

A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War

Ahmad Khalil

School of Law
Vellore Institute of Technology, VIT University
Kelambakkam road
Chennai 600127, Tamil Nadu, India
ahmadkhalil5665@gmail.com

Mohammad Bitar

School of Law, VIT-AP University
Beside AP Secretariat
Andhra Pradesh 522237, India
bitar.20phd7068@vitap.ac.in

S. Anandha Krishna Raj

School of Law
Vellore Institute of Technology, VIT University
Kelambakkam road
Chennai 600127, Tamil Nadu, India
anandha.krishnaraj@vit.ac.in

Abstract: The use of cyber operations in armed conflicts has become a reality, with several states openly admitting to being involved in such activities. An increasing number of nations are developing military cyber capabilities, and the use of these operations is expected to rise. Advancements in offensive cyber capabilities have demonstrated that these operations can significantly impact civilian infrastructure and cause harm to humans. This study explores the complex application of international humanitarian law (IHL) to cyber warfare, focusing on the evolving roles of both state and non-state actors. It examines the difficulties in distinguishing between combatants and non-combatants in the light of the concept of direct participation in hostilities during cyberattacks. Furthermore, this paper examines the responsibilities and legal

consequences for states that direct or control non-state actors and the need to adapt IHL to the specific nature of cyber conflicts. It underscores the crucial need for strong legal frameworks to protect civilians and uphold humanitarian principles in the digital era. This study employs cyberattacks which occurred during the Russian-Ukraine armed conflict as a case study.

Keywords: *cyberattacks, international humanitarian law, non-state actors, responsibility, Russia-Ukraine armed conflict*

1. Introduction

The incorporation of cyberspace into contemporary warfare has ushered in a new era of conflict, necessitating a comprehensive evaluation of how international humanitarian law (IHL) pertains to cyber operations. As the fifth domain of warfare, alongside land, sea, air, and space, cyberspace presents unique challenges and opportunities for both state and non-state actors. It is crucial to adapt existing legal frameworks, such as IHL, to ensure that humanitarian principles and legal restrictions remain paramount in this new battlefield. With the growing recognition of the relevance of IHL to cyber operations from states and international organizations, it is essential to refine these regulations to protect civilians and infrastructure from the severe consequences of cyber warfare (Sohail, 2022). A key aspect of IHL is the principle of distinction, which requires conflict parties to differentiate between combatants and non-combatants as well as target only legitimate military objectives. However, the increasingly blurred lines between civilians and combatants, particularly with the advent of cyber warfare, complicate this principle. Furthermore, the involvement of non-state actors in cyber hostilities challenges the traditional concepts of direct participation in hostilities, necessitating a more nuanced approach to civilian protection in the digital age.

Actors that are non-state, ranging from individual hackers to organized groups, occupy a significant role in cyber warfare. These actors, motivated by economic, political, ideological, or religious considerations, might operate independently or under the direction of a state, often blurring the lines of accountability and responsibility (Sigholm, 2013). The virtual and anonymous nature of cyberspace makes it difficult to determine the source of cyberattacks, presenting important questions about the responsibilities

of states and the legal implications of employing non-state actors as proxies in cyber conflicts.

State responsibility for the actions of non-state actors in cyberspace presents a complex challenge, intricately linked to international law principles and the difficulties of attributing actions in the digital world. The use of non-state actors for cyber operations by states may offer advantages in terms of expertise and evading direct accountability (Sheraz, 2021). However, this practice raises significant legal and ethical issues, particularly concerning the control and direction of these actors and ensuring their compliance with IHL.

As warfare is increasingly shifting to the digital domain, the application of IHL to cyber operations remains a critical concern (Gisel, Rodenhäuser & Dörmann, 2020). Upholding the principles of humanity and legal constraints in cyber warfare is essential for maintaining the integrity of international law and protecting civilians in the continually evolving landscape of modern conflict.

2. Applying IHL to cyber warfare

IHL is a well-established framework that also applies to cyber operations during armed conflicts, as affirmed by the International Committee of the Red Cross (ICRC). This body of law regulates all forms of warfare, whether the methods and means employed are traditional or innovative (ICRC, 2011, p. 36). Cyberspace, recognized as the fifth domain of warfare alongside land, sea, air, and space, is subject to the same legal constraints as the other domains, despite its distinct features. When states adopt IHL treaties, they aim to regulate both current and future conflicts. This foresight is reflected in provisions like Article 36 of the 1977 Additional Protocol (AP I), which requires the review of new weapons, means, and methods of warfare to ensure they comply with existing IHL (Tsybulenko & Kajander, 2022). This demonstrates the adaptability of IHL to new technologies, as confirmed by the International Court of Justice (ICJ) in its 1996 Advisory Opinion on nuclear weapons (1996, para. 86), which states that IHL applies to all forms of warfare and weapons, including future developments. The ICRC extends this principle to cyber operations, asserting that such activities during armed conflicts must adhere to IHL.

The recognition of the applicability of IHL to cyber operations is a constructive move. Nevertheless, the ICRC encourages the refinement of these regulations to more effectively safeguard civilians and civilian infrastructure from the repercussions of cyber warfare. It is important that forthcoming rules bolster and fortify the existing IHL framework. When situations are not explicitly covered by IHL, the Martens Clause offers protection, guaranteeing that individuals, regardless of their status as civilians or combatants, are subject to principles of international law that are derived from custom, humanity, and public conscience.

Asserting that IHL extends to cyber operations does not signify that cyber warfare is sanctioned or that the militarization of cyberspace is endorsed. Instead, it imposes constraints on the development of military cyber capabilities that could violate IHL principles, as highlighted by Henckaerts (2009). The use of force, whether in cyberspace or in traditional warfare, must comply with the United Nations Charter (1945) and customary international law, which emphasize the peaceful resolution of international disputes (Lawand, 2006).

All states are duty-bound to systematically evaluate the legality of new weapons, tactics, and methods of warfare. This obligation arises from the fundamental prohibition against employing illegal means of warfare (Lawand, 2006) and the responsibility to ensure respect for IHL (ICRC, 2019). For states party to Additional Protocol I, Article 36 explicitly mandates such evaluations during the study, development, procurement, or adoption of new weapons. This requirement, which some contend is part of customary international law, underscores the importance of determining whether the use of a new weapon would be banned under IHL or any other applicable international law (AP I, 1977, Art. 36).

