IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

State responsibility for cyberattacks as a use of force in the context of the 2022 Russian invasion of Ukraine

Olena Nihreieva
University of Cadiz. University of Odesa

Date of submission: July 2024
Accepted in: January 2025
Published in: March 2025

Abstract

The article offers a legal analysis of cyberattacks occurring in the context of the ongoing Russian invasion of Ukraine. Various approaches to their consideration in terms of the use of force are explored in the study. The necessity of an interdisciplinary approach is emphasized, as integrating computer science and legal studies is essential for establishing precise criteria for an effective legal framework. While a consensus on highly destructive cyberattacks has emerged, an international legal framework for less destructive cyber operations still needs to be developed. Particular attention is given to the legal positions of several states that are at the forefront of research activities focused on the development of legal regulations for cyberspace. Moreover, various issues concerning state responsibility for cyberattacks are examined. Special emphasis is placed on the challenges of legally attributing cyberattacks to a state, including the matter of state responsibility for the actions of private actors. Lastly, the publication concludes with recommendations regarding the cyberattacks against Ukraine as a use of force and, consequently, as internationally wrongful acts that entail the international responsibility of the Russian Federation.

Keywords

cyberattacks; classification of cyberattacks; cyberattack attribution; state responsibility; use of force; Russian invasion of Ukraine

Responsabilidad estatal por los ciberataques como uso de la fuerza en el contexto de la invasión rusa de Ucrania en 2022

Resumen

El artículo proporciona un análisis jurídico de los ciberataques que se han producido en el contexto de la invasión rusa de Ucrania en 2022. En el estudio se exploran diferentes enfoques para su consideración en términos del uso de la fuerza. Se subraya la necesidad de un enfoque interdisciplinario, ya que sólo la informática y la ciencia jurídica en conjunto pueden proporcionar una visión integrada de los criterios precisos para la elaboración de un marco legal. Si bien se puede llegar a un consenso con respecto a los ciberataques altamente destructivos, aún se debe desarrollar un marco legal internacional para operaciones cibernéticas menos destructivas. Se presta especial atención a las posiciones legales de varios estados que lideran actividades de investigación dedicadas al desarrollo de la regulación legal del ciberespacio. Además, se exploran algunas cuestiones relacionadas con la responsabilidad del estado por los ciberataques. Se da especial énfasis a los desafíos de su atribución jurídica al estado, entre los que se analiza el problema de la responsabilidad estatal por la conducta de personas privadas. Finalmente, la publicación concluye con recomendaciones para considerar los ciberataques contra Ucrania como uso de la fuerza y, en consecuencia, como actos internacionalmente ilícitos que entrañan la responsabilidad internacional de la Federación Rusia.

Palabras clave

ciberataques; clasificación de ciberataques; atribución de ciberataques; responsabilidad del estado; uso de la fuerza; invasión rusa de Ucrania

Introduction

As outlined in the report unveiled on 16 February 2023 by Google's Threat Analysis Group, Russian government-backed attackers have persistently targeted Ukraine and its allies since the onset of the conflict. Their focus has been on cyber operations aimed at NATO member states, strategically seeking advantages during wartime. Attack statistics from 2020 to 2022 have shown a 250% increase in targeting users in Ukraine and over 300% in targeting users in NATO member countries (Google's Threat Analysis Group, 2023). In Ukraine, 50% of the attacks have been directed against governmental and military sectors. In 2023, a 123% surge was observed (Poireault, 2023), including one of the most severe cyberattacks of the war against Ukraine's largest mobile network operator (Hunder *et al*., 2023). In fact, cyberattacks began prior to the invasion (Baezner, 2018). For instance, on 15 February 2022, a large DDoS attack blocked the websites of the Defence Ministry, the army, and Ukraine's two largest banks, affecting mobile applications and the banks' ATMs (Lyngaas & Lister, 2022). The situation repeated on 23 February 2022 (Hopkins, 2022). Although these attacks were serious and potentially damaging for Ukraine's critical infrastructure, under modern international law they have not been definitively classified as armed attacks within the legal framework of the use of force. However, with the increasing activities in cyberspace, many of which pose threats to international and national security, there is a pressing need for the international community to develop effective legal regulation. In the context of the Russian invasion of Ukraine, such legal regulation is crucial, as determining cyberattacks as a use of force raises questions regarding Russia's responsibility for their initiation.

As is evident, the issue of state responsibility for cyberattacks as internationally wrongful acts is examined not only in the context of the use of force but also in relation to breaches of other international state obligations. These include the principle of sovereignty, the principle of non-intervention in domestic affairs (Moynihan, 2021), and the duty to prevent cyberattacks (Madubuike-Ekwe, 2021) arising from a lack of due diligence (Kulesza, 2009). However, within the framework of this paper, cyberattacks as potential violations of the prohibition on the use of force will be given special emphasis.

The above focus establishes the scientific novelty of the study. While there are publications dedicated to the 2022 cyberattacks on Ukraine (Lin, 2022; Google's Threat Analysis Group, 2023; Voo, 2023; Lonergan, 2023; Vinhas de Souza, 2024), few provide a legal analysis of the issue

(Mueller *et al*., 2023; EU, 2023; for the 2022 attack targeting Viasat, see, e.g., Leng, 2023). In this regard, a suitable application of information sources from other fields of study is necessary to address the more specific context of cyberspace.

