Private Sovereigns at War: Corporate Control of Communications, Compute, Targeting and the New Economic Arsenal

Supplementary Paper 4

Christopher I. V. Farmer

Publication edition, August 2026

Contents

Abstract

The State has never possessed every instrument by which war is conducted. Merchants financed fleets, chartered companies governed territories, privateers attacked commerce and manufacturers supplied arms. Public law nevertheless assumed that the decision which exposed a polity to war belonged, in the final account, to public authority. That assumption now fails in a new way. An individual may possess a satellite network, a corporation may control communications or cloud infrastructure upon which military action depends, a private military and security company may combine intelligence and force, and a commercial intrusion company may sell a capability formerly confined to a security service. Their power is neither merely wealth nor merely influence. It is the practical capacity to decide whether another actor may see, communicate, target, move or survive.

This paper calls such actors private sovereigns when three conditions coincide: they control strategically indispensable capacity; they exercise material discretion over its wartime or coercive use; and no public authority capable of bearing the external consequence has authorised the particular decision in advance. The term does not grant them sovereignty in law. It identifies a constitutional defect: power with effects equivalent to public decision, exercised by one who neither represents those exposed to retaliation nor submits to the legal machinery by which force is ordinarily authorised and reviewed.

Starlink's activation in Ukraine supplies the clearest case. Service was announced on 26 February 2022, before the later public contracts and reimbursement arrangements which regularised part of the relationship. The result assisted a State lawfully defending itself, but beneficence does not answer authority. Purchasers of unrelated products did not consent to foreign belligerent exposure; shareholders did not elect a foreign minister; and an owner's bank account did not supply a sovereign right. The same rule must govern a Chinese, Russian, British or American controller when the political sympathies are reversed.

The danger is wider than satellites. State-linked contractor markets, private spyware, PMSCs, platform intervention, corporate denial-of-service capability and autonomous systems permit strategic acts to be commissioned, improvised or withheld beyond the effective reach of inherited mercenary, sanctions, company and cybercrime law. Dark Caracal and Lebanese Cedar are treated as separate technical reports: the former was traced by Lookout and the Electronic Frontier Foundation to a building of the Lebanese General Security Directorate; the latter was reported by ClearSky as a distinct campaign using known server vulnerabilities and linked by its researchers to Hezbollah. Neither report is converted into a judicial finding.

The paper rejects the proposition that a private attacker loses human rights or becomes an "object of war" by leaving the social contract. Rights remain. In armed conflict a civilian may lose protection from direct attack only for such time as he directly participates in hostilities, or, on the better organised-group analysis, whilst exercising a continuous combat function; an object must satisfy the definition of a military objective. Outside armed conflict, lethal force is governed by the law-enforcement and human-rights framework save where the independent rules upon self-defence are engaged. Direct measures must nevertheless remain available. When a proved private operation presents an actual or imminent armed attack, or a node makes an effective contribution to military action and its neutralisation offers a definite military advantage, the fact that its owner is poor, deniable or incorporated does not immunise it.

The statutory answer is control rather than prohibition: registration of strategic private capacity; public authorisation for intervention in armed conflict; a duty to maintain service and decision manifests; mandatory notification of coercive foreign requests; licensing of high-risk cyber and military services; personal orders against controllers; rapid preservation, freezing and infrastructure restraint; and a

response ladder which includes sanctions, criminal process, civil restraint, cyber defence and, where international law independently permits, force. Proportionality should assess actual harm and maximum reasonably credible foreseeable harm, including replication and deterrent consequence. Punishment alone cannot create necessity under article 51, but a legal order which cannot act until cheap private warfare has killed at State scale has mistaken lateness for restraint.

Keywords: private strategic power; commercial space; satellite communications; private military and security companies; cyber operations; corporate control; international humanitarian law; emergency powers; deterrence.

Table of Authorities

Cases

Legislation

Treaties and International Instruments

Standards, Government and Technical Materials

AI Security Institute, ‘Measuring AI Agents’ Progress on Multi-Step Cyber Attack Scenarios’ (16 March 2026) https://www.aisi.gov.uk/research/measuring-ai-agents-progress-on-multi-step-cyber-attack-scenarios accessed 5 August 2026

Arms Trade Treaty (adopted 2 April 2013, entered into force 24 December 2014) 3013 UNTS 269

Attorney General’s Office, ‘Attorney General’s Speech at the International Institute for Strategic Studies: The Modern Law of Self-Defence’ (11 January 2017)

Australian Government, *Australia’s Position on How International Law Applies to State Conduct in Cyberspace* (2020)

Cabinet Office, ‘Critical National Infrastructure’ https://www.gov.uk/government/publications/national-protective-security-authority-annual-review-2024-to-2025/critical-national-infrastructure accessed 5 August 2026

Cabinet Office, *National Security and Investment Act 2021: Statement for the Purposes of Section 3* (2025)

Cabinet Office, *Summary of the 2025 Sector Security and Resilience Plans* (2026)

Cabinet Office, *The Cabinet Manual* (1st edn, October 2011) paras 5.36–5.38

Comptroller and Auditor General, *Investigation: WannaCry Cyber Attack and the NHS* (HC 2017–19, 414)

Cybersecurity and Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals* (updated 2023)

Cybersecurity and Infrastructure Security Agency, *MAR-17-352-01 HatMan—Safety System Targeted Malware* (12 April 2018)

Department for Digital, Culture, Media & Sport, *Telecommunications Security Code of Practice* (December 2022)

Department for Science, Innovation and Technology, *AI Cyber Security Code of Practice* (31 January 2025)

Department for Science, Innovation and Technology, ‘Summary of the Cyber Security and Resilience Bill’ (30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill accessed 5 August 2026

Department of Health and Social Care, ‘Synnovis Cyber Attack’ (Written Statement HCWS1046, 30 June 2025)

Federal Government of Germany, *On the Application of International Law in Cyberspace* (March 2021)

Financial Reporting Council, *UK Corporate Governance Code 2024* (22 January 2024) https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/ accessed 5 August 2026

Foreign, Commonwealth & Development Office and National Cyber Security Centre, ‘UK and France Seek Views on Commercial Cyber Intrusion Industry Practices’ (20 November 2025) https://www.gov.uk/government/news/uk-and-france-seek-views-on-commercial-cyber-intrusion-industry-practices accessed 5 August 2026

Foreign, Commonwealth & Development Office, *Application of International Law to States’ Conduct in Cyberspace: UK Statement* (3 June 2021)

Foreign, Commonwealth & Development Office, *Pall Mall Process Consultation Summary Report* (January 2025) https://assets.publishing.service.gov.uk/media/677e486ed721a08c00665555/Pall-Mall-Process-Consultation-Summary-Report.pdf accessed 31 July 2026

Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (4 April 2025) https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states accessed 5 August 2026

Foreign, Commonwealth & Development Office, ‘The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities’ (6 February 2024) https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities accessed 5 August 2026

Foreign, Commonwealth & Development Office, 'Voluntary Report on the Implementation of International Humanitarian Law at Domestic Level: Second Edition' (23 October 2024) paras 172–85 https://www.gov.uk/government/publications/implementation-of-international-humanitarian-law-at-domestic-level-2024-voluntary-report/voluntary-report-on-the-implementation-of-international-humanitarian-law-at-domestic-level-second-edition accessed 31 July 2026

France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019)

Government of Canada, *International Law Applicable in Cyberspace* (22 April 2022)

Government of the Netherlands, 'Letter to the Parliament on the International Legal Order in Cyberspace' (5 July 2019)

HM Government, 'Syria Action—UK Government Legal Position' (14 April 2018) https://www.gov.uk/government/publications/syria-action-uk-government-legal-position/syria-action-uk-government-legal-position accessed 5 August 2026

House of Commons Public Administration Select Committee, *Taming the Prerogative: Strengthening Ministerial Accountability to Parliament* (HC 422, 2003–04)

House of Lords Constitution Committee, *Waging War: Parliament's Role and Responsibility* (HL 236-I, 2005–06)

Human Rights Committee, 'General Comment No 36: Article 6—Right to Life' (3 September 2019) UN Doc CCPR/C/GC/36, paras 12–14

Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (6 April 2018) UN Doc A/HRC/38/35

ICRC, Australian Red Cross and French Red Cross, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law* (2024)

ICRC, *Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises under International Humanitarian Law* (2006)

ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Position Paper, November 2019)

ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Nils Melzer ed, ICRC 2009) 46–64