The evaluation of the legality of a weapon under IHL must be based on specific rules that apply to the state, which can be either treaty-based or customary IHL (Lawand, 2006). The Martens Clause emphasizes the importance of considering the principles of humanity and public conscience when making these assessments. Although the necessity for a formal legal review is debated, conducting such reviews at the earliest stages of weapon development is crucial for ensuring compliance with IHL and avoiding the potential consequences of deploying prohibited weapons (Wallace, 2018). The legality of a weapon under IHL must be determined by considering the specific rules applicable to the state, regardless of whether it is novel or relies on new technology (Brown & Metcalf, 2014). Although the classification of

a “cyber weapon” is not unequivocally established (Brown & Metcalf, 2014), any tool capable of executing attacks, as defined in IHL, should be considered within its scope (AP I, 1977, Art. 49). For states that have ratified AP I, this obligation extends to the early stages of researching and developing cyber capabilities. These states must undertake legal evaluations that take into account the full range of international law, not just IHL (Lawand, 2006).

In evaluating the legality of novel weapons, states must initially determine whether their use is explicitly prohibited or restricted by IHL. Despite the absence of specific limitations on cyber capabilities at present, future developments, such as cyber arms control agreements, may impose binding restrictions. If no specific restrictions apply, the assessment must then consider general IHL prohibitions, including those against weapons that inflict unnecessary suffering or employ indiscriminate methods of warfare (Lawand, 2006). The intended use of the weapon on the battlefield must also be evaluated to determine whether its deployment would be restricted in any or all circumstances (Lawand, 2006).

In conclusion, incorporating IHL into cyber operations during armed conflicts ensures that the principles of humanity and legal constraints remain paramount, regardless of technological advancements in warfare. This approach not only upholds the integrity of international law but also promotes the protection of civilians and the peaceful resolution of conflicts.

3. Cyber warfare and the concept of direct participation in hostilities

IHL includes a fundamental principle known as distinction, which requires conflict parties to consistently differentiate between combatants and non-combatants, targeting only combatants. Despite the aim of IHL to protect civilian populations, modern conflicts often blur this distinction. Many of today’s conflicts are non-international, involving government forces, organized armed groups, or clashes between such groups within a state. Consequently, hostilities frequently occur in civilian-populated areas, increasing civilian involvement in conflicts. Additionally, the rise of cyber warfare has further enabled civilian participation in hostilities.

The concept of direct participation in hostilities is crucial in IHL, as specified in Article 51(3) of Additional Protocol I (AP I) and Article

13(3) of Additional Protocol II (AP II) to the Geneva Conventions. These articles state that civilians are protected from attacks unless they directly participate in hostilities, but they do not clearly define what constitutes direct participation. Instead, they outline the conditions under which civilians lose their protection. Although not all nations have ratified these protocols, certain provisions are recognized as customary IHL, as detailed in the ICRC's study on Customary IHL (ICRC, 2024). Rule 6 of this study aligns with the principles of AP I and AP II and emphasizes the absence of a clear definition of direct participation in hostilities. Additionally, the ICRC's 2009 *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* and the 2013 *Tallinn Manual* by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) explore the legal implications for civilians involved in hostilities.

In 2003, the ICRC launched a research initiative to elucidate the notion of direct participation in hostilities (DPH) under IHL. This work culminated in the publication of the *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* in 2009. Although this non-binding document has generated controversy, it has been acknowledged for enhancing comprehension of DPH. The Guidance presents ten recommendations for interpreting IHL in relation to DPH, addressing topics such as the classification of civilians in both international and non-international armed conflicts, the role of private contractors, the actions that constitute direct participation in hostilities, and the duration for which protection is forfeited.

The ICRC distinguishes between civilians in international and non-international armed conflicts. In international conflicts, civilians are defined as individuals who are neither members of the armed forces nor participants in a *levée en masse*, as outlined in Articles 50 and 51(3) of Additional Protocol I. In non-international conflicts, civilians encompass anyone not affiliated with state armed forces or organized armed groups associated with a conflict party. Organized armed groups are identified by the persistent combat function of their members, which means that those who regularly engage in hostilities can be targeted at any time (Melzer, 2009).

The main goal of continuous combat function is to differentiate between armed group combatants and civilians who occasionally engage in hostilities. Civilians are typically protected under IHL, but they may lose this protection if they take part in hostilities directly. On the other hand, individuals who have a continuous combat function within organized armed groups can be

lawfully targeted at any moment. This distinction does not apply to supporters of organized armed groups who do not directly participate in hostilities. The *Tallinn Manual* does not explicitly define civilians in the context of cyber hostilities, but it aligns with the ICRC perspective that civilians involved in cyber operations lose their protection during their active involvement. The principle of distinction in IHL is also applicable to cyberattacks, ensuring that civilians are not unlawfully targeted.

The ICRC defines three main requirements for determining direct participation in hostilities: the threshold of harm, direct causation, and belligerent nexus. The threshold of harm signifies that the action must likely have an impact on military operations or lead to the death, injury, or destruction of protected individuals or objects. Direct causation necessitates a clear connection between the action and the resulting harm. Belligerent nexus mandates that the action benefits one party to the conflict while inflicting harm on another. The *Tallinn Manual* generally agrees with these criteria but places greater emphasis on the intention behind the action rather than the probability of harm and recognizes that harm may not always be physical in nature.

There is ongoing debate about the beginning and end of direct participation in hostilities (Henckaerts, 2007, p. 17). The ICRC considers preparatory measures and deployment to and from an act of direct participation as part of direct participation in hostilities (Schmitt, 2013), while the *Tallinn Manual* includes actions immediately before or after the act as well. Regarding the temporal scope of losing protection, the ICRC distinguishes between civilians who occasionally participate in hostilities and those with a continuous combat function (Melzer, 2009). Sporadic participants lose their protected status only during specific acts of participation, whereas individuals with a continuous combat function are always considered targetable. This distinction, often referred to as the “revolving door” concept, is controversial, especially in cyber operations where the timing and effects of participation can be brief and delayed, posing challenges for the application of IHL (Kilovaty, 2016).

