Journal of Digital Sociohumanities
ISSN: 3032-7865 **Vol. 1 No. 2 2024**
Website : https://jds.unand.ac.id
Email : jds@unand.ac.id

Defining the Rules of Engagement: Legal and Ethical Standards in Cyber Conflict

Zaza Tsotniashvili[1]

[1]Caucasus International University, Tbilisi, Georgia

Article information

DOI : 10.25077/jds.1.2.119-132.2024
Correspondence : zaza.tsotniashvili@ciu.edu.ge

Submission Track

Submission : May 27, 2024
Final Review : July 6 , 2024
Accepted : July 8, 2024

Keywords

Cyber conflict, Rules of Engagement, legal standards, ethical standards, international law, cyber warfare

Abstract

In an increasingly digitized world, cyber conflicts are emerging as a critical domain of modern warfare and international relations. This paper examines the legal and ethical standards that govern cyber conflict, aiming to define clear rules of engagement. Through a detailed analysis of current international laws, national legislation, and ethical theories relevant to cyber operations, this research identifies gaps and challenges in the existing frameworks. Case studies of notable cyber incidents illustrate the practical implications of these legal and ethical standards. The study proposes a set of refined rules of engagement designed to address these deficiencies, ensuring ma ore coherent and consistent application of legal and ethical principles in cyber conflict. The findings suggest that while international consensus and cooperation are crucial, there is also a need for dynamic and adaptable rules that can keep pace with rapid technological advancements. This paper contributes to the growing discourse on cyber conflict by providing a comprehensive understanding of the legal and ethical dimensions and offering actionable recommendations for policymakers, legal experts, and cybersecurity practitioners.

INTRODUCTION

In an era where technology permeates nearly every aspect of daily life, the digital realm has become a new battlefield for modern warfare and international relations. As nations and non-state actors increasingly exploit cyberspace for strategic advantage, the need for well-defined rules of engagement in cyber conflict has never been more pressing. The increasing prevalence of cyber-attacks has transformed cyberspace into a new battlefield, necessitating the development of rules of engagement for cyber warfare (Lancelot, 2020). The lack of clear international laws and the challenge of attributing attacks to specific actors complicate efforts to address cyber conflicts (Pipyros et al., 2016). The evolution of cyber warfare has led to the emergence of "state-sponsored hacktivism," blurring the lines between crime, espionage, and conventional warfare (Lucas, 2016). This shift requires new frameworks for just war theory and international law to govern responsible state behavior in cyberspace. Cybersecurity has become a priority in international relations, with countries militarizing cyberspace as a reflection of ongoing global tensions (Spagnol, 2021). To address these challenges, nations must develop internationally agreed-upon definitions of key terminology and concepts such as cyber resilience to better prevent, survive, and recover from cyber-attacks.

Cyber conflicts encompass various activities that threaten national security, economic stability, and societal trust (Glorioso, 2015). These conflicts can include cyber warfare, hacktivism, cybercrime, and cyber terrorism, all of which exploit the increasing dependence of societies on information and communication technologies (Glorioso, 2015). The international community is responding to these challenges by developing voluntary norms of state behavior in cyberspace, which may eventually become binding international law (Roche, 2019). Cybersecurity has become a priority in international relations, with countries militarizing cyberspace and engaging in ongoing confrontations that mirror international

tensions (Spagnol, 2021). To address these issues, there is a need for internationally agreed definitions of key terminology and the development of cyber resilience strategies (Spagnol, 2021). New ethical frameworks and legal standards are also required to govern this evolving domain of unrestricted warfare (Lucas, 2016).

The trend towards increasing cyber activity has spurred considerable research into cyber conflict's legal and ethical dimensions. For example, the Tallinn Manual provided a detailed account of international legal principles that applied to cyber operations, such as sovereignty, state responsibility, and operation during an armed conflict (Schmitt 2013). Legal scholars have looked into existing legal frameworks and how they can be applied in the context of cyber operations, with specific attention to proportionality and precautions in attack (Jensen 2012). Nevertheless, in applying those principles to specific cyber operations, there are challenges that require more specificity and granularity for planners and operators to guide them (Jensen 2012). Finally, the paper briefly considers ethical issues derived from Just War Theory applied to cyber warfare (Taddeo 2012). However, the above measures have not been enforced simply on account of the huge challenge that international law faces in underpinning cyber operations, and this is based both on various interpretations of what constitutes cyber warfare between states but also on who is considered to be actors involved (Pipyros et al. 2016). Such challenges highlight the importance of ongoing research in developing suitable legal and ethical frameworks.

This recent research demonstrates the complexities of cyber conflict and explains why applying traditional laws of armed conflict to cyberspace has proven a challenge. Some studies stress the challenges of cyber-attack identification and ambiguous rules on proportionality (Usman et al., 2022) Lancelot highlights a failure in the development of international rules of engagement to this new battlefield; as such, military strategists predict few legal implications for initiating cyberwarfare and little tit-for-tat retaliation after attacks (2020). While the US military is increasingly considering how to integrate cyber tools in its operational toolkit, designing rules of engagement that are specific to cyberspace operations as they have evolved across thirteen years remains a challenge (Kehler et al., 2017). This concept illustrates that the available legal frameworks are inadequate in regulating cyber operations properly, as cyber warfare can be defined in different ways, based on state-sponsored activities and illegal actions of non-state actors (Pipyros et al., 2016). These observations speak to the necessity of nuanced, flexible rules governing engagement in a quickly changing digital environment.

In order to highlight the legal and ethical consequences, this paper will explore a few of the fifty shades in controlling cyber conflict. Through a careful analysis of international law, national laws and ethical theories that relate to cyber operations conducted within the framework, this research highlights important lacunae in existing frameworks. A review of significant cyber incidents through a perusal case studies, provide essential context around the implications and utility of HGG norms with insights on why clearer rules about when to cross red lines are long overdue.

