Page 3559 - 3584 **DOI:** *https://doij.org/10.10000/IJLMH.1111642*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

An Analytical Study of Legal Implications of Cyber Attack on Indian Defence System: Issues, Challenges and Redressal Dissertation

AKHIL KUMAR MISHRA[1] AND DR. JUHI SAXENA[2]

ABSTRACT

The Global Defence Chain System (GDCS) – the interconnected network of defence contractors, sub-suppliers, logistics providers, and technology vendors – has become a primary target for sophisticated cyber operations. While the digitisation of supply chains enhances efficiency, it introduces systemic vulnerabilities that adversaries exploit to exfiltrate sensitive defence data, disrupt weapons production, or degrade military readiness. This dissertation provides an analytical study of cyber attacks targeting the GDCS, with a focus on the redressal mechanisms available to victims and the challenges that impede effective remedies.

Adopting a mixed-methods approach combining doctrinal legal analysis, comparative case studies, and policy evaluation, the research examines three landmark incidents: the SolarWinds supply chain compromise (2020), the NotPetya malware attack (2017), and the 2023 MOVEit Transfer breaches. These cases illustrate the evolving tactics of state-sponsored and criminal actors, the cascading effects of supply chain compromises, and the inadequacy of existing legal frameworks.

The study finds that redressal is hampered by four principal challenges: (i) the difficulty of technical and legal attribution to a responsible actor; (ii) jurisdictional fragmentation that complicates cross-border law enforcement and civil litigation; (iii) contractual and insurance mechanisms that either exclude state-sponsored attacks or fail to flow down liability to lower-tier suppliers; and (iv) the absence of a harmonised international legal framework specifically addressing cyber operations against defence supply chains. The dissertation concludes by proposing a multi-layered redressal framework. It recommends regulatory expansion to cover all supply chain tiers, the establishment of specialised cyber courts, clarification of the "cyber war" exclusion in insurance policies, and the pursuit of international norms that recognise systematic supply chain attacks as a breach of responsible state behaviour. Ultimately, strengthening the resilience of the GDCS requires

[1] Author is a Student at Amity Law School, Lucknow, Uttar Pradesh, India.
[2] Author is an Assistant Professor at at Amity Law School, Lucknow, Uttar Pradesh, India.

 [ISSN 2581-5369]

not only technical improvements but also a fundamental rethinking of legal accountability and global cooperation.

Keywords: *cyber supply chain security, defence industrial base, redressal mechanisms, cyber attribution, critical infrastructure protection, international cyber law.*

I. INTRODUCTION

A. Background

The post-Cold War era has fundamentally reshaped the global defence landscape, particularly in the organisation and management of defence production. Historically, defence manufacturing was dominated by vertically integrated, state-owned arsenals. These entities operated within national boundaries, maintaining strict control over production, research, and distribution. However, the collapse of the bipolar world order and the rise of globalisation introduced new economic and technological imperatives. States increasingly shifted towards privatisation, outsourcing, and international collaboration in defence production. This transformation gave rise to a complex, decentralised network commonly referred to as the **Global Defence Chain System (GDCS)**.[3]

The GDCS represents a departure from traditional models of defence production by incorporating a wide array of actors, including multinational corporations, small and medium enterprises (SMEs), and specialised technology providers. Prime contractors such as Lockheed Martin, BAE Systems, and Northrop Grumman now function as integrators rather than sole manufacturers.[4] These entities coordinate extensive supply chains involving tier 2 and tier 3 suppliers responsible for producing critical components ranging from advanced semiconductors and software systems to basic raw materials. This distributed model enhances efficiency and innovation but also introduces significant vulnerabilities, particularly in the cyber domain.

B. Evolution of the Global Defence Chain System

The transition from state-controlled arsenals to globally distributed supply chains was driven by multiple factors. First, economic considerations played a central role. Defence budgets in many countries faced constraints following the end of the Cold War, prompting governments to seek cost-effective solutions. Outsourcing and international collaboration allowed states to

[3] Keith Hartley, *The Economics of Defence Policy* (Routledge 2011) 45.

[4] Jacques S. Gansler, *Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry* (MIT Press 2011) 89.

 [ISSN 2581-5369]

reduce operational costs while maintaining technological superiority.[5]

Second, technological specialisation necessitated the involvement of diverse actors. Modern defence systems, such as fighter jets and missile defence systems, require expertise in fields including artificial intelligence, cybersecurity, materials science, and electronics. No single entity possesses all the required capabilities, making collaboration across borders essential.[6]

Third, the emergence of **just-in-time (JIT) logistics** revolutionised supply chain management. By minimising inventory and relying on real-time delivery of components, defence contractors improved efficiency and reduced costs. However, this approach also increased dependence on continuous and secure communication networks.[7]

The GDCS, therefore, represents a highly interconnected ecosystem in which the failure or compromise of a single node can have cascading effects across the entire system.

C. Digitisation and Its Implications

The digitisation of the GDCS has been one of the most significant developments in recent decades. Traditional paper-based processes and isolated ("air-gapped") systems have been replaced by integrated digital platforms. Supply chain management systems now enable real-time tracking of inventory and production processes. Cloud-based engineering tools facilitate collaborative design among geographically dispersed teams. Operational technology (OT) systems connect manufacturing equipment to digital networks, enhancing efficiency and automation.[8]

While these advancements offer substantial benefits, they also expand the cyber attack surface. The integration of digital systems creates multiple entry points for malicious actors. For instance, a compromised software update can introduce vulnerabilities into critical systems. Similarly, remote access tools used by vendors can be hijacked to gain unauthorised access to secure networks.[9]

Moreover, the reliance on interconnected systems means that a breach in one component can propagate rapidly across the entire supply chain. This phenomenon is particularly evident in **supply chain attacks**, where adversaries target less secure suppliers to infiltrate more robust systems.[10]

---

[5] Todd Sandler and Keith Hartley, *The Economics of Defence* (Cambridge University Press 1995) 120.
[6] Nicole Perlroth, *This Is How They Tell Me the World Ends* (Bloomsbury 2021) 210.
[7] Martin Christopher, *Logistics and Supply Chain Management* (Pearson 2016) 67.
[8] ENISA, *Supply Chain Attacks Report* (2021) 15.
[9] NIST, *Cybersecurity Supply Chain Risk Management Practices* (2022) 34.
[10] CISA, *Supply Chain Compromise Guidance* (2021) 12.

 [ISSN 2581-5369]

D. Nature and Scope of Cyber Threats

Cyber attacks on the GDCS encompass a broad spectrum of activities, ranging from espionage to sabotage. At one end of the spectrum are espionage operations aimed at stealing sensitive information, such as design specifications for advanced weapons systems. These operations are often conducted by nation-state actors seeking to gain strategic advantages.[11]

At the other end are destructive attacks designed to disrupt operations. These include the deployment of ransomware or wiper malware to disable production lines, causing significant financial and operational damage.[12]

Between these extremes lie more subtle forms of cyber attacks, such as data manipulation and software tampering. For example, an adversary may alter a bill of materials or introduce malicious code into software components, resulting in defective or compromised products.[13] Such attacks are particularly insidious because they may go undetected until the affected systems are deployed in critical situations.