In summary, the ICRC’s Guidance and the *Tallinn Manual* offer critical insights into direct participation in hostilities, though differences remain. The detailed recommendations of the ICRC and the practical applications in the *Tallinn Manual* contribute significantly to understanding and implementing IHL in both traditional and cyber contexts, aiming to protect civilians while recognizing the complexities of modern warfare.

4. Non-state actors in the context of cyber warfare

The introduction of personal computers greatly expanded the use and programming of digital technologies, which were previously only accessible to specialists. This democratization allowed a wider range of people to learn programming for various purposes, some of which were legitimate and others illicit. The connectivity revolution of the 1990s further enhanced this trend by creating a virtual network that connected digital systems, thereby increasing the reach and potential danger of cyberattacks and amplifying their transnational nature. As a result, a range of targets, including private companies, state infrastructure, the military, and government nerve centres, became vulnerable to attacks from hackers, criminal organizations, terrorists, and foreign authorities. With crime and political/ideological conflicts shifting to cyberspace, individuals and groups took advantage of the internet's ability to compress time and distance, provide anonymity, and operate with minimal regulation. This facilitated illegal activities against private citizens, corporations, states, and international institutions, driven by economic, political, or ideological motivations (McGinn, 1991).

Recently, the battlefield has increasingly moved to digital realms, with both state forces and violent non-state entities extending their operations online. The Georgian cyberattacks are a prime example of the significant participation of non-state actors in cyber warfare, demonstrating their capacity to engage in cyber conflicts either alongside or against state actors (Shakarian, 2011). The unique traits of the virtual world, including its altered sense of time and space, accessibility, geographical dispersion, technological availability, and lack of hierarchical structures, have contributed to the emergence of a new, flattened international political landscape. In this new structure, asymmetric actor relationships appear more balanced, potentially signifying a shift from a state-centric political system to post-international politics, as suggested by van Creveld. This evolution may also hint at the possible decline of Clausewitz's trinitarian model of war, which traditionally involves the people, the army, and the government (van Creveld, 2009).

The range of non-state actors in cyberspace, capable of executing digital force or conducting cyber military operations, is extensive. These entities can come in various forms, from small, informal groups to large, multinational organizations with intricate structures. Their motivations can be attributed to economic, political, ideological, or religious reasons, and their objectives are not always solely military in nature (Czosseck & Ziolkowski, 2013).

These actors may be directed or backed by states, or they may operate independently without any state affiliation. Hackers, in particular, can be valuable assets to states, as they can offer technical expertise and critical information, such as identifying software vulnerabilities. States may utilize hackers for specific cyber operations or purchase information about vulnerabilities that hold significant economic and military value.

Criminal groups have been drawn to the potential profits of cybercrime and have flourished in the digital world (Choo, 2008). These organizations are often structured in a formal and hierarchical manner and engage with the state through economic relationships (Luban *et al.*, 2018). Their efficient operational processes and access to necessary technology make them highly effective in cyber situations. This effectiveness is demonstrated by their alleged involvement, with state support, in cyberattacks during the Russia-Georgia conflict in 2008 and against Kyrgyzstan in 2009 (Shakarian, 2011).

4.1 Participation of NSAs in cyber warfare

The classification of hackers, whether they operate individually or as part of a group, as lawful or unlawful combatants, is a significant aspect of the *jus in bello* categories in armed conflicts. IHL distinguishes between fighters and civilians among those involved in an armed conflict, making it essential to identify lawful and unlawful combatants (AP I, 1977, Art. 43). Participants in armed conflicts, whether through physical or digital means, face specific legal consequences.

In international armed conflict, individuals who hold official combat roles in the armed forces of a belligerent party are considered lawful combatants. These individuals can be lawfully targeted and are entitled to combatant immunity and prisoner-of-war status (Ipsen, 2008). This status also extends to members of groups assimilated into the state's official military forces. According to Article 4A(2) of the Third Geneva Convention, which reflects customary international law, members of militias or volunteer corps, including those of organized resistance movements, belonging to a party to the conflict, are considered combatants if they meet four conditions (Schmitt, 2013). These criteria are: being under the command of a responsible person, wearing a visible and distinctive emblem, carrying arms openly, and complying with the laws and customs of war (Khalil & Raj, 2024). These standards ensure that all parties involved in the conflict adhere to established norms of lawful competency, as outlined in the Geneva Convention III of 1949 (Art. 4).

Civilians who are not part of the armed forces or groups associated with them are protected from the dangers and consequences of war by the law of armed conflict (Bitar & Chakka, 2023). Nevertheless, if they actively participate in hostilities, even by using digital weapons, they lose their non-combatant immunity and can be legitimately targeted (Prescott, 2012).

4.2 The level of organization of NSAs involved in cyber warfare

Hacking groups generally congregate in virtual spaces where they communicate, share information, and make decisions. This virtual setting impacts their internal organization and clashes with the rules of war designed for traditional military units. A strong internal structure is essential for maintaining discipline and complying with the laws of war, which is crucial for gaining combatant status in international armed conflicts. Articles 43(I) of AP I and 4 A(2) of the Third Geneva Convention emphasize the significance of internal discipline and adherence to laws of war for combatant status.

The difference between international and non-international conflicts depends on the organizational structure of the parties involved (Khalil & Raj, 2024). For non-state actors to be covered by IHL, they must show a particular level of structured organization and the capability to carry out extended and coordinated military operations (*Prosecutor v. Boskoski and Tarculovski* [2008], para. 250), as outlined in Article 1 of AP II.

The capacity of digital groups to meet these structural requirements is uncertain. Effective coordination and a hierarchical command structure are necessary for these groups to function cohesively and comply with IHL (*The Prosecutor v. Fatmir Limaj* [2005]). However, the nature of cyber warfare complicates adherence to these rules. Hackers, who often lack military training, might not fully understand the context of their actions, and the absence of visible consequences can reduce moral restraints (Loshin, 2013). Moreover, the anonymity provided by the internet and the protection offered by states makes prosecuting hackers challenging.

Different categories of hacker groups exhibit varying levels of organization. Criminal organizations and cyber mercenaries typically have hierarchical and stable structures that enable coordinated military operations. On the other hand, patriotic hackers and hacktivists generally have more informal and fluid structures, which can impede unified action and compliance with IHL.

