The Role of Law in Protecting Critical Information Infrastructure from Cyber Attacks

Rezuwal Islam
Cyber Law Expert, Dhaka, Bangladesh
Email ID: r.islamcbldhaka@gmail.com

Cybersecurity Law and Policy Review
Volume 1, Issue 1 | 2025 | https://clprj.com/journal/index

Abstract

Critical information infrastructure (CII) — encompassing the digital systems underpinning energy grids, financial networks, telecommunications, water supply, healthcare delivery, and transportation — has emerged as the primary target of sophisticated cyber attacks perpetrated by state and non-state actors alike. The potential for cascading, catastrophic harm from successful attacks on such systems elevates CII protection to a matter of national security and public welfare of the highest order. Yet the legal frameworks charged with protecting critical information infrastructure remain fragmented, underspecified, and frequently inadequate to the threat. This article examines the role of law as a tool for CII protection, tracing the development of legal frameworks across key jurisdictions, assessing the adequacy of existing regulatory instruments, and identifying the structural deficiencies that prevent law from fulfilling its protective function. The article argues that effective legal protection of CII requires a coherent architecture combining mandatory baseline security standards, rigorous incident reporting obligations, meaningful liability frameworks that internalise the security externalities of technology vendors, robust public-private operational partnerships, and coordinated international legal instruments capable of deterring and responding to state-sponsored attacks. Drawing on lessons from comparative regulatory experience and recent high-profile incidents including attacks on colonial pipeline systems, energy grids, and healthcare networks, the article advances a set of normative recommendations for the reform of CII protection law in the digital age.

Keywords: *critical information infrastructure; CII protection; cyber attacks; national security; regulatory frameworks; public-private partnership; incident reporting; international law; liability; resilience*

1. INTRODUCTION

Modern societies are built upon an intricate lattice of digital systems whose uninterrupted operation is a precondition for the delivery of virtually every essential public good and private service. The electricity that powers hospitals, the payment networks that process transactions, the water treatment systems that safeguard public health, the telecommunications infrastructure that connects citizens and governments, and the transportation management systems that coordinate the movement of goods and people — all depend upon networked information technologies that are, by their nature, exposed to the threat of hostile interference from across the globe. This dependency, which deepens

with every advance in digitisation and connectivity, has transformed what were once discrete operational technologies into targets of strategic significance for adversarial states, terrorist organisations, and criminal enterprises with varying motivations but a shared appreciation of the asymmetric leverage that successful attacks on critical systems can provide.

The consequences of major cyber attacks on critical information infrastructure (CII) have been graphically illustrated by a series of landmark incidents in recent years. The attack on Ukraine's power grid in December 2015, which left some 230,000 consumers without electricity, demonstrated the capacity of state-sponsored cyber operations to produce physical effects on critical infrastructure comparable to those of conventional military action. The 2021 Colonial Pipeline ransomware attack, which disrupted fuel supplies across the eastern United States and precipitated panic buying, illustrated the potential for criminal actors to cause widespread societal disruption through attacks on privately owned critical systems. The sustained cyber offensive against Ukrainian critical infrastructure throughout the ongoing conflict with Russia has, with devastating clarity, demonstrated the role of CII attacks as an instrument of hybrid warfare. These incidents are not aberrations; they are harbingers of a threat trajectory that security analysts across the world regard with deep concern.

2. CRITICAL INFORMATION INFRASTRUCTURE: DEFINITION AND THREAT LANDSCAPE

2.1 Defining Critical Information Infrastructure

The concept of critical information infrastructure, while now widely employed in legislative instruments and policy documents across the world, lacks a settled, universally accepted definition. At its broadest, CII refers to the information and communications technology (ICT) systems, networks, and data that are essential to the functioning of infrastructure whose disruption or destruction would have a severe impact on national security, public health and safety, economic stability, or the effective functioning of government. Most jurisdictions identify a set of critical sectors whose infrastructure is deemed to fall within this definition; while the precise boundaries vary, common inclusions are energy (electricity generation, transmission, and distribution; oil and gas pipelines and refining), water supply and treatment, financial services (banking, payments, securities markets), telecommunications, transportation (aviation, rail, maritime, road), healthcare, emergency services, and government and defence systems.

