

Assignment 7.1: Cybersecurity and International Law Case Analysis

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

08/11/2025

Introduction

The growing reliance on interconnected technology ecosystems has magnified the risk of large-scale cyber incidents that transcend national borders. These risks extend beyond traditional cybercrime to sophisticated state-sponsored espionage campaigns targeting both government and private sector networks. One of the most prominent examples is the SolarWinds cyber espionage campaign, uncovered in December 2020. This incident demonstrated the vulnerabilities of global supply chains, the difficulties of enforcing cybersecurity laws across jurisdictions, and the challenges of mounting a coordinated international response.

This paper examines the SolarWinds case as a lens through which to explore the application of international cybersecurity law, jurisdictional barriers, and global cooperation mechanisms. The analysis draws upon the Budapest Convention on Cybercrime, the Tallinn Manual 2.0, the United Nations Charter, and modern trade agreements with cybersecurity provisions. It also evaluates lessons learned from the perspective of a Chief Information Security Officer (CISO) and offers policy recommendations to strengthen international cybersecurity governance.

Case Study Summary

The SolarWinds attack began in early 2020 when advanced threat actors—later attributed to Russia’s Foreign Intelligence Service (SVR), also known as APT29 or Cozy Bear—compromised the build environment for SolarWinds’ Orion platform. By injecting malicious code into Orion updates between March and June 2020, they created the SUNBURST backdoor, which was digitally signed and distributed to approximately 18,000 customers. Because these

updates were delivered through SolarWinds' legitimate update mechanism, the malicious code bypassed typical security measures.

The attack was discovered in December 2020 when cybersecurity firm FireEye detected suspicious activity in its systems and traced it back to the Orion platform. This discovery revealed that victims included the U.S. Department of Homeland Security, the Department of Commerce, the Department of the Treasury, and other federal agencies. Outside the United States, entities in Canada, the United Kingdom, Belgium, Israel, and the United Arab Emirates were also affected. Impacted organizations spanned critical infrastructure sectors, including telecommunications, healthcare, and energy (Coco, 2022).

Technically, the SUNBURST malware was a well-engineered reconnaissance tool that allowed attackers to move laterally within networks, escalate privileges, and exfiltrate sensitive data without triggering standard detection systems. Unlike destructive attacks such as NotPetya, SolarWinds was designed for stealth and persistence. From a geopolitical perspective, it aligned with traditional espionage objectives but raised concerns due to its scale and the exploitation of a trusted supply chain channel (Just Security, 2020).

Legal Implications

Relevant International Laws and Agreements

The Budapest Convention on Cybercrime is the primary binding international treaty addressing cybercrime investigation and cooperation. It criminalizes unauthorized access, system interference, and misuse of devices while promoting evidence-sharing and extradition among signatories. However, Russia is not a signatory, and thus was under no legal obligation to assist

in the investigation or extradition, severely limiting the Convention's practical utility in this case (Council of Europe, 2001).

The Tallinn Manual 2.0 offers non-binding guidance on applying existing international law to cyber operations. Rule 4 emphasizes respect for sovereignty, and Rule 32 notes that cyber espionage generally does not violate international law unless it causes prohibited effects, such as damage to critical infrastructure or injury to persons (Schmitt, 2017). Because SolarWinds did not cause kinetic damage or loss of life, its classification as an unlawful "use of force" under international law is contested.

The UN Charter prohibits the "use of force" against the territorial integrity or political independence of states (Article 2(4)) and allows self-defense in the case of an "armed attack" (United Nations, 1945, Article 51). The SolarWinds intrusion, while serious, did not meet the armed attack threshold, thus limiting U.S. and allied responses to lawful countermeasures like sanctions and diplomatic expulsions (UN, 1945).

Modern trade agreements, such as the U.S.–Mexico–Canada Agreement (USMCA) and the U.S.–Japan Digital Trade Agreement, include cybersecurity cooperation provisions that encourage capacity building, information sharing, and incident response collaboration. However, these agreements are primarily forward-looking and were not designed to address incidents involving a non-party state actor refusing cooperation.

Jurisdictional Challenges

Attribution remains a fundamental challenge in prosecuting cross-border cyber incidents. While the U.S. intelligence community attributed the SolarWinds attack to the SVR, meeting the

evidentiary standards for international prosecution requires access to detailed forensic data—much of which resides within the territory of the alleged perpetrator state. Without extradition agreements or mutual legal assistance treaties (MLATs) with Russia, prosecution was infeasible. Additionally, privacy and surveillance laws vary significantly across jurisdictions, complicating evidence gathering even among allies.

These issues echo the Module 7 learning outcome regarding jurisdictional complexity: national laws differ in their definitions of cybercrime, evidence admissibility, and investigative authority, creating barriers to unified enforcement.