Larger hacker groups often lack a clear hierarchical structure, usually organizing around administrators and affiliated users. The administrators manage the platform and provide direction, but actual actions are typically decided through ad-hoc discussions among members (Khalil, Bitar & Raj, 2024). This decentralized decision-making process and lack of strict internal discipline hinder the group's ability to comply with IHL (Rege-Patwardhan, 2009).

The absence of a formal command and control structure means that hacker groups often cannot prevent individual rogue actions, reducing accountability and compliance with IHL. Consequently, such groups, even when directed by a state, are more likely to be classified as civilians participating directly in hostilities rather than as combatants in international conflicts. This structural deficiency also excludes them from being recognized as parties to non-international conflicts under IHL.

5. State responsibility for the act of NSAs in the context of cyber warfare

States might be motivated to collaborate with or back non-state actors as irregular forces in cyber warfare. The expertise of skilled hackers enables states to carry out or prepare for cyberattacks or defences competently. Hackers can serve as a cost-effective asset due to their expertise, proficiency, and access to technology. Engaging in cyberattacks typically requires minimal experience and equipment, such as a computer and basic internet skills. Hence, non-state actors can quickly assemble a low-cost, easily mobilized cyber army for "crowdsourced" assaults. By harnessing this extensive pool of technologically adept individuals, states can target adversaries while circumventing the political, legal, and military challenges of attribution. The difficulty in tracing attacks back to the state complicates establishing substantial involvement (Loshin, 2013). Furthermore, obfuscation techniques and botnets can further obscure the origin of the attack, potentially evading legal and political consequences.

Utilizing hacker groups as instruments in cyber warfare poses significant challenges, such as difficulty in controlling or halting their actions and the risk of them exceeding their boundaries by targeting unauthorized objectives. This may lead to violation of IHL. However, states may view this lack of adherence to military protocols and humanitarian laws as advantageous,

as non-state actors can operate in cyberspace without being bound by rules and limitations of IHL (Khalil & Raj, 2023). The nature of the attack, the character of the conflict, and the political and legal responsibilities, including the potential for a military response in self-defence, are all dependent on the extent of the relationship between the non-state actor and the state.

Under the international legal framework, the actions of state entities, whether formally acknowledged (*de jure*) or effectively controlled (*de facto*) by the state, are ascribed to the state (ARSIWA, 2001, Art.1). *De jure* state entities, which are recognized by their domestic laws, act on behalf of the state (*Bosnia-Herzegovina v. Yugoslavia* [1996], para. 386). Additionally, if an entity is entirely reliant on and controlled by the state, it is considered *de facto* a state entity, and its actions are ascribed to the state (Bitar & Chakka, 2024). International case law establishes a strict control threshold, requiring that the entity must be entirely reliant on the state for this relationship to be recognized. Any degree of independence disqualifies such a relationship, making it unlikely that hacker groups not officially or covertly integrated into the armed forces, and lacking a sufficient hierarchical structure for strict control, would meet this threshold (Applegate, 2011).

As per Article 8 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA, 2001), which embodies customary international law, the actions of an individual or group are deemed to be those of a state under international law if they act on the instructions or under the direction or control of that state. This implies that individuals or groups not formally part of state structures but operating under state instructions or control are considered state actors. The state's influence must extend to specific tasks or operations, attributing their conduct to the state (*Prosecutor v. Dusko Tadic* [1999], para. 116). The control criterion can encompass a broader relationship between the state and the group. Although non-state actors may not be entirely reliant on the state, they are still subject to its control. The strict "effective control" standard is set by the ICJ case law, where state control is demonstrated through specific operations. In contrast, the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the *Tadic* case suggested a less stringent "overall control" standard for organized and hierarchically structured groups (*Prosecutor v. Dusko Tadic* [1999], para. 131), which involves general state control over the group, not necessarily linked to specific acts.

The ICTY and ICJ differentiate between structured groups and individuals when it comes to determining responsibility. For organized groups, the

ICTY and ICJ require evidence of state control through coordination and assistance in planning. Mere financing or equipping of the group is not enough for attribution (*Prosecutor v. Dusko Tadic* [1999], para.175). The “overall control” criterion has been criticized for linking state conduct too closely to international responsibility (*Bosnia-Herzegovina v. Yugoslavia* [1996], para. 385). For less structured groups and individuals, the ICTY and ICJ apply an “effective control” test, which requires evidence of state instructions for specific actions. The ICTY requires some measure of state authority and specific instructions or public endorsement of the acts, while the ICJ requires state direction or enforcement of the acts. Establishing a close relationship with the group’s higher administrative level is crucial for attribution, but direct control over individual actions remains challenging.

Identifying the state-sponsored cyber activities of non-state actors is a daunting task due to the opaque nature of the internet and the unstable state of digital evidence. It is challenging to prove state involvement or even identify the source of an attack. The digital instructions or evidence of state control can be easily deleted or modified, further complicating traceability, especially given the transnational nature of cyberattacks and the use of obfuscation techniques. The targeted state may require cooperation from countries where the attack originated, traversed, or where the physical devices used in the attack are located. This can be especially difficult if assistance is needed from the state that sponsored the attack. For instance, after the 2007 cyberattacks on its infrastructure, Estonia sought help from Russia to trace the attack’s origin, but Russia declined, despite an existing bilateral legal assistance treaty (Hollis, 2007).

Promptly detecting the origin and character of a cyber assault is of utmost importance since these occurrences can propagate swiftly in the digital domain and have a rapid impact on the intended recipient. Ascribing the conduct of a non-state entity to a sovereign state is vital for evaluating the political and legal repercussions, such as the exercise of the right to self-defence.

6. Cyber warfare between Russia and Ukraine

Russia is alleged to have a lengthy and storied past in the realm of cyber warfare, encompassing both standalone assaults and preparatory attacks for the kinetic armed conflicts. Individuals or groups responsible for cyber

assaults are typically linked to Russian intelligence. However, it is important to recognize that Russia refutes any claims regarding this matter. Below we will review the most important historical events of cyberattacks which were allegedly attributed to Russia.