The definitional challenge has practical significance because the scope of CII designation determines which entities are subject to heightened legal obligations. Over-inclusive definitions impose compliance costs on entities whose disruption would not produce genuinely catastrophic consequences; under-inclusive definitions leave genuinely critical systems outside the protective ambit of the law. The emergence of cloud computing has added a further layer of complexity: the major cloud service providers now underpin vast swathes of critical infrastructure across multiple sectors, yet their classification as CII operators remains legally uncertain in many jurisdictions. The Internet of Things, industrial control systems, and operational technology more broadly — historically isolated from

internet-connected networks — are increasingly interconnected, dramatically expanding the attack surface and, correspondingly, the potential scope of CII designation.

A useful distinction, though not always drawn by legislation, is that between critical infrastructure (the physical systems and facilities that deliver essential services) and critical information infrastructure (the ICT systems that control, monitor, or enable those physical systems). The convergence of information technology (IT) and operational technology (OT) in modern critical systems means that this distinction has eroded substantially in practice; attacks on the ICT layer increasingly produce direct physical consequences, as the Ukraine power grid attacks and the 2021 Oldsmar, Florida water treatment facility intrusion vividly demonstrated.

2.2 The Evolving Threat Landscape

The threats facing critical information infrastructure are diverse in their origin, motivation, and operational character, and are evolving at a pace that challenges regulatory adaptation. Nation-state actors represent the most sophisticated and strategically significant category of threat. Major state-sponsored cyber programmes maintain persistent access to foreign critical infrastructure systems, often for purposes of intelligence collection and pre-positioning for potential disruptive operations. The United States, United Kingdom, and allied nations have publicly attributed CII-targeting operations to Russia (including the SolarWinds supply chain compromise, the Viasat attack, and the sustained campaign against Ukrainian infrastructure), China (including persistent access to US telecommunications and energy infrastructure), North Korea, and Iran. The objectives of state actors range from espionage through pre-positioning to active disruption and, in conflict scenarios, the creation of physical effects designed to degrade an adversary's military or civil capacity.

Criminal actors, though primarily motivated by financial gain rather than strategic disruption, have emerged as a significant CII threat through the deployment of ransomware against critical systems. The professionalisation of the ransomware-as-a-service model has dramatically lowered the barriers to entry for financially motivated attackers, enabling groups with limited technical sophistication to deploy highly capable malicious tools against critical targets. Ransomware attacks on healthcare systems, including the 2020 Universal Health Services attack in the United States and numerous attacks on National Health Service trusts in the United Kingdom, have directly endangered patient safety. The Cl0p ransomware campaign exploiting vulnerabilities in MOVEit Transfer software in 2023 affected hundreds of organisations across multiple critical sectors globally, demonstrating the cascading effects that can flow from attacks on widely deployed software used by CII operators.

3. LEGAL FRAMEWORKS FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

3.1 United States: Presidential Directives, Sector Regulation, and Emerging Mandates

The United States framework for CII protection has evolved through a series of presidential directives and executive orders, sector-specific regulation, and, more recently, legislation

imposing incident reporting and minimum security requirements on critical infrastructure operators. Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, issued in 2013, established the foundational architecture of the US approach, designating sixteen critical infrastructure sectors and assigning lead federal agencies (Sector Risk Management Agencies, or SRMAs) responsibility for coordinating security across each. The concurrent Executive Order 13636 on Improving Critical Infrastructure Cybersecurity directed the development of the NIST Cybersecurity Framework, which, while voluntary for private sector operators, has achieved wide adoption and quasi-regulatory status in some sectors.

The voluntary character of the NIST Framework reflects the broader US regulatory philosophy, which has historically favoured market-based and self-regulatory approaches over direct mandates in the private sector CII domain. The adequacy of this approach has been increasingly questioned in light of persistent incidents, and recent years have seen a significant shift toward mandatory requirements. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) mandates that covered critical infrastructure entities report substantial cyber incidents to CISA within 72 hours and ransomware payments within 24 hours — a significant expansion of mandatory incident reporting, though the implementing regulations defining 'covered entity' and 'substantial incident' remain under development. Executive Order 14028 on Improving the Nation's Cybersecurity, issued in May 2021 in the wake of the SolarWinds compromise and Colonial Pipeline attack, directed a series of security improvements across the federal government and imposed enhanced security requirements on IT service providers contracting with the federal government.