The research tends to analyse the prospects of determining cyberattacks as a use of force, suggesting an approach to classification that would help distinguish between types that either reach the minimum threshold of a use of force or remain below it. Consequently, in the case of the former, the issue of state responsibility for initiating these attacks is addressed. In particular, the perspective of Russia's responsibility for the cyberattacks launched against Ukraine is considered. At the same time, other important issues related to this problem, such as the use of armed force in self-defence and recourse to other legal remedies against cyberattacks (see, e.g., Roscini, 2010; Tsagourias, 2012; Hathaway, O. A. *et al*., 2012; Pérez Sierra, 2021; Oorsprong, Ducheine and Pijpers, 2023), are beyond the scope of this study.

The importance of an interdisciplinary approach to solving the above-mentioned problems cannot be underestimated. Only computer and legal science, in conjunction, can provide an integrated insight into the correct criteria for elaborating a legal framework. An analytical approach based on an interpretative method helps to find the correspondence between the essential elements of state responsibility and the phenomenon under consideration.

The article is structured as follows: Section 1 addresses the classification of cyberattacks, aiming to establish criteria that would delineate those attacks that may potentially constitute the use of force. Consequently, Section 2 discovers the perspectives of state responsibility for cyberattacks, analyzing them through the two-prong structure of their objective and subjective elements. The paper concludes with summarizing remarks.

1. Cyberattacks in the context of the use of force: the issue of classification

The prohibition on the use of force is one of the fundamental principles of international law established in the UN Charter following the conclusion of World War II. To comply with Art. 2 (4) of the Charter, "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations." Violation of this principle constitutes a breach of the international obligations of states, which can be classified as an internationally wrongful act, thereby giving rise to the international responsibility of a state.

The aforementioned simple notions are quite complicated in practice, particularly when we consider that the UN Charter was concluded nearly 80 years ago, at a time when neither the Internet nor cyber technologies existed.

The legal provisions developed by international legal practice are applied to traditional wars waged with kinetic weapons. Simultaneously, the emergence of an entirely different realm in which conflicts can be conducted through new information and communications technologies necessitates either the creation of new international legal norms or the modification and application of existing ones. The latter appears to be the more practical option. Recently, there has been a rapid increase in interest regarding the application of international law to states' conduct in cyberspace. Several states have officially expressed their positions on the matter (UN, 2021). The Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security was established by UN General Assembly Resolution 73/266 in 2018 (UN, 2018). This group comprises experts from 25 states, including Australia, China, Estonia, France, Germany, India, Japan, the Netherlands, the Russian Federation, the United Kingdom, and the United States, among others. It aims to promote shared understandings and effective implementation of possible cooperative measures to address existing and potential threats in the domain of information security (UN, 2018). The group is tasked with studying how international law applies to the use of information and communications technologies by states. It regularly submits reports on the findings of its review, including an annex containing the national contributions of participating governmental experts regarding how international law applies to the use of information and communications technologies by states, to the General Assembly. The acts adopted by the group and the national positions concerning the application of international law in cyberspace provide significant evidence of state practice or *opinio juris* that could lead to the development of international customary law. Notably, in the recent report, many states highlighted that the international community has acknowledged that existing

international law is applicable to state actions in cyberspace (UN, 2021).

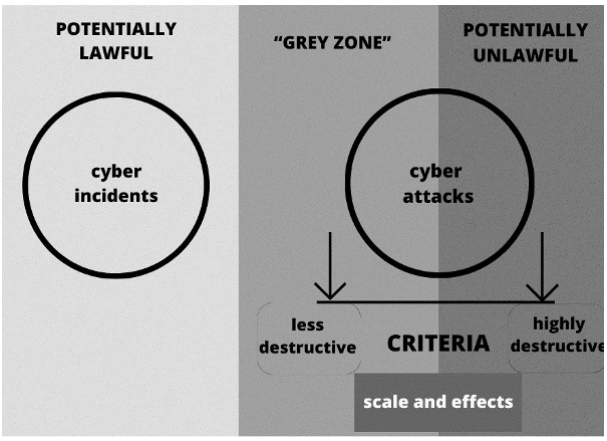
A common point in the aforementioned documents concerns the prohibition of the use of force and the potential classification of cyberattacks as such. Nearly all articulated national positions concur with the assertion that a cyberattack, under specific circumstances, may constitute a use of force or even an armed attack, thereby granting the targeted state a right to self-defence (UN, 2021). The criteria for such a determination present another complex issue.

Legal scholarship identifies three primary approaches to this issue (Leng, 2023, p.202): the "instrument-based" perspective, which regards the information technologies employed to launch cyberattacks as "weapons"; the "purposed-based" view, which asserts that cyberattacks undermining a targeted state's political independence and economic stability share unlawful objectives with conventional attacks when assessed under traditional international law; and the "effects-based" stance, which claims that cyberattacks, whose scale and consequences can be likened to those of kinetic weapon attacks, constitute the use of force. It seems that the last approach can aid in categorizing cyberattacks.