In the spring of 2007, Estonia faced a prolonged and coordinated cyberattack that lasted for three weeks. During this time, a range of entities, including governmental and parliamentary websites, ministries, media outlets, internet service providers, major banks, and small businesses, were targeted. The attackers primarily employed a Distributed Denial of Service (DDoS) method. This cyber offensive coincided with the Estonian government's decision to relocate the Bronze Soldier memorial from Tallinn, which led to significant civil unrest in both Estonia and Russia (*The Economist*, 2010; Traynor, 2007).

A significant volume of malicious network activity has been traced back to sources using the Russian language (Tsybulenko & Kelichavyi, 2018). Despite the Russian government's denial of involvement, these cyberattacks coincided with hostile political rhetoric from Russian officials, adverse economic measures, and a lack of cooperation with the Estonian investigation, potentially encouraging the attackers (Tsybulenko & Francis, 2018). The cyber assaults caused considerable disruption and economic damage in Estonia, with evidence pointing to political motivations behind the attacks. On July 20, 2008, a series of DDoS attacks took the website of Georgian President Saakashvili offline for twenty-four hours. The websites of the National Bank of Georgia and the Georgian parliament were also compromised, defaced with images of Saakashvili and Hitler. Numerous Georgian government servers were targeted and incapacitated, disrupting communication and the dissemination of vital information. This incident was the first recorded case of cyberattacks occurring alongside armed conflict, as highlighted by technical experts (Hart, 2008). The US Cyber Consequences Unit, a US-based research institute, reported that the attacks had "little or no direct involvement from the Russian government or military." They concluded that several attacks originated from computers in Russia, Ukraine, and Latvia, and were carried out by multiple users who voluntarily participated in cyber warfare in support of Russia during the 2008 South Ossetia war. (Gorman, 2009)

Initially, Russia's cyber activities were primarily focused on political warfare and espionage, particularly during operations in Estonia and Georgia. Prior to its military campaign to disrupt Ukraine's critical infrastructure,

Russia targeted Ukraine's power supply with cyber operations (Tsybulenko & Platonova, 2019). Following the illegal annexation of Crimea in 2014, advanced persistent threat (APT) groups like Sandworm were linked to the 2015 BlackEnergy campaign, which targeted Ukrainian power generation and distribution systems (Bingham, 2018). In 2017, Russian-linked groups launched the NotPetya campaign, causing widespread disruptions that extended beyond Ukrainian companies and impacted global logistics (Dhelie *et al.*, 2023).

At the start of the conflict between Russia and Ukraine in 2022, there was a notable increase in cyber operations. However, this upswing did not result in substantial changes in the intensity, techniques, or preferred targets of the attacks. Despite the heightened activity, Russia did not make significant concessions or launch severe cyberattacks. Before the ground war, Russia deployed malware that disrupted the Viasat satellite system, causing a temporary loss of over 30,000 internet connections across Europe, including 5,000 wind turbines (O'Neill, 2022). Since the conflict began, Russia has persistently aimed to weaken Ukraine's command-and-control systems. According to SpaceX management, the company's Starlink network has successfully withstood multiple cyberattacks from Russia since its deployment in Ukraine (Browne, 2022). Additionally, reports suggest that Russian cyber operations have attempted to infiltrate Delta, a targeting fusion software for a specialized Ukrainian military intelligence (Giles, 2023).

The largest cyberattack of the previous year was the assault on Kyivstar in December. As a prominent mobile provider in Ukraine, Kyivstar offers vital services across the country, spanning major cities and remote regions, catering to 24.3 million mobile subscribers and 1.1 million home internet users. It is crucial for numerous state and commercial organizations. The cyberattack caused the destruction of Kyivstar's core systems, affecting 24 million users over several days (Broekstra, 2024). Adam Meyers, head of Counter Adversary Operations at CrowdStrike, pointed out that "the attack coincided with several significant disruptions in Ukraine, such as malfunctioning air raid sirens in Kyiv, disrupted payment terminals and banks, and issues with public transportation payments" (Collins, 2024).

The chief executive officer of Kyivstar and the Ukrainian Security Service (SBU) speculated that the attack was orchestrated by Russian hackers. The Solntsepek group, which is linked to the Sandworm group, claimed responsibility for the attack, reporting to have damaged 10,000 computers,

4,000 servers, and all cloud storage and backup systems. The group stated that Kyivstar was targeted because it provided communication services to the Ukrainian Armed Forces and various government agencies. Illia Vitiyuk, head of the cybersecurity department at the Ukrainian Security Service, disclosed critical details about the hack, asserting that it caused significant harm and was intended to deliver a psychological blow while gathering intelligence.

Sandworm, a notable state-sponsored advanced persistent threat group, boasts an extensive record of conducting cyberattacks on Ukraine. Their portfolio encompasses attempts to meddle with the 2014 elections' outcome by targeting the Ukrainian Central Election Commission (Ancell, 2024). Furthermore, the group is notorious for orchestrating the first-ever blackout caused by hackers in the Ukrainian power grid, which left roughly 260,000 individuals without electricity in October 2022 (Ancell, 2024).

It is widely claimed that entities affiliated with the Russian government conduct assaults on military data and infrastructure. Given the interconnected nature of networks, it is difficult to determine whether attacked individuals are directly actively engaged in hostility. The assault on Kyivstar exemplified this issue, affecting 23 million subscribers by denying them internet access.

Vitiyuk said, “[c]yberattack on Kyivstar was a sophisticated operation and has been frequently referred to as one of the most significant disruptive cyberattacks on Ukrainian networks since the start of the conflict” (Antoniuk, 2024). This deprivation posed a significant threat to civilian lives, as both the provider and Ukrainian government claimed that subscribers typically received warning messages about impending Russian raids, allowing them to take necessary precautions. The challenges associated with identifying civilian and military entities in the event of an attack on agencies and individuals linked to the military and government are exacerbated by the complexity of determining active participation in hostility, as outlined in Articles 50 and 51(3) of AP I. This complexity is further compounded by the difficulties in distinguishing between civilian and military targets. Therefore, the immunity granted to civilians under AP I may be compromised by cyberattacks.

Article 36, which mandates the review of new weapons, has been subject to criticism because of lack of transparency, failure to publish results, and secrecy. Furthermore, it should be noted that AP I is not a treaty to which

all countries are signatories, underlining the need for a separate agreement to regulate or ban new weapons that are incompatible with IHL.