In this work, we aim to define the aforementioned rules that will overcome some of the gaps in existing legal and ethical frameworks but be adaptable enough for changes driven by technological advancement one would expect with respect dynamic nature of digital age. The draft rules propose to advance international consensus and cooperation as well as a predictable application of legal and ethical principles in cyber conflict.

Just like cyber threats themselves are constantly changing, so should the frameworks created to fight them. We hope that this paper will add to existing strands in the cyber conflict literature by providing a more nuanced perspective on its legal and ethical dimensions. With the need to remain vital with so many people working from home, these threats extend beyond defense and security practitioners as they do cyber cops tasked in defending businesses new front porch. This work is novel because it approaches the paradigm from an interdisciplinary perspective by articulating legal and ethical standards with operational case studies to connect theories - theory-based notions on cyber conflict - more coherently into real-world

policy dilemmas.

METHODS

Research Design

This research uses a qualitative method of combining doctrinal legal analysis and ethical evaluation with case study to provide an elaborated explanation as applicable on principles and ideas penalizing cyber Warfare if not supports ROE. We favor a qualitative approach because it is well-suited to delving into complicated legal and ethical dilemmas and can capture the complexity of cyber conflict far more thoroughly than quantitative methods.

Source of Data

Data sources consist of primary legal documents and statutes, secondary authoritative articles (including academic), case studies and expert consultations. These key legal documents will need be surveyed, ranging from international treaties such as the United Nations Charter and the Geneva Conventions to sources like the Tallinn Manual on International Law Applicable to Cyber Warfare. In doing, so the research will draw on classic legal studies and existing literature related to international law, cyber warfare as well as ROE. The more important cyber incidents, such as Stuxnet or WannaCry and the Sony Pictures attack are chosen to be dissected. These include expert consultations, which are structured interviews and surveys with professionals in international law, ethics and cybersecurity.

Data Collection

The data collection process involves several steps to gather comprehensive and relevant information. First, a thorough literature review is conducted to compile and review existing scholarship on international law, cyber warfare, and ROE. Primary legal sources are examined through a detailed doctrinal analysis to extract relevant principles and identify gaps and ambiguities in their application to cyber conflict. A comparative analysis of different national legal frameworks is performed to understand the diversity and commonalities in national legislation on cyber operations. Ethical evaluation involves establishing a theoretical framework based on key ethical theories pertinent to cyber warfare, such as Just War Theory and Utilitarianism. Ethical dilemmas specific to cyber operations, such as attribution, dual-use infrastructure, and proportionality, are identified and analyzed through the lens of these theories.

Significant cyber incidents are selected based on criteria such as impact, international attention, and the diversity of actors involved for the case study methodology. Detailed information on each case is gathered from credible sources, including government reports, academic articles, and media coverage. This comprehensive data collection ensures that the analysis is grounded in real-world contexts and covers various perspectives.

Data Analysis

Data analysis involves a combination of legal interpretive methods, ethical reasoning, and qualitative content analysis. The doctrinal legal analysis interprets primary legal sources to elucidate existing legal principles and identify gaps and ambiguities in their application to cyber conflict. Ethical evaluation applies ethical theories to analyze major ethical dilemmas in cyber operations and develop ethical guidelines for ROE. Case studies are analyzed to assess adherence to legal standards and ethical considerations, identifying lessons learned and implications for ROE.

Based on the findings from doctrinal legal analysis, ethical evaluation, and case studies, this research proposes a set of refined ROE for cyber conflict. The proposed ROE are drafted to reflect best practices and address identified gaps and challenges. To ensure robustness and applicability, the proposed ROE undergo a validation phase involving expert consultations. Feedback from experts in international law, ethics, and cybersecurity is gathered through structured interviews or surveys, analyzed, and incorporated into the final set of proposed ROE. This comprehensive and iterative data analysis process aims to develop

actionable and adaptable ROE that bridge the gap between existing legal and ethical standards and the practical realities of cyber operations.

RESULT

Legal Standards in Cyber Conflict

International Law

The applicability of international law to cyber conflict is a matter of dispute. The Tallinn Manual-a systematic study by international law researchers on more than 95 "black-letter rules" concerning cyber war, including issues surrounding sovereignty, State responsibility, and applied humanitarian law (Schmitt 2013) Newer frameworks like the UN Charter and Geneva Conventions apply in some context to cyber operations but their detailed application is uncertain given that cyberspace has been an entirely new dimension of warfare (Lin, 2012). Lin has also suggested that cyber conflict is different from other conflicts as it produces distinct features of physical defense such as complexity in terms of attributing and the range actors (2012). This is due to the fact that, while certain China and this changes approach sharety of law applicable to cyber conflict as per shared by Euro-Atlantic nations in believing existing international norm are adequate for securing cyberspace (Giles & Monaghan 2014), others such as Russia has diverging viewswould question applicability of legal framework governing usenorms relevant to risk reduction within borders which they perceive fall largely outocomplex layered structure. This controversy also might explain divergent perceptions of state behavior permitted under international humanitarian law and the Law of Armed Conflict in cyberspace (Giles & Monaghan, 2014).

On the most basic level is sovereignty - states have jurisdiction when it comes to their digital infrastructure, and respect for non-interference toes (Heinegg, 2012). But what the hell it means to violate sovereignty in cyberspace is still a mystery. According to Roscini (2014), a cyber operation can be characterize as the use of force under UN Charter when it: 1) employs a weapon; and, 2) has not only physical impact but also threatens essential services in an important scale. States are, on the one hand, sovereign rulers of their cyber infrastructure and yet have a duty to prevent it from being used against other states - also through non-state actors (Jensen 2014). So, Tallinn Manual 2.0 tells us in cyberspace you can classified the sovereignty violation by two ways such as territorial integrity and governmental functions positions against cyber operations. Information collection using cyber exploitation may breach sovereignty, but so is an act of intervention or use of force (Roscini 2014). As Cavelty & Smeets (2023) satated,

> "Over the last decades, cybersecurity has become a top priority for the European Union (EU). As a contribution to scholarship on the 'regulatory security state', we analyze how the European Union Agency for Cybersecurity (ENISA), emerged and stabilized as the EU's key agency for cybersecurity."

