CYBER WARFARE AND STATE RESPONSIBILITY UNDER INTERNATIONAL LAW

E'zoza Xamrayeva

1st-year student, Economics (Russian Group)

Academic Lyceum of the Samarkand Branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

xamrayevaezoza749@gmail.com

Abstract. In the digital era, cyber warfare has emerged as one of the most pressing challenges to international peace and security. Cyber operations may disrupt critical infrastructure, interfere in political processes, and cause significant economic losses without any physical destruction. This article examines the legal principles governing state responsibility for cyber operations under international law, using doctrinal legal analysis, comparative approaches, and case study methodology. Case studies, including the 2007 Estonia cyber incidents, the 2017 NotPetya malware attack, and the 2020 SolarWinds breach, are analyzed. Additional perspectives from China, Iran, and North Korea's cyber activities are discussed to provide a global context. Many operations are widely attributed to state-linked actors by multiple governments, though formal judicial attribution is often absent. The research identifies legal gaps, enforcement challenges, and provides policy recommendations to strengthen accountability and global stability.

Keywords: cyber warfare, state responsibility, international law, sovereignty, attribution, IHL, Tallinn Manual

INTRODUCTION

Cyberspace has become a critical domain alongside land, sea, air, and space in the 21st century. States increasingly rely on digital infrastructure for governance, energy, finance, communication, and national security. Concurrently, cyber operations are employed for political, military, and economic purposes. Unlike traditional warfare, cyber attacks often do not involve physical violence, relying instead on espionage, data manipulation, disruption of critical infrastructure, and interference with political systems. Global cyber incidents, including those linked to China, Iran, and North Korea, demonstrate that state-sponsored cyber activity is no longer confined to regional disputes. China's alleged cyber espionage campaigns, Iran's targeting of energy infrastructure, and North Korea's financially motivated cyber attacks underscore the diverse objectives and global reach of cyber operations.

International law offers guidance through principles such as sovereignty, non-intervention, and prohibition of the use of force under the United Nations Charter (1945) [2]. The International Law Commission (ILC) Articles on Responsibility of States for Internationally Wrongful Acts (2001) provide a framework for attributing responsibility to states [1]. However, rapid technological advancements have created legal ambiguities. Key questions include: When does a cyber operation constitute an internationally wrongful act? How can a state be held responsible in the absence of direct attribution? What role does international humanitarian law (IHL) play during armed conflicts?

METHODS

This research employs several complementary methodologies to ensure a comprehensive analysis of state responsibility in cyber operations. First, a doctrinal legal analysis was conducted by examining primary legal sources such as the UN Charter, the ILC Articles on State Responsibility, and Tallinn Manual 2.0 in order to interpret the legal principles and frameworks applicable to cyber activities. In addition, a comparative analysis of state practices in cyber operations across the United States, the European Union, Russia, China, Iran, and North Korea was carried out to identify similarities, differences, and emerging legal approaches. The study also applies a case study method focusing on major cyber incidents, including the Estonia 2007 cyber attacks, the NotPetya malware attack of 2017, and the SolarWinds breach of 2020, with particular attention to their economic consequences, attribution issues, and legal interpretations. Furthermore, a review of secondary literature, including academic publications, governmental reports, and cybersecurity analyses, was conducted to evaluate existing legal interpretations, operational patterns, and the challenges associated with the enforcement of international law in cyberspace. Together, these methods provide a multidimensional perspective on state responsibility in cyber operations and help identify existing gaps and challenges within the current international legal framework.

RESULTS

Sovereignty and Non-Intervention

Sovereignty confers authority to states over their territory, including digital infrastructure. Cyber operations that disrupt critical systems, even without physical damage, may violate state sovereignty [3]. The principle of non-intervention prohibits coercive interference in internal or external affairs. Operations that manipulate elections, interfere with government networks, or disrupt critical services can constitute unlawful interference if coercive intent is present.

International Humanitarian Law (IHL)

During armed conflicts, cyber operations fall under IHL principles such as distinction, proportionality, and precaution [4]. Attacks targeting military systems may be lawful, while operations affecting civilian infrastructure could violate IHL. Dual-use systems complicate the application of these principles, as a single cyber tool may impact both civilian and military targets.

State Responsibility and Attribution

State responsibility arises when actions attributable to a state constitute internationally wrongful acts [1]. Attribution in cyberspace is technically difficult due to anonymization, proxy servers, and non-state actors. While governments widely attribute certain attacks to state-linked actors, judicial attribution is rare. This creates a gap between political statements and enforceable legal accountability.

Estonia Cyber Incidents (2007)

In April 2007, coordinated attacks targeted Estonian government websites, banks, and media outlets amid political tensions over a Soviet war memorial. Multiple sources attributed the attacks to actors allegedly linked to Russia [5]. Despite widespread attribution, no formal judicial determination confirmed state responsibility.