3.2 European Union: The NIS2 Directive and the Emerging Legislative Architecture

The European Union has developed a substantially more harmonised and prescriptive legal framework for CII protection than the United States, grounded in the NIS2 Directive adopted in December 2022 and requiring transposition by member states by October 2024. NIS2 substantially expands the scope of its predecessor, the NIS Directive of 2016, extending mandatory security and incident reporting obligations to a significantly larger population of 'essential' and 'important' entities across eleven sectors, including energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, and space.

NIS2 imposes a comprehensive set of risk management obligations on covered entities, including measures relating to incident handling, business continuity, supply chain security, network security, encryption, access control, and multi-factor authentication. Incident notification obligations are among the most demanding of any jurisdiction: covered entities must provide an early warning to national authorities within 24 hours of becoming aware of a significant incident, a detailed notification within 72 hours, and a final report within one month. The directive also imposes personal liability on management bodies for failures to comply, and requires member states to impose substantial administrative sanctions (up to €10 million or 2% of global annual turnover for essential entities).

3.3 Other Key Jurisdictions

The United Kingdom, following its departure from the European Union, has developed its CII protection framework primarily through the Network and Information Systems (NIS) Regulations 2018, which implemented the original EU NIS Directive. The UK government has indicated its intention to update these regulations to reflect developments in the threat landscape and lessons from NIS2, though the transposition of equivalent NIS2 provisions is not legally required following Brexit. The Telecommunications (Security) Act 2021 imposes heightened security obligations on telecommunications providers specifically, reflecting the strategic sensitivity of that sector.

China's Cybersecurity Law of 2016 and the subsequent Critical Information Infrastructure Security Protection Regulations of 2021 establish a comprehensive framework for CII designation and protection, imposing stringent localisation, security review, and incident reporting obligations on operators of critical information infrastructure as designated by competent authorities across relevant sectors. The framework reflects a distinctly statist approach, granting the government extensive supervisory and access powers over CII operators' systems and data.

3.4 International Legal Frameworks

At the international level, the legal framework for CII protection is significantly underdeveloped relative to the scale of the threat. There is no binding multilateral treaty specifically addressing the protection of critical information infrastructure from cyber attacks, nor any agreed international standards establishing minimum security requirements for CII operators at the global level. The Budapest Convention on Cybercrime, while providing a framework for international cooperation in cybercrime investigation and prosecution, does not impose substantive CII protection obligations and does not engage with the specific challenge of state-sponsored attacks on foreign CII.

The applicability of existing international law — including the law of state responsibility, the prohibition on the use of force, international humanitarian law, and countermeasures doctrine — to cyber operations against CII has been the subject of substantial scholarly and governmental analysis, most accessibly synthesised in the Tallinn Manual 2.0. The central conclusions of that analysis — that existing international law applies to cyber operations, that attacks on civilian critical infrastructure may constitute internationally wrongful acts or, in armed conflict contexts, violations of international humanitarian law — have achieved broad if not universal acceptance among states. However, the operationalisation of these principles faces profound challenges of attribution, evidentiary standard, and enforcement that render them of limited deterrent effect in practice.

4. STRUCTURAL DEFICIENCIES OF CURRENT LEGAL FRAMEWORKS

4.1 The Voluntary Framework Problem

The most fundamental deficiency of many existing CII protection frameworks — particularly in the United States and, to a lesser extent, other common law jurisdictions — is an excessive reliance on voluntary compliance mechanisms. The economic incentives

facing private sector CII operators do not reliably produce optimal security investment. Security investment reduces the probability of harm to the operator's own systems but also generates positive externalities for interconnected entities and for society at large whose value the investing entity cannot capture. Conversely, security failures by one CII operator can generate cascading harms for interconnected systems and for the public whose costs are not fully borne by the operator responsible. These externality dynamics produce systematic under-investment in security relative to the socially optimal level — a market failure that only mandatory minimum standards can reliably correct.

