JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 39

# The Ethical and Policy Challenges of State-Sponsored Hacking

Ayushi Srivastava

University of Allahabad

**Recommended Citation:**

Srivastava (2026) "The Ethical and Policy Challenges of State-Sponsored Hacking" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 39. (DOI)

**ABSTRACT**

*State sponsored hacking is one of the most destabilizing forces in today's international relations. As governments globally increasingly use cyber means for espionage, sabotage and coercion, the international legal order is lagging behind and can't keep up. The paper examines the ethical and policy challenges that attend state sponsored hacking, particularly the complex and ambiguous relationship between the requirements of national security and the more traditional concepts of sovereignty, human rights and international humanitarian law. It provides an overview of current legal regimes, such as the Tallinn Manual, the UN Charter, and a range of bilateral cybersecurity agreements, and identifies salient current norms gaps through doctrinal and comparative analysis. In reality, these holes appear to enable states to engage in cyber operations in a "grey zone" that is more ambiguous than traditional warfare. The point here is that it is not possible to create binding international norms, the definition of cyber warfare is ambiguous and the attribution mechanism, when it exists at all, is either weak or ambiguous. It concludes with recommendations such as the need for a framework of multilateral treaties and enhancing domestic accountability measures so that states are not able simply to act elsewhere without repercussions.*

**KEYWORDS**

*State-Sponsored Hacking, Cyber Warfare, International Law, Sovereignty, Attribution, Tallinn Manual, Cyber Espionage, Policy Reform*

## INTRODUCTION

A ransomware attack on Colonial Pipeline in the United States caused fuel shortages on the East Coast in May 2021. The attack raised concerns about the susceptibility of infrastructure to cyber intrusions and sparked a debate about the role of states in organizing, enabling or tolerating such attacks. State sponsored hacking is a part of geographical life. It means hacking that is done by or on behalf of a state and is often aimed at governments, corporate bodies or civil society groups. These operations are typically conducted under the radar of conflict and are hard to fit into existing definitions of war.

State-sponsored hacking means hacking that is done by, or on behalf of, a state, and often aimed at other governments, corporate bodies or civil society groups for various purposes, such as gathering intelligence or disrupting political systems. These operations are typically conducted under the radar of armed conflict and are hard to fit into existing definitions of war. The actors are sometimes government hackers and sometimes private contractors, who operate in a legal grey zone that current international law cannot fully capture.

This paper examines the ethical and policy aspects of state sponsored hacking. The main research question is: What are the current shortcomings in legal and ethical frameworks to regulate state sponsored cyber operations and what reforms are necessary? Section 2 reviews the literature and legal framework. Section 3 describes the methodology. Section 4 examines issues, shortcomings of existing law, and alternatives. Policy implications and potential reforms are explored in Section 5 and key findings and recommendations are provided in Section 6.

## LITERATURE REVIEW

There are academic works dealing with state sponsored hacking. The transformative power of cyberspace as a space has been acknowledged for a long time. However law has not been advancing as quickly as technology. The Tallinn Manual 2.0 is the extensive attempt to apply current international law to cyber operations.[1] It finds that states are internationally responsible

[1]Michael N. Schmitt ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge Univ. Press, 2d ed. 2017).

for the cyber activities of their organs or agents and that cyber activities that cross the "armed attack" threshold engage the right to self-defence under Article 51 of the UN Charter.[2]

The Tallinn Manual is not legally binding; it represents the views of independent experts and not of states. Scholars such as Michael Schmitt have suggested that the Manual offers helpful normative guidance but point out that state practice and opinio juris the two foundations of customary international law are far from settled in the cyber arena.[3]

Ethically, philosophers and legal scholars have applied the principles of just war theory to the permissibility of cyber attacks. O'Connell has maintained that the IHL principles of distinction, proportionality and military necessity are applicable to cyber operations, albeit with great difficulty.[4] Cyber weapons are notoriously hard to contain; the Stuxnet worm, allegedly developed by the United States and Israel to infiltrate Iranian nuclear facilities, infected computers across many countries worldwide.[5]

There is a lack of research on the subject of cyber espionage in existing literature. As Buchan points out, peacetime cyber espionage is not banned by any international agreement, yet it has significant impacts on national security, economic competitiveness and individual privacy rights.[6]

In-country, there have been concerns that there are no effective oversight mechanisms for state cyber operations. Presidential directives in the U.S. are classified documents that govern offensive cyber operations.[7] The United Kingdom and India also lack publicly available statutory regimes dedicated to state sponsored cyber activity.