The concept of self-defense in cyberspace, as articulated in Article 51 of the UN Charter, is a complex issue. Scholars generally agree that cyber-attacks that cause harm are comparable to kinetic attacks, especially those targeting critical infrastructure, and can justify self-defense (Focarelli, 2015). However, attribution remains a significant challenge, with some arguing that existing international law standards can cover cyber attacks (Tsagourias, 2012), while others propose that international law must evolve to recognize attacks on critical national infrastructure as a use of force, regardless of the source (Jensen, 2007). The right to respond must be immediate due to the instantaneous nature of cyber attacks, despite traditional obstacles of attribution and characterization (Jensen, 2007). For private entities, executing counterstrikes poses risks related to cross-border issues and potential legal liabilities (Brown, 2015). The debate continues whether a law enforcement paradigm or military response is more appropriate for addressing cyber attacks (Focarelli, 2015).

The application of International Humanitarian Law (IHL) to cyber warfare presents significant

challenges, particularly regarding the principles of distinction and proportionality. The interconnectedness of military and civilian cyber infrastructure makes it difficult to distinguish between legitimate military targets and protected civilian objects (Geiss & Lahmann, 2012). This interconnectedness may lead to more frequent violations of the principles of distinction and neutrality in cyber warfare than conventional conflicts (Kelsey, 2008). The potential humanitarian impact of cyber operations on civilian populations is substantial, as attacks can affect critical infrastructure like air traffic control systems or nuclear plants (Droege, 2012). While IHL principles apply to cyber warfare, their interpretation and application in this domain remain contentious (Chang, 2017). To address these challenges, proposed solutions include exempting crucial civilian cyber infrastructure, creating "digital safe-havens," and dynamically interpreting the concept of "damage to civilian objects" within the principle of proportionality (Geiss & Lahmann, 2012).

National Legislation

There is wide variance in the development and coherence of these matters even within national legislations on cyber conflict and cybersecurity. Distinctive nations have built up strong lawful frameworks at first while others are falling behind(Shackelford & Craig, 2014) Because cyberspace is interconnected by definition, the nature of a comprehensive law enforcement strategy would mean international cooperation and agreements to build up defenses against both public infrastructure and private ones (Kosseff, 2018). Efforts to modernize cybersecurity laws, standardize legal requirements reduce unnecessary burdens by aiding the harmonization of incentives and regulations ensuring secure supply chains (Kosseff, 2018). In the U.S., legislative efforts to amend existing laws governing cybercrimes and cybersecurity through (Flowers et al. 2013), Nonetheless, the international community has not agreed on many aspects of cyber law yet; one example is what actions should be characterised as offensive or use of force in cyberspace (Kanuck, 2010). The absence of accord reveals a need for ongoing discussions and collaboration between countries to formulate sound strategies on cybersecurity (Shackelford & Craig, 2014).

The U.S., for instance, has developed a robust policy framework to govern cyber operations - with both offensive and defensive elements. The DoD Cyber Strategy defines its three primary missions as defending the DoD information network, supporting military operational and contingency plans through cyber operations when directed, and protecting against significant threats to critical infrastructure (Schmidt 2015). These strategies debatably align with the cyber defense and deterrence priorities of protecting critical infrastructure (Shackelford, 2020). Background adapted from the principles of deterrence in nuclear strategy, there is a role for The concept of an offense defense balance and/or general but active denial-based (to maintain comprehensive security) defence such as that notionally adopted within cybersecurity.(Elliot 2011). National and international legal frameworks, as well norms governing the collateral damage of cyber operations inform how politically motivated actors are likely to use this medium in inciting or employing mass violence. (Theohary & Harrington 2014) Further, the U.S. strategy notes that securing shared critical infrastructure is interdependent with allies like Canada (Shackelford 2020).

In contrast, the legal frameworks in many other nations are still evolving. Some countries focus primarily on cybersecurity from a civilian protection perspective, lacking clear policies on military cyber engagements. This disparity leads to significant challenges in international collaboration and the establishment of universally accepted standards.

Case Studies

Analyzing real-world cases helps illustrate the application and limitations of legal standards in cyber conflict. The Stuxnet attack on Iran's nuclear facilities in 2009-10 has been studied by many as an important milestone that confirmed the arrival of cyber warfare. Richardson (2011) provides the most detailed argument for Stuxnet being a cyber-armed attack under international humanitarian law, conforming to principles of distinction and proportionality. However, Haataja & Akhtarkhavari (2018)

critique the law's anthropocentric and materialist view of violence, suggesting it fails to account for non-material harm in cyberspace. Caso (2014) examines the Tallinn Manual's application to Stuxnet, classifying it as an illegal act of force. These analyses highlight the challenges in applying traditional legal frameworks to cyber conflicts, emphasizing the need for evolving international law interpretations to address cyber warfare's unique aspects.

The NotPetya episode (2017) is another important example demonstrating the difficulties of controlling autonomous cyber operations-one with implications on a large scale and unrestricted by selectivity (Kaminska et al., 2021). This attack, attributed to state actors linked to Russia, targeted Ukraine's infrastructure but rapidly spread globally, causing widespread collateral damage (Trautman & Ormerod, 2018). Such an incident also highlights the importance of prudent state behavior in cyberspace - to zero collateral damage operations or prey strike reviews (Kaminska et al, 2021). The international reaction to NotPetya became an early lesson on the need for public attribution by states in forming a rudimentary global order in cyberspace. The international response to NotPetya emphasized the importance of public attribution in developing an embryonic international regime for cyberspace. The NotPetya incident also highlighted the evolving threats of ransomware to corporations and the need for enhanced cybersecurity measures (Trautman & Ormerod, 2018). García-Vargas et al. (2023) mentioned that:

> "Another important aspect to explore in future research is a possible adaptation of the system to simulate other types of situations. In fact, we have already constructed a variation to the system that corresponds more closely to a situation of cyberbullying than one of cyber-conflict. In the situation reported here, the aggression is bilateral and there is no clear power imbalance between the two mutually aggressive alleged peers."