However, before delving into its investigation, it must be noted that not every situation involving the use of or damage to information and communication technologies qualifies as a cyberattack. For instance, the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" of 2017 distinguishes between cyber incidents, which are events of an unintentional nature, and cyberattacks, which are deliberate acts threatening the cybersecurity of the state. Consequently, the latter can be further divided into highly destructive and non-destructive cyberattacks. Cyber incidents almost fall outside the scope of state responsibility (the issue of strict liability should be considered separately). Interestingly, a commentator suggests it to be an independent model that allows for the classification of every cyberattack against critical national infrastructure as an armed attack (Madubuike-Ekwe, 2021, p.637). Cyberattacks of both types raise more questions, as illustrated in Figure 1.

A distinction should also be made between cyberattacks and cyber exploitation or computer exploitation enabling operations. The latter is used to achieve illegal access to computer systems or individual computers, normally to obtain information, and therefore, they are not conducted without "a hostile intent" (Roscini, 2010, p. 93). It is suggested that such acts can constitute a modern form of espionage, which, however, is not prohibited under international law (Ibid) and, thus, cannot be regarded as an internationally wrongful act.

Figure 1. Cyberattacks from the international responsibility perspective



Source: own creation

The classifications above could help establish criteria for categorizing cyberattacks within the legal regime of the use of force. In fact, the consequences of cyberattacks can be so severe and damaging that they may be likened to a genuine armed attack. This is particularly evident when cyberattacks occur in the context of an armed conflict or as a precursor to one.

In fact, the potential for expanding the scope of current international law to regulate cyberspace is enabled by the provisions of the UN Charter, particularly Art. 2(4), which establishes that it can be applied to any use of force, irrespective of the weapons used.

However, there is currently no consensus on the minimum criteria needed to address the question of whether a cyberattack constitutes a use of force under international law. According to the approach outlined in the Tallinn Manual 2.0, prepared by the NATO Cooperative Cyber Defence Centre of Excellence, a cyber operation qualifies as a use of force when its scale and effects are comparable to non-cyber operations that reach the level of a use of force (Schmitt, 2017). This position is supported by several governments, including the Federal Government of Germany in its policy paper "On the Application of International Law in Cyberspace" from March 2021, which refers to the

International Court of Justice's *Nicaragua judgment* (ICJ, 1996). It asserts that if the scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it may constitute a breach of Art. 2(4) of the UN Charter (Germany, 2021). Similarly, France reaffirms that a cyberattack could be regarded as an armed attack within the framework of Article 51 of the UN Charter if it exhibits "a scale and severity comparable to those resulting from the use of physical force" (France, 2021). For the sake of completeness, it is essential to note that the concepts of use of force, armed attack, and aggression are distinct and cannot be automatically equated. Furthermore, there is an ongoing debate regarding whether the term "force" should be understood in a narrow sense of military force or be interpreted more broadly to include economic and political pressures as well (for further details, see Dörr, 2019, ¶. 11-20). This study does not examine the latter interpretation, as it is focused solely on the narrower meaning of "force" as defined in the UN Charter.

Nevertheless, analysing the 2022 invasion cyberattacks on Ukraine through the lens of less severe forms of the use of force, which have lower and more easily attainable thresholds, remains a challenging task. This is largely due to the fact that "the parameters of the scale and effects criteria remain unsettled beyond the indication that they need to be grave" (UK, 2021). Despite this, the author of the Tallinn Manual, along with many national governments, "found the focus on scale and effects to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not", interpreting them as "a shorthand term that captures the quantitative and qualitative factors to be analysed in determining whether a cyber operation qualifies as a use of force" (Nihreieva, 2022).

The proposed criteria to consider include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality. Among these, severity is "self-evidently the most significant factor in the analysis" (Schmitt, 2017). A crucial suggestion for understanding the scale of harm states: "consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force," whereas "those generating mere inconvenience or irritation will never do so" (Ibid). This approach is also supported by national statements; for instance, France's position holds that a cyberattack could be regarded as an armed attack "if it caused substantial loss of life or considerable physical or economic damage" (France, 2021). The UK's statement has noted that "factors in considering the scale and effects of an attack may include the (actual or anticipated) physical destruction of property, injury, and death" (UK, 2021). Thus, the aforementioned limits of discretion are rather narrow, given that the effects may involve physical destruction of property, injury, and death.

Such an approach is helpful but still leaves many questions unanswered. For instance, the cyberattacks on Ukraine were highly invasive and of a military nature, yet they did not cause physical harm to individuals or property. However, it may be inferred with a high degree of probability that these attacks were part of a broader plan for subsequent aggression, aimed at weakening Ukraine's economy and military. In fact, findings from current analyses of cyberattacks indicate that since 2022, Ukraine has endured at least two types of attacks: disruptive attacks aimed at destroying data and rendering targeted systems inoperable, and espionage attacks intended to establish a foothold and exfiltrate data from targeted systems (Knapczyk, 2022).