Another problem cited in the literature is the attribution problem — the difficulty of determining with certainty who is responsible for a cyber operation. Healey notes that cyber operations are often conducted via third-party servers and under false flag representations, making the process of determining responsibility both technically and politically complex.[8]

---

[2]U.N. Charter art. 51.
[3]Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, 56 Vill. L. Rev. 569 (2011).
[4]Mary Ellen O'Connell, Cyber Security Without Cyber War, 17 J. Conflict & Sec. L. 187, 187–209 (2012).
[5]Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon 1–22 (Crown Publishers 2014).
[6]Russell Buchan, Cyber Espionage and International Law 43–58 (Hart Publishing 2018). Note: the volume was published by Hart/Bloomsbury with ISBN 9781782257363; some sources cite 2019 as review-publication year.
[7]Presidential Policy Directive 20 (Oct. 2012) (classified); National Security Presidential Memorandum 13 (Aug. 2018) (classified).
[8]Jason Healey ed., A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, at 112–30 (Cyber Conflict Studies Ass'n 2013).

## METHODOLOGY

The method of this paper is largely doctrinal in nature, with comparative and critical analysis. Doctrinal research comprises the systematic study of primary legal sources, such as treaties, judicial rulings and state practice, alongside secondary sources such as scholarly commentaries and expert instruments like the Tallinn Manual. The doctrinal approach is suitable here since the main problem is one of designing the legal framework: determining the relevance of existing norms to cyber operations, identifying where they fall short, and determining how they can be better adapted.

The paper also uses comparative analysis, looking at how various jurisdictions including the United States, Russia, China, the United Kingdom and India regulate domestic cyber activities and outline their views on international cyber norms. The comparative analysis is useful because state sponsored hacking is a cross-border affair; any effective response must be sensitive to different national perspectives.

Finally, the paper presents case studies of large-scale, state-sponsored cyber incidents from Stuxnet to the interference in the 2016 U.S. presidential election to SolarWinds to bring general principles of law and ethics into focus with concrete facts.

## DEFINING STATE- SPONSORED HACKING: THE THRESHOLD PROBLEM

It is vital to first understand what constitutes "state-sponsored hacking" and why it is so hard to define before any ethical or legal analysis can begin. In the widest sense, it refers to any action undertaken by a government agency using the internet, whether done directly, with government funding, or under the tacit approval or participation of a government. Its spectrum runs from direct military cyber action to intrusions for intelligence gathering purposes, to the passive acceptance of criminal ransomware groups targeting foreign adversaries.

The UN International Law Commission's 2001 Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) constitute the most important body of rules governing attribution of private acts to states under international law. Under Article 8 of ARSIWA, the

conduct of a private person or group must be "acting on the instructions of, or under the direction or control" of a state for that conduct to be attributable to the state.[9]

But the "effective control" standard established by the International Court of Justice in *Military and Paramilitary Activities in and Against Nicaragua* has been challenged in the cyber arena. States consistently reject claims that hacking groups operating within their borders are subject to their control; and the technical nature of cyber operations makes it difficult to determine what level of control is required under international law.[10]

## THE ETHICAL DIMENSIONS: SOVEREIGNTY, PROPORTIONALITY, AND HUMAN RIGHTS

Ethically, state sponsored hacking poses deep questions about the rights and obligations of states in the digital world. The three principles given special consideration here are respect for sovereignty, proportionality, and protection of human rights.

Cyber intrusions directly engage the principle of state sovereignty. If one state penetrates the computer networks of another state's government ministries, it is impairing that state's sovereignty over its own affairs. This is addressed in the Tallinn Manual 2.0, which provides that "A State may not engage in cyber operations that affect the sovereignty of another State in a manner that violates that State's sovereignty."[11] This principle is not contained in any binding treaty, and its scope and application remain disputed.