The application of existing legal standards to cyber conflict faces several challenges. Attribution remains a significant hurdle due to cyberspace's anonymity and transnational nature, complicating efforts to identify and hold perpetrators accountable (Abu Alead & Altalibe, 2023; Watney, 2014). The lack of a comprehensive international treaty addressing cyber warfare contributes to legal uncertainty (Nyabuto, 2018; Usman et al., 2022). The absence of precise regulations for proportionality and the difficulty in determining the threshold for prohibited intrusions further complicate the application of international law to cyber conflicts (Usman et al., 2022; Watney, 2014). Although previous frameworks, such as the UN Charter and Tallinn Manual offer guidelines for trusting cyber warfare (Usman et al., 2022; Watney, 2014), these framings lack coverage of all dimensions. To respond to these gaps, the legal review of weapons needs increased consistency and greater preparedness by some in the international community,to apply International Humanitarian Law (Nyabuto:2018).

There is also a need for greater clarity and consensus on key definitions, such as what constitutes a use of force or an armed attack in cyberspace. The development of cyber-specific protocols under existing international law could enhance legal clarity and facilitate more consistent application across different jurisdictions.

The integration of cyber operations into international and national legal frameworks is an imperative but complex endeavor. While existing laws provide a foundation, they must evolve to address the unique characteristics and challenges of cyberspace effectively. This requires ongoing dialogue and collaboration among states, legal experts, and technologists to develop robust, universally accepted legal standards for cyber conflict.

Ethical Standards in Cyber Conflict

Ethical Theories

Cyber conflict raises complex ethical issues stemming from multiple potential standards. Although developed primarily for the context of conventional warfare, Just War Theory is not well-suited to cope with cyberwarfare due to its intrinsic lack of direct physical injury and challenges in attribution (Dipert

2010: Taddeo 2012). To address these limitations the alternative framework of Information Ethics has been suggested (Taddeo 2012). Cyber processes move at a far more rapid pace, requiring speedy decision-making that may include assistance or be automated by autonomous systems, and therefore, raise concerns about compliance with ethical imperatives (Prescott 2014). Significant efforts should be made to develop the moral and professional character of future cyber commanders, as well as their understanding of military ethics issues such as the same Laws of Armed Conflicts (LOAC) through unique approaches which include a "Ordinary Soldiers" lesson plan by synthesizing these elements in an information operations-like setting for better relevance with holistic operation environment like that described above. Ethical principles and international regulations of cyber warfare are making it strive in the digital world as a new reality adapted to face these challenges (Dipert, 2010; Denning, 2009).

Just War Theory is traditionally applied to the context of armed conflict and comprises two main components: *jus ad bellum* (the right to go to war) and *jus in bello* (the right conduct in war). In cyber conflict, *jus ad bellum* demands that cyber attacks be employed as a last resort and for a just cause, such as self-defense. *Jus in bello* requires that cyber operations distinguish between combatants and non-combatants and that any harm caused is proportional to the military advantage gained.

Utilitarianism, which advocates for actions that maximize overall happiness or well-being, can also be applied to cyber conflict. Cyber attacks, to be legitimate national security tools, have to conform to moral concerns and the common good (Lonsdale, 2020). Utilitarianism: Greatest happiness for the greatest number, proposed to help create a just society and equitably distribute resources (Ikegbu & Diana-Abasi, 2017). Barrett (2013) evaluates their legitimacy using just war criteria, considering rights forfeiture and impacts on combatants and civilians. Shaw (2016) offers a thorough utilitarian investigation of the ethics of war, including pacifism, humanitarian intervention, and civilian immunity. Together, these works imply a role for utilitarian values in ethical thinking about the conduct of a cyber conflict that requires assessing likely and potential impacts on society to maximize utility (e.g., overall well-being) while assuring minimal harm. Tsotniashvili (2024) proposed that:

> "The Integration of Artificial Intelligence (AI) has revolutionized the landscape of militaryoperations, introducing cutting-edge technologies that enhance efficiency, decision-making, andstrategic planning. This article explores the multifaceted role of AI in military applications, focusing on its impact on operations, predictive analysis through machine learning algorithms, andthe challenges and solutions in the realm of cybersecurity" (Tsotniashvili, 2024)

Cyber conflict introduces unique ethical dilemmas that complicate adherence to traditional moral principles. One of the most significant challenges is the attribution problem. The cyberwarfare attribution problem is often worse for the prospective victim than if they were successful in self-docile regulation because of a series of deterrence and due escalation. Attribution challenges undermine deterrence but may also inhibit conflict escalation by reducing the political appetite for draconian forms of retribution (Jardine & Porter 2020). The non-kinetic nature of cyberwarfare and its ability to cause loss without physical effects or humans creates s (Dipert, 2010), leaving the traditional just war criteria combined with international law applications complex. These arguments lead to discussions on whether or not cyberspace conflicts can be governed through the existing frameworks (Lucas, 2014). Attribution is a multilateral challenge -technological, geopolitical, and legal-ghosting attacks may disrupt international relations (Alead & Altalibe, 2023). Consequently, cyber warfare may result in protracted bouts of low-level, multilateral warfare, requiring the development of models that seek to balance ethical concerns with functional strategies to reduce total harm (Dipert 2010).

"The need for cyber ethics is a result of the adverse effects brought by computers in the community not only in the social realm but also in the educational arena. This is because although every users has benefited from the consumption of computers, there have been some adverse issues accompanied by their use. It includes issues related to loss of privacy, Inappropriate content online, unfair use of copyright

policies, cyberbullying, plagiarism, poor netiquette in interaction online." (Santhosh T, 2024)

Another dilemma is the dual-use nature of many cyber targets. Unlike traditional warfare, many cyber targets serve civilian and military purposes, such as communication networks, power grids, and financial systems (Dipert, 2010; Droege, 2012). Striking these targets can lead to severe civilian harm, raising questions about the proportionality and necessity of such actions.