The historical record of voluntary frameworks is not encouraging. Despite the broad adoption of the NIST Cybersecurity Framework, major US critical infrastructure sectors have experienced persistent, significant cyber incidents that suggest baseline security standards remain inadequate in many organisations. The Government Accountability Office has repeatedly found that federal agencies responsible for overseeing CII sectors have not comprehensively assessed the cyber risks facing their sectors or ensured that operators have implemented adequate protections. The shift toward mandatory requirements under CIRCIA and various sector-specific mandates represents a belated recognition of the inadequacy of the voluntary model, but the transition remains incomplete.

4.2 The Coverage Gap Problem

Existing CII protection frameworks frequently contain significant coverage gaps that leave genuinely critical systems outside the protective ambit of legal obligations. These gaps arise from multiple sources: the failure to designate all critical sectors and entities, the exclusion of small and medium-sized enterprises that may operate critical systems, the inadequate treatment of supply chain and third-party service providers (including cloud providers, managed service providers, and industrial control system vendors), and the failure to keep pace with changes in infrastructure architecture that shift operational dependence to new categories of system.

The supply chain gap is particularly consequential. The most devastating recent CII incidents — the SolarWinds compromise, the Kaseya VSA attack, the MOVEit exploitation — involved adversaries targeting widely used IT management and service delivery software rather than directly attacking the CII operators themselves. Existing legal frameworks typically impose obligations on CII operators but do not comprehensively regulate the technology vendors and service providers whose products and services underpin those operators' systems. A framework that imposes rigorous security obligations on a power company while leaving the software vendor whose product controls the company's SCADA systems unregulated addresses only part of the security challenge.

4.3 The Incident Reporting and Information Sharing Deficit

Effective CII protection requires timely, comprehensive, and accurate information about incidents and threats — both to enable effective operational response and to provide the regulatory intelligence necessary for evidence-based policy development. Current incident reporting frameworks in many jurisdictions are inadequate on multiple dimensions. Where reporting is mandated, notification timeframes are frequently too long to enable effective government response; the thresholds triggering reporting obligations are often unclear or

set too high, resulting in significant under-reporting; and the information actually reported is frequently too vague or incomplete to be operationally useful.

The chilling effect of legal liability on incident disclosure represents a significant structural barrier to information sharing. Organisations that disclose cyber incidents face potential exposure to civil litigation, regulatory sanctions, reputational damage, and in some cases criminal liability. Without robust legal protections for good-faith incident disclosure — including liability safe harbours, confidentiality protections for shared information, and prohibition on the use of disclosed information as a basis for enforcement action — the incentives against disclosure will systematically override the public interest in comprehensive incident reporting.

4.4 The Liability Framework Incoherence

The liability frameworks applicable to CII protection are characterised by significant incoherence that distorts security incentives in ways that undermine the protective function of law. In many jurisdictions, the civil liability exposure facing a CII operator for a security incident falls on the operator regardless of whether the incident resulted from a failure to implement reasonable security measures or from a sophisticated, state-sponsored attack that no reasonable precautions could have prevented — a liability design that fails to distinguish outcomes the law should incentivise from those it cannot. Simultaneously, the technology vendors and service providers who supply the insecure products and services deployed in critical systems frequently face minimal civil liability for the downstream consequences of their security failures, as a result of contractual limitation of liability clauses and the absence of product liability frameworks applicable to software.

5. A NORMATIVE FRAMEWORK FOR LEGAL REFORM

5.1 Mandatory Baseline Security Standards

The foundational element of an effective legal framework for CII protection must be mandatory baseline security standards applicable to all operators of designated critical information infrastructure. These standards should be outcome-based rather than prescriptive, specifying the security outcomes that CII operators are required to achieve — resilience against defined threat scenarios, capacity for timely incident detection and response, ability to maintain or rapidly restore essential services following a significant incident — rather than the specific technical controls through which those outcomes must be achieved. Outcome-based regulation preserves operational flexibility, accommodates the diversity of CII operators' technical environments, and avoids the risk that prescriptive technical standards become obsolete as the threat landscape and underlying technology evolve.