The principle of proportionality grounded in Just War theory and international humanitarian law (IHL) requires that any harm inflicted by a cyber operation be proportionate to the expected military gain. The principle is especially complex to implement in cyberspace where the impact of malware is hard to control and unpredictable. The Stuxnet worm designed to disrupt Iranian

[9]Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 8, in Report of the International Law Commission on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 45 (2001) [hereinafter ARSIWA].

[10]Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 109–115 (June 27) [hereinafter Nicaragua Judgment].

[11]Michael N. Schmitt ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge Univ. Press, 2d ed. 2017), Rule 4 (Sovereignty), r. 4 cmt.

centrifuges was found on computers in numerous countries, illustrating how cyber weapons can cause disproportionate and unintended harm.

Human rights concerns are also pressing. Cyber espionage inevitably entails the interception of personal correspondence, implicating the right to privacy under Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[12] The Human Rights Committee has established that the ICCPR extends to activities conducted outside the state's territory, yet enforcement mechanisms remain weak.[13]

## THE LEGAL FRAMEWORK: GAPS AND INADEQUACIES

The current international legal framework was developed without considering cyberspace, and its application to state-sponsored hackers remains highly contestable. Key areas of uncertainty include: the prohibition on the use of force, the law of armed conflict, and the regulation of cyber espionage.

Article 2(4) of the UN Charter bars the use or threat of force against the territorial integrity or political independence of any state.[14] Whether a cyber operation amounts to a "use of force" under Article 2(4) is hotly debated. The Tallinn Manual proposes a "scale and effects" standard as a threshold for a cyber operation to constitute a use of force, but this standard lacks precision in practice.[15] Most state sponsored cyber operations other than those causing damage to critical infrastructure are likely to fall below this threshold.

When a country uses cyber operations. It leads to a big conflict, the laws that apply to armed conflicts are used. The Tallinn Manual says that cyber operations can be seen as acts of war if they cause death, injury or a lot of damage to property.. Most of the time countries use cyber operations for things like spying or stealing intellectual property and these things do not cause

[12]International Covenant on Civil and Political Rights art. 17, opened for signature Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].
[13]Human Rights Comm., General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17), ¶ 1, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).
[14]U.N. Charter art. 2, ¶ 4.
[15]Michael N. Schmitt ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge Univ. Press, 2d ed. 2017), r. 69 (Use of Force) & cmt.

enough harm to be considered acts of war. This creates a lot of confusion about what is legal and what is not.

Perhaps most significant is the absence of a binding international prohibition on cyber espionage. While there is no explicit ban on espionage in international law, the scale, speed and reach of cyber espionage today far exceed the norms of previous eras. A 2015 bilateral agreement between the U.S. and China to refrain from cyber-enabled intellectual property theft for commercial gain was a positive step, yet it is non-binding and difficult to enforce.[16]

## DOMESTIC LEGAL FRAMEWORKS AND ACCOUNTABILITY GAPS

In most countries, state-sponsored cyber operations are legally regulated in a fragmented or opaque manner at the domestic level. The legal underpinnings of offensive cyber operations in the United States are largely classified presidential directives. A report by the Cyberspace Solarium Commission in 2020 found areas that need attention and suggested new laws to make it clear who is in charge of cyber operations and how they are overseen.[17]

In the United Kingdom the Investigatory Powers Act, 2016 gives intelligence services the power to hack into computers.[18] India does not have laws for cyber operations and the existing Information Technology Act 2000[19] and the National Cyber Security Policy 2013[20] are not good enough to deal with modern cyber threats.

Transparency is even lower in Russia and China, where considerable state sponsored hacking activity exists. Both states have resisted proposals to limit their cyber operations under international standards, preferring the framing of "information security" which includes control of online content over the technical cybersecurity focus favoured by Western states. This has posed a significant obstacle to multilateral agreement.

[16]Press Release, White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (last visited Jul. 16, 2026).
[17]Cyberspace Solarium Comm'n, Final Report 57–75 (2020), https://www.solarium.gov/report (last visited Jul. 16, 2026).
[18]Investigatory Powers Act 2016, c. 25, pts. 5–6 (UK) (authorising targeted and bulk equipment interference warrants).
[19]Information Technology Act, No. 21 of 2000 (India).
[20]Ministry of Elec & Info. Tech., Govt of India, National Cyber Security Policy 2013 (2013).

