Research article
UDC 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them

Mohammad Minhazur Rahman ✉
State University of Bangladesh, Dhaka, Bangladesh

Tapos Kumar Das
Jahangirnagar University, Dhaka, Bangladesh
City University of Hong Kong, Hong Kong

Keywords

cyberattack,
cybercrime,
digital technologies,
human rights,
international convention,
international law,
law,
legal liability,
principle of due diligence,
principle of proportionality,
principles of international law

Abstract

Objective: to categorize cyber attacks in the national and international legal sytems and to define legal measures to counter them at the international level.

Methods: include doctrinal legal analysis, formal legal, comparative legal methods, synthesis, induction, deduction, as well as methods of legal forecasting and modeling. International legal documents and acts of national legislation, judicial precedents, and doctrinal sources were studied.

Results: the article defines the legal consequences of cyberattacks, identifies difficulties in determining and holding individuals and organizations accountable for their commission, identifies national measures to counter cyberattacks based on the principle of proportionality, and systematizes the international legal framework for responding to cyberattacks. The main focus is on the urgent problems of identifying and verifying cyber weapons, establishing international standards for their use, developing methods of disarmament or limiting offensive cyber capabilities. The authors raise the issue of ensuring humanitarian activities, protecting critical infrastructure and the population through cybersecurity measures in wartime. The legal framework is analyzed; gaps and other defects are identified in the current regulation of exercising jurisdiction in such areas of cyber activity as international transactions, data localization and extraterritorial enforcement of national legislation. The parameters were developed and described within

✉ Corresponding author

which states may conduct proactive cyber operations to prevent or deter cyberattacks (cyber countermeasures). The main parameters are due diligence, legal decisions on using cyber countermeasures, proportionality of protection measures to the consequences of illegal actions.

Scientific novelty: this is due to the progressive solutions in the field of international legal regulation of cyber countermeasures by states responding to cybercrime. The solutions are formulated taking into account the impact of the countermeasures on human and civil rights and freedoms, including the right to privacy and freedom of speech.

Practical significance: the research results can be used to develop and improve international legal instruments in the field of combating cyberattacks and ensuring cybersecurity, and can serve as a model for national legislators when designing law-making solutions to counter cybercrime.

For citation

Rahman, M. M., & Das, T. K. (2024). Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them. *Journal of Digital Technologies and Law, 2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

Content

Introduction

The increased frequency of cyberattacks in today's world poses serious threats to the safety and security of nations. As nations try to figure out how to defend themselves from cyberattacks, the legal implications of cyberwarfare and countermeasures have become important fields of study. This research sheds light on numerous areas of international law by exploring the legal implications and issues involved with various parts of countermeasures in cyberwarfare. Identifying the people or organisations responsible for cyberattacks is a major obstacle to resolving the problem (Etzioni & Rice, 2015). Correctly attributing cyberattacks is essential for developing efficient countermeasures. But attribution of it is difficult because of the nature of the internet, which allows for anonymity and the adoption of sophisticated tactics to conceal identities. This research revisits the existing legal frameworks and proposes techniques to establishing responsibility when it comes to attributing cyberattacks in the context of countermeasures.

Proportionality as it relates to defences against cyberwarfare is another important topic covered in this research. The application of proportionality in evaluating the extent and severity of countermeasures is becoming increasingly important as nations respond to cyberattacks. Given the asymmetric nature of cyber operations and the broad collateral harm they can do, the legal rules for establishing the proportionality of countermeasures need to be carefully examined (Roscini, 2014). Existing legal standards and concepts are examined in this research, as well as their relevance to cyber countermeasures. International collaboration is essential in the face of increasingly complex and transnational cyber threats. This research looks at the legal structures and procedures that promote international collaboration in the face of cyberattacks. The exchange of information, coordination of actions, and development of effective measures to counteract cyber threats all need cooperation between governments.

This research also examines the advantages and disadvantages of international cooperation in the field of cyber countermeasures by examining existing international legal instruments and cooperative channels. While states are the dominant participants in cyberwarfare, cybercriminals and hacktivist organisations have emerged as significant players as well (Buchan, 2012). That's why this research evaluates the difficulties of holding non-state actors accountable for cyberattacks and examines the legal remedies accessible to nations for responding within the bounds of international law. Concerns about the possible violation of fundamental human rights, such as the right to privacy and freedom of speech, emerge as nations engage in defensive or offensive cyber operations. To find a middle ground between national security concerns and the preservation of individual rights, this research investigates the legal frameworks and concepts regulating the junction of cyber countermeasures and human rights. In addition, this research analyses the parameters within which nations may legitimately conduct pre-emptive cyber operations to either prevent or discourage cyberattacks (Hollis & Finnemore, 2016).

This research investigates the limits and policies of pre-emptive cyber countermeasures by examining the current rules of anticipatory self-defence and their relevance in the cyber countermeasure. The research also investigates the necessity of due diligence as a criterion for governmental accountability in cyber countermeasures and examines the norms and duties imposed on nations for deciding the legitimacy of their cyber countermeasures, and sheds light on the potential repercussions and remedies for governments that engage in illegal cyber activities. The difficulties of defining, verifying, and regulating cyber weapons are also explored in this research and it looks at the standards for using cyber weapons in the context of countermeasures, as well as the legal frameworks and prospective procedures for disarming or limiting offensive cyber capabilities (Liivoja & Väljataga, 2021). Additionally, the legal frameworks governing intelligence actions in cyberspace are investigated, along with the bounds of acceptable espionage, the range of legitimate state interests, and the possible influence on international relations. This research argues that understanding of legal implications and difficulties of cyber intelligence collection can be improved by this approach (Putman & Albright, 2018).

In addition, this research investigates how cybersecurity safeguards might aid in the safety of populations, vital infrastructure, and humanitarian efforts in times of war. By doing so, it sheds insight on the possible roles and duties of states and non-state actors in preserving cyberspace during wars by investigating the legal requirements of states and the potential synergies between cybersecurity and international humanitarian law. Finally, the research looks into the difficulties and legal precedents of asserting jurisdiction over illegal cyber actions. Examining the jurisdictional challenges that arise from cross-border cyber operations, data localisation, and the extraterritorial implementation of national laws, this research finally examines the possibilities for international legal collaboration (Andrew & Bernard, 2021). This research intends to further the establishment of legal frameworks and norms governing countermeasures in cyberwarfare by exploring these many and under-researched areas of international law aspiring to deal with the difficulties and ambiguities of cyber threats and to further the knowledge of the legal consequences of this changing landscape (Knowles & Thomas, 2016).

Three significant research questions will be explored in this research. Firstly, the author will investigate how the legality and illegality of cyberattacks are classified under international law and treaties, and will compare and contrast how these classifications are used in various jurisdictions and settings. Secondly, existing legal frameworks and techniques used by governments and international organizations to respond to and mitigate cyberattacks will be examined, and potential limits of the approaches of cyber countermeasures as well as self-defence strategies will be identified and explored from an international law perspective. Thirdly, given the dynamic nature of the global digital ecosystem, this research will seek to explore ways in which international law and institutions could be better leveraged or altered to meet the growing problem of cyberattacks.

Furthermore, this research concerns unexplored questions relevant to the legal consequences of cyber countermeasures that are complex and multidimensional, necessitating an all-encompassing research technique to answer them. To give a thorough examination of the topic, this research will combine qualitative research methodologies with doctrinal approaches. Scholarly publications, books, legal texts, case law, and international legal instruments will all be reviewed as part of this research (Wren & Wren, 1986). Insight into the various cyber countermeasures' legal frameworks, philosophies, and arguments will be gained from these sources. The legal implications of countermeasures, attribution difficulties, and particular cases of cyberattacks will all be examined through case studies. There will be an examination of how various legal systems and international cooperation mechanisms deal with cyberattacks (Van Hoecke, 2011). To determine what works and what may be improved, this research will compare and contrast key international treaties, agreements, and cooperative approaches taken so far. To clarify the legal standards, norms, and principles controlling the many components of cyber countermeasures, the author will perform a doctrinal study of international legal instruments such as treaties, customary international law, and pertinent legal principles (Watkins & Burton, 2013).