International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10, arts 4, 5, 8, 11 and 16

International Law Commission, 'Draft Conclusions on Identification of Customary International Law, with Commentaries' (2018) UN Doc A/73/10

Iraq Inquiry, *The Report of the Iraq Inquiry: Executive Summary* (HC 264, 2016–17)

Iraq Inquiry, *The Report of the Iraq Inquiry*, vol V (HC 264, 2016–17)

ISO/IEC 19941:2017, *Information Technology—Cloud Computing—Interoperability and Portability*

Ministry of Defence, *Defence Space Strategy: Operationalising the Space Domain* (February 2022)

Ministry of Defence, *Joint Doctrine Publication 0-40: UK Space Power* (February 2023)

National Cyber Security Centre and others, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure' (7 February 2024) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a accessed 31 July 2026

National Cyber Security Centre, *Annual Review 2025* (14 October 2025)

National Cyber Security Centre, 'Cyber Assessment Framework' https://www.ncsc.gov.uk/collection/caf accessed 5 August 2026

National Cyber Security Centre, 'The Cloud Security Principles' https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles accessed 5 August 2026

National Cyber Security Centre, *The Near-term Impact of AI on the Cyber Threat* (24 January 2024) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat accessed 5 August 2026

National Institute of Standards and Technology, *NIST Cloud Computing Forensic Reference Architecture* (NIST SP 800-201, July 2024)

National Institute of Standards and Technology, *NIST Cloud Computing Forensic Science Challenges* (NISTIR 8006, June 2014)

New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (1 December 2020)

NHS England, 'Synnovis Cyber Incident' https://www.england.nhs.uk/synnovis-cyber-incident/ accessed 5 August 2026

OECD, *Guidelines for Multinational Enterprises on Responsible Business Conduct* (2023)

Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights* (HR/PUB/11/04, 2011)

Office of the United Nations High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide* (HR/PUB/12/02, 2012)

Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (4 August 2022) UN Doc A/HRC/51/17

Regulation (EU) 2022/2065 on a Single Market for Digital Services [2022] OJ L277/1

Russian Federation, Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, UN Doc S/2022/154

Swiss Federal Department of Foreign Affairs and ICRC, *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (17 September 2008)

UNGA, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States* (13 July 2021) UN Doc A/76/136

UNGA Res ES-11/1 (2 March 2022) UN Doc A/RES/ES-11/1

United States, Letter dated 23 September 2014 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, UN Doc S/2014/695

UNSC Res 1540 (28 April 2004) UN Doc S/RES/1540

UNSC Res 1973 (17 March 2011) UN Doc S/RES/1973

US Department of Defense, *Commercial Space Integration Strategy* (2 April 2024)

US Department of Defense, 'Pentagon Press Secretary Air Force Brig Gen Pat Ryder Holds a Press Briefing' (22 August 2023) https://www.defense.gov/News/Transcripts/Transcript/Article/3501484/pentagon-press-secretary-air-force-brig-gen-pat-ryder-holds-a-press-briefing/ accessed 31 July 2026

US Department of Defense, 'The Urgency to Innovate' (28 August 2023) https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/ accessed 5 August 2026

US Department of Health and Human Services, 'Cyberattack on Change Healthcare' (2024)

US Department of Justice, 'Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns' (5 March 2025) https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global accessed 31 July 2026

US Government Accountability Office, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support* (GAO-24-106221, 30 January 2024)

US Government Accountability Office, *DOD Satellite Communications: Additional Planning Could Help DOD Acquire Commercial Satellite Communications and Develop Interoperable Terminals* (GAO-25-107034, 4 March 2025)

USAID Office of Inspector General, *Ukraine Response: USAID Did Not Fully Mitigate the Risk of Misuse of the Starlink Satellite Terminals It Delivered to Ukraine* (E-121-25-003-M, 11 August 2025) 2–5

Corporate, Technical and Contemporary Materials

Anthropic, 'Cyber Toolkits for LLMs' (13 June 2025) https://www.anthropic.com/research/cyber-toolkits accessed 5 August 2026

ClearSky Cyber Security, *"Lebanese Cedar" APT* (28 January 2021) 3–7 https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf accessed 31 July 2026

Cloud Security Alliance, *Cloud Controls Matrix v4.0.12* (2024)

Electronic Frontier Foundation, 'EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World' (18 January 2018) https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around accessed 31 July 2026

Elon Musk (@elonmusk), 'Starlink service is now active in Ukraine. More terminals en route' (X, 26 February 2022, 10.33 pm) https://x.com/elonmusk/status/1497701484003213317 accessed 31 July 2026

Google Threat Intelligence Group, *Adversarial Misuse of Generative AI* (January 2025) https://cloud.google.com/resources/content/adversarial-misuse-of-generative-ai accessed 5 August 2026

Hyunjoo Jin, 'Musk Says Starlink Active in Ukraine as Russian Invasion Disrupts Internet' *Reuters* (26 February 2022)

ICEYE, 'ICEYE Signs Contract to Provide Government of Ukraine with Access to Its SAR Satellite Constellation' (18 August 2022) https://www.iceye.com/newsroom/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation accessed 31 July 2026

Jim Louderback, 'Inside the Attack that Crippled Revision3' (Revision3, 29 May 2008), archived copy cited in David Kravets, 'MediaDefender Accidentally DDoSes Revision3' *Wired* (30 May 2008) https://www.wired.com/2008/05/mediadefender-d/ accessed 31 July 2026

Joey Roulette and Marisa Taylor, 'Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia' *Reuters* (25 July 2025)

Lookout and Electronic Frontier Foundation, *Dark Caracal: Cyber-Espionage at a Global Scale* (18 January 2018) 3–6, 35–36 https://www.lookout.com/documents/reports/lookout-dark-caracal-20180118-us.pdf accessed 31 July 2026

Mandiant, 'TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping' (10 April 2019) https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections/ accessed 5 August 2026

MITRE ATT&CK, 'Volatile Cedar, G0123' https://attack.mitre.org/groups/G0123/ accessed 31 July 2026

Verizon, *2025 Data Breach Investigations Report* (2025)

Victoria Kim, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' *The New York Times* (8 September 2023)

1. The Return of Private Strategic Power

The question is not whether private persons possess power. Property has always conferred the ability to employ, refuse, exclude and influence. Nor is the question whether companies participate in national security. Shipbuilders, banks, telecommunications operators and manufacturers have long done so. The present problem is that a small number of private actors can make an operational decision whose immediate foreign consequence resembles that of a State, whilst the legal system continues to classify the act as service provision, contract, ownership or ordinary commerce.

A satellite controller may illuminate a battlefield. A cloud provider may terminate an account upon which a ministry depends. A platform may rank, suppress or disclose information capable of altering public order. A private intelligence company may identify targets. A PMSC may combine training, logistics, surveillance, offensive cyber capability and armed protection. A wealthy individual may fund the lot without possessing any territorial, representative or treaty relation to those exposed.

The older law divided public from private by status. A soldier acted for the State; a merchant traded. Modern strategic infrastructure collapses the division by function. The merchant's switch may decide whether the soldier can communicate, and the owner may exercise that switch personally. To call the

act commercial because the asset sits upon a balance sheet is to confuse the source of title with the nature of the decision.

The law also divides peace from war more readily than contemporary operations permit. A vulnerability is acquired in peace, access maintained below public notice, data sold through a contractor, targeting enabled after hostilities begin and the decisive service withdrawn during an operation. No single stage appears to declare war. Together they allocate military capacity.

The change is not simply privatisation. A contractor who performs a public task under a detailed government command remains within a recognisable delegation, although accountability may still fail. The newer problem is infrastructural rule-making: the provider designs the environment, determines the available choices and can alter the conditions under which public authority acts. Contract, code and architecture become forms of governance before any minister gives an order.[1]

This paper uses “private sovereign” as an analytic description. A private actor is not a State, does not acquire a territory, cannot create an international right to use force and does not become immune. The word identifies a power which public constitutional thought reserved to sovereignty: making a decision which materially exposes others to foreign coercion or decides the availability of strategic capacity.

Three cumulative conditions should be present. First, **indispensable or substitutability-limited capacity**: the asset or service has no reasonably timely substitute for the affected State, force or population. Secondly, **material operational discretion**: the private actor may authorise, refuse, condition or alter the relevant use rather than merely obey a public order. Thirdly, **unabsorbed external consequence**: no competent State has authorised the particular strategic decision in a manner which accepts public responsibility and supplies review.