Privacy is also a critical ethical consideration (Miller et al., 2021; Power et al., 2021). Cyber operations often involve extensive surveillance and intelligence-gathering, which can infringe upon the privacy rights of individuals. Balancing national security interests with protecting individual privacy rights presents a significant ethical challenge.

Case Studies

Real-world cyber incidents are a powerful source of knowledge for considering the ethical implications of this type of conflict. The 2017 WannaCry ransomware attack represents one example that illustrates the ethical challenges as well as the large-scale consequences of cyber warfare (Botes & Lenzini, 2022). The implementation of the indictment containing stages such as deployment, installation, destruction, and command-and-control performed by WannaCry indicated for modern cyberweapons a level equivalent to conventional military weapon systems (Kao et al., 2019). The attack had global implications, underlining the ethics of cyberweapons. Whether they can be trusted to work reliably is so precise as to rule out collateral damage and if a response to physical effects is practical (Rowe 2010). These concerns underscore the pressing requirement for cyberraft treaties and ethics (Rowe, 2010; Botes & Lenzini, 2022).

The 2014 Sony Pictures hack credited to North Korea also raised ethical dilemmas of state holding corporations for ransom via cyber-attacks (Haggard & Lindsay, 2015). The hack exposed corporate data and imperiled the lives of those engaged in producing the film, exemplifying further ethical divergences regarding state-to-non-state targeting to achieve political objectives (Lucas, 2015). The incident led to widespread global chilling of free speech, with Sony initially deeming the film unacceptable and causing self-censorship across the entertainment industry (Wilton 2017). The Huffington Post counters that the method by which this attack was carried out is a probable example of "soft war," an ongoing transformation between state and non-state actors working in digital gray areas apparently outside existing international laws, mirrors earlier situations -the Ebola circumstances are globalist ones as there have been no clear sections for defense against such online pathogens. The Sony hack underscores the changing face of cyber threats - and the ways in which enterprises, society, and free speech values can be protected from them.

Challenges and Gaps

Several challenges impede the establishment of coherent ethical standards in cyber conflict. One significant issue is the lack of consensus on ethical frameworks applicable to cyber warfare. While traditional military ethics provide some guidance, the unique nature of cyberspace demands the development of new ethical principles tailored to its characteristics.

Finally, there is the problem of international cooperation and consistency. Ethical standards can vary widely between cultures and legal systems, complicating efforts to establish universally accepted norms. This disparity often leads to unilateral actions that do not consider the broader ethical implications for the international community.

The ethical landscape of cyber conflict is complex and evolving. While traditional ethical theories such as Just War Theory and Utilitarianism provide a starting point, the unique challenges of cyberspace necessitate the development of new ethical guidelines. Addressing these challenges requires a collaborative effort among states, ethicists, and technologists to create a coherent and universally accepted set of ethical standards for cyber conflict.

Rules of Engagement for Cyber Conflict

Rules of Engagement (ROE) in cyber operations present unique challenges compared to traditional warfare. While the classic ROE concept can be adapted for cyber operations, customization may be necessary to address the specific characteristics of autonomous weapons and cyber capabilities (Boddens Hosang, 2020). The formulation of cyber-specific ROEs is complicated by issues related to command and control, escalation of force, and limited operational experience (Kehler et al., 2017). The lack of international rules for cyberwarfare and difficulties in attribution pose significant challenges for cyber-diplomacy and national security (Lancelot, 2020). To meet obligations under the Law of Armed Conflict and ROE, cyber commanders may need to rely on autonomous decision-making processes (ADPs) due to the potential near-light speed of cyber operations (Prescott, 2013). Developing effective, legally compliant ADPs and addressing the unique aspects of cyber operations is crucial for establishing a comprehensive framework for cyber ROE.

The existing rules of engagement for cyber conflict are often derived from broader military doctrines, international laws, and national cybersecurity and defense policies. These rules typically cover aspects such as:

- Authorization: Cyber operations must be authorized by a legitimate authority, often at the highest levels of government or military command.
- Objectives: Operations should have clearly defined and lawful objectives, consistent with national security goals and international legal obligations.
- Proportionality: Actions in cyberspace must be proportional to the threat or attack they aim to counter, ensuring that the response does not inflict excessive harm relative to the military advantage gained.
- Distinction: Cyber operatives must distinguish between military and civilian targets, aiming to minimize harm to civilian infrastructure and lives.
- Attribution: Efforts must be made to accurately identify the origin of cyber attacks before responding, to avoid misattribution and unjust retaliation.
- Collateral Damage: Any potential collateral damage must be assessed and minimized, with operations designed to limit impact on civilian systems.

To address the unique challenges of cyber conflict and enhance current frameworks, the following refined Rules of Engagement are proposed:

- All cyber operations should be meticulously documented, with records maintained for accountability and future review. Transparency with relevant international bodies, where feasible, can also help build trust and cooperation.
- Invest in and utilize advanced technologies and international cooperation for accurate attribution of cyber attacks. This includes collaborative frameworks for information sharing and joint investigation mechanisms.
- Implement systems for real-time ethical and legal assessments during cyber operations. This could involve the use of dedicated oversight teams or AI-driven tools to ensure compliance with ethical and legal norms.
- Develop and maintain predefined engagement protocols for different types of cyber threats. These protocols should be regularly updated to keep pace with evolving threat landscapes and technological advancements.
- Strengthen international collaboration to develop universally accepted ROE. Engage with international organizations like the United Nations and regional bodies to harmonize cyber

conflict norms and standards.