If we compare them, particularly the first group, with kinetic attacks, a question arises: how would one define a missile attack that, due to luck or the efficiency of national defence forces, has not resulted in human casualties or property losses? It is undoubtedly a clear example of an armed attack. In this context, it seems that a significant cyberattack, the consequences of which were mitigated due to the effectiveness of cybersecurity measures, could be likened to kinetic armed attacks, provided that other crucial criteria, such as state attribution, are also met (Nihreieva, 2022).

It seems that Australia adopts a more comprehensive approach to interpreting the effects and scope of a cyberattack. Its policy statement acknowledges "a consideration of the intended or reasonably expected direct and indirect consequences of the cyber activity, including, for instance, whether the activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') in the form of injury or death to individuals, or damage or destruction (including to their functioning) of objects or critical infrastructure" (Australia, 2021). This perspective facilitates not only the assessment of the damage inflicted but also the anticipated consequences. Furthermore, damage need not necessarily result in human death or injury or the complete destruction of an object or critical infrastructure but may also encompass damage to their functioning.

It is worth mentioning that scholars also emphasize the need to establish "international rules not just for the rare high-end destructive or widely disruptive cyber operations, but also for lower-level operations" (Eichensehr, 2022), which is more difficult due to the uncertain immediate effects of such attacks. In practice, these less destructive cyberattacks often reside within the "grey zone" of international law. Because legal norms do not directly address them, these operations remain neither permitted nor forbidden, allowing states to exploit them.

The obstacle hindering the development of a legal framework for such attacks is the vague threshold that complicates the differentiation between highly destructive and less destructive cyberattacks. In "real-world" conditions, the characteristics of weapons, the scale of attacks, and the resulting damage are sufficiently clear to identify the use of armed force. Therefore, it is not particularly challenging to ascertain whether an attack was highly destructive and whether the weapons employed were considerably dangerous. Conversely, "cyberweapons" are difficult to characterize in this manner because the success of a cyber operation often does not rely on computer technology, but on other unpredictable factors, such as the target's cyber defence, the ingenuity, and professionalism of the attackers, among others.

In this regard, an alternative approach can be proposed. The classification of cyberattacks can be based, for example, on the differentiation of targets. The UK National Cyber Security Centre has ranked cyberattacks into six categories: from those that "cause sustained disruption of UK essential services or affect UK national security, leading to severe economic or social consequences or loss of life" (1st level) to those targeting an individual or indicating preliminary cyber activity against a small or medium-sized organization (6th level) (UK National Cyber Security Centre, 2018). This approach relies on a mixed target-effects criterion. It appears that this suggestion could also assist in distinguishing between highly destructive and less destructive cyberattacks. Please refer to Figure 2 for further details.

However, the characteristics of a cyberattack can be considered to be additional factors, including scale, intensity, duration, and type of attack (for instance, DDoS attacks are regarded as significantly more dangerous than DoS attacks (Morris, 2021). Additionally, attack layers align with the Open Systems Interconnection (OSI) model of the ISO (attacks on the physical level can be particularly hazardous, even though they can inflict substantial damage at every level) (Kumar *et al*., 2014), among others.

Figure2. Cyberattacks destructiveness

Category	Target	Effects	Level of destructiveness
1 National cyber emergency	national security, state essential services	sustained disruption, severe economic or social consequences, loss of life	highly destructive
2 Highly significant incident	central government, essential services, large proportion of population, economy	serious impact	highly destructive
3 Significant incident	large organization or wider / local government	serious impact	less destructive
4 Substantial incident	medium-sized organization	serious impact	less destructive
5 Moderate incident	small organization	serious impact	less destructive
6 Localized incident	individual	serious impact	less destructive

level of destructiveness

Source: own creation

Thus, categorizing cyberattacks within computer science can greatly aid in addressing their classification within the international legal framework. This could streamline the process of holding states and other actors accountable for perpetrating such attacks.

Regarding the situation in Ukraine, another crucial question arises: can a prior cyberattack signify the onset of a subsequent armed conflict? By this reasoning, the war in Ukraine could be traced back to at least 15 February 2022. This is vital for determining Russia's accountability in this matter.

2. State responsibility for cyberattacks

The beginning of Russia's invasion of Ukraine is marked by the events of 24 February 2022, the day Russia officially launched a large-scale military offensive against Ukraine. However, as previously noted, significant violations of Ukraine's sovereignty had been occurring before this date. In accordance with Par. 2 of Art. 14 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, the breach of an international obligation by an act of a State having a continuing character extends over the entire period during which the act continues and remains inconsistent with the international obligation (ILC, 2008). Therefore, establishing the initial date of violations is

crucial for the purposes of international responsibility. This process, however, must begin by demonstrating that wrongful conduct attributable to a state has occurred. Accordingly, to determine the date of the commencement of aggression or at least the use of force against Ukraine, we need to ascertain whether the cyberattacks can be classified as internationally wrongful acts for the purposes of the international responsibility of the Russian Federation. In this context, Art. 2 of the aforementioned Draft Articles, which outlines the elements of an internationally wrongful act of a state, is highly significant. According to this article, a state commits an internationally wrongful act when its conduct consists of an action or omission:

a) is attributable to the state under international law; and

b) constitutes a breach of an international obligation of the state (*Ibid*).