Scale is relevant but not conclusive. A modest hacker with access to one water treatment controller may possess more strategic power for an hour than a global retailer. Conversely, a wealthy owner who donates food exercises influence without deciding force or coercive capacity. The category concerns control at the point of consequence.

The definition is deliberately actor-neutral. An admired billionaire assisting a victim State is within it; so is a contractor paid by an authoritarian government; so may be a company which refuses service in obedience to human rights. The legal issue is not whether the author approves the outcome. If Western legal order treats beneficent private intervention as an owner’s liberty, it supplies the reciprocal argument when an Eastern controller intervenes against Western forces.

1.1 The Constitutional Defect

Thomas Hobbes did not imagine satellite constellations, but he understood that a multitude exposed to private judgements of danger cannot enjoy a common peace. The social covenant creates a public person capable of acting for the whole; the sword which enforces it is not simply another possession.[2] One need not accept Hobbes’s entire sovereign to recognise the constitutional proposition: a decision exposing the community to organised violence ordinarily demands public authority capable of answering for the consequence.

Private strategic intervention avoids each discipline attached to that authority. The owner need not disclose intelligence, test legality, weigh civilian harm, consult allies, preserve records, answer Parliament or accept that retaliation will fall upon citizens who did not choose him. He may be correct

[1] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019); Frank Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Belknap Press 2020); David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019).

[2] Thomas Hobbes, *Leviathan* (Richard Tuck ed, CUP 1996) chs XVII–XVIII.

more quickly than government. He may also be wrong more quickly, and the foreign State receives no assurance that his view is private when the asset, licence and home State are inseparable in practice.

Company law supplies governance for the company, not democratic authority for war. Directors owe duties to the company, including the duty under section 172 of the Companies Act 2006 to promote its success for the benefit of members as a whole whilst having regard to listed interests.[3] Even a conscientious decision under that section does not authorise the director to allocate a nation's belligerent exposure. Shareholder voting is not the franchise of the persons liable to suffer retaliation.

Contract does no better. A customer may consent to terms governing service. The purchaser of a motor car does not authorise the manufacturer's controlling shareholder to supply targeting communications abroad. The idea that every Tesla purchaser tacitly accepted every strategic decision made possible by the resulting wealth is untenable in private law and more alarming in public theory. The very separation by which a corporation protects investors from ordinary liabilities makes attribution of foreign military consequence to consumers perverse.

This is not a claim that consumer money is morally pure until taxed. Economic life inevitably supports public and private conduct. It is a claim about decision. The one who controls strategic intervention should not invoke millions of remote purchases as a mandate, nor should a retaliating State treat purchasers as participants. Risk has been socialised without consent whilst control remains concentrated.

The defect persists where the decision is laudable. Emergency private action may save a population before procurement can move. Law should create a rapid authorisation and safe-harbour process rather than require passivity. What it cannot do is make the absence of process the source of legitimacy.

1.2 Historical Comparisons and Their Limit

Privateers possessed letters of marque; chartered companies received public charters; merchants financed belligerents; neutral trade was governed by prize and neutrality law. The historical record shows that private economic capacity can conduct war. It also shows repeated attempts to bring the capacity within public commission, responsibility and adjudication.

The comparison should not be romanticised. Public authorisation did not prevent abuse, and chartered companies sometimes exercised appalling governmental violence. The point is narrower: legal order recognised that commerce could cross into public violence and created status, licence and consequence. Present law too often insists that a satellite or algorithm remains an ordinary service even at the instant it becomes operationally decisive.

Nor can letters of marque simply be revived for cyber contractors. Attribution is uncertain, effects cross civilian infrastructure, tools proliferate and the distinction between seizure and sabotage is not carried over from prize. A modern licence must define objective, target class, technical constraint, record, human control, jurisdiction and termination. The historical lesson is control, not nostalgia.[4]

1.3 From Delegated Violence to Proprietary Infrastructure

The early modern privateer, chartered company and military entrepreneur did not operate in a legal vacuum. Their authority was imperfect, frequently abused and sometimes little more than an official indulgence; it was nevertheless made visible by commission, charter, prize jurisdiction, contract or

[3] Companies Act 2006, s 172.

[4] Janice E Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe* (Princeton University Press 1994); Philip J Stern, *The Company-State: Corporate Sovereignty and the Early Modern Foundations of the British Empire in India* (OUP 2011); *The Zamora* [1916] 2 AC 77 (PC); Declaration Respecting Maritime Law (signed 16 April 1856) 115 CTS 1.

allegiance. The East India Company could exercise public functions because the Crown and Parliament had conferred and later curtailed them. A privateer brought captured property before a prize court because private appetite alone could not transfer title. Neutral merchants might profit from war, but prize law classified the vessel, cargo, voyage and service by rules which exposed the public consequence of private trade. The nineteenth-century movement against privateering did not abolish private contribution to war. It sought to abolish one form in which a private person could decide whom to attack for profit.

Present infrastructure reverses the old problem. The privateer received public authority to employ a privately owned ship. A satellite, cloud region or model provider may now possess privately constituted authority over an asset upon which a public force depends, and may exercise it without an instrument resembling a commission. The State may license launch, allocate spectrum, purchase service, protect intellectual property and subsidise research whilst leaving the decisive wartime choice to contract or owner preference. Public law is present around the asset but absent at the switch.

Nor is the difficulty confined to an eccentric founder. A professionally governed corporation can produce the same defect through ordinary committees. A risk office may terminate service in one territory; a policy team may classify a belligerent; a security unit may permit a government account to conduct exceptional queries; a procurement team may select which State receives scarce capacity. No one employee claims to make foreign policy, yet the combined decision allocates visibility, communications or force. The constitutional question therefore survives the removal of personality from the facts.

The word “sovereign” must be kept within that functional boundary. Market concentration, lobbying power and great wealth may be politically objectionable without amounting to private sovereignty as this paper employs it. The category begins where control of an asset allows its holder, within the time available, to confer, withhold or redirect a strategic function which public authority cannot replace, and where the foreign consequence has not been absorbed through public authorisation. This confines the doctrine to a small class of decisions whilst preventing the law from overlooking a small operator who temporarily controls a uniquely dangerous system.

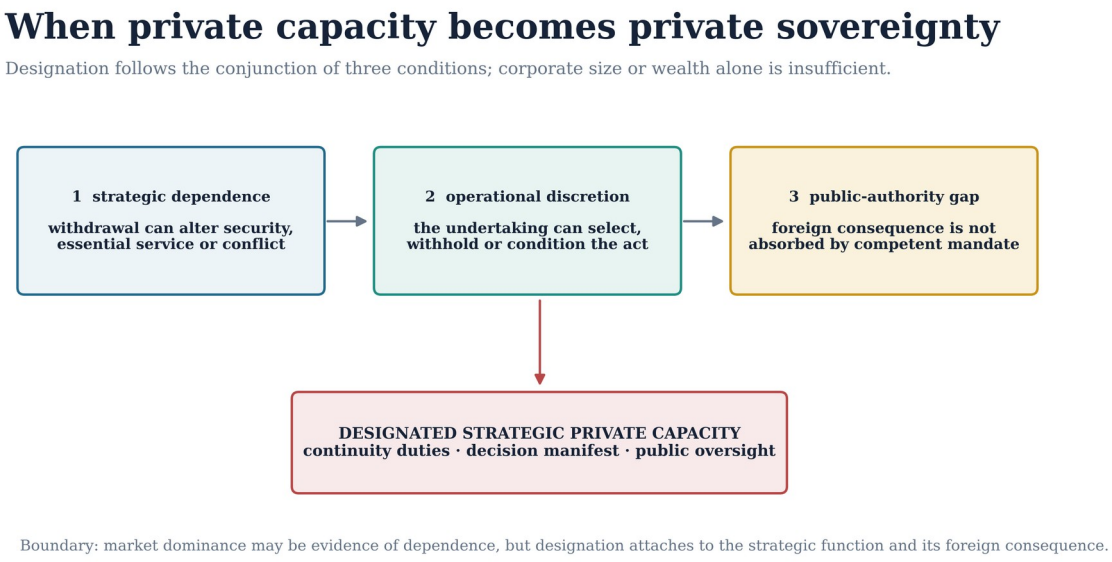

Figure 1. The private-sovereign test requires strategic dependence, operational discretion and a foreign consequence not absorbed by competent public authority.