Despite the aforementioned issues, as both parties in the conflict are signatories to AP I, there should be no impediment to its application. Compliance with Articles 36 and 51(3) of AP I is a responsibility that falls on both Russian and Ukrainian forces. It is imperative that both parties adhere to the provisions of AP I to ensure the protection of civilians and to maintain the integrity of the international legal framework governing hostility.

Sandworm, an advanced persistent threat group suspected to be run by Russia's military cyber warfare unit, was held responsible for the attacks by ARSIWA, Article 8 of which holds Russia accountable. Although not a legally binding international treaty, ARSIWA is widely regarded as reflecting customary international law, which Russia, along with many other states, acknowledges and applies in their practices. Subsequently, the alleged hacking group Blackjack, with links to Ukraine's primary intelligence agency, SBU, targeted a Moscow-based internet provider in retaliation for the Kyivstar incident. The SBU has been connected to Blackjack previously (Pearson & Balmforth, 2024; Rommen, 2024). The hackers reportedly deleted twenty terabytes of data at M9 Telecom, a small Russian internet and television provider, resulting in some Moscow residents losing internet access (Muncaster, 2024).

The precise timeline for the M9 Telecom cyber incident remains undivulged. Nevertheless, the deliberate targeting of a Moscow-based internet service provider and the subsequent cautionary notice regarding a more severe attack on Kyivstar indicate an escalation in cyber warfare between Ukraine and Russia. These developments exemplify the burgeoning cyber conflict and strategic employment of cyberattacks as components of state policy by both countries.

If it is proven that Blackjack was responsible for the operation and that they are affiliated with the SBU, then responsibility will be assigned to Ukraine according to Article 8 of ARSIWA, in the same way that Russia bears responsibility.

If it is verified that the Sandworm and Blackjack collectives conducted cyberattacks under the authority of, or in accordance with, the instructions of the Russian and Ukrainian governments, they will be deemed state actors. This classification implies that individuals or organizations that act outside state frameworks but follow the guidelines of or are subject to the direction

of the state can be connected to the state for specific operations or missions. Thus, the actions of these non-state entities can be credited to the state.

The criterion of control may extend to a broader connection between the state and group. Although non-state actors may not be entirely reliant on the state, they are subject to its authority. This relationship must be closely tied to specific tasks or operations influenced by the state to ensure that the activities of these groups are attributed to the state in accordance with international law.

The attribution of the hacking groups Blackjack to the SBU and Sandworm to Russia's military intelligence service adds a layer of state involvement, signifying that cyber activities extend beyond non-state actors to nation-state-sponsored groups engaging in offensive cyber operations. This involvement highlights the growing trend of state actors utilizing cyber capabilities for strategic purposes, further complicating the international cyber conflict landscape.

7. Conclusion

Integrating IHL into cyber operations is vital for maintaining legal and humanitarian principles amid technological advancements. The ICRC emphasizes that the adaptability of IHL to new technologies, including cyber warfare, requires ongoing refinement to enhance civilian protection. The concept of direct participation in hostilities, especially in cyber contexts, complicates distinguishing between combatants and civilians. *Guidance* from the ICRC and the *Tallinn Manual* provide critical insights to protect civilians while acknowledging the complexities of modern warfare.

Non-state actors (NSAs) significantly impact cyber warfare, leveraging the unique characteristics of the digital domain. Their diverse motivations and organizational structures complicate the application of IHL. Whether state-directed or independent, their actions challenge the established legal framework of armed conflicts.

State responsibility for NSA actions in cyber warfare further complicates the legal landscape. Attribution of cyberattacks to states is difficult due to anonymity and obfuscation techniques. Establishing accountability is crucial for addressing the political and legal consequences of cyberattacks, including the right to self-defence.

Cyberattacks during the Russia-Ukraine conflict are frequently attributed to individuals or groups linked to the governments' intelligence services, despite consistent denials from the respective governments. These incidents demonstrate the interplay between political motives and military strategies in cyber operations. The Kyivstar cyberattack highlighted the severe impact on civilian infrastructure and the challenges of distinguishing between military and civilian targets and who directly participates in hostilities in cyberspace. The attribution of these groups to state actors underscores the intricacies of cyber conflict and the need for clear legal frameworks to establish state responsibility and safeguard civilian infrastructure in accordance with IHL. In summary, the interplay between IHL, cyber operations, and NSAs demands continuous legal adaptation to ensure compliance, protect civilians, and uphold the rule of law in the digital age.

Ahmad Khalil is a Syrian PhD candidate and research associate of law at VIT University, Chennai, India. He holds a graduate degree in law from Tishreen University, Latakia, Syria, and is enrolled in Syrian Lawyers Syndicate. Additionally, he received a fully funded scholarship to pursue a master's degree in international and comparative law at KIIT University, India. He is currently in the final stages of his PhD studies in international law and technology. Ahmad has authored more than five Scopus-indexed publications, focusing on artificial intelligence, international humanitarian law, and cyber warfare.

Mohammad Bitar received his LLB degree from Damascus University, Syria in 2015, an LLM degree in international and comparative law from Kalinga Institute of Industrial Technology, Bhubaneswar, India in 2020, and is currently a PhD research scholar at the School of Law, VIT-AP University, Amaravati, India. His research area covers international humanitarian law and human rights.

Associate Professor **S. Anandha Krishna Raj**, PhD completed his graduation in law from Chennai, at Dr. Ambedkar Government Law College affiliated to the Tamil Nadu Dr. Ambedkar Law University and is enrolled in the New Delhi Bar Council to practice in Supreme Court of India. He has completed his master's LLM from Krukshetra University and has an MA (in sociology) from Jawaharlal Nehru University. Later, he completed his MPhil and PhD in international law at Jawaharlal Nehru University. Currently, he is working as an associate professor of law at VIT School of Law, VIT University, Chennai, Tamil Nadu, India. His academic publications have appeared in various international and national journals.