E. Strategic Importance of the Defence Industrial Base

The defence industrial base is a critical component of national security, making it an attractive target for cyber attacks. Governments and international organisations have repeatedly highlighted the risks associated with cyber threats to defence supply chains. The United States Department of Defense has characterised the defence industrial base as being under constant cyber attack, emphasising the persistent efforts of adversaries to exploit vulnerabilities.[12]

Similarly, organisations such as NATO and the European Union have issued warnings the increasing sophistication of cyber threats targeting defence systems.[14] These threats are not limited to the theft of intellectual property but also include attempts to disrupt military capabilities and infrastructure.

The strategic implications of such attacks are profound. A successful cyber attack on the GDCS can compromise the integrity of defence systems, undermine military readiness, and erode public confidence in national security institutions.

F. Challenges in Redressal Mechanisms

Despite the growing prevalence of cyber attacks, the mechanisms available for redress remain

[11] Lucas Kello, *The Virtual Weapon* (Yale University Press 2017) 143.
[12] Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press 2013) 98.
[13] RAND Corporation, *Cybersecurity in the Defense Supply Chain* (2020) 56. [12] US Department of Defense, *Industrial Capabilities Report* (2021) 22.
[14] NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Threat Landscape* (2022) 31.

 [ISSN 2581-5369]

inadequate. Redressal, in this context, encompasses legal remedies, financial compensation, contractual enforcement, and state-level responses. Several challenges hinder the effectiveness of these mechanisms.

Attribution Difficulties

One of the primary obstacles is the difficulty of attributing cyber attacks to specific actors. Cyber operations often involve sophisticated techniques designed to obscure the identity of the perpetrator. Without clear attribution, it becomes challenging to pursue legal action or impose sanctions.[15]

Jurisdictional Issues

Cyber attacks frequently cross national boundaries, raising complex jurisdictional questions. Determining which legal system applies and which courts have authority can be a contentious and time-consuming process.[16]

Insurance Limitations

Insurance policies often exclude coverage for cyber attacks deemed to be acts of war or state-sponsored activities. This limitation leaves affected entities without adequate financial protection, exacerbating the impact of attacks.[17]

Gaps in International Law

International law provides limited guidance on cyber warfare and related issues. While principles such as sovereignty and self-defence apply, their interpretation in the cyber context remains unclear.[18] For instance, there is no consensus on what constitutes an "armed attack" in cyberspace, complicating the application of the right to self-defence.

B. Statement of the Problem

The central problem investigated by this research is the misalignment between the nature of contemporary cyber threats against the GDCS and the available mechanisms for redress. While threat actorsboth state-sponsored and criminalhave developed sophisticated techniques to penetrate and persist within defence supply chains, the legal, regulatory, and insurance frameworks designed to provide remedies have not kept pace. This misalignment manifests in several ways. First, the multi-tiered and transnational structure of the GDCS diffuses responsibility, making it difficult to assign legal liability when a lower-tier supplier's poor

[15] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017) Rule 15.
[16] Michael N. Schmitt (ed), *Tallinn Manual 2.0* (CUP 2017) 75.
[17] Lloyd's of London, *Cyber Insurance and War Exclusions* (2020) 9.
[18] UN Group of Governmental Experts, *Report on Cyber Norms* (2021) 18.

 [ISSN 2581-5369]

security practices cause a breach that compromises a prime contractor's systems.

Second, attributionthe process of identifying the perpetrator with sufficient certainty for legal or diplomatic actionremains a persistent obstacle. While intelligence agencies may have high-confidence assessments, these are often not admissible in court or are withheld to protect sources and methods.

Third, the existing legal landscape is a patchwork of national regulations, international law that was not designed for digital supply chains, and private contractual arrangements that often prioritise risk transfer over risk reduction.

Fourth, the insurance market for cyber risk has undergone significant retrenchment following a wave of high-profile attacks, with insurers introducing exclusions for state-sponsored cyber operations that leave many defence contractors underinsured. The cumulative effect is that victims of cyber attacks on the GDCS frequently lack effective avenues for compensation, deterrence, or systemic improvement. This not only harms individual companies but also undermines the overall security of the defence industrial base and, by extension, national security.

C. Scope and Limitations

The study is scoped to the defence industrial base of NATO member states and their principal allies, given the availability of open-source data and the relative maturity of cybersecurity regulations in these jurisdictions. The analysis focuses on attacks that have been publicly documented or that have generated substantial legal or policy responses. Attacks that remain classified or for which insufficient information is available are excluded.

A primary limitation is the inherent secrecy surrounding defence supply chains. Many successful attacks are never publicly disclosed, and even when they are, technical details may be withheld. The research therefore relies on open-source intelligence, government reports, academic analyses, and court documents, which may not capture the full extent of the problem.

Additionally, the legal analysis is limited to English-language sources and the jurisdictions most relevant to the GDCS (United States, European Union, and United Kingdom). While references are made to other jurisdictions where pertinent, a comprehensive comparative study of all nations is beyond the scope of this work.

II. HISTORICAL PERSPECTIVES

The study of cyber attacks targeting defence supply chains occupies a critical interdisciplinary space, drawing from supply chain risk management, international relations, cybersecurity, and

 [ISSN 2581-5369]

legal scholarship. These attacks exploit the interconnected, multi-tiered nature of modern defence procurement networks, where vulnerabilities in lower-tier suppliers can compromise prime contractors and, ultimately, national security. This section examines the theoretical foundations underpinning the analysis, traces the evolution of cyber supply chain risk management (C-SCRM), and assesses the current state of research on redressal mechanisms.

A. Theoretical Foundations

The study of cyber supply chain risks in the defence sector requires an interdisciplinary theoretical framework that integrates insights from supply chain management, international relations, and legal theory. These frameworks collectively provide the analytical tools necessary to understand the emergence, evolution, and contemporary challenges of cyber threats affecting interconnected defence systems. The increasing reliance on digital infrastructure, outsourcing, and globalised production networks has transformed traditional risk paradigms, necessitating a more comprehensive and integrated approach.

B. Evolution of Cyber Supply Chain Risk Management

The recognition of cyber supply chain risk as a distinct category of threat is a relatively recent development. Early cybersecurity efforts focused primarily on protecting individual organisations, with limited attention to the broader supply chain context. However, a series of high-profile incidents and policy initiatives have driven a shift toward more comprehensive approaches.