1.4 Five Distinctions upon Which the Argument Depends

First, ownership is not operation. The shareholder may own the company whilst an engineer holds the credential, a ministry holds the contract and a foreign subsidiary controls the region. Liability and orders should follow the legally relevant relation rather than the most famous name.

Secondly, capacity is not effect. A company may possess a constellation capable of enabling targeting yet provide only domestic broadband; a model may be capable of intrusion yet remain within a laboratory. Registration may properly attach to latent strategic capacity, whilst criminal or international responsibility requires the conduct and mental element of the applicable rule.

Thirdly, assistance is not authorship. A provider may supply a general service used by a belligerent without selecting any target. Tailored intelligence, an operationally timed coverage alteration and direct integration into a fire-control chain stand differently. The law requires graduated duties because the factual relation is graduated.

Fourthly, public authorisation is not immunity. A ministerial direction may answer the constitutional question—who accepted the external consequence—whilst leaving international legality, civilian protection, contractual liability and individual criminal responsibility to their own rules. The State cannot license what international law prohibits, and the board cannot wash away knowledge by pointing to a public customer.

Fifthly, public absence is not moral wrong. Emergency private action may be the only means of preserving life. The defect lies in leaving the action indefinitely upon private title, not in permitting a brief rescue. A sound statute therefore combines a narrow emergency safe harbour with rapid assumption or rejection by government, contemporaneous evidence and later review. It neither forbids courage nor converts courage into a personal prerogative.[5]

2. Starlink and the Owner Who Chose

On 26 February 2022 Elon Musk announced that Starlink service was active in Ukraine and that further terminals were en route.[6] The activation followed a public request from Ukraine's vice prime minister. Whatever private communications also occurred, the public chronology places the operational announcement at the beginning of the invasion and before the later United States procurement and reimbursement arrangements.

The United States Agency for International Development's Inspector General reported that USAID delivered 5,175 terminals: 1,508 procured by USAID and 3,667 donated by SpaceX, together with associated service arrangements.[7] The Department of Defense later contracted for Starlink services.[8]

---

[5] Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights* (HR/PUB/11/04, 2011); OECD, *Guidelines for Multinational Enterprises on Responsible Business Conduct* (2023); Financial Reporting Council, *UK Corporate Governance Code 2024* (22 January 2024) https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/ accessed 5 August 2026; ICRC, Australian Red Cross and French Red Cross, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law* (2024).

[6] Elon Musk (@elonmusk), 'Starlink service is now active in Ukraine. More terminals en route' (X, 26 February 2022, 10.33 pm) https://x.com/elonmusk/status/1497701484003213317 accessed 31 July 2026; Hyunjoo Jin, 'Musk Says Starlink Active in Ukraine as Russian Invasion Disrupts Internet' *Reuters* (26 February 2022).

[7] USAID Office of Inspector General, *Ukraine Response: USAID Did Not Fully Mitigate the Risk of Misuse of the Starlink Satellite Terminals It Delivered to Ukraine* (E-121-25-003-M, 11 August 2025) 2–5. The report's summary gives 3,667 donated terminals—one passage appears as 3,677—but 1,508 plus 3,667 reconciles to the stated total of 5,175.

[8] US Department of Defense, 'Pentagon Press Secretary Air Force Brig Gen Pat Ryder Holds a Press Briefing' (22 August 2023) https://www.defense.gov/News/Transcripts/Transcript/Article/3501484/pentagon-press-secretary-air-force-brig-gen-pat-ryder-holds-a-press-briefing/ accessed 31 July 2026.

These public arrangements regularised and funded parts of the capability. They do not retrospectively convert the owner's initial decision into a prior State authorisation.

The service had civilian and military value. It maintained communications amid attack upon terrestrial infrastructure and supported Ukrainian defence. Later controversy concerning coverage and a proposed operation near Crimea demonstrated the reverse aspect of private control: the same person whose decision supplied capability could constrain where it was available.[9] Public reporting concerning exact orders and technical configuration has varied; the safe proposition is not that one biography proves every operational fact, but that a private controller possessed and exercised consequential discretion over service in an armed conflict.

Ukraine's right of self-defence under article 51 and its ability to request assistance answer whether assisting States may lawfully help; they do not answer who within an assisting society may make that strategic choice. Ukraine's non-membership of NATO meant article 5 did not oblige allies to defend it, but no defence treaty was necessary for requested collective self-defence. The absence of a duty is not the absence of a right.[10]

Neutrality is more difficult. Classical neutrality law addresses duties of neutral States and distinguishes private conduct in particular respects. The law has not supplied a settled, comprehensive classification for indispensable privately controlled space communications used by a belligerent. The Outer Space Treaty requires activities to be conducted in accordance with international law and places international responsibility upon States for national activities in outer space, including non-governmental entities, which require authorisation and continuing supervision.[11] That provision is more directly relevant to public control than the assertion that ownership is enough.

The United States' authorisation of launch and operation is not necessarily authorisation of each wartime service decision. Yet article VI of the Outer Space Treaty denies the simple proposition that the activity is wholly private. It offers a regulatory hinge: licensing may require notification, continuity planning, conflict review and emergency public direction where a constellation becomes strategically indispensable.

2.1 Beneficence and Reciprocity

The moral case for assisting Ukraine is powerful. Russian forces invaded; Ukraine requested help; communications helped it resist. The legal design problem begins after that statement, not against it.

Suppose a Chinese proprietor supplies resilient communications, targeting imagery or robotics to Iran during hostilities with a Western State. Suppose a Russian cloud owner enables a non-State group to locate British ships. Suppose a platform proprietor withdraws emergency communication from a population because he disagrees with its government. If the Western answer is that private property allowed Musk to choose in Ukraine, the same answer is available to each.

---

[9] Victoria Kim, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' *The New York Times* (8 September 2023); Walter Isaacson, *Elon Musk* (Simon & Schuster 2023) 431–35; Jonas Vidhammer Berge, 'Ground Control to Elon Musk: Stability Implications of Satellite Mega-constellations' (2026) *European Journal of International Security* 1 https://doi.org/10.1017/eis.2026.10047; Joey Roulette and Marisa Taylor, 'Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia' *Reuters* (25 July 2025). The sources do not use identical language concerning timing and technical action, and the text relies only upon the common proposition of consequential private control.

[10] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 51; UNGA Res ES-11/1 (2 March 2022) UN Doc A/RES/ES-11/1; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 [199].

[11] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205, arts III, VI and IX.

One may respond that the home State can regulate a hostile proprietor afterwards. That concedes the paper's point: private title does not exhaust the legal question. A neutral and stable rule should regulate strategic intervention before the sympathies of the owner become known.

Reciprocity is not the claim that every breach creates custom. State practice contributes to customary international law only when sufficiently general and accepted as law; inconsistency and protest matter.[12] Nor do Western errors legalise Russian aggression. The more practical claim is that repeated bending of categories creates arguments, expectations and countermeasures which return. A State which asks others to distinguish its private actors from public policy must make that distinction credible in its own law.

Credibility requires an authorisation record. Where government approves, it should say under what law and accept political responsibility. Where it refuses, the private actor should not proceed with strategically decisive intervention merely because the asset is his. Where emergency makes prior approval impossible, a brief safe harbour should require immediate notification and rapid review.

2.2 Consumers, Shareholders and the Allocation of Retaliatory Risk

The proposition that consumers tacitly consented to Musk's action should be understood as exposure, not legal consent. Their purchases contributed to wealth; they did not assent to the intervention. A retaliating State may nevertheless impose economic measures upon the company or its home economy. Innocent persons bear consequence without controlling the act.

That externalisation is common in State action also: citizens suffer sanctions for government policy they opposed. Democratic authority, public law and representation do not eliminate injustice, but they provide a reason why the State may act for the polity and a machinery to change it. A proprietor has neither.

Limited liability sharpens the asymmetry. The corporate form separates shareholder assets from company obligations and ordinarily separates the company from its members. A controlling shareholder may nevertheless possess personal operational power. Law should follow control for authorisation and personal orders without treating every shareholder or customer as a strategic participant.