References

- Ancell, N.** (2024), 'Everything We Know About the Kyivstar Cyberattack,' *Cybernews*, January 5. Retrieved from <https://cybernews.com/cyber-war/kyivstar-cyberattack/> [accessed Aug 2024]
- Antoniuk, D.** (2024), 'Ukraine Gathers Evidence to Prosecute Hackers behind Kyivstar Attack in Hague,' *The Record*, April 4. Retrieved from <https://therecord.media/kyivstar-cyberattack-war-crimes-prosecution-ukraine> [accessed Aug 2024]
- Applegate, S.** (2011), 'Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare,' *IEEE Security & Privacy*, vol. 9, no. 5, pp. 16–22. <https://doi.org/10.1109/MSP.2011.46>
- ARSIWA (2001), Draft Articles on Responsibility of States for Internationally Wrongful Acts, International Law Commission, United Nations.
- Bingham, C. M.** (2018), *Russia's Continued Cyber Operations Targeting its Adversaries' Energy Sectors*, MA thesis, Utica College.
- Bitar, M. & Chakka, B.** (2023), 'Responsibility for Violation of Rights of Migrants in Libyan Detention Centre,' *Mizan Law Review*, vol. 17, no. 2, pp. 315–342. <https://doi.org/10.4314/mlr.v17i2.4>
- Bitar, M. & Chakka, B.** (2024), 'Enforced Disappearances in Iraq: Attribution of Accountability to Government Under International and Domestic Legal Framework,' *LUMS Law Journal*, vol. 10, no. 1.
- Bosnia-Herzegovina v. Yugoslavia* [1996], ICJ, Judgment of 11 July 1996 in the Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide, 11.7.1996.
- Broekstra, A.** (2024), *Digital Battlegrounds: Evaluating the Impact of Cyber Warfare on International Humanitarian Law in the Russian-Ukraine War* [Independent thesis], Malmö University.
- Brown, G. D. & Metcalf, A. O.** (2014), 'Easier Said Than Done: Legal Reviews of Cyber Weapons,' *Journal of National Security Law & Policy*, vol. 7, pp. 115–139. <https://doi.org/10.2139/ssrn.2643688>
- Browne, E.** (2022), 'Elon Musk Says Starlink Has Resisted Hacking Attempts from Russia "So Far,"' *Newsweek*, May 11. Retrieved from <https://www.newsweek.com/elon-musk-starlink-resisted-hacking-attempts-russia-1705495> [accessed Aug 2024]
- Choo, K. K. R.** (2008), 'Organised Crime Groups in Cyberspace: A Typology,' *Trends in Organized Crime*, vol. 11, pp. 270–295. <https://doi.org/10.1007/s12117-008-9038-9>
- Collins, B.** (2024), 'The Aftermath of the Kyivstar Cyber Attack Is a Warning for Us All,' *Techradar*, January 5. Retrieved from <https://www.techradar.com/pro/>

- the-aftermath-of-the-kyivstar-cyber-attack-is-a-warning-for-us-all [accessed Aug 2024]
- Czosseck, C. & Ziolkowski, K.** (2013), 'State Actors and Their Proxies in Cyberspace,' *Peacetime Regime for State Activities in Cyberspace*, pp. 7–9.
- Dhelie, M. S.; Flåte, C. D.; Lie, L. M. & Sulg, E.** (2023), *Methods Used in Cyberattacks in the War Between Russia & Ukraine* [BA thesis], NTNU.
- Geneva Convention (III) Relative to the Treatment of Prisoners of War Adopted on 12 August 1949 by the Diplomatic Conference for the Establishment of International Conventions for the Protection of Victims of War, held in Geneva from 21 April to 12 August, 1949, entry into force 21 October 1950.
- Giles, K.** (2023), *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*, Chatham House, London: Royal Institute of International Affairs. <https://doi.org/10.55317/9781784135898>
- Gisel, L.; Rodenhäuser, T. & Dörmann, K.** (2020), 'Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts,' *International Review of the Red Cross*, vol. 102, no. 913, pp. 287–334. <https://doi.org/10.1017/S1816383120000387>
- Gorman, S.** (2009), 'Hackers Stole IDs for Attacks,' *The Wall Street Journal*, August 17. Retrieved from <https://www.wsj.com/articles/SB125046431841935299#articleTabs%3Darticle> [accessed Aug 2024]
- Hart, K.** (2008), 'Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar,' *The Washington Post*, August 14. Retrieved from <https://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html> [accessed Aug 2024]
- Henckaerts, J. M.** (2007), 'Customary International Humanitarian Law: A Response to US Comments,' *International Review of the Red Cross*, vol. 89, no. 866, pp. 473–488. <https://doi.org/10.1017/S1816383107001129>
- Henckaerts, J. M.** (2009), 'Customary International Humanitarian Law: Taking Stock of the ICRC Study,' *Nordic Journal of International Law*, vol. 78, no. 4, pp. 435–468. <https://doi.org/10.1163/090273509X12506922106795>
- Hollis, D. B.** (2007), 'Why States Need an International Law for Information Operations,' *Lewis & Clark Law Review*, vol. 11, no. 4, pp. 1023–1068.
- ICRC (2011), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 31IC/11/5.1.2, Geneva: International Committee of the Red Cross.
- ICRC (2019), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, Geneva: International Committee of the Red Cross.