Scholars often interpret this provision as a combination of an objective and a subjective element. There is also a so-called "negative prerequisite" of international responsibility, which is the absence of circumstances precluding lawfulness (for more on the theory of international responsibility, see Crawford *et al*., 2010; D'Aspremont, 2012; Besson, 2022). However, this aspect will not be addressed in this paper.

To begin with, an objective element of cyberattacks should be analysed. The cyberattacks perpetrated against Ukraine constitute a violation of international obligations if they qualify as a use of force. As has already been emphasised at the outset of the paper, according to Art. 2 (4) of the UN Charter, the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations, constitutes a breach of the obligations of UN member states under the Charter. It is debatable whether cyberattacks alone can amount to aggression, whose prohibition holds the status of *jus cogens* (Roscini, 2007; Green, 2011; Helmersen, 2014; ILC, 2022). However, when part of a conventional attack classified as aggression, they contribute to the breach. In this context, Russia's behaviour provides substantial evidence of serious violations not only of its bilateral obligations to Ukraine but also of its obligations *erga omnes*.

As mentioned earlier, cyberattacks are also considered violations of the principles of sovereignty and non-intervention, as well as the duty to prevent them. A more detailed analysis is required to clarify the nature of the breaches under consideration. Although it lies beyond the scope of this paper, the principle of non-intervention is worth mentioning to illustrate the issue. Despite being binding under customary international law and applying *erga omnes*, there remains considerable debate regarding the *jus cogens* status of this principle (Jamnejad and Wood, 2009; Aloupi, 2015; Roscini, 2024). However, it appears that at present, this status is denied, except for the aspect concerning the prohibition of aggression.

Establishing the existence of the second element of an internationally wrongful act, namely its attribution to a state, is considerably more challenging due to the blurred lines between state and non-state actors' involvement in the war in Ukraine (Eichensehr, 2022). Nevertheless, as provided by customary international law, demonstrating this element is indispensable for the purposes of international responsibility (Crawford, 2006, ¶. 65). At the same time, it remains a critical point in the special context of cyberattacks.

Cyber attribution is the process of tracking and identifying the perpetrator of a cyberattack, which is directly related to the attribution of international responsibility. Three types of attribution should be distinguished:

1) technical attribution (factual and technical in nature),

2) political attribution (a policy matter), and

3) legal attribution.

For the purposes of state responsibility, the latter is crucial. The legal position of Canada is based on the idea that "attribution in its legal sense is of course distinct from the technical identification (or technical attribution) of the actor responsible for malicious cyber activity, whether state or non-state, as well as from the public denunciation of the responsible actor (political attribution)" (Canada, 2022).

This statement brings us to the central issue of cyber attribution. In accordance with Art. 4 – 10 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, a state is responsible not only for the acts (including actions and omissions) of its organs or equivalent entities, but also for the actions of non-state actors, such as cyber firms, hacktivists, or terrorist groups, acting on its instructions or under its direction or control (the so-called "effective control") (Schmitt, 2019). In the latter scenario,

demonstrating a direct link between a state and individuals or a group responsible for cyberattacks proves exceptionally challenging. That is why the standards of "overall control" (Shakelford, 2010) and "control and capabilities" (Stockburger, 2017) are proposed to reduce the level of control requirements needed for attribution. In this connection, changes to the evidentiary threshold for judicial determination are also suggested (Aravindakshan, 2020).

Simultaneously, the German government has reiterated its legal position as follows: "a sufficient level of confidence for an attribution of wrongful acts needs to be reached" (Germany, 2021). In this regard, "processes of data forensics, open-source research, human intelligence and reliance upon other sources – including, where applicable, information and assessments by independent and credible non-state actors" are required (Germany, 2021).

Consequently, the report issued on 16 February 2023 by Google's Threat Analysis Group is highly relevant. It indicates that cyberattacks on Ukrainian and NATO institutions are carried out by the hacker groups FrozenLake, Coldrive, Summit, FrozenBarentz, and FrozenVista, which are linked to the Russian government (Google's Threat Analysis Group, 2023). Moreover, recent research has demonstrated a direct connection between the most notorious cyber threat groups involved and Russian special services (Knapczyk, 2022).

Relevant evidence may also be provided if an international tribunal assesses a cyber operation (Schmitt, 2019). Indicators such as the state-controlled nature of Russian cyberspace, technical details, and the use of the Russian language in malicious code can serve as circumstantial evidence (Aravindakshan, 2020). However, proving the connection can be significantly easier if a state acknowledges the necessary nexus.

In this context, the recent proposal by the chairman of the Committee on Information Policy of the Parliament of the Russian Federation should be taken into account. According to this proposal, individuals acting in the interests of the state in the field of computers and the Internet could be exempt from both administrative and criminal liability (Sokolov & Lisitsyna, 2023). He also compared the destruction of an enemy firing point by conventional weapons with cyber ones, emphasizing that in both instances, "it is a war and when a soldier shoots back, he should not be responsible for the murder" (*Ibid*). Evidently, this call appears to be more of an incitement, which "entails state responsibility... only to the extent it amounts to direction and control" (Roscini, 2010, p.101). For definitive attribution, a state should publicly endorse the attacks.