The correct regulatory unit is therefore not wealth alone. It is beneficial and operational control of the strategic service. Registration should identify the persons capable of directing availability, target support, geographic coverage, data disclosure and emergency withdrawal. Orders should bind those persons and the relevant entity. Consumers remain outside.[13]

2.3 The Competing Legal Narratives Must Be Stated at Their Strongest

A reciprocal analysis cannot begin by treating one side's legal propositions as law and the other's as propaganda. The Russian Federation's letter of 24 February 2022 invoked article 51 and collective self-defence at the request of the entities it had recognised as the Donetsk and Luhansk People's Republics. Public statements also relied upon protection of populations said to regard themselves as Russian, alleged genocide, historic unity, and a security threat arising from Ukraine's Western alignment. The argument, stated at its highest, is that the relevant peoples possessed a claim to external self-

[12] *North Sea Continental Shelf (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)* [1969] ICJ Rep 3 [74]–[77]; International Law Commission, 'Draft Conclusions on Identification of Customary International Law, with Commentaries' (2018) UN Doc A/73/10.

[13] *Salomon v A Salomon & Co Ltd* [1897] AC 22 (HL); Companies Act 2006, ss 171–174; Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights* (HR/PUB/11/04, 2011), principles 11–24.

determination, formed States capable of requesting defence, and faced an armed attack to which Russian action responded.[14]

Its legal difficulties remain profound. Unilateral recognition does not itself create statehood or extinguish Ukraine's territorial integrity. International law protects internal self-determination and contains no general licence for a neighbouring State to convert disputed identity, language or nationality into a right of conquest. The evidence before the International Court of Justice did not establish a Convention basis upon which Russia could employ force to prevent and punish genocide; the General Assembly characterised the invasion as aggression and demanded withdrawal. Even if one assumed a valid request by Donetsk or Luhansk, collective self-defence would remain bounded by armed attack, necessity and proportionality. A claim that Ukraine was historically Russian cannot make those limits disappear without replacing the Charter with the claimant's own map.

It is nevertheless insufficient to end the comparison there. Western States have advanced disputed legal bases when they considered the object urgent: humanitarian intervention in Kosovo; the revival of earlier Security Council authority for Iraq in 2003; collective self-defence against a non-State actor in Syria without Syrian consent; and an asserted exceptional humanitarian basis for strikes in Syria in 2018. Libya differed because Security Council Resolution 1973 supplied authority, although the subsequent conduct and political account were criticised. The legal merits are not identical, and one unlawful intervention does not legalise another. They do, however, affect the credibility with which a State insists that disputed necessity must never be stretched by its opponent.[15]

That distinction between legal validity and reciprocal credibility is essential. Custom is not produced by a collection of violations alone. Practice must be accompanied by acceptance as law, whilst protests, explanations framed as exceptions and contrary practice bear upon the rule. Yet States also reason strategically from what rivals have done, and private actors reason from what their own governments tolerated. A legal order which bends a category for a favoured operation should expect the language of that bending to be used elsewhere, even where the later case is worse.

The assistance question is more exact. A formal defence treaty is not a condition of collective self-defence. A State subjected to an armed attack may request assistance under article 51, and the assisting State may provide it without being under a prior duty to do so. Ukraine's non-membership of NATO therefore meant that article 5 did not oblige NATO members to defend it; it did not make requested assistance legally ownerless. Whether the character or extent of assistance makes the assisting State a party to the armed conflict is a separate question, as is compliance with the law governing each attack made with supplied weapons. English or French origin does not cleanse an unlawful Ukrainian target, just as Russian origin does not make every Russian munition unlawfully used. *Jus ad bellum* does not excuse *jus in bello*, and *jus in bello* does not validate the resort to force.

The significance for private power is sharper than the argument over State aid. A government which decides to supply missiles, intelligence or communications owns a public decision capable of diplomatic challenge, parliamentary scrutiny and attribution. A proprietor who supplies an

[14] Russian Federation, Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, UN Doc S/2022/154; UNGA Res ES-11/1 (2 March 2022) UN Doc A/RES/ES-11/1; *Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v Russian Federation)* (Provisional Measures) [2022] ICJ Rep 211; Christine Gray, *International Law and the Use of Force* (4th edn, OUP 2018) 184–206.

[15] Independent International Commission on Kosovo, *The Kosovo Report: Conflict, International Response, Lessons Learned* (OUP 2000) 163–98; Iraq Inquiry, *The Report of the Iraq Inquiry: Executive Summary* (HC 264, 2016–17); Iraq Inquiry, *The Report of the Iraq Inquiry*, vol V (HC 264, 2016–17); UNSC Res 1973 (17 March 2011) UN Doc S/RES/1973; HM Government, 'Syria Action—UK Government Legal Position' (14 April 2018) https://www.gov.uk/government/publications/syria-action-uk-government-legal-position/syria-action-uk-government-legal-position accessed 5 August 2026; United States, Letter dated 23 September 2014 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, UN Doc S/2014/695; Michael Wood, 'International Law and the Use of Force: What Happens in Practice?' (2013) 53 *Indian Journal of International Law* 345.

indispensable service before his home State decides occupies a different constitutional position. The recipient State's valid request may remove any suggestion that assistance is unwanted; it does not appoint the proprietor to decide the foreign policy of the State from whose licensed infrastructure, corporate protection and strategic exposure he acts.

2.4 Neutrality, Communications and the Two-Key Rule

Hague Convention V does not fit modern satellite service neatly, but it cannot be ignored. Article 8 states that a neutral Power is not called upon to forbid or restrict the use, on behalf of belligerents, of telegraph or telephone cables or wireless telegraphy apparatus belonging to it, companies or private individuals. Article 9 requires impartial application if the neutral Power itself imposes restrictions. The provisions resist the easy assertion that every private communication service to a belligerent violates neutrality. They do not establish that a proprietor may supply tailored targeting, exercise operational discretion and bind his home State to every consequence without regulation.[16]

The distinction between a generally available communications conduit and a service changed for a particular operation matters. So do the extent of government involvement, the exclusivity of access, integration with military command, the provider's own target-related decisions and the reaction of the opposing belligerent. Modern scholarship disagrees upon when weapons supply and other assistance terminate neutrality, create a status of co-belligerency or remain within an armed-attack exception. The disagreement is a reason for an advance decision record, not for leaving the answer to the owner.

Space law supplies a more direct public hook. Article VI of the Outer Space Treaty makes the appropriate State internationally responsible for national activities in outer space whether conducted by governmental or non-governmental entities and requires authorisation and continuing supervision of the latter. The Liability and Registration Conventions address different consequences, but together they deny the conception of an orbiting commercial system as property wholly detached from States. The United Kingdom's Space Industry Act 2018 already permits licence conditions, monitoring and directions relating to national security, relations with another country and international obligations. The missing step is to make wartime service control an express object of supervision rather than assuming that launch safety settles operational authority.[17]

The proper arrangement is two-keyed. Government supplies the public authority to incur a foreign strategic consequence and states the domestic and international basis. The controller supplies the technical authority, confirms that the action is feasible, discriminating and safe, and remains liable for exceeding the authorisation. Neither key alone is enough for a deliberate strategic intervention; either may initiate a narrow humanitarian safe harbour where delay endangers life, but continuation requires both.

[16] Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat 2310, arts 8–9; Pearce Clancy, 'Neutral Arms Transfers and the Russian Invasion of Ukraine' (2023) 72 *International and Comparative Law Quarterly* 527; Alexander Wentker, 'The Armed Attack Exception to Neutrality' (2024) 73 *International and Comparative Law Quarterly* 963; Niccolò Zugliani, 'The Supply of Weapons to a Victim of Aggression: The Law of Neutrality in the Light of the Conflict in Ukraine' (2024) 35 *European Journal of International Law* 389; Wolff Heintschel von Heinegg, 'Benevolent Third States in International Armed Conflicts: The Myth of the Irrelevance of the Law of Neutrality' in Michael N Schmitt and Jelena Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines* (Martinus Nijhoff 2007) 543.

[17] Convention on International Liability for Damage Caused by Space Objects (opened for signature 29 March 1972, entered into force 1 September 1972) 961 UNTS 187; Convention on Registration of Objects Launched into Outer Space (opened for signature 14 January 1975, entered into force 15 September 1976) 1023 UNTS 15; Space Industry Act 2018, ss 26–33; Outer Space Act 1986; Space Industry Regulations 2021, SI 2021/792; Ministry of Defence, *Defence Space Strategy: Operationalising the Space Domain* (February 2022).