- ICRC (2024), *Rule 6. Civilians' Loss of Protection from Attack*, Geneva: International Committee of the Red Cross. Retrieved from <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule6> [accessed Aug 2024]
- International Court of Justice Advisory Opinion Legality of the Threat or the Use of Nuclear Weapons, 8.7.1996.
- Ipsen, K.** (2008), 'Combatants and Non-Combatants,' in D. Fleck (ed.) *The Handbook of International Humanitarian Law*, Oxford: Oxford University Press.
- Khalil, A.; Bitar, M. & Raj, S. A. K.** (2024), 'Navigating Legal Frontiers in Cyber Warfare: Insights from the Russia-Ukraine Conflict,' *The Lawyer Quarterly*, vol. 14, no. 2, pp. 252–267.
- Khalil, A. & Raj, S. A. K.** (2023), 'Assessing the Legality of Autonomous Weapon Systems: An In-depth Examination of International Humanitarian Law Principles,' *Law Reform*, vol. 19, no. 2, pp. 372–392.
<https://doi.org/10.14710/lr.v19i2.58497>
- Khalil, A. & Raj, S. A. K.** (2024), 'Deployment of Autonomous Weapon Systems in the Warfare: Addressing Accountability Gaps and Reformulating International Criminal Law,' *Balkan Social Science Review*, vol. 23, no. 23, pp. 261–285.
<https://doi.org/10.46763/BSSR242323261kr>
- Kilovaty, I.** (2016), 'ICRC, NATO and the US—Direct Participation in Hacktivities—Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law,' *Duke Law & Technology Review*, vol. 15, pp. 1–38.
- Lawand, K.** (2006), 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977,' Geneva: International Committee of the Red Cross.
- Loshin, P.** (2013), *Practical Anonymity: Hiding in Plain Sight Online*, Oxford: Newnes.
- Luban, D.; O'Sullivan, J. R. & Stewart, D. P.** (2018), *International and Transnational Criminal Law*, New York: Aspen Publishing.
- McGinn, R. E.** (1991), *Science, Technology, and Society*, Englewood Cliffs, NJ: Prentice Hall.
- Melzer, N.** (2009), *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, Geneva: ICRC.
<https://doi.org/10.1017/S0272503700034388>
- Muncaster, P.** (2024), 'Ukrainian "Blackjack" Hackers Take Out Russian ISP,' *Infosecurity Magazine*. Retrieved from <https://www.infosecurity-magazine.com/news/ukrainian-blackjack-hackers/> [accessed Aug 2024]
- O'Neill, P. H.** (2022), 'Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion,' *MIT Technology Review*, May 10. Retrieved from <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/> [accessed Aug 2024]

- Pearson, J. & Balmforth, T.** (2024), 'Hackers Hit Moscow Internet Provider in Response to Kyivstar Cyber Attack—Source,' *Reuters*, January 9. Retrieved from <https://www.reuters.com/technology/cybersecurity/hackers-hit-moscow-internet-provider-response-kyivstar-cyber-attack-source-2024-01-09/> [accessed Aug 2024]
- Prescott, J. M.** (2012), 'Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States?' in C. Czosseck, R. Ottis & K. Ziolkowsky (eds.) *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, pp. 1–16. Tallinn: NATO CCDCOE Publications. <https://doi.org/10.2139/ssrn.2283741>
- Prosecutor v. Boskoski and Tarculovski* [2008], ICTY Trial Chamber, IT-04-82-T, 10.7.2008.
- Prosecutor v. Dusko Tadic* [1999], ICTY Appeal Chamber, Appeal Judgement, IT-94-1-A, 15.7.1999.
- Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977
- Rege-Patwardhan, A.** (2009), 'Cybercrimes Against Critical Infrastructures: A Study of Online Criminal Organization and Techniques,' *Criminal Justice Studies*, vol. 22, no. 3, pp. 261–271. <https://doi.org/10.1080/14786010903166965>
- Rommen, R.** (2024), 'Ukraine's "Blackjack" Hackers Breached 500 Russian Military Sites and Caused Chaos, Says Military Intelligence,' *Business Insider*, January 21. Retrieved from <https://www.businessinsider.in/international/news/ukraines-blackjack-hackers-breached-500-russian-military-sites-and-caused-chaos-says-military-intelligence/articleshow/107015698.cms> [accessed Aug 2024]
- Schmitt, M. N.**, ed. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9781139169288>
- Shakarian, P.** (2011), 'The 2008 Russian Cyber Campaign Against Georgia,' *Military Review*, vol. 91, no. 6, pp. 63–70.
- Sheraz, M. M.** (2021), 'The State Responsibility for the Actions of Non-State Actors in Cyber Space Based Operations,' *PalArch's Journal of Archaeology of Egypt/Egyptology*, vol. 18, no. 10, pp. 1229–1238.
- Sigholm, J.** (2013), 'Non-State Actors in Cyberspace Operations,' *Journal of Military Studies*, vol. 4, no. 1, pp. 1–37. <https://doi.org/10.1515/jms-2016-0184>
- Sohail, H.** (2022), 'Fault Lines in the Application of International Humanitarian Law to Cyberwarfare,' *Journal of Digital Forensics, Security and Law*, vol. 17, no. 1, art. 8. <https://doi.org/10.15394/jdfsl.2022.1761>
- The Economist* (2010), 'War in the Fifth Domain,' July 1. Retrieved from <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain> [accessed Aug 2024]

- The Prosecutor v. Fatmir Limaj, Haradin Bala and Isak Musliu* [2005], ICTY Trial Chamber, Judgment IT-03-66-T, 30.11.2005.
- Traynor, I.** (2007), 'Russia Accused of Unleashing Cyberwar to Disable Estonia,' *The Guardian*, May 17. Retrieved from <https://www.theguardian.com/world/2007/may/17/topstories3.russia> [accessed Aug 2024]
- Tsybulenko, E. & Francis, J. A.** (2018), 'Separatists or Russian Troops and Local Collaborators? Russian Aggression in Ukraine: The Problem of Definitions,' in S. Sayapin & E. Tsybulenko (eds.) *The Use of Force Against Ukraine and International Law*, The Hague: T.M.C. Asser Press/Springer, pp. 123–144. https://doi.org/10.1007/978-94-6265-222-4_6
- Tsybulenko, E. & Kajander, A.** (2022), 'Customary International Humanitarian Law and Article 36 of Additional Protocol I to the Geneva Conventions: A Stopgap Regulator of Autonomous Weapons Systems?' *TalTech Journal of European Studies*, vol. 12, no. 2, pp. 87–112. <https://doi.org/10.2478/bjes-2022-0013>
- Tsybulenko, E. & Kelichavyi, B.** (2018), 'International Legal Dimensions of the Russian Occupation of Crimea,' in S. Sayapin & E. Tsybulenko (eds.) *The Use of Force Against Ukraine and International Law*, The Hague: T.M.C. Asser Press/Springer, pp. 277–296. https://doi.org/10.1007/978-94-6265-222-4_13
- Tsybulenko, E. & Platonova, A.** (2019), 'Violations of Freedom of Expression and Freedom of Religion by the Russian Federation as the Occupying Power in Crimea,' *Baltic Journal of European Studies*, vol. 9, no. 3(28), pp. 134–147. <https://doi.org/10.1515/bjes-2019-0026>
- Van Creveld, M.** (2009), *Transformation of War*, New York: Simon and Schuster.
- Wallace, D.** (2018), 'Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis,' *Tallinn Paper*, no. 11, pp. 22–45.