In addition, such a statement can be seen not only as Russia acknowledging the link between the state and cyberattacks conducted by private individuals, but it also raises significant questions about the legal status of these individuals under international humanitarian law.

Concluding remarks

The lessons learned from the war in Ukraine suggest a growing likelihood of future conflicts incorporating a cyber component. Some scholars predict that cyberattacks could evolve into a pivotal instrument in these conflicts (Piella, 2022). Consequently, it is crucial to develop a suitable legal framework that accommodates the newly emerged phenomena of cyberspace. Given their potential for intimidation and destabilization, cyberattacks should be recognized alongside other forms of weaponry used to undermine the independence and integrity of a sovereign state.

Certainly, not every cyberattack can be classified as a use of force. Developing robust criteria is crucial. Given the specifics of the cyber industry, emphasis could be placed on a mixed target-effects approach, while considering factors such as scale, massiveness, intensity, long-lasting nature, type of attack, and various layers. The aforementioned criteria could serve as a foundation for formulating relevant legal regulations at both international and national levels. In this context, for instance, the provisions of the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (particularly, Art. 1) could be enhanced with a more detailed definition of cyberattacks and their categories, which would necessitate different response measures.

Therefore, we propose that the cyberattacks on Ukraine on 15 February 2022, along with subsequent incidents, should be classified as a use of force due to their significant invasive and military nature, as well as their connection to subsequent armed attacks employing conventional weapons, which constitutes a breach of international obligations. Although attributing legal responsibility for these actions is complex, it can be analysed through a variety of information sources, including both publicly accessible

and privately gathered data. As a result, the cyberattacks conducted even before 24 February 2022 can be regarded as internationally wrongful acts. This leads to the question of the responsibility of the Russian Federation for its actions and omissions, at least from 15 February 2022, when one of the largest cyberattacks in Ukraine's history occurred. The Government of Ukraine can adopt this stance in the post-war settlement regarding issues of reparations.

Therefore, Ukraine's experience with cyberwarfare offers valuable evidence that can contribute to the development of norms in various branches of international law, including the use of force, international responsibility, international humanitarian law, and international criminal law. The expanding state practice is anticipated to soon attain the requisite threshold for the establishment of pertinent customary law.

Acknowledgements

This paper and the research undertaken to prepare it would not have been possible without the exceptional support of my colleagues from the University of Cadiz (Spain), particularly Full Professor in International Law Alejandro del Valle Gálvez. Their enthusiasm and help have inspired me and kept my work on track from the very beginning to the final draft.

References

ALOUPI, N. (2015). "The Right to Non-intervention and Non-interference". *Cambridge International Law Journal*, vol. 4, no. 3, pp. 566-587. DOI: https://doi.org/10.7574/cjicl.04.03.566

ARAVINDAKSHAN, S. (2021). "Cyberattacks: a Look at Evidentiary Thresholds in International Law". *Indian Journal of International Law*, vol. 59, pp. 285-299. DOI: https://doi.org/10.1007/s40901-020-00113-0

AUSTRALIA (2021). *Australia's International Cyber and Critical Tech Engagement Strategy*. Department of Foreign Affairs and Trade, [online]. Available at: https://www.dfat.gov.au/sites/default/files/international-cyber-critical-technology-engagement-strategy-2021.pdf

BAEZNER, M. (2018, October). *Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict*. Version 2. Zürich: CSS, ETH.

BESSON, S. (ed.) (2022). *Theories of International Responsibility Law*. Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781009208550

CANADA (2022, April 22). *International Law Applicable in Cyberspace*. Government of Canada [online]. Available at: https://www.international.gc.ca/world-monde

CRAWFORD, J. (2006). "State Responsibility". *Max Planck Encyclopedia of Public International Law* [online]. Available at: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1093

CRAWFORD, J. et al. (eds.) (2010). *The Law of International Responsibility. Oxford Commentaries on International Law*. Oxford: Oxford Academic. DOI: https://doi.org/10.1093/law/9780199296972.001.0001

D'ASPREMONT, J. (2012). "The Articles on the Responsibility of International Organizations: Magnifying the Fissures in the Law of International Responsibility". *International Organizations Law Review*, vol. 9, no. 1, pp. 15-28. DOI: https://doi.org/10.1163/15723747-00901009

GREEN, J. A. (2011). "Questioning the Peremptory Status of the Prohibition of the Use of Force". *Michigan Journal of International Law*, no. 32, pp. 215-257.