To answer the research questions, this research will also need the interpretation and application of legal rules and precedents. The focus of this research has been narrowed to the difficulties and legal implications of developing responses against cyberattacks. The author's knowledge and experience in this continuously developing field are the primary limitations on the research (Tyler, 2017). Despite these limitations, it is expected that this research will make a significant addition to the knowledge of the legal consequences and difficulties of cyber warfare countermeasures.

1. Challenges Relating to Legality or Illegality of Cyberattacks

1.1. Attribution Conundrum of Cyberattacks

Since cyberattacks frequently leave no evidence, attribution of these offences may be a challenging and time-consuming operation (Tsagourias & Farrell, 2020). Attribution refers to the steps used to identify a cyberattack's origin. According to Michael Schmitt, cyberattack attribution is a difficult and complicated problem. Responsibility for cyberattacks cannot be determined by the legal system. However, there are a variety of legal frameworks and innovative approaches that can help in attributing cyber attacks. Adopting these models and procedures can help states deal with cyber threats more effectively. According to Michael Schmitt, it is difficult to establish liability in the event of a cyberattack due to the absence of a uniform legal framework. However, using innovative techniques and legal frameworks can improve nations' abilities to identify cyber assaults and develop effective countermeasures (Schmitt, 2013). This indicates that juridical instruments currently exist that can aid with attribution in the event of cyber

emergencies. James A. Lewis argues that identifying the perpetrators of a cyberattacks is a crucial first step in responding to a catastrophic event in cyberspace. Taking appropriate legal, diplomatic, or military response is difficult if the perpetrators cannot be identified. The anonymity of the internet and the difficulties of acquiring proof make it difficult to pin down who is behind cyberattacks. However, several options exist for improving the attribution of cyberattacks. States may strengthen their defences against cyber threats by employing these methods and resources (Lewis, 2018). This suggests that there are viable approaches to enhancing attribution processes, notwithstanding the difficulties.

Similarly, Gabriella Blum (Wittes & Blum, 2016) highlights that cyberattack attribution is an important topic in international law. It is challenging to hold nations accountable for conduct in cyberspace without attribution. The principles of state responsibility, due diligence, and proportionality are only a few of the legal frameworks that might be used to the problem of attributing attacks via the internet. However, these models are intricate and tricky to put into action. More definition and agreement are needed on the legal principles for assigning blame for cyberattacks. Blum stresses the necessity to make nations accountable for their acts in cyberspace and the importance of attribution for international law. Some of the legal principles she discusses that can be applied to attributing cyberattacks include state responsibility, due diligence, and proportionality (Wittes & Blum, 2016). The intricacy and real-world challenges of implementing these systems are also acknowledged by Blum. She stresses the importance of better defining and agreeing upon the legal norms that regulate attribution. Attributing a cyberattack to a specific attacker may not always be easy. Attribution has far-reaching legal implications. If one country can prove that another is responsible for a cyberattack, it may be able to sue the offending nation in court. But it may be impossible for a state to take legal action in the event of a cyberattack if it cannot determine who was responsible for it (Ohlin et al., 2015).

There are other innovative methods that may be utilised to attribute cyberattacks in addition to the existing legal frameworks. Collecting and analysing digital evidence left behind by cyberattacks is known as cyber forensics. This data can be utilised to pin down the perpetrators of cyber operations. The attribution of cyberattacks can be strengthened by international collaboration. The investigation into cyberattacks can be aided by states sharing information and resources. The attribution of cyberattacks may be further strengthened through public-private collaborations. Cyberattack data from private entities can be shared with government agencies. Governments can utilise this data to better understand and attribute cyber threats (Klimburg, 2018). As cyberattack attribution is a difficult and convoluted problem, domestic legal systems cannot be relied upon to assign responsibility for cyberattacks. Attributing cyber assaults, however, can be aided by a number of legal frameworks and creative methods. States can better respond to cyber threats by adopting these frameworks and methods.

1.2. Accountability Challenges of Non-State Entities

Non-state entities evading responsibility for cyberattacks present substantial difficulties in the contemporary international law framework. International law scholars acknowledge the difficulties in prosecuting non-state actors for cyber assaults. However, within the framework of international law, governments have a number of legal tools to respond to such attacks. State accountability, legal countermeasures, cyber operations with specific targets, and international cooperation are all viable solutions (Buchanan, 2017). To meet their international legal commitments, governments must give careful consideration to the legality and proportionality of their actions.

According to Michael N. Schmitt (1999), cyber operations carried out by non-state actors are subject to the same traditional rules of international law as those carried out by states, such as the concept of state accountability and the avoidance of intervention. Schmitt emphasises that conventional norms of international law might still apply to non-state entities participating in cyber assaults. A state can be held liable for the activities of a non-state actor by invoking the principle of state responsibility. When non-state actors conduct cyber operations from one state against another, the ban of involvement may also apply. According to him, one of the biggest obstacles to holding non-state actors responsible for their acts is the lack of a clear legal framework controlling the attribution of cyberattacks to non-state actors. To guarantee that their actions are legitimate and successful, states must collaborate to build a shared understanding of the legal standards regulating cyber operations (Schmitt, 1999). Michael Schmitt draws attention to the difficulty and absence of a clear legal framework in attributing cyberattacks to non-state actors. The term attribution describes the procedure of pinpointing the origin of a cyberattack. It is difficult to hold non-state actors accountable for their conduct in the absence of a defined legal framework. Schmitt contends that governments must work together to establish uniform legal norms for cyber activities. States' responses to cyber threats can be successful and compliant with the law if they are based on a shared understanding.

Tallinn Manual 2.0 also suggests that legal solutions available to states for dealing with cyber activities carried out by non-state actors include diplomatic, economic, and legal sanctions. According to the Tallinn Manual 2.0, governments have a wide range of options for responding to cyberattacks by non-state actors. These forms of repercussions might be either diplomatic or economic or even legal in nature, according to the nature of the offence and the circumstances. Similarly, according to Matthew C. Waxman, targeted cyber operations have been employed by states against non-state actors to impede their operations, weaken their capabilities, and make them pay the price for their hostility. Waxman encourages the use of targeted cyber operations by nations to stop the operations and resources of non-state entities doing hostile action. Such actions can be used

to dissuade future cyberattacks by imposing penalties on the attackers (Waxman, 2011). However, international law should be used to evaluate the legitimacy and proportionality of such measures.

1.3. Cooperation Imperative in Cyberterrorism

According to the U.N. General Assembly Resolution 71/256, states should work together to ensure that all efforts to prevent and defeat the threat of cyberterrorism are lawful under all applicable international treaties. The resolution passed by the General Assembly also highlights the significance of governments working together to combat terrorism, particularly cyberterrorism, while adhering to their respective commitments under international law (Mačák, 2016). Therefore, while reacting to cyber assaults by non-state actors, nations should think about international legal frameworks. According to Gabriella Blum, in any endeavour to hold non-state actors responsible, the lack of collaboration from other nations is a fundamental challenge that must be addressed. The effectiveness of state responses depends on states working together to establish cooperative mechanisms. Gabriella Blum argues that attempts to hold non-state actors responsible for cyberattacks are hindered by a lack of cooperation from other nations. When dealing with cyber threats from non-state actors, cooperation among governments is essential for gathering and sharing information, exchanging knowledge, and coordinating operations. Blum asserts that, in order to effectively respond to cyber threats, nations need to establish structures for collaboration (Lewis et al., 2019). Agreements to share data, conduct combined research, and coordinate responses are all examples of such systems. States' ability to respond to non-state actors participating in cyberattacks can be strengthened by encouraging collaboration. As discussed above, attributing cyberattacks to non-state actors is not governed by any clear international law framework. This ambiguity makes it more challenging for governments when holding non-state actors responsible for their acts. It might be challenging to track down and identify non-state actors. Even if non-state actors have been effectively ascribed to an assault, this challenge might make it hard for states to take measures against them.