- Establish specific guidelines for operations involving dual-use infrastructure. This includes conducting thorough risk assessments and developing contingency plans to mitigate potential civilian harm.
- Conduct comprehensive post-operation reviews to assess the effectiveness, compliance, and impact of cyber operations. Hold individuals and entities accountable for any breaches of ROE or unintended consequences.
- Create adaptive ROE frameworks that can be quickly updated in response to new threats and technologies. This involves establishing processes for continuous

To operationalize these proposed ROE, the following strategies should be considered:

- Training and Education: Provide comprehensive training for cyber operatives on the legal and ethical aspects of cyber warfare, including scenario-based exercises to practice adherence to ROE.
- Technological Integration: Develop and deploy advanced technologies for real-time monitoring and compliance checks during cyber operations, leveraging AI and machine learning where appropriate.
- Policy Integration: Ensure that national cyber policies and strategies explicitly incorporate the refined ROE, with clear guidance on their application and enforcement.
- International Forums and Agreements: Actively participate in international forums to advocate for and contribute to the development of global standards for ROE in cyber conflict.

The establishment and implementation of clear, comprehensive, and adaptive Rules of Engagement for cyber conflict are essential to navigate the complexities of the digital battlefield. By integrating legal and ethical standards, these ROE can help ensure that cyber operations are conducted responsibly, minimizing harm and enhancing global security and stability.

DISCUSSION

The convergence of legal and ethical standards in cyber conflict is crucial to effective governance and conflict management in cyberspace. This research highlights several critical insights. First, existing international laws, such as the United Nations Charter and the Geneva Conventions, provide a foundational framework for addressing cyber conflict but require significant adaptation to be fully effective in the digital realm. The Tallinn Manual represents a pivotal effort in this domain, offering a detailed interpretation of how international law applies to cyber warfare. However, its non-binding nature limits its enforcement capabilities and universal acceptance.

Ethically, theories such as Just War Theory and Utilitarianism provide valuable perspectives but need refining to address the unique characteristics of cyber operations. The principle of distinction, for instance, faces severe challenges in cyberspace, where military and civilian infrastructures are often intertwined. Similarly, proportionality in cyber responses must consider not only immediate effects but also potential long-term impacts on civilian populations.

This research underscores the necessity for policymakers to prioritize the development of comprehensive, coherent rules of engagement (ROE) that integrate both legal and ethical considerations. Policymakers must engage with international bodies to advocate for legally binding treaties or agreements that address the specifics of cyber warfare, building on the foundations of the Tallinn Manual and other frameworks.

For military strategists and cybersecurity practitioners, these findings suggest an urgent need to invest in technology and training that support accurate attribution and proportional responses. Enhanced

capabilities in attribution will not only improve the precision of defensive and offensive cyber operations but also enhance the credibility and legitimacy of state actions in the eyes of the international community.

Ethically, the findings highlight the critical importance of safeguarding civilian infrastructure and minimizing collateral damage. The principle of precaution should be integral to all cyber operations, requiring operatives to anticipate and mitigate potential harms to civilian entities. Additionally, privacy considerations must be balanced against national security imperatives, demanding transparent policies and oversight mechanisms to prevent abuses.

The rapid evolution of cyber threats necessitates ongoing technological adaptation. Governments and organizations must continuously update their cyber strategies and ROE to keep pace with emerging threats and technological advances. This requires a dynamic and flexible approach to cybersecurity, including real-time ethical and legal assessments during cyber operations and post-operation reviews to evaluate performance and compliance.

Several areas warrant further research. First, more empirical studies are needed to understand current and proposed ROE's real-world application and effectiveness in cyber conflict. Additionally, interdisciplinary research that combines insights from law, ethics, technology, and international relations can offer more holistic solutions to the challenges identified.

Research should also focus on developing tools and frameworks for better attribution of cyber attacks. This includes leveraging AI and machine learning advances to improve detection and identification processes. Moreover, studies need to explore the long-term societal impacts of cyber operations, particularly regarding privacy, civil liberties, and public trust in digital infrastructure.

This research faces several limitations, including the rapidly changing nature of cyber threats and the evolving legal landscape. The non-binding nature of many legal frameworks discussed, such as the Tallinn Manual, limits their practical enforceability. Furthermore, the diversity of national legislations and ethical perspectives complicates the establishment of universally accepted standards.

Defining clear and comprehensive rules of engagement for cyber conflict is vital for navigating the complexities of this new domain of warfare. By integrating robust legal and ethical standards, the international community can enhance accountability, minimize civilian harm, and promote cyberspace stability. The proposed ROE provides a foundation for this endeavor, but its successful implementation requires continuous adaptation, international cooperation, and a concerted effort to bridge the gap between law, ethics, and technology. Through such measures, policymakers, military strategists, and cybersecurity professionals can better manage and mitigate the risks associated with cyber conflict, ensuring a more secure and just digital world.

CONCLUSION

This research has delved into the intricate interplay between legal and ethical standards in cyberspace, seeking to define clear and robust rules of engagement (ROE) that can guide responsible conduct in this digital domain. The proposed refined ROE in this study represents a synthesis of legal, ethical, and practical considerations distilled from the analysis and insights generated. These proposed guidelines, designed to be adaptable, transparent, and internationally harmonized, offer a roadmap for navigating the challenging terrain of cyber conflict. By incorporating advanced attribution mechanisms, real-time ethical assessments, and robust international collaboration, the proposed ROE aims to enhance accountability, minimize collateral damage, and promote strategic stability in cyberspace.

Looking forward, future research should continue to explore the evolving dynamics of cyber conflict, examining the impact of emerging technologies, geopolitical shifts, and evolving legal and ethical norms on cyberspace governance. Interdisciplinary collaboration, stakeholder engagement, and ongoing dialogue will be essential in refining and operationalizing the proposed ROE, ensuring its relevance and

effectiveness in the face of evolving threats.

In conclusion, the quest to define the rules of engagement for cyber conflict is an ongoing and dynamic endeavor as technology continues to reshape the contours of warfare and diplomacy. By grounding our approach in legal principles, ethical frameworks, and practical insights, we can navigate the complexities of the digital battlefield with clarity, responsibility, and foresight, ultimately striving to create a safer and more secure cyberspace for all stakeholders.