Baseline standards should be developed through a structured process that draws upon the technical expertise of national cybersecurity agencies, the operational knowledge of CII operators and their representative organisations, and independent academic and civil society expertise. They should be subject to periodic mandatory review — at intervals of no greater than three years — and should be capable of rapid update through streamlined administrative processes where the threat landscape demands. Graduated standards that

impose more rigorous requirements on the most critical systems and those most frequently targeted by sophisticated adversaries represent a proportionate approach that concentrates compliance burdens where security benefits are greatest.

5.2 Comprehensive and Tiered Incident Reporting

An effective incident reporting framework for CII should be designed around three distinct objectives: enabling effective government operational response to ongoing incidents; providing regulatory intelligence for the development and enforcement of security standards; and, where appropriate, generating public accountability for serious security failures. These objectives are not always aligned, and a well-designed framework must address each explicitly. For operational response purposes, immediate notification to the national cybersecurity agency of significant incidents — within a maximum of 24 hours of initial detection — is essential to enable government assistance to affected operators and to provide early warning of attacks that may affect multiple organisations.

Reporting obligations should be accompanied by robust legal protections for disclosed information, including strict confidentiality obligations binding on receiving agencies, prohibition on the use of disclosed information as the primary basis for enforcement action against the disclosing entity, and explicit liability safe harbours for good-faith incident disclosure. These protections are not concessions to be reluctantly granted but essential preconditions for a reporting regime that generates comprehensive rather than selective disclosure. The experience of aviation safety reporting systems — which achieve high rates of disclosure of safety incidents through robust non-punitive reporting cultures and strong legal protections for disclosures — provides an instructive model for the design of CII incident reporting frameworks.

5.3 Supply Chain and Third-Party Risk Management

Addressing the supply chain vulnerability that has produced some of the most damaging recent CII incidents requires a two-pronged legal approach. First, CII operators should be required, as part of their baseline security obligations, to implement comprehensive third-party and supply chain risk management programmes — assessing the security of technology vendors and service providers whose products or services could materially affect the security of critical systems, imposing contractual security requirements on those providers, and maintaining visibility into the software components deployed in critical systems through software bills of materials (SBOMs). Second, and more ambitiously, legal frameworks should impose direct security obligations on technology vendors and managed service providers whose products or services are widely deployed in critical infrastructure contexts.

The second prong represents a more fundamental departure from existing regulatory models and faces significant political resistance from the technology industry. Nevertheless, the case for imposing minimum security obligations on critical technology vendors is compelling: it addresses the liability gap identified in Part Four, creates incentives for security investment at the point in the supply chain where it is most technically efficient, and prevents vendors from externalising the costs of their security failures onto CII operators and the public. The EU's Cyber Resilience Act represents the most ambitious attempt yet to implement this approach, and its entry into application will

provide valuable evidence regarding its practical effects on both security outcomes and market dynamics.

5.4 Public-Private Operational Partnerships

Law can and should provide the structural framework for operational partnerships between government and private CII operators that go beyond the compliance relationship implicit in a regulatory model. The most valuable contribution that government can make to CII security is often the sharing of intelligence regarding threats that private operators cannot themselves identify — including attribution of attacks to specific nation-state groups, advance warning of active campaigns, and technical indicators of compromise derived from classified intelligence. Legislative frameworks should establish clear mechanisms for the declassification and secure sharing of actionable threat intelligence with CII operators, including the establishment of security clearance frameworks that permit private sector security personnel to receive and act upon classified threat information.

5.5 International Legal Cooperation and Deterrence

The international legal framework for CII protection requires development on two distinct tracks. The first is the continued elaboration and operationalisation of the norms governing responsible state behaviour in cyberspace, with particular attention to the norm against attacks on critical infrastructure in peacetime. The 2015 UN GGE consensus report's articulation of this norm as a non-binding expectation of responsible state behaviour requires translation into more specific and operationalisable commitments — ideally through a binding multilateral instrument that establishes clear prohibitions and accountability mechanisms, though the prospects for such an instrument in the near term remain limited given the geopolitical divisions between major cyber powers.