For several reasons, including political concerns and fear of retaliation, nations may be hesitant to collaborate with other states in examining and punishing non-state actors. The inability to work together can make it hard for governments to hold non-state actors responsible for their behaviour. Although difficult, nations can have legal recourse when reacting to cyber assaults from non-state actors. The issue with the non-state actor or the state that is suspected of harbouring the non-state actor can be resolved diplomatically by the state involved (Mazanec, 2015). Economic sanctions can be imposed by states on either the non-state actor or the state that is allegedly providing safe haven to the

non-state actor. When responding to cyber assaults by non-state actors, states have the option to employ military action. However, this choice should be made only when all other options have been exhausted, as it might have serious repercussions, including an increase in aggression.

1.4. Human Rights Concerns in Cyberattacks

Human rights may also be adversely affected by cyberattacks. Cyberattacks may be used for many various purposes, including data collection without authorization, speech censorship, and system disruptions. Journalists, activists, and members of marginalised communities are especially susceptible to these effects. In the context of cyber countermeasures, there are a number of legal mechanisms that control the trade-off between national security objectives and human rights considerations (Kulesza & Balleste, 2015). The right to privacy and the ability to express oneself are just two of the many rights guaranteed by international human rights law. Even in the sake of national security, nations must uphold these freedoms. The law of armed conflict, often known as international humanitarian law, governs all armed conflicts. This law regulates the employment of physical and virtual weapons of destruction. Human rights may be afforded more protection at the national level, or the application of cyber countermeasures may be restricted under specific conditions. There are a variety of measures states may take to guarantee that their cyber activities are in line with universal human rights principles. The right to privacy and the freedom of speech are two human rights that states must uphold in the setting of cyber countermeasures.

Cyber countermeasures taken by states must be appropriate to the severity of the cyber threat. States may use any cyber countermeasures they see appropriate to accomplish this (Watt, 2021). When employing cyber countermeasures against any state or non-state actors, states must take every possible safety measure to ensure no civilians or civilian properties are harmed. Any damage caused by a state's cyber actions must be paid for. UN Human Rights Council in their Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression expressed that human rights must be included in the design and implementation of cybersecurity policies and procedures. It stresses the need of adhering to human rights standards while implementing cybersecurity measures and countermeasures. The measures must be lawful, necessary, proportionate, and non-discriminatory, and they must not single out or discriminate against any particular persons or groups. In the Case of Delfi AS v. Estonia, the ECtHR has repeatedly affirmed that the right to freely disseminate and discuss any and all ideas, regardless of how well they are accepted or whether they are considered objectionable, is a cornerstone of a democratic society. The importance of free speech in a democratic society is underscored by this case (Wagner et al., 2019). It stresses that the scope of this freedom includes not just

generally well-liked but also potentially contentious information and opinions. Therefore, even when dealing with controversial material, cyber defences should make sure this right is protected.

Also, article 19 of the ICCPR states that everyone has the right to express themselves in any way they see fit, whether verbally, in writing or print, in art, or through any other medium of their choosing; this includes the freedom to seek for, receive, and disseminate information and ideas of any type, across any and all borders. This legal provision emphasises the expansive nature of this right, which encompasses the freedom to access, consume, and distribute information and ideas in any media. The freedom of expression and information in the digital sphere must be protected from infringement by governments. To ensure that cyber operations are conducted in accordance with international human rights norms, a clear and comprehensive legislative framework is required (Mihr, 2017). The accountability, monitoring, and judicial review aspects of this system are essential. Before launching any kind of cyber operation, states must first complete extensive human rights impact assessments. They have to analyse how any limits could affect rights like privacy and freedom of speech, and make sure they aren't more severe than is absolutely required to achieve the legitimate goals at hand. Safeguards for due process, effective remedies for suspected violations, and independent and open methods of supervision must be implemented. Without jeopardising legitimate security concerns, states should tell the public on the goals, scope, and effect of cyber activities to foster openness and public accountability. They need to work together on a global scale to create guidelines for safeguarding human rights online (Mihr, 2016). The creation of all-encompassing norms and regulations is facilitated by working together with other governments, international organisations, and the general public. States can find a middle ground between human rights and national security concerns by ensuring that their cyber activities are in line with international human rights norms.

2. Scopes and Limitations of Countermeasures against Cyberattacks

2.1. Proportionality Calibration in Cyber Operations

One of the cornerstones of international law is the concept of proportionality, which forbids the use of force that is disproportionate to the severity of the threats. The same rule applies to cyber operations as it does to any other type of military combat. A countermeasure's proportionality must be evaluated in light of the specifics of the attack it is designed to repel. A retaliatory tactic that causes more damage than the first assault is likely to be deemed disproportionate. The countermeasure ought to be exactly what is needed to stop the cyberattack. A disproportionate response is one that goes beyond what is required to stop the attack. The countermeasure should not backfire and generate more problems than it solves. If the negative effects of the countermeasure are out of proportion to the benefits,

then the countermeasure is unfair. Applying the idea of proportionality to cyber operations might be challenging due to the unique nature of cyber activities (Dwan et al., 2022). For instance, cyber activities might have unforeseen consequences and very hard to be traced. Cyber operations pose a unique set of challenges when it comes to determining the proportionality of countermeasures, which necessitates taking into account the specific features of cyberattacks and their consequences for the concept of proportionality. Many scholars of international law have shed light on the relevance of current proportionality principles to cyber operations. According to Michael N. Schmitt, states must evaluate the potential collateral damage to civilian objects and measure it against the potential military advantage in order to meet the proportionality standard. Schmitt stresses the necessity to weigh the military advantage obtained from cyber operations against the predicted harm to civilian objects. Cyber strikes fall under this concept of proportionality, where governments should weigh the possible military benefit against any collateral harm to civilian infrastructure like crucial systems or important services (Schmitt, 2012).

According to the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, cyber operations that cause severe damage to essential infrastructure or casualties might be deemed an act of war. This suggests that while weighing the potential outcomes of such cyber operations, the criterion of proportionality must be employed. Damage to important infrastructure, loss of life, or injuries to individuals are all indicators that a cyber-operation has crossed the line into an act of war. Similarly, according to Marco Roscini (2014), a State Party to a Conflict must not undertake a cyberattack against a civilian object if the predicted civilian damage or accidental injury would be disproportionate to the expected military advantage, according to the principle of proportionality. Roscini emphasises the significance of limiting cyber assaults' effects on innocent people. When conducting a cyberoperation, the predicted harm to civilian objects or persons must not exceed the projected military gain. This idea still holds water in the realm of cyberwarfare (Roscini, 2014). Again, according to Christopher C. Joyner (2011), cyberwarfare must be governed by the concept of proportionality, which states that a combatant may not utilise force greater than the danger posed by the armed forces of the state being attacked. According to Joyner, the use of force in cyberwarfare should be limited to what is both required and commensurate to the danger posed by the military capabilities of the targeted state. That means cyber operations shouldn't do more damage than is absolutely essential to stop the current threat.