## THE ATTRIBUTION PROBLEM AND ITS LEGAL CONSEQUENCES

The attribution problem is too significant to ignore when discussing the legal and ethical issues surrounding state sponsored hacking. Determining who is responsible for a cyber operation is a technical and political problem. Sophisticated attackers can operate through multiple jurisdictions, use borrowed infrastructure, and forge the digital signatures of other groups to disguise their identity. States may actively seek ambiguity so as to avoid responsibility while retaining the strategic benefits of an operation.

The legal implications are serious. When the source of an intrusion is not identified, a target state is unable to exercise its right of self-defence, bring action before an international court, or initiate countermeasures under ARSIWA. In the case of the 2016 hack of the Democratic National Committee (DNC), the U.S. government attributed the breach to Russian state intelligence agencies based on technical analysis, human intelligence, and geopolitical context.[21]

Proposals have been advanced for an independent international cyber attribution body similar to the Organisation for the Prohibition of Chemical Weapons to conduct technical investigations and provide impartial evaluations.[22] Such a framework would be politically challenging to establish, but it would help alleviate the credibility deficit in cyber accountability.

## DISCUSSION

The foregoing analysis is deeply troubling. As states adopt cyber technologies as instruments of foreign policy, the international law and ethics that govern state action are clearly ill-equipped for the cyber era. The identified gaps the threshold problem, the absence of binding norms on cyber espionage, accountability gaps in domestic law, and the attribution problem intertwine and reinforce each other, fostering a "policy vacuum" that permits harmful state cyber conduct.

Several policy implications flow from these findings. First, the international community needs to move beyond current non-binding instruments such as the Tallinn Manual and the UN Group of Governmental Experts (GGE) framework toward a binding multilateral treaty on state conduct

[21]Off. of the Dir. of Nat'l Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution 1 (Jan. 6, 2017).
[22]Herbert Lin & Amy Zegart eds., Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations 2019

in cyberspace. Such a treaty should specify minimum standards of conduct, processes for attribution and dispute resolution, and accountability mechanisms for violations.

Second, domestic legal frameworks need to be reformed to provide meaningful oversight over state cyber operations. This means enacting clear legislation defining the legal authority for offensive cyber operations, requiring judicial approval for intrusive operations, and mandating independent review and public reporting consistent with national security constraints.

Third, confidence-building measures between the major cyber powers, especially the United States, Russia, and China are needed. The risk of escalation could be reduced by direct communication channels, agreed red lines, and mutual commitments to avoid attacking critical civilian infrastructure. Existing bilateral pacts, such as the 2015 Obama-Xi agreement, lack enforcement capacity and have not been consistently honoured.

Finally, international human rights institutions need to place greater emphasis on the human rights dimensions of state-sponsored cyber operations. The UN Special Rapporteur on the Right to Privacy has highlighted how surveillance activities by states can infringe on the privacy rights of individuals around the world and called for greater accountability.[23]

## CONCLUSION

State sponsored hacking is one of the most pressing legal and ethical challenges of the twenty-first century. This paper has argued that the international legal system grounded in principles of sovereignty, the prohibition on the use of force, and international humanitarian law does not exist in a form adequate to regulate low-intensity, deniable, and pervasive cyber operations carried out by states.

The ethical issues are equally serious. State cyber operations that inflict indiscriminate harm, compromise the privacy of millions of people, and undermine democratic processes systematically erode the foundational principles of international law: proportionality, distinction, and respect for human rights. These incidents are manifestations of a broader normative vacuum governing state behaviour in cyberspace.

[23]Special Rapporteur on the Right to Privacy, Report of the Special Rapporteur on the Right to Privacy: Surveillance and Human Rights, U.N. Doc. A/HRC/39/29 (Aug. 3, 2018).

The road ahead demands both ambition and pragmatism. Internationally, a multilateral cyber treaty while politically challenging is essential. Domestically, states must establish clear and transparent legal frameworks affording authority and accountability for cyber operations. Technically, investment in attribution capabilities and confidence-building mechanisms is vital for reducing the risk of unintended escalation.

Cyberspace is not ungoverned territory. It is part of the same world in which states bear rights and obligations and in which individuals possess dignity and rights deserving protection. The challenge for policymakers, lawmakers, and scholars is to ensure that law does not fall so far behind technology that the technology operates beyond the law entirely.