DÖRR, O. (2019). "Use of Force, Prohibition of". *Max Planck Encyclopedia of Public International Law* [online]. Available at: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e427

EICHENSEHR, K. (2022). "Ukraine, Cyberattacks, and the Lessons for International Law". *AJIL Unbound*, no. 116, pp. 145-149. DOI: https://doi.org/10.1017/aju.2022.20

EU (2023). *The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict*. EP/EXPO/A/COMMITTEE/FWC/2019-01/Lot4/1/C/20 [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

FRANCE (2021). *International Law Applied to Operations in Cyberspace, Paper shared by France with the Open-ended Working Group established by Resolution 75/240*, [online]. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

GERMANY (2021, March). *On the Application of International Law in Cyberspace, the Federal Government of Germany* [online]. Available at: https://www.auswaertiges-amt.de

GOOGLE'S THREAT ANALYSIS GROUP (2023, February 16). "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape". *Google* [online]. Available at: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

HATHAWAY, O. A. et al. (2012). "The Law of Cyber-Attack". *California Law Review*, vol. 100, no. 4, pp. 817-885.

HELMERSEN, S.T. (2014). "The Prohibition of the Use of Force as Jus Cogens: Explaining Apparent Derogations". *Netherlands International Law Review*, vol. 61, no. 2, pp. 167-193. DOI: https://doi.org/10.1017/S0165070X14001168

HOPKINS, V. (2022, February 15). "Ukraine Says Cyberattack Was Largest in Its History". *The New York Times* [online]. Available at: https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html

HUNDER, M., LANDAY, J.; BERN, S. (2023, December 13). "Ukraine's Top Mobile Operator Hit by Biggest Cyberattack of War". *Reuters* [online]. Available at: https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

ILC (2001). «Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries». *Yearbook of the International Law Commission*, 2001, vol. II, Part Two [online]. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

ILC (2022). «Draft Conclusions on Identification and Legal Consequences of Peremptory Norms of General International Law (Jus Cogens)». *Yearbook of the International Law Commission*, 2022, vol. II, Part Two [online]. Available at: https://legal.un.org/ilc/texts/instruments/english/draft_articles/1_14_2022.pdf

ICJ (1996). "Legality of the Threat or Use of Nuclear Weapons". Advisory Opinion of 8 July 1996. *I.C.J. Reports*, p.226.

JAMNEJAD, M., WOOD, M. (2009). "The Principle of Non-intervention". *Leiden Journal of International Law*, vol. 22, no. 2, pp. 345-381. DOI: https://doi.org/10.1017/S0922156509005858

KNAPCZYK, P. (2022, August 18). "Overview of the Cyber Weapons Used in the Ukraine – Russia War". *Trustwave* [online]. Available at: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

KULESZA, J. (2009). "State Responsibility for Cyber- Attacks on International Peace and Security". *Polish Yearbook of International Law*, no. 29, pp. 139-152.

KUMAR, S.; DALAL, S.; DIXIT, V. (2014). "The OSI Model: Overview on the Seven Layers of Computer Networks". *International Journal of Computer Science and Informational Technologies Research*, vol. 2, no. 3, pp. 461-466.

LENG, Y. (2023). "When Can Cyberattack Constitute Use of Force: A Case Study of Cyberattack in the Russia-Ukraine". *Conflict Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries*, pp.201-207. DOI: https://doi.org/10.54254/2753-7048/17/20231249

LIN, H. (2022, fall). "Russian Cyber Operations in the Invasion of Ukraine". *The Cyber Defense Review*, pp. 31-45.

LONERGAN, E.D. (2023). "The Implications of Cyber Proxies in the Ukraine Conflict". In: J. A. Lewis, G. Wood (eds.). *Evolving Cyber Operations and Capabilities Report*, pp. 5-14. Washington: Center for Strategic and International Studies.

LYNGAAS, S.; LISTER, T. (2022, February 15). "Cyberattack Hits Websites of Ukraine Defense Ministry and Armed Forces". *CNN* [online]. Available at: https://edition.cnn.com/2022/02/15/world/ukraine-cyberattack-intl/index.html

MADUBUIKE-EKWE, J. N. (2021). "Cyberattack and the Use of Force in International Law". *Beijing Law Review*, no. 12, pp. 631-649. DOI: https://doi.org/10.4236/blr.2021.122034

MORRIS, E. (2021, February 17). "DoS vs. DDoS: Which Attack Is More Dangerous and Why?". *Cybrary* [online]. Available at: https://www.cybrary.it/blog/dos-vs-ddos-which-attack-is-more-dangerous-and-why/

MOYNIHAN, H. (2021). "The Vital Role of International Law in the Framework for Responsible State Behavior in Cyberspace". *Journal of Cyber Policy*, vol. 6, no. 3, pp. 394-410. DOI: https://doi.org/10.1080/23738871.2020.1832550

MUELLER, G. B. et al. (2023) "Cyber Operations during the Russo-Ukrainian War from Strange Patterns to Alternative Futures". *Center for Strategic and International Studies* [online]. Available at: https://www.jstor.org/stable/pdf/resrep52130.pdf

NIHREIEVA, O. (2022). "The 2022 Russian Invasion of Ukraine through the Prism of International Law: a Critical Overview". *Peace & Security*, no. 10. DOI http://dx.doi.org/10.25267/Paix_secur_int.2021.i10.1203

OORSPRONG, F.; DUCHEINE, P.; PIJPERS, P. (2023). "Cyber-Attacks and the Right of Self-Defense: A Case Study of the Netherlands". *Policy Design and Practice*, vol. 6, no. 2, pp. 217-239. DOI: https://doi.org/10.1080/25741292.2023.2179955

PÉREZ SIERRA, I. (2021). "La legítima defensa del Estado frente a ataques cibernéticos según el Derecho internacional". *Global Strategy Report* [online], no. 25. Available at: https://global-strategy.org/la-legitima-defensa-del-estado-frente-a-ataques-ciberneticos-segun-el-derecho-internacional/

PIELLA, G.C. (ed.) (2022). *La guerra de Ucrania. Los 100 días que cambiaron Europa*. Madrid: Catarata.