Proportionality in cyber operations is determined by evaluating the projected military advantage against the anticipated harm to civilian objects, according to legal academics (Frowe, 2022). Cyberattacks are unlike any other type of attack and must be carefully considered within the context of proportionality due to their potential to cause damage to key infrastructure or result in civilian harm. The propriety and legality of cyber operations in light of the probable effects can be evaluated using the current legal

norms and principles relevant to proportionality in armed engagements. States with far fewer resources than their targets are able to undertake cyberattacks. The attacker's capabilities may be unknown or hard to predict, making it difficult to determine whether or not a countermeasure is proportionate. Complexity and unpredictability are two hallmarks of cyber operations (Schmitt, 2011).

Due to the difficulty in anticipating all of the potential outcomes, it can be challenging to determine whether or not a countermeasure is proportionate. It can be challenging to identify the origin of cyber assaults because they might be launched from anywhere. Because of this, it may be difficult to zero in on the right target for a countermeasure. Cyberattacks might be trickier to assess in terms of their scope and severity. Cyber assaults can inflict a lot of harm, but it can be hard to tell how much because of their anonymity and complexity. This might make it hard to judge if a response is appropriate given the severity of the attack. Cyber countermeasures may be more challenging to justify. With so many potential ways to respond to cyber threats, deciding whether or not to take protective action can be challenging. It is also challenging to determine the likelihood that a response may be deemed excessive increases under certain circumstances. Cyber countermeasures may make it harder to foresee potential outcomes.

2.2. Obstacles of Global Collaboration

There are a variety of obstacles that prevent governments from working together to create legitimate cyber countermeasures. Cyber activities are not governed by any universally accepted set of laws. This ambiguity might hinder state cooperation in creating efficient countermeasures. Attributing cyberattacks to a specific attacker is often challenging. Since nations may be unsure about whom to target in the event of a cyberattack, this challenge can complicate responses to such strikes (Friis & Ringsmose, 2016). There can be a broad variety of intentional and unforeseen consequences from cyberattacks. But working together as nations to create legitimate and effective cyber defences is essential. Both the difficulties and the potential solutions have been pointed out by legal experts. For example, according to Duncan Hollis (Hollis & Finnemore, 2016), the interconnectedness of cyberattacks and vulnerabilities necessitates international collaboration to solve the issue, since no one state can do so successfully on its own. Hollis highlights the realisation that no one state can adequately confront cyber dangers alone and the underlying interconnectivity in cyberspace. This emphasises the need for governments to work together to exchange knowledge, skills, and resources in order to strengthen their cyber defences.

Again, according to Christopher S. Yoo, the costs of information gathering, coordination, and enforcement can be reduced, and the success rate of cybersecurity activities can be increased by the widespread dissemination of relevant data on behalf of the states. Yoo stresses the need of sharing knowledge in the field of cybersecurity. State-to-state information sharing procedures can improve cybersecurity while cutting

expenses related with data collection and coordination. More effective defences against cyberattacks may be achieved through the exchange of threat intelligence, best practises, and technical skills (Yoo & Blanchette, 2015). The United States International Strategy for Cyberspace mandates that together with other countries, the United States will strengthen cyber standards based on respect for human rights and endeavour to lessen the likelihood of conflict caused by the spread and use of information and communication technologies. It emphasises cooperative efforts across country boundaries to spread best practises in cybersecurity and encourage accountable behaviour. By working together, nations may more easily create and execute standards and guidelines that protect human rights while also making the internet safer for everyone.

Tallinn Manual 2.0 also suggests the same approach by stating that cyber defence agreements between states might lay out the precise cooperation steps that can be taken to aid one another in the event of a cyberattack. When it comes to cyber countermeasures, the Tallinn Manual 2.0 also recommends bilateral agreements between nations. Such agreements can lay the groundwork for sharing information and resources in the event of a cyber crisis or attack. Mutual trust is fostered and cyber security initiatives may be tackled more efficiently through bilateral agreements (Tsagourias, 2012). Furthermore, UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security recommends that to improve all nations' abilities to avoid, investigate, respond to, and recover from ICT-related incidents, governments must collaborate in designing and implementing capacity-building measures, including aid and collaboration. To improve all governments' abilities to respond to ICT-related incidents, the UN GGE stresses the necessity of collaboration in capacity building, including aid and cooperation. Collaboration and coordination among nations is greatly aided by international organisations like the United Nations (Henriksen, 2019).

Scholars of the international law have noted the benefits and drawbacks of international cooperation in the development of legitimate and efficient defences against cyber threats. Cyberspace's interconnectedness makes it imperative for nations to work together, share data, and increase their collective preparedness. While multilateral institutions like the United Nations can help coordinate efforts and provide assistance for the creation of standards and capacity-building programmes, bilateral agreements can define particular cooperation actions. Collectively, state governments may strengthen their cybersecurity capabilities and respond to cyberattacks by using these tools. Despite the difficulties, there are several openings for international cooperation on the creation of legitimate yet efficient cyber defences (Katagiri, 2021). It is possible for international organisations like the United Nations to facilitate cooperation between governments in order to create efficient countermeasures. These groups can serve as a meeting place for countries to collaborate on strategies for countering cyber threats. Effective countermeasure development can also benefit from bilateral agreements between governments. These pacts can serve as a basis for governments to coordinate their responses to cyber threats and share information about them.

The Global Information Sharing and Analysis Centre (GISAC) is another structure that can help encourage cooperation between governments in order to create more effective responses (Faga, 2017). These tools can help nations coordinate their reactions to cyber threats and share information about them. Significant obstacles exist for international cooperation in the development of effective and legal defences against cyber threats. On the other hand, there are a lot of ways in which people could work together. Cybersecurity is a shared responsibility, and governmental cooperation can lead to more robust measures of defence.

2.3. Legal Labyrinth of Anticipatory Self Defence

Pre-emptive cyber operations by nations to prevent or deter impending cyber assaults are a topic of continuous discussion, as are the conditions under which such operations can be legally conducted. Existing conventions and legal frameworks concerning anticipatory self-defence are not always relevant in the cyberattacks, and there is insufficient agreement on this matter. The UN Charter, the ICJ's Nicaragua judgement, and customary international law are the most important rules and legal frameworks pertaining to anticipatory self-defence (Dean, 2013). The use of force against the sovereignty or territorial integrity of a state is explicitly forbidden under the United Nations Charter. To counter this, Article 51 of the UN Charter permits nations to use force in self-defence if they feel they are being attacked. The International Court of Justice ruled in Nicaragua Case that a person has the right to use force in self-defence even if an assault has not yet happened. Nonetheless, the ICJ emphasised that the risk of attack had to be instant, overwhelming, and leaving no choice of means, and no moment for deliberation. The right to self-defence is also recognised under customary international law. Customary international law provides guidance in self-defense situations, although its content is not always crystal apparent. Some legal scholars maintain that nations must use every available diplomatic route to settle a conflict before resorting to force. However, there are many who argue that governments have the right to employ force in self-defence in the face of an assault, even if diplomatic solutions to the conflict are still possible.

There is continuous discussion over whether or not current norms and legal frameworks pertaining to anticipatory self-defence apply in the cyberattacks (Lucas, 2016). Experts are divided on whether or not self-defence concepts can be applied to the cyber world, with some saying they can and others saying they can't because of the special nature of cyber assaults. The difficulty of attributing attacks is a major obstacle to self-defence strategies in the cyber world. In the real world, identifying the perpetrator of an assault is usually not too difficult. However, tracing the origin of an assault in the cyber realm can be tricky. This complicates the ability of nations to assess threats and exercise self-defence rights. Another issue in bringing traditional concepts of self-defence into the cyberspace is determining how close an assault actually is. In the real world, it's usually easy to tell if an assault is going to happen soon. However, gauging the imminent threat of an assault

in the cyber sphere can be challenging. This complicates the question for governments of whether or not they have the right to exercise self-defence in the face of an imminent threat (Levite & Perkovich, 2017).