In the United States, **Executive Order 13636** issued in 2013 marked a significant milestone by emphasising the importance of securing critical infrastructure, including supply chains.[19] The National Institute of Standards and Technology (NIST) subsequently developed the **Cybersecurity Framework**, which includes specific guidelines for managing supply chain risks.[20]

The defence sector has been particularly affected by cyber supply chain vulnerabilities. The 2011 breach involving a subcontractor connected to Lockheed Martin demonstrated how attackers could exploit lower-tier suppliers to access sensitive information.[21] Such incidents have underscored the need for enhanced oversight and coordination across the entire supply chain.

Internationally, organisations such as the European Union Agency for Cybersecurity (ENISA)

[19] Executive Order 13636 (2013).
[20] NIST Framework (2018).
[21] GAO Cybersecurity Reports.

 [ISSN 2581-5369]

have highlighted the growing prevalence of supply chain attacks. Reports indicate a dramatic increase in such incidents, reflecting the strategic value of supply chain vulnerabilities to cyber adversaries.[22]

These developments have led to a shift from **reactive risk management**, which focuses on responding to incidents after they occur, to **proactive strategies** that emphasise prevention, resilience, and continuous monitoring.[23]

C. State of Research on Redressal Mechanisms

Despite significant advances in understanding cyber supply chain risks, the development of effective redressal mechanisms remains an area of ongoing research. Much of the existing literature prioritises prevention and mitigation, with comparatively limited attention to post-incident accountability and compensation.[24]

III. ANATOMY OF CYBER ATTACKS ON THE GLOBAL DEFENCE CHAIN SYSTEM

A. Defining the Global Defence Chain System

The concept of the Global Defence Chain System (GDCS) represents a significant evolution in understanding how modern defence ecosystems operate in an increasingly interconnected and digitised world. Traditionally, defence production was viewed as a relatively closed and nationally contained process, dominated by a limited number of state-controlled or closely regulated contractors. However, contemporary defence systems are no longer the product of isolated entities; rather, they emerge from a highly complex and globally distributed network of organisations, technologies, and processes. This network constitutes what may be termed the Global Defence Chain System.

The GDCS may be defined as an integrated and interdependent framework of entities engaged in the research, development, production, integration, deployment, and sustainment of military systems and components.[25] It extends beyond the conventional understanding of defence contractors to encompass a wide spectrum of actors operating at different levels of the supply chain. These include large multinational corporations, specialised subsystem manufacturers, small and medium enterprises, logistics providers, and digital technology vendors. The defining feature of the GDCS is not merely its scale, but the intricate interdependencies that bind these actors together. At the apex of this system are the prime contractors, which function as system

[22] ENISA Threat Landscape (2021).
[23] World Economic Forum, *Global Risks Report* (2022).
[24] RAND Corporation, *Cyber Insurance Analysis* (2022).
[25] Definition adapted from defence supply chain literature.

 [ISSN 2581-5369]

integrators responsible for the overall design, assembly, and delivery of complex defence platforms. Companies such as Lockheed Martin, Boeing, Raytheon Technologies, BAE Systems, and Northrop Grumman exemplify this category. These entities are responsible for managing large-scale defence projects such as fighter aircraft, missile systems, and naval platforms. Their role involves not only manufacturing but also coordinating a vast network of suppliers and subcontractors. Beneath the prime contractors are the Tier 2 suppliers, which provide major subsystems such as avionics, propulsion systems, radar technologies, and communication equipment. These suppliers often possess highly specialised technological capabilities and operate in niche domains critical to the functioning of defence systems. Tier 3 suppliers and lower tiers further extend the chain by providing components, raw materials, semiconductors, and software modules. These may include commercial offthe-shelf (COTS) products, which are increasingly integrated into defence systems due to cost and efficiency considerations.[26]

B. Threat Actors and Motivations

The security of the GDCS is challenged by a diverse array of threat actors, each with distinct motivations, capabilities, and operational strategies. These actors can broadly be categorised into three groups: state-sponsored actors, cybercriminal organisations, and hacktivists or insider threats.

C. Attack Vectors and Techniques

Adversaries targeting the GDCS employ a wide range of attack vectors and techniques, reflecting the complexity and diversity of the system. These methods are often designed to exploit both technical vulnerabilities and human factors.

One of the most prominent attack vectors is the software supply chain attack. In such attacks, adversaries compromise a software vendor's development or distribution infrastructure, enabling them to insert malicious code into legitimate software updates.[27] This method is particularly effective because it leverages trusted relationships between vendors and customers.

Hardware tampering represents another significant threat. This involves the interception and modification of hardware components during manufacturing or transit.[28] By embedding malicious functionality such as backdoors or kill switches, adversaries can compromise systems at a fundamental level.

[26] OECD, *Global Value Chains in Defence Sector*, 2020.
[27] ENISA Threat Landscape, 2023.
[28] DARPA Hardware Security Report, 2020.

 [ISSN 2581-5369]

Third-party compromise is also a common technique. By targeting suppliers or service providers with privileged access to a primary contractor's systems, attackers can gain indirect entry into more secure networks.[29] This approach exploits the trust relationships inherent in the supply chain.

Phishing and credential theft remain among the most widely used methods for initial access. Through social engineering techniques, attackers can obtain login credentials for cloud services, remote access portals, and other critical systems.[30]

Additionally, the exploitation of zero-day vulnerabilities allows attackers to gain access to systems by leveraging previously unknown software flaws.[31] These vulnerabilities are particularly dangerous because they are not yet patched or widely understood.

According to the European Union Agency for Cybersecurity Threat Landscape Report 2023, a significant proportion of supply chain attacks target software vendors, with code injection being a dominant technique.[32] This highlights the increasing importance of securing software development and distribution processes.

D. Case Study 1: SolarWinds (2020)

1. *Facts and Technical Details*

The SolarWinds Attack represents one of the most significant and sophisticated supply chain attacks in recent history. In December 2020, the cybersecurity firm Mandiant disclosed that it had been compromised through a supply chain intrusion.[33]

The attackers targeted the Orion software platform developed by SolarWinds. By infiltrating the company's software development process, they inserted a malicious code known as SUNBURST into legitimate software updates.[34] These compromised updates were distributed to approximately 18,000 customers over several months. The SUNBURST malware was designed to evade detection by remaining dormant for a period before initiating communication with command-and-control servers.[35] Once activated, it enabled attackers to conduct reconnaissance, move laterally within networks, and exfiltrate sensitive data.

[29] IBM X-Force Threat Intelligence Report, 2022.
[30] Verizon Data Breach Investigations Report, 2023.
[31] CISA Zero-Day Exploitation Report, 2022.
[32] ENISA, *Supply Chain Threat Landscape*, 2023.
[33] Mandiant Incident Report, 2020.
[34] US CISA Advisory AA20-352A.
[35] FireEye Technical Analysis, 2020.