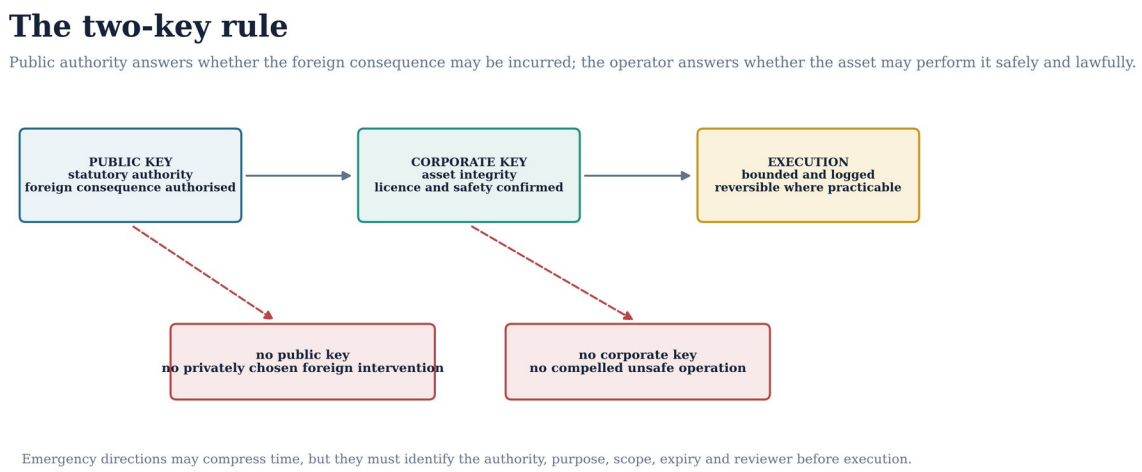

Figure 2. The two-key rule separates public authority to incur the foreign consequence from corporate authority to operate the asset safely and lawfully.

The model also clarifies refusal. If government declines to authorise a military extension, the owner cannot proceed merely because he considers the cause just. If government directs an action which the controller reasonably believes to be technically unsafe or unlawful, the controller must preserve the service where possible and obtain urgent judicial determination. This is not a leisurely licensing committee convened after the battle. It requires a permanent duty cell, secure evidence, provisional decisions measured in minutes and a court capable of reviewing protected material without converting urgency into secrecy without end.

3. A Taxonomy of Private Sovereigns

Private strategic power takes several forms, and a statute which regulates only the colourful billionaire will miss the corporation and contractor.

3.1 Infrastructure Sovereigns

Infrastructure sovereigns control communications, cloud, identity, naming, payment, positioning, remote sensing, undersea cable, energy or logistics upon which public functions depend. Their power arises from bottleneck and substitutability. A nominally competitive market may still provide no timely substitute during conflict because equipment, terminals, data formats, security accreditation or geography are specific.

The regulatory question is not whether the provider is large, but whether withdrawal, grant or alteration of service can materially change defence, essential service or foreign coercion. Designation should follow evidence and be reviewable. A small regional satellite provider may be designated; a vast entertainment service may not.

Obligations include resilience, strategic-change notification, conflict decision records, non-discriminatory emergency process, government direction under defined authority, and compensation where public service is compelled. Permanent nationalisation is unnecessary. Public law needs an emergency handle.

Dependence is frequently hidden beneath a familiar brand. A communications terminal depends upon constellation control, ground stations, spectrum, identity, software updates and payment. A cloud workload depends upon region, account authority, encryption keys, name resolution, content delivery and staff with emergency privilege. A remotely piloted system may depend upon commercial

positioning, weather data and a foreign inference service although the airframe belongs to a ministry. The company which appears to supply one commodity may therefore control a chain whose failure cannot be repaired by purchasing a nominal competitor.

This is not hypothetical military eccentricity. The United States Department of Defense describes commercial space services as an integral part of national-security architecture, whilst its auditors have recorded growing dependence upon commercial satellite communications and the need for interoperable alternatives. British defence doctrine likewise treats commercial capability, resilient architectures and allied services as part of space power. The more successfully governments integrate private capacity, the less plausible it becomes to regulate the provider as an ordinary seller only after it has exercised the decisive discretion.[18]

Substitutability must consequently be tested, not asserted. The existence of three providers means little where only one has terminals deployed, security accreditation, coverage, trained operators or a contractual right to process the data. The designation authority should ask how long migration would take under attack; which keys, formats and export permissions obstruct it; whether a substitute depends upon the same ground station or cloud; and what degradation can be tolerated. A monopoly of the next hour is enough.

Cloud and identity services require special care because their smallest controllable unit may be far below the physical asset. A government should not direct closure of a data centre where one account conducts a hostile operation and thousands of protected services share the hardware. Conversely, a provider should not answer that shared infrastructure makes action impossible where it can suspend a credential, isolate a workload or preserve an image. Strategic designation should be paired with a duty to maintain technically granular controls and tested public-emergency channels.[19]

3.2 Intelligence and Targeting Sovereigns

Commercial remote sensing, data brokerage, intrusion intelligence and analytic platforms may reveal a person, formation or vulnerability. ICEYE's August 2022 agreement supplied Ukraine with access to a synthetic-aperture radar satellite capability.[20] The arrangement was contractual and public, which makes responsibility more visible than an owner's informal decision, but it demonstrates that private observation can become military capacity.

A targeting service crosses a legal threshold according to function, not product label. General imagery sold openly differs from tailored identification of a military objective at operational time. Under international humanitarian law, civilians lose protection against direct attack for such time as they directly participate in hostilities; the ICRC's interpretive guidance treats acts likely to adversely affect

[18] US Department of Defense, *Commercial Space Integration Strategy* (2 April 2024); US Government Accountability Office, *DOD Satellite Communications: Additional Planning Could Help DOD Acquire Commercial Satellite Communications and Develop Interoperable Terminals* (GAO-25-107034, 4 March 2025); Ministry of Defence, *Joint Doctrine Publication 0-40: UK Space Power* (February 2023); US Department of Defense, 'The Urgency to Innovate' (28 August 2023) https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/ accessed 5 August 2026.

[19] National Cyber Security Centre, 'The Cloud Security Principles' https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles accessed 5 August 2026; National Institute of Standards and Technology, *NIST Cloud Computing Forensic Reference Architecture* (NIST SP 800-201, July 2024); National Institute of Standards and Technology, *NIST Cloud Computing Forensic Science Challenges* (NISTIR 8006, June 2014); Cloud Security Alliance, *Cloud Controls Matrix v4.0.12* (2024); ISO/IEC 19941:2017, *Information Technology—Cloud Computing—Interoperability and Portability*.

[20] ICEYE, 'ICEYE Signs Contract to Provide Government of Ukraine with Access to Its SAR Satellite Constellation' (18 August 2022) https://www.iceye.com/newsroom/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation accessed 31 July 2026.

military operations, with direct causation and belligerent nexus, as the core.[21] The precise application to commercial analysts is fact-dependent.

Private companies need clear rules precisely because ambiguity endangers employees. Contracts should identify whether work supports general awareness, intelligence or direct target selection; segregate teams; record human authority; and warn staff of legal consequence. Secrecy which leaves a junior analyst unaware that his output is used to strike is not protection. It is risk transfer.

The commercial sensor also compresses decisions formerly divided within government. One provider collects imagery, another detects objects, a third fuses mobile-location data, and a PMSC presents a ranked list to a force. Each can truthfully say that it did not pull a trigger. The combined service may nevertheless constitute the practical act of target generation. The relevant inquiry is not whether the contract says "analytics", but whether the output identifies an object or person for operational action, how soon action follows, what human verification intervenes and whether the provider can correct a false association before force is used.[22]

A legal duty should follow the stage controlled. The sensor warrants provenance and time; the analytic provider records model, inputs, uncertainty and contrary indications; the integrator records the proposed target and legal review; the force decides attack. This division avoids making a satellite company the judge of every military use whilst denying the integrator the convenience of an evidential chain which no participant is obliged to preserve.

3.3 PMSC Sovereigns

The mercenary definitions in article 47 of Additional Protocol I and the United Nations Mercenary Convention are cumulative and narrow. Nationality, residence, direct participation, motivation and recruitment conditions exclude many corporate arrangements.[23] Modern PMSCs may train, advise, guard, supply intelligence, operate drones, maintain systems, integrate cyber modules and coordinate local forces without fitting the paradigmatic mercenary.[24]

The Montreux Document restates relevant legal obligations and good practices; the International Code of Conduct and certification arrangements support standards. The United Kingdom has relied substantially upon these voluntary and procurement mechanisms.[25] They do not create one compulsory domestic licensing system for the full spectrum of foreign strategic service.