Pre-emptive cyber operations, in which a state proactively takes action to stop or discourage an assault, are a contentious topic of discussion among experts. Existing norms and legal frameworks relating to anticipatory self-defence are not always obvious or appropriate in the cyber sphere, and there is no clear consensus on this topic. According to the judgement of Nicaragua v. United States of America (1986), a case adjudicated by the International Court of Justice (ICJ), in the event of an invasion or other armed attack, every sovereign state has the right to employ military action to defend its territory. It reaffirms the inherent right to self-defence. The ICJ ruled that the right to self-defence includes the ability to take action in the face of an immediate threat of violence (Travis, 2016). The ICJ also ruled that self-defence actions including the use of force have to be justified.

According to Michael Schmitt, to be justified in using force in anticipatory self-defense, it must be necessary, proportional, and used in response to an imminent, unlawful armed attack. He suggests that anticipatory self-defence is only justified in cases when the use of force is necessary and appropriate, the threat of an armed assault is imminent, and there are no legitimate alternatives to the use of force[1]. Similarly, Bruce Schneier asserts that states must avoid engaging in pre-emptive cyber operations as they are potentially devastating and unstable. It will be harder for nations to work together to address cyber security concerns if these tensions intensify. He foresees that pre-emptive cyber operations will lead to greater disputes and make it harder for nations to work together to address cyber security threats (Schneier, 2013). Altogether these assertions by international law scholars highlights that pre-emptive cyber operations are controversial and the law is still being worked out on. The legislation is still developing, and there is no unanimous agreement on the topic. But the imminence of the threat, the need of the use of force, the proportionality of the use of force, and the differentiation between combatants and civilians are all criteria that legal academics have highlighted as crucial to the legitimacy of pre-emptive cyber operations.

The dangers and rewards of conducting pre-emptive cyber operations must be weighed against these legal constraints. Pre-emptive cyber actions carry the danger of sparking a wider war (Ossoff, 2021). They may backfire if they harm international ties and make it harder for governments to work together on cyber security. Pre-emptive cyber operations are controversial, and the choice to use them must be taken on a case-by-case basis. The legal, strategic, and political implications of such operations must be carefully considered by states before they are carried out.

[1] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

3. Instrumentalising International Law and Institutions to Address Cyberattacks

3.1. Confronting the Lacuna in International Cybersecurity Norms

The existing state of international organisations is unable to deal with the complexity and fluidity of cyber threats. The United Nations Group of Governmental Experts (GGE) is another example of it. The GGE's efforts to build voluntary, normative frameworks are hampered by the fact that they are consensus-based, making them slower to evolve and sometimes leading to impasse as a result of competing national interests and geopolitical conflicts. The inability of existing international law to judge and execute penalties against governments that commit or assist cyberattacks is another serious problem. Because existing enforcement procedures are mostly based on conventional conceptions of war, there is a vacuum in institutional protections for governments that conduct hostile cyber operations. This highlights the need for a new International Convention to define illicit cyber actions more precisely and provide efficient mechanisms for adjudication and enforcement. Due to the ever-evolving nature of technology, a new International Convention is also required.

Current technological advancements are outstripping the ability of existing international law and institutions to respond effectively. For instance, the emergence of quantum computing and cyberattacks driven by artificial intelligence presents new issues that are not yet accounted for by existing frameworks. A Convention with an eye on the future can be of assistance by being built with adaptability and flexibility from the ground up, so that it can grow and change in tandem with technology development. Moreover, the idea of global collaboration highlights the importance of a new International Convention (Gow et al., 2019). Cybersecurity is an international issue that calls for concerted effort. Different national interests and a lack of confidence have made it difficult for existing international entities to create considerable global collaboration. Fostering collaboration, boosting trust, and guaranteeing collective cybersecurity can all be facilitated by a globally agreed-upon framework provided by an international convention. It is encouraging that existing international bodies have tried to tackle the problem of cyberattacks. However, due to the ever-changing nature of cyber dangers and the limitations of existing international legal and institutional frameworks, the response to these risks has been inadequate thus far. A new international convention aimed at countering cyber dangers has great promise. This framework has the potential to be transparent, all-encompassing, and flexible in order to facilitate international collaboration, define criminal actions, and establish enforcement procedures.

A major step toward a more secure and safe internet would be the adoption of such a convention. When it comes to settling disputes and interpreting international law, the International Court of Justice (ICJ) and other international judicial authorities have been at the forefront (Harrison Dinniss, 2012). However, there are several obstacles to their

efficiency and compatibility in dealing with cyberattacks. The ICJ must have jurisdiction over a matter to rule on it, and this is normally accomplished with the cooperation of the participating governments. However, it is challenging to establish the people involved and acquire their agreement in cyberattacks since their origins are often unknown and they can be organized from various jurisdictions. In making their decisions, the ICJ and other comparable tribunals frequently look to precedent and established principles of international law. Since cyberwarfare is still in its infancy, few examples may serve as guides. Given the complexity and novelty of cyber warfare, it may be challenging for the court to apply existing legal rules (Bucci, 2018).

Cases heard by international courts might take years to resolve due to the complexity of the law involved. However, cyberattacks happen at breakneck speed and require fast response and resolution. It is difficult for these organizations to adequately resolve cyber conflicts due to a mismatch between the pace of judicial proceedings and the fast expanding cyber scene. There is no agreement on how sovereignty, non-intervention, and the use of force under traditional international law are to be interpreted in the context of cyber operations. In 2018, UK Attorney General Jeremy Wright gave a lecture in which he argued that a country's cyber infrastructure should be considered part of its sovereign territory[2]. Because of these discrepancies, international courts may issue decisions that are at odds with one another. The United Nations Charter, the Geneva Conventions, and a few other non-binding, normative rules form the backbone of international law's determination of what is and is not permissible. The problems of attribution, non-physical injury, and governmental accountability in cyberspace are not easily addressed by these laws because they were written for a time before the Internet. The ease with which cyberattacks may be routed across numerous countries makes, for instance, tracking them back to a state actor challenging when they occur. The legal evaluation of such operations is further complicated by the lack of clarity on what constitutes an 'armed attack' in cyberspace.

Introducing clear definitions, standards, and norms that are tailored to the digital realm can be made possible by a new International Convention (Nissenbaum, 2015). Existing legal frameworks present major obstacles to enacting countermeasures against cyberattacks. It is debatable whether or not governments have the right to self-defence against cyberattacks under Article 51 of the United Nations Charter. And unlike traditional combat, there is no consensus on whether or not such actions are necessary or proportionate in cyberspace (Cornish, 2021). Clearer standards for countermeasures might be established with the creation of a new International Convention that incorporates concepts of proportionality, need, and differentiation specific to cyberspace. The United Nations and other already-existing international organizations have taken some important

[2] Schmitt, M. (2022, 24 May). The United Kingdom on International Law in Cyberspace. EJIL: Talk! https://clck.ru/3F3MMo

steps in combating cybercrime. However, they are not always successful because of things like conflicting laws and jurisdictional issues. To properly deal with cyberattacks, international law and institutions must be instrumentalised. To do so, however, would need extensive changes to adapt to the ever-changing nature of cyber threats and circumvent the challenges presented by the digital realm. The frequency and severity of cyberattacks can be mitigated by the adoption of new international conventions that define, standardize, and enforce countermeasures.