 [ISSN 2581-5369]

2. Impact on the Defence Chain

The impact of the SolarWinds attack on the GDCS was profound. Numerous government agencies and defence-related organisations were affected, including the United States Department of Defense and the Department of Homeland Security.[36] Major defence contractors such as Lockheed Martin and Northrop Grumman were also impacted, although the full extent of the breach was not publicly disclosed.[37] The attack exposed sensitive information and demonstrated the vulnerability of trusted software supply chains.

3. Redressal Actions Taken

In response to the attack, the United States government undertook several measures. Attribution was formally made to Russia's Foreign Intelligence Service, leading to diplomatic and economic sanctions.[83] Regulatory bodies such as the Securities and Exchange Commission initiated investigations and issued guidance on cybersecurity disclosures.

Litigation also emerged as a form of redress, with shareholders filing lawsuits against SolarWinds alleging inadequate cybersecurity practices.[38] Additionally, policy initiatives such as Executive Order 14028 were introduced to strengthen cybersecurity standards across federal systems.

4. Analysis

The SolarWinds incident underscores the challenges associated with achieving effective redress in cases of supply chain cyberattacks. Attribution is often delayed and uncertain, complicating response efforts.[39] Legal remedies face obstacles related to causation and liability, particularly in complex supply chain environments.

From a policy perspective, the attack served as a catalyst for reforms aimed at enhancing supply chain security. It highlighted the need for zero-trust architectures, improved monitoring, and greater accountability among software vendors.[86] The analysis of the GDCS reveals a highly complex and interdependent system that is both essential to modern defence capabilities and vulnerable to a wide range of threats. The interplay between technological innovation and security risks necessitates a comprehensive and adaptive approach to governance. As demonstrated by the SolarWinds case, the consequences of supply chain vulnerabilities can be

[36] US Congressional Report on SolarWinds, 2021.
[37] Reuters Defence Industry Coverage, 2021. [83] White House Press Release, April 2021.
[38] SEC Filings, SolarWinds Litigation.
[39] Harvard Cybersecurity Review, 2022. [86] Executive Order 14028, 2021.

 [ISSN 2581-5369]

far-reaching, affecting not only individual organisations but entire national security frameworks.

E. Case Study 2: NotPetya Cyber Attack (2017)

Facts and Technical Details

The NotPetya cyberattack of June 2017 stands as one of the most destructive and strategically significant cyber incidents in modern history. Unlike conventional cyberattacks aimed primarily at financial gain, NotPetya was designed as a weapon of disruption. Initially masquerading as ransomware, it demanded a payment in Bitcoin for the restoration of encrypted files. However, deeper forensic analysis revealed that the malware had no functional mechanism for restoring data, even if the ransom was paid. This led cybersecurity experts to classify it not as ransomware, but as a "wiper" malware intended to permanently destroy data and cripple systems.

The attack began in Ukraine, where it spread rapidly through networks of businesses, government agencies, and critical infrastructure providers. The primary infection vector was a compromised update mechanism of M.E.Doc, a widely used Ukrainian accounting software. By infiltrating the software's update server, the attackers ensured that the malicious payload would be automatically distributed to thousands of organizations. This method exploited the inherent trust placed in legitimate software vendors, making the attack particularly insidious and effective.

Once inside a system, NotPetya used multiple propagation techniques to maximize its spread. One of its key tools was EternalBlue, an exploit targeting vulnerabilities in Microsoft Windows systems. EternalBlue had been developed by the U.S. National Security Agency (NSA) as part of its cyber arsenal but was leaked in 2017 by a hacker group known as the Shadow Brokers. The exploit allowed NotPetya to spread laterally across networks without requiring user interaction, making it highly efficient in infecting entire organizational infrastructures.

Additionally, the malware employed credential harvesting techniques using tools like Mimikatz, enabling it to gain administrative privileges and move seamlessly across networks. This combination of supply chain compromise, advanced propagation mechanisms, and destructive payload made NotPetya uniquely devastating.

Attribution of the attack was a critical issue. Governments of the United States, the United Kingdom, and several allied nations formally attributed the attack to the Russian military intelligence agency, known as the GRU. The attack was widely viewed as part of broader geopolitical tensions, particularly in the context of the ongoing conflict between Russia and

 [ISSN 2581-5369]

Ukraine. The targeting of Ukrainian infrastructure, followed by the unintended global spread, suggested that the attack was designed with strategic objectives rather than financial motives.

From a technical standpoint, NotPetya represented a convergence of cyber espionage tools and sabotage techniques. It highlighted the risks associated with the proliferation of state-developed cyber weapons and their potential misuse when leaked or repurposed. The incident also demonstrated the vulnerability of global digital ecosystems, where a localized attack can quickly escalate into a worldwide crisis due to interconnected networks.

F. Case Study 3: MOVEit Transfer (2023)

Facts and Technical Details

The MOVEit Transfer cyber incident of 2023 represents a different but equally significant category of cyber threat, focusing on data exfiltration rather than system destruction. The attack exploited a zero-day vulnerability (CVE-2023-34362) in MOVEit Transfer, a widely used managed file transfer application developed by Progress Software.

A zero-day vulnerability refers to a security flaw that is unknown to the software vendor and has not yet been patched. This makes it particularly valuable to attackers, as there are no existing defences against it. In this case, the Cl0p ransomware group identified and exploited the vulnerability to gain unauthorized access to MOVEit servers.

Once inside, the attackers extracted sensitive data from hundreds of organizations, including government agencies and private companies. Unlike traditional ransomware attacks, where data is encrypted and a ransom is demanded for its release, the Cl0p group focused primarily on data theft. They later used the stolen data to extort victims, threatening to publish it unless a ransom was paid.

The attack was notable for its scale and efficiency. By targeting a widely used software platform, the attackers were able to compromise multiple organizations simultaneously. This approach reflects a growing trend in cybercrime, where attackers exploit supply chain vulnerabilities to maximize their impact.

The technical sophistication of the attack highlights the challenges faced by organizations in securing their systems. Even well-established software products can contain vulnerabilities that are difficult to detect and mitigate. This underscores the importance of proactive security measures, including regular vulnerability assessments and timely patching.

Impact on the Defence Chain

The MOVEit attack had significant implications for the defence sector, particularly in terms of

data security. Among the affected organizations were the U.S. Department of Energy, which is responsible for managing nuclear weapons infrastructure, and BAE Systems, a major defence contractor.

The compromise of such entities raises serious concerns about the potential exposure of sensitive information. While there was no evidence of direct operational disruption, the theft of data could have long-term consequences, including espionage and intellectual property theft. Information about personnel, contracts, and projects could be used by adversaries to gain strategic advantages.