A more immediately achievable objective is the strengthening of international mechanisms for mutual legal assistance in CII incident investigation and attribution. The Budapest Convention's framework for expedited preservation and production of electronic evidence, enhanced by the Second Additional Protocol, provides a foundation that should be broadened through wider ratification and updated to address the specific evidentiary needs of CII incident investigations. Bilateral agreements for the sharing of attribution intelligence and the coordination of diplomatic and economic countermeasures against state sponsors of CII attacks represent a further avenue for strengthening the international deterrence framework.

The development of effective deterrence against state-sponsored CII attacks — one of the most significant and persistent challenges in this field — ultimately requires a credible and proportionate response framework. Legal frameworks should clearly authorise appropriate countermeasures in response to internationally wrongful cyber attacks on CII, provide for the imposition of targeted sanctions against state and non-state actors responsible for significant CII attacks, and establish mechanisms for attributing attacks publicly and with sufficient evidentiary basis to withstand legal and political challenge. The Cyber Diplomacy Toolbox developed within the European Union, which provides for a graduated framework of diplomatic and economic measures in response to malicious cyber activities, represents a valuable model for institutionalising the countermeasure framework in law.

6. CONCLUSION

The protection of critical information infrastructure from cyber attacks is among the most urgent and consequential challenges confronting legal systems in the digital age. The stakes — the uninterrupted delivery of essential services upon which human welfare, public safety, economic stability, and national security depend — could scarcely be higher. Yet the legal frameworks currently charged with meeting this challenge are, in most jurisdictions and at the international level, substantially inadequate to the threat.

The structural deficiencies identified in this article — the over-reliance on voluntary frameworks, the coverage gaps that exclude genuinely critical systems and their supply chains, the incident reporting and information sharing deficits, and the incoherence of liability frameworks that fail to align legal consequences with security incentives — are not superficial imperfections amenable to marginal adjustment. They reflect deeper tensions in the organisation of CII protection law: between the imperatives of security and the constraints of regulatory legitimacy and market freedom; between the need for rapid operational response and the deliberative processes of lawmaking; between the national architecture of legal authority and the transnational character of the threat; and between the urgency of immediate protective action and the fundamental importance of preserving the civil liberties that security measures must not inadvertently erode.

REFERENCES

Anderson, R., 'Security Engineering: A Guide to Building Dependable Distributed Systems' (3rd ed., John Wiley & Sons, 2020).

Australia, Security of Critical Infrastructure Act 2018 (Cth), as amended by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth).

Budapest Convention on Cybercrime (Council of Europe), ETS No. 185, opened for signature 23 November 2001, entered into force 1 July 2004.

China, Cybersecurity Law of the People's Republic of China (2016).

China, Regulations on the Security Protection of Critical Information Infrastructure (2021).

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103, 136 Stat. 49.

Cybersecurity and Infrastructure Security Agency (CISA), 'Cross-Sector Cybersecurity Performance Goals' (CISA, 2022).

Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022.

Executive Order 14028, 'Improving the Nation's Cybersecurity' (12 May 2021), 86 Fed. Reg. 26633.

European Union Agency for Cybersecurity (ENISA), 'Threat Landscape for Critical Infrastructure 2023' (ENISA, 2023).

Fidler, D.P., 'Cyberspace, Terrorism and International Law' (2016) 21(3) Journal of Conflict & Security Law 475.

Government Accountability Office (GAO), 'Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid', GAO-21-81 (2021).

Kshetri, N., 'The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives' (Springer, 2010).

Lewis, J.A., 'Significant Cyber Incidents since 2006' (Center for Strategic and International Studies, updated 2024).

Markopoulou, D., Papakonstantinou, V. and de Hert, P., 'The New EU Cybersecurity Framework: The NIS2 Directive, ENISA's Role and the European Cyber Defence Policy' (2019) 35(6) Computer Law & Security Review 105336.

National Institute of Standards and Technology, 'Cybersecurity Framework 2.0' (NIST, 2024).

Network and Information Systems (NIS) Regulations 2018 (UK), SI 2018/506.

Network and Information Security 2 Directive (NIS2), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

Telecommunications (Security) Act 2021 (UK), c. 31.

United Nations Group of Governmental Experts, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', A/76/135 (14 July 2021).

United States, 'National Cybersecurity Strategy' (The White House, March 2023).

Zetter, K., 'Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon' (Crown Publishers, 2014).

Zetter, K., 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (Wired, 3 March 2016).