3.2. Need for Translating Legal Standards to the Cyberspace

Due to the unconventional nature of cyber operations, it might be difficult to apply traditional legal standards like distinction, proportionality, and military necessity in case of cyberattacks and cyber countermeasures. For example, combatants and civilians must be treated differently, and only legitimate military targets should be attacked, according to the concept of distinction. Because of the anonymity and attribution issues inherent in cyberspace, determining the origin and type of an attack is a major difficulty in cyberwarfare. Distinction in cyberspace has serious difficulties because to the overlap between military and civilian computer systems, networks, and infrastructure. Again, according to the concept of proportionality, an attack can only be launched if the anticipated military benefit justifies the risk to people and civilian infrastructure. Accurately assessing the probable implications of an attack and estimating the collateral damage it may create is difficult in the context of cyber warfare. A cyber operation's unforeseen secondary implications and cascade impacts can be hard to foresee due to the interrelated structure of computer systems and networks. Moreover, to achieve legitimate military objectives, force may be used, however using excessive force is forbidden under the concept of military necessity (Singer & Friedman, 2014). The definition of a legitimate military aim in cyberwarfare is problematic and complicated. In addition to conventional military targets, key infrastructure, economic systems, and information networks are common cyber operations. Since the impacts of cyber operations may reach well beyond traditional military objectives, determining when they become unnecessary is a significant difficulty.

According to Michael Schmitt (2013), the same distinction, proportionality, and military necessity rules that apply to conventional conflict also apply to cyber warfare. He says that sides to a fight must tell the difference between civilians and combatants and aim their strikes solely at the former. Parties to a conflict are bound by the concept of proportionality to employ only the level of force that is both necessary and proportional to their expected military advantage. The parties to a war are bound by the concept of military necessity to employ no more force than is strictly required to accomplish an aim that can be justified by the use of force. Cyberwarfare may be viewed through the same lens as conventional warfare, according to Michael Schmitt, who stresses the need of using the concepts of difference, proportionality, and military necessity. He contends that in the event of a cyberattack, the parties involved should

still identify fighters from civilians and focus their attacks on the former. The principle of proportionality dictates that only a reasonable scale of force should be employed to achieve a particular military objective. According to the principle of military necessity, force should only be used when absolutely necessary to achieve a legitimate military objective. Schmitt argues that these guidelines can let nations engage in cyber operations while remaining compliant with international norms (Schmitt, 2013).

Similarly, according to Professor Cordula Droege (2012), the peculiarities of cyber operations make it impossible to apply the traditional criteria of distinction, proportionality, and military necessity to cyber conflict. Cyber activities, he says, can have unforeseen implications and are sometimes hard to identify. According to Droege, nations must find novel approaches of applying the criteria of difference, proportionality, and military necessity to cyberwarfare. He argues that distinction, proportionality, and military necessity might be difficult to apply to cyber operations due to their specific nature. Droege agrees that determining responsibility for the effects of cyber operations may be challenging. Therefore, nations, in his view, need to innovate in order to adapt these ideas to cyber warfare (Droege, 2012). The complexity of cyber operations necessitates novel approaches and concepts. Furthermore, according to Russel Buchan (Buchan, 2012), they must be interpreted in a way that takes into account the special nature of cyber operations. The impacts of cyber operations can be both physical and non-physical, he explains. According to Buchan, governments must exercise caution while conducting cyber operations so as not to contravene these values. Buchan suggests bringing distinction, proportionality, and military necessity to cyber conflicts as a means of striking a fair balance. However, he does note that these notions need to be interpreted with the specifics of cyber operations in mind. Cyber operations may have several concrete and intangible implications, as Buchan acknowledges. Therefore, he warns against straying from the norms of caution and responsibility when conducting cyber operations (Buchan, 2012).

3.3. The Inadequacy of Traditional Warfare Principles in Cyberspace

One of the biggest problems with creating cyber warfare principles that are in line with traditional combat is attribution. Cyberattacks can be difficult to trace back to their source (Denardis, 2020). This is due to the fact that tracing the initiation of a cyberattack might be tricky in some cases. This makes it harder to hold governments responsible for their actions and discourage attacks before they happen. When adapting traditional methods of conflict to the digital domain, it might be difficult to rule out unintended consequences. Cyberattacks can have a wide variety of physical and non-physical effects. An assault on a government's computer network, for instance, may have the unintended consequence of bringing down essential services like the electricity grid or the water supply. This complicates the task of ensuring that cyber activities are reasonable and appropriate. Cyber operations are intricate and not always easy to grasp (Winterfeld & Andress, 2013).

Because of this, it is hard to apply the concepts of proportionality, differentiation, and military necessity. It may be difficult to tell if a cyber operation is aimed against a military target or a civilian population. Assessing the possible physical and non-physical implications of a cyberattacks can be challenging as well.

There are a number of problems that must be solved before the traditional principles of armed conflict can be adapted to cyber warfare. Cyberwarfare is difficult to define precisely because of this. Because of this, it's hard to establish universally accepted principles for conducting cyber warfare on a global scale. Cyber security lacks a worldwide regulatory framework. This hinders the ability of nations to work together to combat cyber threats (Whyte & Mazanec, 2018). The rate of technical development in the cyber sphere is really quick. This makes it challenging to adopt new laws and norms to manage emerging cyber dangers in a timely manner. Despite the obstacles, efforts should be made to modify the norms of conventional combat to apply to cyber battle. Rules and conventions to control cyberwarfare are necessary due to the increasing danger posed by it.

3.4. Complex Landscape beyond Sovereign Borders

The legal foundations defining jurisdiction over cyber actions are complicated and developing, according to Michael Schmitt (2012). States have considerable leeway in selecting how they will exercise jurisdiction over cyber operations, and there is no one international convention that tackles this issue directly, as he points out. Schmitt asserts that nations may be directed by a variety of overarching principles, such as the concepts of territoriality, nationality, and universality (Schmitt M. N., 2012). A nation-state's ability to regulate online behaviour inside its borders is grounded on the idea of territoriality. This implies that even if the victims of a cybercrime are situated in another country, the perpetrators can be brought to justice by the state in which the crime was committed (Schmitt, 2014). Nationality principle holds that a country is liable for the criminal acts of its residents wherever in the whole world, including when they are committed through the internet. Therefore, regardless of the location of the victims, a state can seek charges against its own nationals who commit cybercrimes. The concept of universality states that any cybercrime that satisfies the definition of a crime under international law can be prosecuted by any state, regardless of where the crime was done or by whom. It is possible to prosecute cybercriminals in a state even though they are not residents of that state if their conduct amount to crimes under international law and their victims are located in a different country (Shackelford, 2014).

But Thomas J. Holt et al. (2015) argues that there are major challenges in establishing jurisdiction over conduct performed in cyberspace. He points out the challenges of tracing the origin of cyber actions and the worldwide impact they might have. Holt highlights that, in order for nations to exert authority over cyber activities, they need to innovate new forms of cooperation. This is because it is sometimes difficult to determine the origin of a cyberattack when one is started. As a result, it

becomes more challenging to hold governments accountable for their conduct and to dissuade potential assaults. The possibility of unforeseen effects is another difficulty in establishing jurisdiction over cyber activity. The impacts of cyber assaults, both physical and otherwise, can be rather diverse. An assault on a government's computer network, for instance, may have the unintended consequence of bringing down essential services like the electricity grid or the water supply (Shackelford, 2012). This complicates the task of ensuring that cyber activities are reasonable and appropriate. As the usage of cyber activities grows, the difficulties in establishing and enforcing jurisdiction over them are only going to increase, according to Peter M. Shane (Shane & Hunker, 2013). According to him, states need to get creative in order to deal with the difficulties of enforcing their authority over online activity. It is expected that the difficulties of exercising jurisdiction over cyber operations would increase as cyber technology develops further. To meet these difficulties, states will need to innovate new forms of cooperation and coordination (Shane & Hunker, 2013). They'll also have to write up some brand-new rules for controlling online behaviour.