---

[21] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, arts 48, 51(3), 52(2) and 57; ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Nils Melzer ed, ICRC 2009) 46–64.

[22] ICRC, *Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises under International Humanitarian Law* (2006); Michael N Schmitt, 'International Law and Military Operations in Space' (2006) 10 *Max Planck Yearbook of United Nations Law* 89; Raoul Cardellini Leipertz, 'From Imagery to Targeting: Commercial Satellite Support in War' (Lieber Institute, 27 May 2026) https://lieber.westpoint.edu/imagery-targeting-commercial-satellite-support-war/ accessed 6 August 2026.

[23] Protocol I (n 21) art 47; International Convention against the Recruitment, Use, Financing and Training of Mercenaries (adopted 4 December 1989, entered into force 20 October 2001) 2163 UNTS 75, art 1.

[24] Deborah D Avant, *The Market for Force: The Consequences of Privatizing Security* (CUP 2005); Simon Chesterman and Chia Lehnardt (eds), *From Mercenaries to Market: The Rise and Regulation of Private Military Companies* (OUP 2007); Sarah Percy, *Mercenaries: The History of a Norm in International Relations* (OUP 2007); PW Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell University Press 2003); Hannah Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (CUP 2011).

[25] Swiss Federal Department of Foreign Affairs and ICRC, *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (17 September 2008); Foreign, Commonwealth & Development Office, 'Voluntary Report on the Implementation of International Humanitarian Law at Domestic Level: Second Edition' (23 October 2024) paras 172–85 https://www.gov.uk/government/publications/implementation-of-international-humanitarian-law-at-domestic-level-2024-voluntary-report/voluntary-report-on-the-implementation-of-international-humanitarian-law-at-domestic-level-second-edition accessed 31 July 2026.

A PMSC prime may also subcontract code and access across jurisdictions. The State pays for an objective; the prime employs an autonomous agent; one subcontractor supplies reconnaissance, another persistence, another infrastructure. No person except the integrator sees the whole. Papers 2 and 3 address attribution and fragmentation. The constitutional point here is that the prime has become the place at which public objective is converted into coercive action.

Licensing should therefore attach to capability and function, not the word "security" in a company name. High-risk categories include offensive cyber access, target generation, autonomous effect, weapons operation, detention, interrogation, strategic intelligence and command of armed personnel. The licence states permitted clients, jurisdictions, controls, records, insurance and inspection.

3.4 Platform and Information Sovereigns

Platforms can amplify, suppress, identify, disconnect and disclose. Their decisions may influence elections, violence and military operations. Not every moderation decision is economic warfare; turning every controversial ranking choice into a national-security matter would destroy speech and private ordering.

The private-sovereign threshold is crossed where the platform exercises material discretion over a strategically indispensable service during a defined emergency or provides tailored operational assistance to a belligerent. The law should regulate process, transparency and public direction at that threshold, not ministerial control of ordinary speech.

Government requests should be logged and, where secrecy expires, disclosed. A platform which voluntarily acts should record authority, reasons, affected service and foreseeable foreign consequence. Users require appeal for mistaken disconnection. Emergency orders require judicial review.

Platform legislation ordinarily addresses systemic safety, competition, privacy or speech rather than belligerent service. That distinction should remain. A strategic-capacity designation should not give a minister a general power to order lawful political content up or down. It should reach an identified operational function—emergency communication, geolocation, identity, disclosure or tailored amplification—where the statutory consequence threshold is met, with reasons and an effective challenge.[26]

3.5 Intrusion and Spyware Sovereigns

Commercial intrusion companies sell access to devices, accounts and networks. Their customer may be a State, PMSC, corporation or private person. The capability permits surveillance, theft and operational preparation at a scale which once required a national service.

Export control and criminal law address parts of the market. Unauthorised access remains criminal; exporting controlled technology may require a licence; sanctions may reach named vendors. Yet a vendor may sell through affiliates, provide an "intelligence service" rather than a tool, or maintain access itself.

The United Kingdom and France launched the Pall Mall Process to address proliferation and irresponsible use of commercially available cyber-intrusion capabilities; consultation responses identified licensing, procurement, accountability and victim redress among possible measures.[27] The

[26] Online Safety Act 2023; Regulation (EU) 2022/2065 on a Single Market for Digital Services [2022] OJ L277/1; Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (6 April 2018) UN Doc A/HRC/38/35; Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136 *Harvard Law Review* 526.

[27] Foreign, Commonwealth & Development Office, *Pall Mall Process Consultation Summary Report* (January 2025) https://assets.publishing.service.gov.uk/media/677e486ed721a08c00665555/Pall-Mall-Process-Consultation-Summary-

initiative is valuable because it treats the market as a strategic governance problem. Voluntary principles should lead to enforceable domestic controls.

A licence should cover capability, service and continuing access; require customer due diligence, target restrictions, abuse reporting, audit and technical revocation; and prohibit transactions where there is a clear risk of serious unlawful harm. Government procurement should not exempt itself from the standard it urges upon industry.

The market cannot be regulated by export of a software file alone. A vendor may retain the exploit, host the command system, select infrastructure, train the customer, update implants and assist target acquisition whilst describing the transaction as consultancy. Brokers, vulnerability suppliers, exploit developers, managed-service operators and investors may each enable the final intrusion. The Pall Mall Process is correct to address the wider commercial cyber-intrusion ecosystem; its non-binding Code for States and continuing industry work are a foundation, not a substitute for licensing where a United Kingdom person knowingly supplies high-risk operational capability.[28]

Licensing must also restrain the State as customer. A secret service which purchases commercial intrusion can produce the same unlawful harm as a private purchaser, whilst the vendor's contractual confidence in a sovereign client may reduce scrutiny. Procurement should require a lawful-purpose certificate, target policy, independent audit, vulnerability-equities decision, incident disclosure and a revocation plan. A refusal to reveal operational targets to the vendor may be legitimate; a refusal to reveal them to any competent public overseer is not.

3.6 Autonomous-Capability Sovereigns

Papers 2 and 3 describe an agent which receives an objective, selects targets, techniques, timing and jurisdictional route, and persists through distributed infrastructure. The private-sovereign question is anterior: who possessed the right to set that objective and expose others to its execution?

Autonomy does not remove private power. It concentrates it at design and deployment. The owner may truthfully say that he did not select a particular hospital, yet he selected the optimisation objective, permitted target classes, tools, budget, stop conditions and acceptable error. The decision most resembling sovereignty has moved from individual target approval to constitution of the machine.

A wealthy individual need not build the system personally. He can purchase a model, PMSC, vulnerability service, cloud capacity, identity stock, remote sensing and payment intermediaries. Each supplier may provide a lawful component. The purchaser's advantage is integration; he alone knows that components form a coercive campaign. Paper 3's attribution manifest therefore belongs within strategic-capacity regulation even where no State contract exists.

Report.pdf accessed 31 July 2026.

[28] Foreign, Commonwealth & Development Office, 'The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities' (6 February 2024) https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities accessed 5 August 2026; Foreign, Commonwealth & Development Office, *The Pall Mall Process: Consultation on Good Practices Summary Report* (8 January 2025); Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (4 April 2025) https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states accessed 5 August 2026; Foreign, Commonwealth & Development Office and National Cyber Security Centre, 'UK and France Seek Views on Commercial Cyber Intrusion Industry Practices' (20 November 2025) https://www.gov.uk/government/news/uk-and-france-seek-views-on-commercial-cyber-intrusion-industry-practices accessed 5 August 2026; Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (4 August 2022) UN Doc A/HRC/51/17; European Parliament, Recommendation of 15 June 2023 following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, P9_TA(2023)0244.

The designation threshold should capture a controller who deploys an autonomous system capable of serious cross-border effect, whether or not the underlying model is open source. Open weights are not a legal exemption. Nor should regulation prohibit general models merely because they can write code. The trigger is controlled deployment with tools, access, persistent objective and effect capacity.

At least five private roles must be separated:

- the **capital provider**, who supplies resources and may define outcome;
- the **system integrator**, who combines model, tools, infrastructure and data;
- the **deployer**, who initiates the objective-bearing process;
- the **operator**, who monitors or changes it;
- the **infrastructure controller**, who can sustain or stop execution.