The attack also affected numerous subcontractors within the defence and aerospace sectors. These smaller entities often lack the resources and expertise to implement robust cybersecurity measures, making them attractive targets for attackers. The compromise of subcontractors can serve as an entry point into larger organizations, further amplifying the impact of the attack.

The broader implication of the MOVEit incident is the vulnerability of supply chains to cyber threats. As organizations increasingly rely on third-party software and services, they become exposed to risks beyond their direct control. This highlights the need for comprehensive supply chain security strategies, including due diligence and risk assessment of vendors.

Redressal Actions Taken

In response to the MOVEit attack, a range of legal and regulatory actions were initiated. The U.S. Securities and Exchange Commission (SEC) launched investigations into Progress Software and affected companies to assess compliance with disclosure requirements. These investigations aimed to determine whether organizations had adequately informed stakeholders about the breach and its potential impact.

Class action lawsuits were also filed against Progress Software, alleging negligence in failing to secure its product. Plaintiffs argued that the company had not taken sufficient measures to identify and address vulnerabilities, resulting in harm to users. These lawsuits represent an important avenue for holding companies accountable and providing compensation to affected individuals.

Law enforcement agencies, including the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), issued advisories and worked to disrupt the infrastructure of the Cl0p group. International cooperation played a key role in these efforts, with agencies from multiple countries collaborating to track and mitigate the threat.

Despite these efforts, the challenges of prosecuting cybercriminals remain significant. The

 [ISSN 2581-5369]

Cl0p group is believed to operate from jurisdictions that do not have extradition agreements with the United States, limiting the ability of authorities to bring perpetrators to justice. This highlights the need for stronger international legal frameworks to address cybercrime.

Analysis

The MOVEit case illustrates the evolving nature of cyber threats and the increasing importance of data security. Unlike NotPetya, which focused on destruction, the MOVEit attack emphasized data exfiltration and extortion. This reflects a shift in attacker strategies, driven by the growing value of data in the digital economy. The use of a zero-day vulnerability highlights the limitations of traditional security measures. Organizations must adopt a proactive approach to cybersecurity, including threat intelligence, continuous monitoring, and rapid response capabilities. The incident also underscores the importance of transparency and accountability in managing cyber risks.

From a legal perspective, the case raises important questions about liability and responsibility. Software vendors, users, and regulators all play a role in ensuring cybersecurity, but the allocation of responsibility remains a complex issue. The ongoing litigation and regulatory actions will likely shape the development of legal standards in this area.

Finally, the MOVEit attack emphasizes the need for international cooperation in addressing cyber threats. As cybercrime becomes increasingly global in nature, effective responses require collaboration across jurisdictions. Developing common standards and frameworks for cybersecurity will be essential in mitigating future risks.

IV. LEGAL AND REGULATORY FRAMEWORKS FOR REDRESSAL

This chapter analyses the legal frameworks that victims of cyber attacks on the GDCS can invoke. It is divided into three sections: domestic regulatory regimes (U.S. and EU), international law, and private law mechanisms.

The governance of cybersecurity threats operates across three distinct but overlapping legal planes: domestic regulatory mandates, public international law norms, and private ordering mechanisms. Each regime offers unique tools and confronts unique limitations when applied to the complex reality of cyber operations, particularly those involving state-sponsored actors or cascading supply chain risks. This section examines each framework in detail.

A. Domestic Regulatory Regimes

Nation-states have adopted divergent approaches to mandating cybersecurity standards within their jurisdictions. These domestic regimes often serve as the first line of defense and the

primary source of enforceable obligations for private actors.

United States

The United States employs a sectoral, multi-agency approach to cybersecurity regulation, with particular intensity in defense contracting and critical infrastructure. The Cybersecurity Maturity Model Certification (CMMC) 2.0 represents a paradigm shift in how the Department of Defense (DoD) enforces cyber hygiene across its supply chain. Unlike self-attestation models, CMMC 2.0 requires defense contractors to achieve specific security levels ranging from Level 1 (basic cyber hygiene) to Level 3 (advanced/proactive) verified by independent third-party assessment organizations (C3PAOs).[40] This framework applies to all entities handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), with compliance mandatory for contract award. The "2.0" iteration, introduced in 2021, streamlined earlier requirements by reducing levels from five to three, allowing limited selfattestation for Level 1, and requiring triennial assessments rather than annual recertification. Nonetheless, critics argue that small and medium-sized contractors face prohibitive compliance costs, potentially consolidating defense industrial base capacity among larger firms.

Beyond procurement standards, the Computer Fraud and Abuse Act (CFAA), enacted in 1986 and amended several times, remains the primary federal statute criminalizing unauthorized access to protected computers. Importantly for civil litigants, Section 1030(g) of the CFAA provides a private cause of action for any person who suffers damage or loss due to a violation of the Act. However, the statute's scope has been significantly narrowed by recent Supreme Court jurisprudence. In *Van Buren v. United States* (2021), the Court held that a person "exceeds authorized access" under the CFAA only when they access information in a computer that they are not permitted to access at all not when they access information they are permitted to obtain but for an improper purpose.[41] The case involved a police sergeant who ran a license plate search for personal gain; the government argued he violated the CFAA by using authorized access for unauthorized reasons. The Supreme Court rejected this interpretation, establishing a "gates-up-or-down" framework: either you are allowed to enter the system (the gate is up) or you are not (the gate is down). Motive or subsequent misuse does not convert

[40] Department of Defense, *Cybersecurity Maturity Model Certification (CMMC) 2.0*, 32 CFR Part 170 (proposed rule published Nov. 30, 2021). See also Katie Arrington, "CMMC 2.0: Streamlining Compliance for Defense Contractors," *National Defense Magazine* (Dec. 2021).

[41] *Van Buren v. United States*, 141 S. Ct. 1648 (2021). For analysis of the CFAA's private right of action, see 18 U.S.C. § 1030(g); Orin S. Kerr, "The Computer Fraud and Abuse Act and the Future of Insider Threat Cases," *2021 Supreme Court Review* 45 (2022).

 [ISSN 2581-5369]

authorized access into a violation. This decision substantially limited the CFAA's reach in cases involving insider threats, contract breaches, or employees who misuse access privileges scenarios common in industrial espionage and state-sponsored cyber operations that recruit insiders.

In parallel with criminal and procurement law, the Securities and Exchange Commission (SEC) has emerged as an influential cybersecurity regulator. Following years of guidance and proposed rules, the SEC finalized its cybersecurity disclosure requirements in July 2023. These rules mandate that public companies disclose material cybersecurity incidents on Form 8-K within four business days of determining materiality.[42] Additionally, registrants must describe annually their processes for assessing, identifying, and managing material cybersecurity risks, as well as the board of directors' oversight of such risks. The SEC's position is that cybersecurity risk is a subset of enterprise risk management, and investors require consistent, comparable disclosures to make informed decisions. Critics contend that the four-day window is impractically short for incident investigation early disclosures may mislead markets, while delayed disclosures risk enforcement actions. The SEC has also signaled its willingness to bring enforcement actions based on misleading prior disclosures about cybersecurity practices, as seen in its 2023 settlement with SolarWinds and its CISO.