REFERENCES

Alead, R. M. S. A., & Altalibe, A. a. A. (2023). Attribution Challenges in the era of Cyber warfare: Unraveling the identity of Cyber-Attackers. *Deleted Journal*, *3*(16), 5287–5309. https://doi.org/10.21608/hiss.2023.337323

Barrett, E. T. (2013). Warfare in a new domain: the ethics of military cyber-operations. *Journal of Military Ethics*, *12*(1), 4–17. https://doi.org/10.1080/15027570.2013.782633

Botes, M., & Lenzini, G. (2022). When Cryptographic Ransomware Poses Cyber Threats: Ethical Challenges and Proposed Safeguards for Cybersecurity Researchers. In *European Symposium on Security and Privacy Workshops*. https://doi.org/10.1109/eurospw55150.2022.00067

Brown, C. S. D. (2015). Cyber-Attacks, retaliation and risk. In *Advances in digital crime, forensics, and cyber terrorism book series* (pp. 166–203). https://doi.org/10.4018/978-1-4666-8456-0.ch008

Bruch, C., Altman, S., Al-Moumin, M., Troell, J., & Roffman, E. (2007). Legal frameworks governing water in the Middle East and North Africa. *International Journal of Water Resources Development*, *23*(4), 595–624. https://doi.org/10.1080/07900620701488539

Caso, J. S. (2014). The rules of engagement for cyber-warfare and the Tallinn Manual: A case study. In *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*. https://doi.org/10.1109/cyber.2014.6917470

Cavelty, M. D., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274

Chang, Z. (2017). Cyberwarfare and international humanitarian law. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2973182

Denning, D. E. (2008). The Ethics of Cyber Conflict. In *The Handbook of Information and Computer Ethics* (pp. 407–428). Wiley Telecom. https://doi.org/10.1002/9780470281819.ch17

Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics*, *9*(4), 384–410. https://doi.org/10.1080/15027570.2010.536404

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

Elliott, D. (2011). Deterring strategic cyberattack. *IEEE Security & Privacy*, *9*(5), 36–40. https://doi.org/10.1109/msp.2011.24

Flowers, A., Zeadally, S., & Murray, A. (2013). Cybersecurity and US Legislative Efforts to address Cybercrime. *Journal of Homeland Security and Emergency Management*, *10*(1). https://doi.org/10.1515/jhsem-2012-0007

Focarelli, C. (2015). Self-defence in cyberspace. In *Edward Elgar Publishing eBooks*. https://doi.org/10.4337/9781782547396.00023

García-Vargas, L., Durán-Aponte, E., & Chaux, E. (2023). The Role of Third Parties in Cyber Conflicts: The sima Simulator. *Revista Colombiana De Psicología/Revista Colombiana De Psicologia*, *32*(1), 67–81. https://doi.org/10.15446/rcp.v32n1.96322

Geiß, R., & Lahmann, H. (2012). Cyber Warfare: applying the principle of distinction in an interconnected space. *Israel Law Review*, *45*(3), 381–399. https://doi.org/10.1017/s0021223712000179

Giles, K., & Monaghan, A. (2014). *Legality in Cyberspace: an adversary view*. https://doi.org/10.21236/ada597232

Glorioso, L. (2015). Cyber Conflicts: Addressing the regulatory gap. *Philosophy & Technology*, *28*(3), 333–338. https://doi.org/10.1007/s13347-015-0197-8

Gray, C. W. (1993). *Evolving legal frameworks for private sector development in Central and Eastern Europe*. http://documents.worldbank.org/curated/en/922841468770973557/Evolving-legal-frameworks-for-private-

sector-development-in-Central-and-Eastern-Europe

Haataja, S., & Akhtar-Khavari, A. (2018). Stuxnet and international law on the use of force: an informational approach. *Cambridge International Law Journal*, *7*(1), 99–121. https://doi.org/10.4337/cilj.2018.01.05

Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony hack : exporting instability through cyberspace. *Asia-Pacific Issues*, *117*, 1. https://scholarspace.manoa.hawaii.edu/bitstream/10125/36444/1/api117.pdf

Ikegbu, E. A., & Diana-Abasi, F. I. (2017). Utilitarianism as a veritable vehicle for the promotion of a just society. *LWATI*, *14*(2), 121–137. https://www.ajol.info/index.php/lwati/article/download/162939/152449

Jardine, E., & Porter, N. D. (2020). Pick Your Poison: The Attribution Paradox in Cyberwar. *SocArXiv*. https://ideas.repec.org/p/osf/socarx/etb72.html

Jensen, E. T. (2002). Computer attacks on critical national infrastructure: a use of force invoking the right of Self-Defense. *Stanford Journal of International Law*, *38*, 207. https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1212&context=faculty_scholarship

Jensen, E. T. (2012). Cyber attacks: Proportionality and precautions in attack. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2154938

Jensen, E. T. (2014). Cyber Sovereignty: The way ahead. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466904

Kanuck, S. (2010). Sovereign Discourse on Cyber Conflict under International Law. *Texas Law Review*, *88*(7), 1571. http://static1.1.sqspcdn.com/static/f/956646/23348437/1377029193930/Kanuck+Sovereign+Discourse+Texas+Law+Review.pdf?token=OB2H803ZUnuwTFVt%2FzHzCpZkzm0%3D

Kao, D., Hsiao, S., & Tso, R. (2019). Analyzing WannaCry Ransomware Considering the Weapons and Exploits. In *21st International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/icact.2019.8702049

Kehler, C. R., Lin, H., & Sulmeyer, M. (2017). Rules of engagement for cyberspace operations: a view from the USA. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyx003

Kelsey, J. T. (2008). Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review*, *106*(7), 1427–1451. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1381&context=mlr