POIREAULT, K. (2023, September 27). "Cyber-Attacks on Ukraine Surge 123%, but Success Rates Plummet". *Infosecurity Magazine* [online]. Available at: https://www.infosecurity-magazine.com/news/cyberattacks-ukraine-surge-success/

ROSCINI, M. (2007). "Threats of Armed Force and Contemporary International Law". *Netherlands International Law Review*, no. 54, pp. 229-277. DOI: https://doi.org/10.1017/S0165070X0700229X

ROSCINI, M. (2010). "World Wide Warfare – Jus ad bellum and the Use of Cyber Force". *Max Planck Yearbook of United Nations Law*, no.14, pp. 85-130. DOI: https://doi.org/10.1163/18757413-90000050

ROSCINI, M. (2024). *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*. Oxford: Oxford Academic. DOI: https://doi.org/10.1093/oso/9780198786894.001.0001

SHACKELFORD, S. (2010). "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem". In: C. Crosseck & K. Podins (eds.). *Conference on Cyber Conflict: Proceedings 2010*, pp. 198-208. Tallinn: CCD COE Publications.

SCHMITT, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781316822524

SCHMITT, M. (2019, October 14). "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis". *Just Security* [online]. Available at: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

SOKOLOV, K.; LISITSYNA, M. (2023, February 10). "In Russia They Proposed to Exempt 'White Hackers' from Responsibility". *RBC* [online]. Available at: https://www.rbc.ru/politics/10/02/2023/63e640ff9a7947218b188cf5

STOCKBURGER, P. Z. (2017). "Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents". In: H. Rõigas, R. Jakschis, L. Lindström and T. Minárik (eds.). *9th International Conference on Cyber Conflict: Defending the Core*, pp. 149-162. Tallinn: NATO CCD COE Publications. DOI: https://doi.org/10.23919/CYCON.2017.8240334

TSAGOURIAS, N. (2022). "Cyber Attacks, Self-Defense and the Problem of Attribution". *Journal of Conflict and Security Law*, vol. 17, no. 2, pp. 229-244. DOI: https://doi.org/10.1093/jcsl/krs019

UK (2021, June 3). *Application of International Law to States' Conduct in Cyberspace: UK Statement*, Policy paper [online]. Available at: https://www.gov.uk/government/publications

UK NATIONAL CYBER SECURITY CENTRE (2018, April 11). "New Cyber Attack Categorization System to Improve UK Response to Incidents".

UN (2018). *Advancing Responsible State Behavior in Cyberspace in the Context of International Security*, *Resolution of the General Assembly* No. A/RES/73/266 [online]. Available at: https://digitallibrary.un.org/record/1658328?v=pdf

UN (2021). *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266*, Resolution of the UN General Assembly, A/76/136.

VINHAS DE SOUZA, O. (2024). "Russia's Invasion of Ukraine and National Cyber Security Strategies: Quantitative Comparison". *Applied Cybersecurity & Internet Governance*, vol. 3, no. 1, pp. 261-271. DOI: https://doi.org/10.60097/ACIG/190346

VOO, J. (2023). "Lessons from Ukraine's Cyber Defense and Implications for Future Conflict". In: J. A. Lewis, G. Wood (eds.). *Evolving Cyber Operations and Capabilities Report*, pp. 15-22. Washington: Center for Strategic and International Studies.

Recommended citation

Olena Nihreieva (2025). "State responsibility for cyberattacks as a use of force in the context of the 2022 Russian invasion of Ukraine". *IDP. Internet, Law and Politics Journal*, no. 42. UOC [Accessed: dd/mm/yy]. DOI: http://dx.doi.org/10.7238/idp.v0i42.430724

About the authors

Olena Nihreieva
University of Cadiz. University of Odesa
olena.nihreieva@uca.es

Visiting Professor at the University of Cadiz (Spain) (2022 – 2024). Associate Professor in International Law, Odesa Mechnikov National University (Ukraine). Currently, her research focuses on the issues relating to International Humanitarian Law and International Internet Law. Other fields of her scientific interest are international lawmaking and enforcement, particularly within the field of International Economic Law. She has also conducted studies of Maritime Law, and her PhD thesis is dedicated to *Legal Regulations of Ship Mortgage*. She has been publishing in English, Ukrainian and Russian. Recent works include: *Legality of Economic Sanctions as a Means of International Obligations Enforcement* (2024); *The Law of Ukraine "On Virtual Assets" in the Context of the FATF Standards National Implementation* (2023); *2022 Russian Invasion of Ukraine through the Prism of International Law: a Critical Overview* (2022) and *Categorising UK cyber incidents* (2023).