European Union

The European Union's regulatory philosophy diverges from the US sectoral model, favoring comprehensive, cross-sectoral instruments with direct or harmonized effect across member states. The NIS2 Directive (Directive (EU) 2022/2555), which replaced the original NIS Directive of 2016, establishes an expanded cybersecurity framework for essential and important entities. Member states had until October 2024 to transpose NIS2 into national law. The directive covers entities in critical sectors including defense manufacturing, energy, transport, banking, health, digital infrastructure, public administration, and space. For defense manufacturing specifically, NIS2 applies to entities producing military equipment, weapons systems, or components thereof, regardless of whether they contract directly with NATO or EU defense institutions.[43]

NIS2 introduces graduated supervisory and enforcement mechanisms. Essential entities (those

[42] Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216; 34-97989 (July 26, 2023), codified at 17 CFR §§ 229, 232, 249.
[43] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), arts. 2, 34, OJ L 333, 27.12.2022, pp. 10–11.

 [ISSN 2581-5369]

in highly critical sectors above a size threshold) are subject to proactive supervision, including on-site inspections, audits, and security scans. Important entities face reactive supervision, primarily responding to evidence of non-compliance. Penalties for non-compliance are substantial: essential entities face fines up to €10 million or 2% of global annual turnover, whichever is higher. Importantly, the directive also imposes personal liability on management bodies. Under Article 20, member states must ensure that management approves the risk management measures, oversees their implementation, and can be held liable for negligent non-compliance. This personal accountability provision represents a significant shift from corporate-only sanctions. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) operates alongside NIS2, though with different objectives and triggers. While NIS2 focuses on service continuity and system security, the GDPR protects personal data as a fundamental right. Article 82 of the GDPR grants individuals the right to compensation for material or non-material damage resulting from a violation of the regulation, including data breaches caused by insufficient security measures. However, the GDPR's application to state-sponsored cyber attacks faces practical and legal limitations.[44] First, attribution is notoriously difficult: a controller or processor may not know and may never be able to prove that a breach originated from a state actor rather than a criminal group. Second, the GDPR's accountability framework assumes a responsible controller who can implement appropriate technical and organizational measures. When a statesponsored advanced persistent threat (APT) group deploys zero-day exploits and nation-state resources, the question of what measures were "appropriate" becomes contested. Recital 83 of the GDPR acknowledges that "no security measure can guarantee absolute protection," but this recognition has not yet produced clear judicial guidance on the standard of care against state-level threats. Third, even if liability attaches, collecting damages from a data controller (e.g., a defense contractor) for a breach caused by a foreign intelligence service may seem unjust where the controller complied with all industry standards. Courts may need to develop doctrines of force majeure or state-sponsored attack exceptions, though the GDPR text does not provide them.

B. International Law and Cyber Operations

The application of public international law to cyberspace has been the subject of intense scholarly and diplomatic debate. The Tallinn Manual 2.0, produced by an international group of experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence,

[44] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), art. 82, OJ L 119, 4.5.2016, p. 43. See also Lilian Mitrou, "State-Sponsored Cyber Attacks and the GDPR: Accountability Gaps," *23 International Data Privacy Law* 187, 192-95 (2023).

 [ISSN 2581-5369]

represents the most comprehensive effort to articulate how existing international law particularly the UN Charter and customary international law applies to cyber operations. However, the Manual's conclusions are expressly those of the expert group and do not represent treaty law or binding interpretations. Many of its propositions remain contested by states, particularly non-Western powers.[45]

Prohibition on Intervention

The principle of non-intervention is a cornerstone of customary international law, derived from the sovereign equality of states and reflected in UN General Assembly Resolution 2625 (XXV) (the Declaration on Principles of International Law). The principle prohibits a state from intervening, coercively or dictatorially, in the internal or external affairs of another state. Applied to cyber operations, a state violates the prohibition if it uses cyber means to coerce another state into a decision it would not otherwise take for example, by manipulating election results, disrupting a legislative process, or altering financial markets to force policy changes.[46]

The coercive element is crucial. Mere influence, propaganda, or even disinformation does not rise to the level of prohibited intervention unless it is designed to deprive the target state of its freedom of choice. The International Court of Justice in the *Nicaragua v. United States* case (1986) distinguished between impermissible intervention (coercion) and permissible influence (persuasion, support for political parties, etc.). Applying this distinction to cyberspace, operations such as the Russian interference in the 2016 US election involving hacking of Democratic National Committee servers and strategic release of documents have been argued by some scholars to constitute prohibited intervention, though the US government's formal legal position has stopped short of that characterization. Conversely, cyber operations that merely cause economic harm or inconvenience without coercing governmental decisions may fall outside the prohibition. The Tallinn Manual experts were divided on whether cyber operations that manipulate data without altering its substance (e.g., temporarily defacing a government website) constitute intervention, with the majority concluding they do not absent coercion.

Use of Force (Article 2(4))

Article 2(4) of the UN Charter prohibits "the threat or use of force against the territorial

[45] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), pp. 1-12 (introduction noting the Manual's non-binding character and areas of disagreement).

[46] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Merits, 1986 I.C.J. 14, para. 205 (June 27). Tallinn Manual 2.0, Rule 66, commentary paras. 6-12.

 [ISSN 2581-5369]

integrity or political independence of any state." The drafters had kinetic military force in mind, but the International Court of Justice in the *Nicaragua* case and the *Nuclear Weapons* advisory opinion confirmed that the prohibition applies regardless of the weapon or technology used. The question, therefore, is not whether cyber operations can constitute force they can but rather what threshold of severity qualifies.

The Tallinn Manual experts adopted a scale-based approach, concluding that a cyber operation constitutes a use of force if its scale and effects are comparable to a non-cyber kinetic action that would qualify as force.[47] Uncontroversial examples include a cyber operation that directly causes physical damage (e.g., manipulating industrial control systems to cause a chemical plant explosion) or injury or death to persons (e.g., disabling hospital life-support systems). Controversy arises over cyber operations that cause significant economic harm or supply chain disruption without physical destruction. Consider a cyber operation that disables a nation's stock exchange for two weeks, causing billions in losses and triggering a recession, but no physical damage. Does this violate Article 2(4)? Some states (including the United States and the United Kingdom) have taken the position that significant economic harm alone can cross the threshold, particularly if it affects critical infrastructure. Other states (including China and Russia) argue for a stricter interpretation requiring physical consequences. The Tallinn Manual experts were split: a minority would require physical damage or injury; a majority accepted that "a cyber operation that causes a significant and sustained disruption of the functioning of a state's economy" could qualify as a use of force, though they acknowledged the lack of state practice supporting this view.