Jurisdictional problems over cyber operations are complicated and constantly developing. Since cyber activities are not addressed by a single international convention, individual governments have considerable leeway in establishing the scope of their own jurisdiction. However, there are a number of broad principles that may be used to govern the behaviour of nations. These concepts include territoriality, nationality, and universality. There are substantial difficulties in enforcing jurisdiction over cyber activity (Roscini, 2010). The perpetrators of cyberattacks are not always obvious, and their effects can be felt all around the world. The successful exercise of jurisdiction over cyber activities requires new forms of cooperation between states. As the usage of cyber activities increases, the difficulties in exercising jurisdiction over them are likely to persist. The difficulties of asserting state authority over online activity require states to take proactive measures. Cyber security lacks a worldwide regulatory framework. This hinders the ability of nations to work together to combat cyber threats. The rate of technical development in the cyber sphere is really quick (Gheciu & Wohlforth, 2018). This makes it challenging to adopt new laws and norms to manage emerging cyber dangers in a timely manner. Cyber security challenges are not being addressed with enough international collaboration. This complicates efforts to create and implement global standards for cyber behaviour.

Conclusion

The legal consequences and difficulties of cyberattacks and cyber countermeasures have been investigated in this research. It has been highlighted how difficult it is to pinpoint the origin of cyberattacks and how crucial it is to take proportionality into account when formulating cyber countermeasures. The research has also discussed the effect of cyber countermeasures on human rights, the legal consequences of countermeasures

against non-state actors, and the legal foundations for international cooperation. In addition, it has examined the legal parameters for pre-emptive cyber operations, the level of state accountability, the difficulties of defining and verifying cyber weapons, the regulatory structures for intelligence operations, the function of cybersecurity measures in safeguarding civilians and critical infrastructure, the difficulties of establishing jurisdiction over cyber activities, and the relationship between cybersecurity and the right to development. By incorporating these less explored issues of international law framework, the research hopes to contribute to the formation of legal frameworks and norms controlling countermeasures in cyber warfare, therefore promoting inclusive and sustainable growth while maintaining the preservation of individual rights and international cybersecurity. As the globe becomes more linked, cyber-related risks remain a pressing concern that makes national borders ineffective and challenges the limits of current international legal systems. The 'grey zone' of undefined legal principles that characterises the digital realm makes it difficult to determine whether or not cyberattacks are actually criminal. The lack of consensus on a generally enforceable definition of cyberattacks and on how conventional principles of international law apply to these modern difficulties is a significant lacuna in the legal system. An entirely separate International Convention is required to address the intricacies of the cyberspace. Existing frameworks have their limits and jurisdictional issues that a Convention similar to this may help clear up. The work is challenging, but it is necessary to maintain global stability in an era when wars are just as likely to be fought online as they are on the ground. International bodies have tried to tackle the problem of cyberattacks. However, a proper response has been elusive due to the ever-changing nature of cyber threats and the limitations of existing international law and institutional frameworks. There is hope in a new international convention that aims to deal with cyber dangers. This framework has the potential to be transparent, all-encompassing, and flexible in order to facilitate international collaboration, define criminal actions, and establish enforcement procedures. Such a Convention would be a huge step forward in making the internet a more secure and safe place. Therefore, it is essential to re-evaluate and adapt the current legal infrastructure, or to investigate the possibility of establishing a specific international agency, that can effectively respond to the peculiarities of cyber warfare.

References

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic. a

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001
Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.
Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0
Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246
Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583
Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960
Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001
Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878
Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466
Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001
Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759
Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice : Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002

Nissenbaum, D. (2015). *A Street Divided : Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288
Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.
Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.
Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526
Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838
Shane, P. M., & Hunker, J. A. (Eds.) (2013). Cybersecurity : Shared Risks, Shared Responsibilities. Carolina Academic Press.
Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001
Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217
Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2
Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057
Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410
Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.
Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724
Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352
Watt, E. (2021). State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Elgar. https://doi.org/10.4337/9781789900101
Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.
Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504
Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier.
Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.
Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.
Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Authors information

Mohammad Minhazur Rahman – LLM, Lecturer, Department of Law, State University of Bangladesh
Address: South Purbachal, Kanchan, Dhaka-1461, Bangladesh
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450

Tapos Kumar Das – LLM, Associate Professor, Department of Law & Justice, Jahangirnagar University; PhD Student, School of Law, City University of Hong Kong
Address: Savar, Dhaka-1342, Bangladesh; 83 Tat Chee Avenue, Kowloon Tong, Kowloon, Hong Kong
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 1, 2024
Date of approval – April 18, 2024
Date of acceptance – December 13, 2024
Date of online placement – December 20, 2024

Научная статья
УДК 34:004:341.4:004.8
EDN: https://elibrary.ru/nnftqi
DOI: https://doi.org/10.21202/jdtl.2024.46

Противодействие кибератакам: пробелы международного права и перспективы их преодоления

Мохаммад Минхазур Рахман ✉

Государственный университет Бангладеш, Дакка, Бангладеш

Тапос Кумар Дас

Джахангирнагарский университет, Дакка, Бангладеш
Городской университет Гонконга, Гонконг

Ключевые слова

кибератака,
киберпреступность,
международная конвенция,
международное право,
права человека,
право,
принцип должной осмотрительности,
принцип соразмерности,
принципы международного права,
цифровые технологии

Аннотация

Цель: категорирование кибератак в национальном и международном правопорядках и определение юридических мер противодействия им на международном уровне.

Методы: представлены доктринальным юридическим анализом, формально-юридическим, сравнительно-правовым методами, синтезом, индукцией, дедукцией, а также методикой правового прогнозирования и моделирования. Исследованию подверглись международно-правовые документы и акты национального законодательства, судебные прецеденты, доктринальные источники.

Результаты: в статье определены юридические последствия кибератак, выявлены трудности определения и привлечения лиц и организаций к ответственности за их совершение, обозначены национальные меры противодействия кибератакам на основе принципа пропорциональности, систематизированы международно-правовые основы реагирования на кибератаки. Основное внимание в работе уделено актуальным проблемам выявления и проверки кибероружия, установления международных стандартов его использования, разработки методов разоружения или ограничения наступательных кибервозможностей. Поставлен вопрос обеспечения гуманитарной деятельности, защиты важнейших объектов инфраструктуры, а также населения с помощью мер кибербезопасности в военное время. Проанализированы правовые основы и выявлены пробелы и иные дефекты действующего регулирования в осуществлении юрисдикции в таких областях кибердеятельности, как международные операции, локализация данных и экстерриториальное исполнение национального законодательства.

✉ Корреспондирующий автор

Разработаны и описаны параметры, в рамках которых государства вправе проводить упреждающие кибероперации для предотвращения или сдерживания кибератак (киберконтрмеры), основными из которых являются проявление должной осмотрительности, законность принятии решения о применении киберконтрмер, соразмерность защиты от последствий совершения противоправных действий.

Научная новизна: обусловлена представленными в статье прогрессивными решениями в области международно-правового регулирования принятия государствами киберконтрмер в ответ на киберпреступления, сформулированными с учетом влияния обозначенных мер противодействия на права и свободы человека и гражданина, в том числе такие как право на неприкосновенность частной жизни и свобода слова.

Практическая значимость: результаты проведенного исследования могут быть взяты за основу при разработке и совершенствовании международно-правовых инструментов в области борьбы с кибератаками и обеспечения кибербезопасности, а также могут послужить образцом для национального законодателя при проектировании правотворческих решений противодействия киберпреступлениям.