NotPetya Malware (2017)

NotPetya primarily targeted Ukrainian systems but spread globally, affecting multinational corporations and causing estimated economic losses exceeding $10 billion. Greenberg (2019) notes that governments attributed the attack to Russian military-linked actors, though no legal proceedings occurred [6]. Unlike ransomware, NotPetya aimed to disrupt infrastructure rather than extort money.

SolarWinds Breach (2020)

The SolarWinds operation compromised U.S. government networks through a sophisticated supply-chain attack. Multiple agencies reported the breach and widely attributed it to state-linked actors, although formal legal attribution was not established [7]. The incident exposed vulnerabilities in supply chains and demonstrated the limits of existing enforcement mechanisms.

DISCUSSION

The analysis of the Estonia 2007, NotPetya 2017, and SolarWinds 2020 incidents highlights the complexity of attributing cyber operations to states. While governments often publicly attribute cyber attacks to state-linked actors, formal judicial attribution remains rare. This demonstrates a significant gap in enforceability under international law, where political attribution does not automatically translate into legal responsibility [5].

The Estonia incidents illustrate that even politically sensitive attacks targeting essential services may not lead to formal accountability, emphasizing the challenge of linking state responsibility to observable cyber activities. Similarly, NotPetya demonstrates that cyber operations can produce extensive economic damage without any physical destruction, raising questions about the interpretation of "use of force" under the UN Charter [6].

The SolarWinds breach highlights another challenge: supply chain vulnerabilities. Even with advanced forensic techniques, it is difficult to produce conclusive evidence linking cyber operations to specific states [7]. This problem is exacerbated by the rise of AI-driven malware, autonomous systems, and quantum computing, which further blur the line between civilian and military targets.

Global context: Other states, such as China, Iran, and North Korea, have conducted cyber operations with strategic, political, or financial objectives. These operations illustrate that cyber warfare is no longer geographically limited and that international law must address cross-border consequences. The lack of binding international norms and cooperative enforcement mechanisms allows some states to operate with minimal accountability, relying on voluntary compliance rather than enforceable obligations:

Attribution is the most critical challenge, complicated by anonymization and proxy use.

Economic and political disruptions from cyber operations may not clearly fall under "use of force."

Existing IHL principles are insufficient for dual-use systems in cyberspace.

International collaboration is essential to enforce norms and share evidence effectively.

Overall, the discussion shows that while legal principles provide a foundation, they are insufficient without operational mechanisms and clarity in defining wrongful acts. Strengthening international law requires both interpretive clarity and practical enforcement measures.

Policy Recommendations

Develop international cyber norms: Multilateral agreements should clearly define when cyber operations constitute acts of aggression, intervention, or internationally wrongful acts. These norms must account for both physical and economic impacts.

Establish mechanisms for attribution: Institutions for forensic collaboration, evidence-sharing, and standardized investigative methods should be created to improve credibility and accuracy of attribution.

Strengthen international cooperation: Organizations like the UN, NATO, and regional coalitions should coordinate collective responses, ensure accountability, and provide technical assistance to member states.

Integrate cyber operations into legal frameworks: International humanitarian law and international criminal law should explicitly recognize cyber warfare and include provisions for dual-use infrastructure and civilian protection.

Promote cybersecurity capacity-building: Support developing states in securing critical infrastructure, improving cyber resilience, and training personnel to detect, prevent, and respond to attacks.

Encourage transparency and reporting: States should adopt reporting standards for cyber incidents affecting critical infrastructure, enabling international monitoring and analysis.

Develop economic impact metrics: Standardized measures of economic losses from cyber operations can help clarify legal responsibility and guide compensation mechanisms.

These recommendations aim to strengthen accountability, reduce legal gaps, and enhance global stability in cyberspace.

CONCLUSION

Cyber warfare presents a complex and evolving challenge for international law. While sovereignty, non-intervention, and state responsibility provide a legal foundation, ambiguities persist, especially regarding attribution, enforcement, and dual-use infrastructure. Case studies—Estonia, NotPetya, and SolarWinds—illustrate that cyber operations are widely attributed but rarely formally prosecuted, highlighting limitations in current international legal frameworks. The rise of AI-driven malware, autonomous cyber systems, and global interconnectedness further complicates state responsibility.

To address these challenges, international law must: Strengthen legal frameworks to define wrongful acts in cyberspace; Clarify state responsibilities, including economic and political disruptions; Promote multilateral cooperation, evidence-sharing, and capacity-building.

By implementing these measures, the global community can ensure accountability, protect critical infrastructure, and maintain stability in an increasingly digital world.

REFERENCES:

1.International Law Commission. Articles on Responsibility of States for Internationally Wrongful Acts. UN, 2001. Available at: https://legal.un.org/ilc/texts/9_6.shtml

2.United Nations. Charter of the United Nations, 1945.

3.Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.

4.Kerr, Ian. Cyber War and International Law. Oxford University Press, 2018.

5.Nakashima, Ellen. Reports on Estonia Cyber Incidents, 2007.

6.Greenberg, Andy. Sandworm. Doubleday, 2019.

7.U.S. Cybersecurity and Infrastructure Security Agency reports on SolarWinds, 2020.