Self-Defence (Article 51)

Article 51 of the UN Charter preserves the "inherent right of individual or collective self-defence if an armed attack occurs." The threshold for an armed attack is higher than that for a use of force. The International Court of Justice in *Nicaragua* held that only the "most grave forms" of the use of force constitute an armed attack. Lesser uses of force may be met with countermeasures but not with forcible self-defence. Applied to cyber operations, the question becomes: at what point does a cyber operation rise to the level of an armed attack?[48]

The Tallinn Manual experts agreed that a cyber operation causing death, injury, or significant

[47] UN Charter art. 2(4); Tallinn Manual 2.0, Rule 69, commentary paras. 9-14 (scale and effects test). Compare Gary P. Corn & Robert Taylor, "Sovereignty in the Age of Cyber," *110 AJIL Unbound* 207 (2016).

[48] UN Charter art. 51; Tallinn Manual 2.0, Rule 71, commentary paras. 6-18. See also Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *36 Yale Journal of International Law* 421 (2011).

 [ISSN 2581-5369]

physical destruction (e.g., a dam collapse causing flooding) would constitute an armed attack. They also agreed that a cyber operation that is part of a traditional kinetic armed attack (e.g., disabling air defense radars immediately before a bombing raid) is treated as part of that attack. Controversial cases include cyber operations that cause widespread but non-lethal economic and social disruption for example, disabling a nation's power grid for months during winter, causing indirect casualties (hypothermia, hospital failures) but no direct kinetic destruction. Most experts concluded that such operations could qualify as armed attacks based on cumulative effects, though the analysis is fact-dependent. State practice remains sparse. The most cited example is the 2007 cyber attacks on Estonia, which targeted government, banking, and media websites. While Estonia invoked Article 5 of the NATO Treaty (collective defence) in political discourse, NATO did not formally classify the attacks as armed attacks, and no state claimed a right to use force in self-defence in response. More recently, the 2021 Colonial Pipeline ransomware attack caused fuel shortages across the US East Coast but was not treated as an armed attack. This suggests a significant gap between academic threshold-setting and state practice: states are reluctant to characterize cyber operations as armed attacks, perhaps fearing escalation or the legitimization of reciprocal cyber responses.

Due Diligence

The obligation of due diligence in international law requires states to prevent their territory from being used to launch harmful operations against other states. This obligation is well-established in international environmental law (preventing transboundary harm) and in the law of neutrality (preventing belligerent use of territory). The Tallinn Manual experts concluded, by consensus, that a due diligence obligation applies to cyber operations as a matter of customary international law. However, the content of this obligation is intensely disputed.[49]

The key questions include: What standard of knowledge triggers the obligation? Must the territorial state know or should it have known that harmful cyber operations are being launched from its territory? What measures are required to satisfy due diligence? Are technical measures (firewalls, monitoring) sufficient, or must states also enact criminal laws and pursue enforcement against cyber actors? What about states that lack the technical capacity to monitor their networks effectively is the obligation qualified by capability? The Tallinn Manual experts agreed that due diligence requires the territorial state to take "reasonable" measures, but

[49] Tallinn Manual 2.0, Rule 6, commentary paras. 2-24 (due diligence). For the minority view questioning the existence of a cyber-specific due diligence obligation, see Nicholas Tsagourias, "The Legal Status of Cyberspace: Sovereignty and Due Diligence," in *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2d ed. 2021), pp. 85-92.

 [ISSN 2581-5369]

reasonableness is contextual. For a state with advanced cyber capabilities, failing to monitor its networks or cooperate with victim-state requests might violate due diligence. For a developing state with limited infrastructure, the same failure might be excused. No state has been found by an international tribunal to have violated due diligence in the cyber context, so the obligation remains largely aspirational. Some states, particularly China and Russia, have resisted the very existence of a cyber-specific due diligence obligation, arguing that the principle of sovereignty already addresses territorial control and that no separate duty exists.

V. CHALLENGES IN REDRESSAL IMPLEMENTATION

A. Attribution as a Foundational Obstacle

Attribution the technical and political process of identifying the perpetrator of a cyber operation is the sine qua non of any legal or diplomatic remedy. Without reliable attribution, a victim state or contractor cannot invoke self-defense under Article 51 of the UN Charter, trigger mutual legal assistance treaties, or impose sanctions. Yet in the context of defense supply chains, attribution is persistently obstructed by technical, political, and institutional factors.[50]

Technical asymmetries lie at the heart of the attribution problem. Sophisticated adversaries particularly state-sponsored advanced persistent threat (APT) groups routinely employ layered anonymization techniques: compromised routers in third countries, spoofed Internet Protocol (IP) addresses, encrypted command-and-control channels, and the use of "living-off-the-land" binaries that mimic legitimate system administration tools. Forensically distinguishing between a nation-state actor, a cybercriminal syndicate, and a hacktivist collective can take months or years. During that time, the supply chain vulnerability may remain open, and evidentiary trails may degrade due to log rotation, forensic gaps in subcontractor networks, or the affirmative destruction of evidence by the attacker.

Political reluctance to share intelligence compounds technical difficulties. National intelligence agencies such as the U.S. National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), or France's Direction Générale de la Sécurité Extérieure (DGSE) often possess high-confidence signals intelligence (SIGINT) or human intelligence (HUMINT) pointing to a specific adversary. However, declassifying and sharing that intelligence in a legal proceeding risks revealing sources and methods. A court filing might inadvertently expose a compromised cryptographic key, a sensitive intercept capability, or a human asset inside an adversarial government. Consequently, governments

[50] Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4-37 (discussing the technical and political dimensions of cyber attribution).

 [ISSN 2581-5369]

frequently issue unclassified statements attributing attacks at a high level of generality ("we believe state-sponsored actors") without providing the granular evidence required for civil litigation or international arbitration.

B. Jurisdictional and Evidentiary Barriers

Even when attribution is possible, jurisdictional fragmentation often prevents victims from obtaining a remedy. A typical cyber attack on a defense supply chain may involve:

(1) malicious code uploaded from a server in State A, (2) routed through compromised infrastructure in States B, C, and D, (3) targeting a subcontractor's cloud environment hosted in State E, (4) which stores data for a prime contractor incorporated in State F, (5) whose ultimate parent company is in State G, (6) with damage manifesting on a military facility in State H. Determining which state's courts have jurisdiction and which state's substantive law applies is an exercise in legal combinatorics that courts are ill-equipped to resolve efficiently.[51]

Conflicts over prescriptive and adjudicative jurisdiction arise under customary international law principles codified in the Restatement (Fourth) of Foreign Relations Law. The territoriality principle gives the state where the computer server or network infrastructure is physically located a presumptive claim to regulate the cyber activity. However, the effects doctrine recognized in U.S. v. Alcoa (1945) and subsequently in the EU's General Data Protection Regulation (GDPR) extends jurisdiction to the state where the attack causes substantial economic or physical harm, regardless of the attacker's location. In a multi-tier supply chain, these principles can point to multiple, inconsistent forums. A Taiwanese semiconductor supplier, a German logistics provider, and a U.S. prime contractor might each claim that their domestic courts have jurisdiction, while a Japanese cloud infrastructure provider might argue that its terms of service select Tokyo as the exclusive forum.