Для цитирования

Рахман, М. М., Дас, Т. К. (2024). Противодействие кибератакам: пробелы международного права и перспективы их преодоления. *Journal of Digital Technologies and Law*, *2*(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46

Список литературы

Andrew, J., & Bernard, F. (Eds.) (2021). *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509938865

Bucci, S. (2018). Strategic Cyber Deterrence: The Active Cyber Defense Option by Scott Jasper. Rowman & Littlefield, 2017, 255 pp. *Strategic Studies Quarterly*, *12*(2), 134–135.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. https://doi.org/10.1093/jcsl/krs014

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic. Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Dean, S. E. (2013). Cyber Defense: securing military systems and critical civilian infrastructure from an electronic. *HRISQ*, *XIII*(3), 911.

Denardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press. https://doi.org/10.2307/j.ctvt1sgc0

Droege, C. (2012). Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross*, *94*(886), 533–578. https://doi.org/10.1017/s1816383113000246

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, *3*, 52. https://doi.org/10.5204/lthj.1583

Etzioni, A., & Rice, C. J. (2015). *Privacy in a Cyber Age*. Springer. https://doi.org/10.1057/9781137513960

Faga, H. P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of Law & Politics*, *10*, 27. https://doi.org/10.1515/bjlp-2017-0001

Friis, K., & Ringsmose, J. (Eds.) (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge & CRC Press. https://doi.org/10.4324/9781315669878

Frowe, H. (2022). *The Ethics of War and Peace: An Introduction*. Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781003275466

Gheciu, A., & Wohlforth, W. C. (2018). *The Oxford Handbook of International Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198777854.001.0001
Gow, J., Dijxhoorn, E., Clare Kerr, R., & Verdirame, G. (Eds.) (2019). *Routledge Handbook of War, Law and Technology*. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315111759
Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press. https://doi.org/10.1017/cbo9780511894527
Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, *5*(1), 3. https://doi.org/10.1093/cybsec/tyy009
Hollis, D. B., & Finnemore, M. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge. https://doi.org/10.4324/9781315777870
Joyner, C. C. (2011). United States foreign policy interests in the Antarctic. *The Polar Journal*, *1*(1), 17–35. https://doi.org/10.1080/2154896x.2011.569384
Katagiri, N. (2021). Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009
Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.
Knowles, J., & Thomas, P. A. (2016). *Effective Legal Research*. Sweet & Maxwell.
Kulesza, J., & Balleste, R. (2015). *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.
Levite, A., & Perkovich, G. (2017). Understanding cyber conflict. Georgetown University Press. https://doi.org/10.1353/book62546
Lewis, D. A., Modirzadeh, N. K., & Blum, G. (2019). Quantum of Silence: Inaction and Jus Ad Bellum. *Harvard Law School Program on International Law and Armed Conflict*. https://doi.org/10.54813/azzk2231
Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic & International Studies; Rowman & Littlefield.
Liivoja, R., & Väljataga, A. (Eds.) (2021). *Autonomous Cyber Capabilities under International Law*. NATO Cooperative Cyber Defence Centre Of Excellence 2021.
Lucas, G. (2016). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001
Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://doi.org/10.1093/jcsl/krw014
Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1d989jr
Mihr, A. (2017). *Cyber Justice : Human Rights and Good Governance for the Internet*. Springer.
Mihr, A. (2016). Cyber justice: cyber governance through human rights and a rule of law in the Internet. *US-China Law Review*, *13*(4). https://doi.org/10.17265/1548-6605/2016.04.002
Nissenbaum, D. (2015). *A Street Divided : Stories from Jerusalem's Alley of God*. St Martin's Press.
Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.) (2015). *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford University Press.
Ossoff, W. (2021). Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace. *Harvard International Law Journal*, *62*(1), 298.
Putman, W. H., & Albright, J. R. (2018). *Legal Research, Analysis, and Writing*. Cengage Learning.
Roscini, M. (2010). World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law Online*, *14*(1), 85–130 https://doi.org/10.1163/18757413-90000050
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Schmitt, M. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*, *56*, 569.
Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54*, 13–37.
Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 1998–1999.
Schmitt, M. N. (2012). "Attack" as a Term of Art in International Law: The Cyber Operations Context. In *4th International Conference on Cyber Conflict (CYCON 2012)*, Tallinn, Estonia (pp. 1–11).
Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (2014). Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, *54*, 698.

Schneier, B. (2013). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer.

Shackelford, S. J. (2012). Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance. *American University Law Review*. https://doi.org/10.2139/ssrn.2132526

Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. https://doi.org/10.1017/cbo9781139021838

Shane, P. M., & Hunker, J. A. (Eds.) (2013). Cybersecurity : Shared Risks, Shared Responsibilities. Carolina Academic Press.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

Travis, P. (2016). We're Going to Nicaragua: The United States, Nicaragua, and Counterterrorism in Central America during the 1980s. *Journal of Terrorism Research*, *7*, 38. https://doi.org/10.15664/jtr.1217

Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — the Use of Force. In *Yearbook of International Humanitarian Law* (Vol. 15, pp. 19–43). https://doi.org/10.1007/978-90-6704-924-5_2

Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, *31*(3), 941–967. https://doi.org/10.1093/ejil/chaa057

Tyler, T. R. (2017). Methodology in Legal Research. *Utrecht Law Review*, *13*(3), 130–141. https://doi.org/10.18352/ulr.410

Van Hoecke, M. (2011). *Methodologies of Legal Research*. Bloomsbury Publishing.

Wagner, B., Kettemann, M. C., & Vieth, K. (2019). *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Edward Elgar Publishing. https://doi.org/10.4337/9781785367724

Watkins, D., & Burton, M. (2013). *Research Methods in Law*. Routledge. https://doi.org/10.4324/9780203489352

Watt, E. (2021). State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Elgar. https://doi.org/10.4337/9781789900101

Waxman, M. (2011). Cyber-Attacks as "Force" under UN Charter Article 2(4). *International Law Studies*, *43*.

Whyte, C., & Mazanec, B. (2018). *Understanding Cyber-Warfare: Politics, Policy and Strategy*. Routledge. https://doi.org/10.4324/9781315636504

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Elsevier.

Wittes, B., & Blum, G. (2016). *The Future of Violence – Robots and Germs, Hackers and Drones*. Basic Books.

Wren, C. G., & Wren, J. R. (1986). *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (2nd ed.). A-R Editions.

Yoo, C. S., & Blanchette, J.-F. (2015). *Regulating the Cloud*. MIT Press. https://doi.org/10.7551/mitpress/9780262029407.001.0001

Сведения об авторах

Мохаммад Минхазур Рахман – магистр права, преподаватель, кафедра права, Государственный университет Бангладеш
Адрес: Бангладеш, 1461, г. Дакка, Канчан, Саут Пурбачал
E-mail: sabitminhaz@gmail.com
ORCID ID: https://orcid.org/0009-0004-9764-5450

Тапос Кумар Дас – магистр права, доцент, кафедра права и юстиции, Джахангирнагарский университет; кандидат на соискание степени PhD, Школа права, Городской университет Гонконга
Адрес: Бангладеш, 1342, г. Дакка, Савар; Гонконг, Коулун, Коулун Тонг, Тат Чи Авеню, 83
E-mail: taposlaw@juniv.edu
ORCID ID: https://orcid.org/0000-0002-3349-8947

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 1 апреля 2024 г.
Дата одобрения после рецензирования – 18 апреля 2024 г.
Дата принятия к опубликованию – 13 декабря 2024 г.
Дата онлайн-размещения – 20 декабря 2024 г.