Kosseff, J. (2018). Developing collaborative and cohesive cybersecurity legal principles. In *10th International Conference on Cyber Conflict*. https://doi.org/10.23919/cycon.2018.8405022

Lancelot, J. F. (2020). Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, *4*(4), 240–254. https://doi.org/10.1080/23742917.2020.1798155

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, *94*(886), 515–531. https://doi.org/10.1017/s1816383112000811

Lonsdale, D. J. (2020). The Ethics of Cyber attack: pursuing legitimate security and the common good in contemporary conflict scenarios. *Journal of Military Ethics*, *19*(1), 20–39. https://doi.org/10.1080/15027570.2020.1764694

Lucas, G. (2017). *Ethics and Cyber warfare*. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001

Lucas, G. R. (2014). Ethics and Cyber Conflict: A Response toJME12:1 (2013). *Journal of Military Ethics*, *13*(1), 20–31. https://doi.org/10.1080/15027570.2014.908012

Miller, S., Regan, M., & Walsh, P. F. (2021). National Security intelligence and Ethics. In *Routledge eBooks*. https://doi.org/10.4324/9781003164197

Nyabuto, C. R. (2018). Game of Code: Challenges of Cyberspace as a domain of Warfare. □*the* □*Strathmore Law Review*, *3*(1), 49–72. https://doi.org/10.52907/slr.v3i1.102

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and international humanitarian law. *Information & Computer Security/Information and Computer Security*, *24*(1), 38–52. https://doi.org/10.1108/ics-12-2014-0081

Pistor, K., Keinan, Y., Kleinheisterkamp, J., & West, M. D. (2003). The Evolution of Corporate Law: A Cross-Country Comparison. *Social Science Research Network*. https://doi.org/10.2139/ssrn.419881

Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing privacy rights and surveillance analytics: a decision process guide. *Journal of Business Analytics*, *4*(2), 155–170. https://doi.org/10.1080/2573234x.2021.1920856

Prescott, J. M. (2014). Building the ethical cyber commander and the law of armed conflict. *Rutgers Computer & Technology Law Journal*, *40*(1), 42.

Richardson, J. C. (2011). Stuxnet as Cyberwarfare: Applying the law of War to the virtual battlefield. *Social Science Research Network*. https://doi.org/10.2139/ssrn.1892888

Roche, E. M. (2019). The search for global cyber stability. *Journal of Information Technology Cases and Applications/Journal of Information Technology Case and Application Research*, *21*(2), 68–73. https://doi.org/10.1080/15228053.2019.1636570

Roscini, M. (2015). Cyber operations as a use of force. In *Edward Elgar Publishing eBooks*. https://doi.org/10.4337/9781782547396.00022

Rowe, N. C. (2010). The ethics of cyberweapons in warfare. *International Journal of Technoethics*, *1*(1), 20–31. https://doi.org/10.4018/jte.2010081002

Santhosh, T., & Thiyagu, K. (2024). Fostering Responsible Behavior online- Relevance of Cyber Ethics education. *Malaysia Online Journal of Educational Techology*, *12*(1), 32–38. https://doi.org/10.52380/mojet.2024.12.1.428

Schmidt, L. (2015). Perspective on 2015 DOD Cyber Strategy. In *RAND Corporation eBooks*. https://doi.org/10.7249/ct439

Schmitt, M. N. (2013). Tallinn Manual on the international law applicable to cyber warfare. In *Cambridge University Press eBooks*. https://doi.org/10.1017/cbo9781139169288

Shackelford, S. (2020). Review of Cyber operations Strategies of the United States and Canadian Governments: A Comparative analysis. *Social Science Research Network*. https://doi.org/10.2139/ssrn.3727510

Shackelford, S., & Craig, A. (2014). Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. *Stanford Journal of International Law*, *50*, 119.

Shaw, W. H. (2016). Utilitarianism and the ethics of war. In *Routledge eBooks*. https://doi.org/10.4324/9780203538333

Spagnol, G. (2021). Cyberspace: an advantageous terrain for war? In *Advanced sciences and technologies for security applications* (pp. 117–128). https://doi.org/10.1007/978-3-030-67973-6_8

Stöcker, C., Bennett, R., Nex, F., Gerke, M., & Zevenbergen, J. (2017). Review of the current state of UAV Regulations. *Remote Sensing*, *9*(5), 459. https://doi.org/10.3390/rs9050459

Taddeo, M. (2012). An analysis for a just cyber warfare. In *4th International Conference on Cyber Conflict* (pp. 1–10).

Theohary, C. A., & Harrington, A. I. (2014). Cyber Operations in DOD Policy and Plans: Issues for Congress. In *Congressional Research Service*. http://goodtimesweb.org/overseas-war/2015/R43848.pdf

Trautman, L. J., & Ormerod, P. (2018). Wannacry, Ransomware, and the Emerging Threat to Corporations. *86 Tennessee Law Review*, *503*. https://doi.org/10.2139/ssrn.3238293

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244. https://doi.org/10.1093/jcsl/krs019

Tsotniashvili, Z. (2024). Silicon Tactics: Unravelling the Role of Artificial Intelligence in the Information Battlefield of the Ukraine Conflict. *Asian Journal of Research*, *9*, 54–64.

Usman, H., Ahmed, R. I., & Ali, S. S. (2022). Navigating the Gray Area: A Comprehensive Analysis of Cyber Warfare and its Relationship to the Law of Armed Conflict. *Global Legal Studies Review*, *VII*(III), 32–36. https://doi.org/10.31703/glsr.2022(vii-iii).05

Von Heinegg, W. H. (2012). Legal implications of territorial sovereignty in cyberspace. *International Conference on Cyber Conflict*, 1–13. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6243962

Watney, M. (2014). Challenges pertaining to cyber war under international law. In *3rd International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec*. https://doi.org/10.1109/cybersec.2014.6913962

Wilton, C. (2017). Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the modern world. *Pace I.P., Sports & Entertainment Law Forum*, *7*(1), 1. https://doi.org/10.58948/2329-9894.1058