer millions in lost profits. And what can be seen today is that cyber attacks are becoming increasingly sophisticated and destructive, hitting the sharpest and most vulnerable targets, and the international legal framework is evolving too slowly. The latter aspect is also true for domestic remedies.

The damages of civilian victims of cyber attacks may be hardly covered by insurance, the cases of Mondelez and Merck companies (hit by NonPetya cyber attack) being the vivid example as their insurers denied to cover damages assessing cyber attacks as war-risk and hostile act exclusionary clauses that exclude coverage (the court proceedings of both cases are underway in the US courts). There are two sides to this coin: insured victims of cyber attacks can resort to their insurance to cover the damage, being virtually unaffected

and incurring huge losses otherwise risking their solvency. Although insurance companies are justifiably careful to avoid covering damage from cyber attacks, because such unpredictable compensation risks the insurer's solvency. Chopra argues the need for a new federally supported cybersecurity insurance program, specifically tailored to cover losses that can arise from cyber-attacks (Chopra, 2021) though we believe such a proposal may be viable only for economically fit States.

Although cyber-related insurance mechanisms seem like an inevitable future for the global reinsurance industry, as cyber threats will pose high-priority problems for states and businesses.

Nevertheless, every state will seek redress from cyber intruders, and this must be backed by a viable international legal framework, which is now "under construction".

6. Conclusions

Cyber attacks are an evolving, complex and global threat to the security of states and civilian organizations, but the challenges of addressing these challenges range from attribution to accountability for malicious and destructive cyber activity. The most vulnerable victims of cyber attacks are civilians, individuals and businesses who literally have no way to cover their economic losses because the attackers remain undetected or beyond the reach of litigation.

Insurance schemes do not work because insurers claim that cyber attacks exclude military risks by excluding coverage, which is reasonable, although it leaves victims of cyber attacks without the possibility of redress. States, though, in maintaining their security and cybersecurity, must develop an appropriate strategic environment, legal and infrastructural framework.

Public international law in modern conditions has a number of problems that make it difficult to fully protect cyberspace from attacks, assaults and threats. All this makes it necessary to review the provisions and rules of global Internet norms within the framework of public international law. Only by strengthening cooperation between countries, working closely together to develop common standards and regulations, and clarifying the mechanism for responding to cyber attacks can there be a chance to create a secure cyber infrastructure.

International law as it currently stands provides a meager legal basis for critical guidance on responsible state behavior in cyberspace, the necessary levels of attribution to establish state or non-state responsibility for cyber attacks.

Economic losses from cyber attacks can be covered by insurance schemes, although analysis has shown that they do not work because insurers argue that cyber attacks exclude military risk insurance clauses that exclude coverage, which is reasonable, although it leaves victims of cyber attacks without the ability to recover damages. The article complements current research with a comprehensive analysis of legal and economic issues and calls for the development of an appropriate policy environment, legal and infrastructural framework. The need for a joint international structure was stressed, since it is hardly possible to impose civil liability under national laws, since cyber attacks are predominantly transnational in nature. A joint structure is also needed to prevent, deter and respond to state-sponsored cyber attacks.

References:

Ali, A. J. (2013). Cyber attacks: a menace to global trade. *Competitiveness Review*, 23, 1. DOI: https://doi.org/10.1108/cr.2013.34723aaa.001

Aravindakshan, S. (2021). Cyber attacks: a look at evidentiary thresholds in International Law. *Indian Journal of International Law*, 59, 285–299. DOI: https://doi.org/10.1007/s40901-020-00113-0

Chopra, A. (2021). Cyber attack intangible damages in virtual world: Property insurance companies declare war on cyber-attack insurance claims. *Ohio State Law Journal*, 82(1), 121-[ii].

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Delerue, F. (2020). Measures of Self-Help against State-Sponsored Cyber Operations. In Cyber Operations and International Law (Cambridge Studies in International and Comparative Law, pp. 423–490). Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781108780605.015

Eichensehr, K. E. (2020). The law and politics of cyber attack attribution. *UCLA Law Review*, 67(3), 520–598.

Fogt, M. M. (2021). Legal challenges or "gaps" by countering hybrid warfare building resilience in jus ante bellum. *Southwestern Journal of International Law*, 27(1), 28–100.

International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019 (2020). *International Review of the Red Cross*, 102(913), 481–492. DOI: https://doi.org/10.1017/S1816383120000478

INTERPOL (2020). Cybercriminals targeting critical healthcare institutions with ransomware. Available at: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

National Research Council (2009). "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities".

Nori Katagiri (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, 7(1), tyab009. DOI: https://doi.org/10.1093/cybsec/tyab009

Korhonen, O. (2015). Deconstructing the Conflict in Ukraine: The Relevance of International Law to Hybrid States and Wars. *German Law Journal*, 16(3), 452–478. DOI: https://doi.org/10.1017/S2071832200020940

Madubuike-Ekwe, J. N. (2021). Cyber attack and the Use of Force in International Law. *Beijing Law Review*, 12, 631–649. DOI: https://doi.org/10.4236/blr.2021.122034

Mihaylov, V., & Sitek, S. (2021). Trade wars and the changing international order: a crisis of globalization? *Miscellanea Geographica*, 25(2), 99–109. DOI: https://doi.org/10.2478/mgrsd-2020-0051

Andrew Radin, Hybrid Warfare in the Baltics: Threats and Potential Responses (RR-1577-AF, Santa Monica, CA: RAND Corporation, 2017).

Russia's Approach to Cyber Warfare (September, 2016) CNA's Occasional Paper series. Available at: https://apps.dtic.mil/sti/pdfs/AD1019062.pdf

Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. Available at: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

Watts, S. (2016). Beyond State-Centrism: International Law and Non-state Actors in Cyberspace. *Journal of Conflict and Security Law*, 21(3), 595–611. DOI: https://doi.org/10.1093/jcsl/krw019

Wan, K. S. (2020). Notpetya, not warfare: rethinking the insurance war exclusion in the context of international cyber attacks. *Washington Law Review*, 95(3), 1595–1620.

Cyberwarfare and Cyberterrorism: In Brief (2015, March). Congressional Research Service. Available at: https://fas.org/sgp/crs/natsec/R43955.pdf