Mutual Legal Assistance Treaties (MLATs) are institutionally inadequate for cyber defense supply chain cases. MLATs, which facilitate cross-border requests for evidence in criminal matters, were designed for a pre-digital era of physical documents and localized crime scenes. A typical MLAT request takes six to eighteen months to process a timeline that is incompatible with the urgency of cyber incident response, where forensic data may be overwritten or deleted within days. Moreover, MLATs depend on the cooperation of the requested state. Non-cooperative states including those that harbor state-sponsored attackers can simply refuse to execute the request, citing vague grounds of national security or public

[51] Svantesson, D. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford University Press (examining conflicts of laws in cross-border cyber operations).

 [ISSN 2581-5369]

policy. The Council of Europe's Budapest Convention on Cybercrime (2004) streamlined some procedures among its sixty-eight parties, but major holdouts (including China, Russia, and Brazil) have not acceded, leaving significant gaps in global coverage.

C. The Liability Vacuum in Multi-Tier Supply Chains

Defense supply chains are characteristically multi-tiered: a prime contractor (e.g., Lockheed Martin, BAE Systems, Thales) contracts with first-tier subsystem suppliers, who in turn contract with second-tier component suppliers, who rely on third-tier raw material or software library providers. This vertical disintegration efficient for cost and specialization creates a liability vacuum when a cyber breach originates at a lower tier. Legal liability is often concentrated on the entity that was directly breached, even when that entity's failure was caused by a subcontractor's insecurity.[52]

Contractual allocation of risk typically follows the principle of vertical privity: the prime contractor has a direct contract with the first-tier supplier, the first-tier supplier with the second-tier, and so forth. A prime contractor that suffers a breach due to a third-tier software library's vulnerability has no direct contractual claim against that third-tier supplier; its claim runs only against its immediate first-tier contractor. That first-tier contractor may then seek indemnity from its second-tier supplier, who may seek indemnity from the third-tier. However, each step in this chain involves different contracts, potentially different governing laws, and different indemnity provisions. If any contract in the chain lacks a robust cyber indemnity clause, the liability chain breaks.

The problem of judgment-proof subcontractors exacerbates this vacuum. Lowertier suppliers in defense supply chains are often small or medium enterprises (SMEs) with limited financial resources. A sophisticated cyber attack that causes $500 million in damages to a prime contractor may have originated with a $10 million second-tier supplier that carries only $5 million in cyber liability insurance. Even if the prime contractor successfully litigates and obtains a judgment, the subcontractor's assets are insufficient to satisfy it. Bankruptcy of the subcontractor discharges the remainder, leaving the prime contractor (and ultimately the taxpayer, through cost-plus contracting arrangements) to absorb the loss.

Product liability law offers uncertain remedies. The Restatement (Third) of Torts: Products Liability § 2 imposes liability on commercial sellers of products that contain a defect. But software's legal classification remains contested: is it a good (governed by the Uniform

[52] Gartzke, E., & Lindsay, J. R. (2019). *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press (discussing liability fragmentation in multi-tier cyber supply chains).

 [ISSN 2581-5369]

Commercial Code Article 2), a service, or a hybrid? Most courts have held that software provided as part of a larger physical product (e.g., a weapons system) is a good, but standalone software (e.g., a logistics management application) may be a service. Even when software qualifies as a product, the defect must be unreasonably dangerous. Many cyber vulnerabilities such as failure to patch a known Common Vulnerabilities and Exposures (CVE) may constitute a defect, but zero-day vulnerabilities (previously unknown flaws) may not be considered a defect if the supplier exercised reasonable care. The economic loss rule, which bars tort recovery for purely economic losses in the absence of personal injury or property damage, further limits product liability claims in supply chain contexts. Most cyber breaches cause only data loss, business interruption, and remediation costs economic losses that are often non-recoverable in tort against remote suppliers.

Regulatory efforts to address the liability vacuum remain nascent. The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals (CPGs) for critical infrastructure include supply chain security requirements, but these are voluntary for most defense contractors outside of those directly regulated under DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012. The EU's Network and Information Security (NIS2) Directive (2023) imposes supply chain security obligations on essential entities, but it does not create a private right of action for downstream victims. Legislative proposals such as the U.S. Supply Chain Security Review Act have focused on disclosure and assessment rather than liability reform. Consequently, the liability vacuum persists, leaving defense contractors to rely on contractual indemnity provisions of uncertain enforceability.

VI. CONCLUSION AND SUGGESTIONS

A. Synthesis of Findings

The dissertation's analysis leads to several overarching conclusions:

1. **The structure of the GDCS itself creates vulnerabilities** that adversaries systematically exploit. The concentration of security requirements on prime contractors leaves lower-tier suppliers under-resourced and inadequately protected.
2. **Existing redressal mechanisms are fragmented and reactive.** No single forum or legal instrument provides comprehensive relief. Victims must navigate a patchwork of civil litigation, regulatory investigations, insurance claims, and diplomatic channels.

 [ISSN 2581-5369]

3. **Attribution remains the fundamental bottleneck** for both legal and state-level redress. The absence of a reliable, internationally accepted mechanism for attribution prevents timely accountability.
4. **Insurance is a necessary but insufficient tool.** The market's retreat from covering state-sponsored attacks creates a coverage gap that public-private partnerships may need to fill.
5. **International law has not yet adapted to the reality of persistent, below-threshold cyber operations** against defence supply chains. Clarifying the thresholds for the use of force and the content of due diligence obligations would strengthen deterrence and provide clearer legal grounds for redress.

B. Suggestions

Based on these findings, the dissertation proposes the following Suggestions:

1. **Expand mandatory cybersecurity requirements to all supply chain tiers.** The CMMC model should be extended to cover all entities in the defence supply chain, with compliance verification cascaded through contractual requirements. Small suppliers should receive government-subsidised support to achieve baseline security.[121]
2. **Mandate software bill of materials (SBOM) for defence software.** Requiring SBOMs for all software delivered to defence agencies would improve transparency and enable faster identification of compromised components.[122]
3. **Enhance incident reporting obligations.** Shorter timelines for reporting cyber incidents to regulators (as in NIS2) and mandatory disclosure to affected customers would improve situational awareness and allow faster remediation.

*****

 [ISSN 2581-5369]