International Collaboration and Response

The private sector drove the initial response. FireEye's disclosure and Microsoft's technical analysis provided the foundation for broader mitigation efforts. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, directing federal agencies to disconnect affected Orion products (CISA, 2020). The FBI, NSA, and Office of the Director of National Intelligence (ODNI) formed a Cyber Unified Coordination Group to coordinate the response.

Internationally, the United Kingdom's National Cyber Security Centre, Canada's Communications Security Establishment, and Australia's Cyber Security Centre issued joint advisories. However, no central global body coordinated these efforts, and responses varied in scope and timing. The lack of a unified legal mechanism for cross-border investigation limited the depth of information sharing.

Russia denied involvement and did not participate in any cooperative investigative processes. This refusal underscored the limitations of current international law in compelling cooperation from a non-signatory, adversarial state.

Legal and Diplomatic Consequences

In April 2021, the United States imposed sanctions on Russia, citing the SolarWinds campaign among other malicious cyber activities (White House, 2021). These sanctions included the expulsion of ten Russian diplomats and restrictions on certain Russian technology companies. While lawful under international law as acts of retorsion, these measures did not deter future Russian cyber operations, illustrating the limited deterrent effect of current diplomatic tools in the cyber domain.

Lessons Learned as a CISO

Supply Chain Risk Management

Organizations must recognize that vendor compromise can be as dangerous as a direct breach. This requires thorough vendor security assessments, contractual security requirements, and use of Software Bills of Materials (SBOMs) to track dependencies.

Zero Trust Architecture

Trust should never be assumed, even for internal systems. Implementing least-privilege principles, segmentation, and continuous verification can limit attacker movement once inside.

Incident Response Preparedness

Incident response plans should account for multi-jurisdictional coordination, including pre-established channels with international partners and private sector intelligence-sharing organizations.

Threat Intelligence Integration

Timely integration of threat intelligence from sources such as Information Sharing and Analysis Centers (ISACs) can speed detection and mitigation of sophisticated attacks.

Leadership and Communication

During a crisis, transparent communication with stakeholders—including customers, regulators, and the public—is essential. A CISO must also manage internal morale, maintain trust in security teams, and ensure continuous improvement after the incident.

Policy Recommendations

1. Expand Budapest Convention Membership

Encouraging major cyber powers outside the Convention to join would standardize cooperation, expedite evidence sharing, and create formal investigative channels.

2. Establish a UN-Led Cyber Attribution Mechanism

A neutral, expert-driven body could assess evidence, attribute attacks with high confidence, and issue public reports that carry international legitimacy.

3. Harmonize Evidence Standards

Aligning evidentiary procedures across jurisdictions would reduce delays caused by incompatible legal systems, enabling faster collaborative responses.

4. Enhance Supply Chain Security Requirements

Mandating SBOMs, secure development lifecycle adherence, and regular third-party audits would reduce the risk of software supply chain compromise.

5. Update Tallinn Manual Guidance

Clarifying when large-scale espionage campaigns targeting critical infrastructure rise to the level of sovereignty violations or prohibited intervention would help guide lawful state responses.

6. Create Bilateral and Multilateral Rapid Response Protocols

Formalizing cross-border cyber incident protocols, modeled on NATO's cooperative cyber defense framework, would enable faster, coordinated responses to global-scale incidents.

Conclusion

The SolarWinds cyber espionage campaign revealed deep vulnerabilities in both the technical fabric of global supply chains and the legal frameworks intended to govern state behavior in cyberspace. While current instruments like the Budapest Convention and Tallinn Manual provide some structure, they fall short in cases involving non-signatory, state-sponsored actors. Addressing these gaps will require expanding treaty participation, harmonizing evidence-sharing laws, and establishing rapid response mechanisms that transcend political divisions. Without these reforms, the international community will remain reactive rather than proactive in the face of future large-scale cyber intrusions.

References

- CISA. (2020, December 13). Emergency directive 21-01: Mitigate SolarWinds Orion code compromise. Cybersecurity & Infrastructure Security Agency.
<https://www.cisa.gov/ed2101>
- Coco, A. (2022). Illegal: The SolarWinds hack under international law. *European Journal of International Law*, 33(4), 1275–1303. <https://doi.org/10.1093/ejil/chac077>
- Council of Europe. (2001). Convention on Cybercrime (ETS No. 185).
<https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=185>
- Just Security. (2020, December 18). Russia's SolarWinds operation and international law.
<https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/>
- Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. <https://doi.org/10.1017/9781316822524>
- United Nations. (1945). Charter of the United Nations.
<https://www.un.org/en/about-us/un-charter>
- White House. (2021, April 15). Executive Order on blocking property with respect to specified harmful foreign activities of the Government of the Russian Federation. The White House.
<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/15/executive-order-on-blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/>