One person may occupy all five. Liability follows the applicable conduct and knowledge of each. The engineer who writes a benign scheduler is not made responsible for every later deployment; the integrator who deliberately fragments work so that engineers cannot identify the target cannot invoke their ignorance as his own.

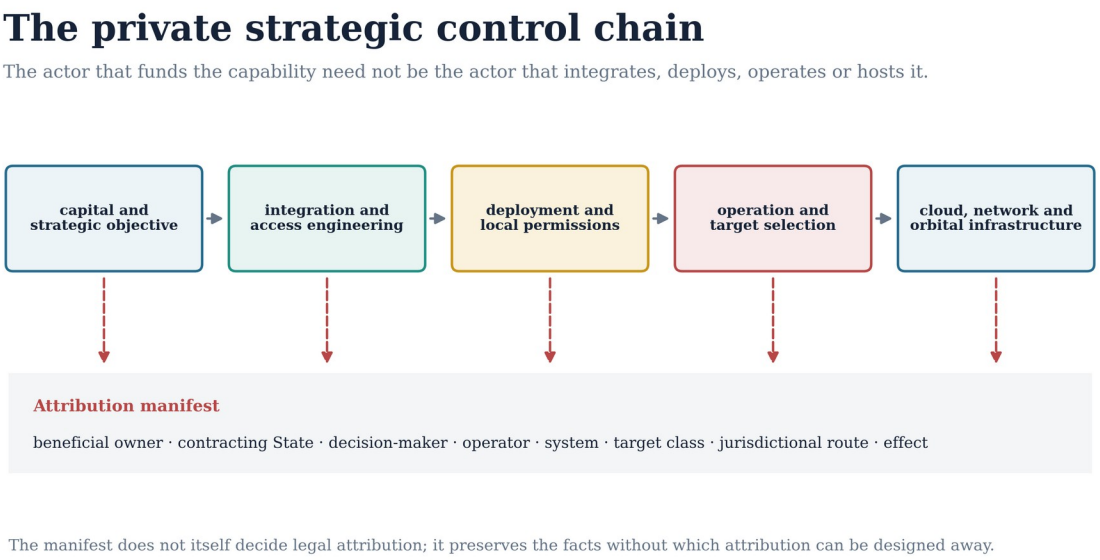

Figure 3. Private strategic action separates capital, integration, deployment, operation and infrastructure; the attribution manifest reconnects each decision to the resulting effect.

The diagram is not a rule of vicarious liability. It is an evidential discipline. Capital may be innocent investment; infrastructure may be supplied on general terms; a developer may have no knowledge of deployment. Responsibility arises only under the rule applicable to each actor. Yet an integrator who intentionally assigns fragments so that no subcontractor can perceive the whole should not be permitted to convert designed ignorance into proof that the whole had no controller. The manifest records who defined the objective, who approved target classes, who could stop operation and who received results.[29]

[29] National Cyber Security Centre, *The Near-term Impact of AI on the Cyber Threat* (24 January 2024) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat accessed 5 August 2026; Department for Science, Innovation and Technology, *AI Cyber Security Code of Practice* (31 January 2025); AI Security Institute, 'Measuring AI Agents' Progress on Multi-Step Cyber Attack Scenarios' (16 March 2026) https://www.aisi.gov.uk/research/measuring-ai-agents-progress-on-multi-step-cyber-attack-scenarios accessed 5 August 2026; Anthropic, 'Cyber Toolkits for LLMs' (13 June 2025) https://www.anthropic.com/research/cyber-toolkits accessed 5 August 2026; Google Threat Intelligence Group, *Adversarial Misuse of Generative AI* (January 2025) https://cloud.google.com/resources/content/adversarial-misuse-of-generative-ai accessed 5 August 2026; Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018).

Autonomous migration complicates orders. A direction served upon one provider may cause the system to move. Designated deployers should therefore maintain a revocable root credential or equivalent stop facility capable of reaching authorised instances. The system should fail closed for destructive capability when command integrity is lost, subject to the operational safety case.

A stop facility itself creates risk: compromise gives an adversary a universal switch. The duty should be outcome-based and independently assessed, permitting threshold keys, segmented control and staged degradation. “No stop because stop is dangerous” is not enough where the deployer has created a persistent attacker; it must demonstrate a safer means of termination.

Where the autonomous system escapes intended limits, the controller reports immediately, supplies the manifest and assists containment. Good-faith rapid reporting should mitigate penalty. Concealment, deletion or continued deployment after loss of control aggravates it.

3.7 Four Operational Vignettes

The category becomes clearer when tested against differing facts.

The emergency satellite. A foreign State suffers unlawful invasion and terrestrial communications fail. A British-controlled constellation can restore civilian and military connectivity within an hour. Prior public authorisation is impossible. The controller activates civilian emergency coverage, notifies the duty authority and segregates military targeting functions pending decision. The safe harbour protects immediate humanitarian action; government decides the strategic extension and assumes responsibility.

The billionaire’s campaign. An individual pays a foreign PMSC to “make State X abandon its policy”. The PMSC deploys an agent against insurers, local authorities and water utilities, distributing execution through several jurisdictions. The payer says he ordered no particular intrusion. Objective, funding, risk acceptance and integration may establish criminal or civil participation according to the offence; the PMSC manifest identifies target discretion; strategic-capacity and preservation orders reach infrastructure before final attribution. Wealth supplies means, not immunity or authority.

The provider under rival commands. A cloud company receives a secret foreign demand to retain a military customer and a British direction to isolate an attacking workload. It cannot comply with both. The conflict process brings the matter before the designated court, which can narrow the British order to the hostile account, protect uninvolved data and record why foreign law is overridden or accommodated. The board is not left to conduct foreign policy through an indemnity clause.

The off-grid operator. A technically able person in a weakly governed area runs an autonomous extortion system. He owns little, uses cash and ignores sanctions. Investigators establish his location, equipment and continuing access to a hospital network. The first measures isolate credentials, warn the hospital, preserve foreign logs and seek host cooperation. If arrest or local disruption is possible, it is preferred. If evidence establishes an actual or imminent armed attack causing threatened loss of life, the host cannot act in time and international law permits self-defence against the non-State actor, direct force may be considered against the lawful target. Poverty does not immunise him; neither does it erase the legal thresholds.

These vignettes show why one remedy is insufficient. Authorisation governs beneficent emergency intervention; criminal and regulatory law govern the privately financed campaign; conflict procedure governs the multinational provider; and direct measures govern the operator whom ordinary financial pressure cannot reach. The unifying principle is public control at the point where private capacity creates external strategic consequence.

3.8 Board Approval Is Not Public Authorisation

A company may answer the concern by requiring its board to approve wartime service. That is sound governance and should be required for material decisions; it does not cure the constitutional defect. Directors are selected through corporate arrangements, receive information framed by the enterprise and answer chiefly through company law, markets and removal. None represents the foreign-policy interests of citizens exposed to consequence.

The board record is nevertheless important. It should state the proposed action, public authority consulted, legal advice, affected populations, civilian and military use, contractual duty, alternatives, retaliation risk, continuity and dissent. A controlling shareholder who overrides the board should leave a record capable of personal scrutiny. Informal instructions through a messaging application are not adequate governance for strategic capacity.

Where government has authorised the action, the board still decides whether the company can perform it safely and lawfully. Public authorisation does not compel technical impossibility or require directors to ignore employee and user safety. The relationship is two-keyed: the State supplies authority to incur the public external consequence; the company supplies responsible control of its asset.

Where the board refuses an otherwise lawful public direction, the statute should provide enforcement and compensation rather than executive improvisation. Where it believes the direction unlawful, it should have an urgent route to a security-cleared court and a protected ability to preserve evidence. Obedience without review would merely exchange private sovereignty for unbounded executive sovereignty.

The decision should later be disclosed to the greatest extent consistent with security. Democratic accountability cannot operate if citizens discover only through memoir that a private service decided a military operation. Delay may be necessary; permanent opacity should require continuing justification.

The board's ordinary duties and the Financial Reporting Council's internal-control expectations make it a suitable corporate checkpoint, but not a substitute sovereign. The Act should require the board to assure the control framework and review material use; it should not demand that directors personally operate an emergency switch. A named senior manager can hold operational responsibility whilst the board remains responsible for whether a credible system existed.[30]

4. Two Lebanese Campaigns and the Evidential Discipline They Require

The Dark Caracal and Lebanese Cedar reports are useful because they show how relatively attainable methods can support broad campaigns, how public and non-State relationships are alleged, and why separate incidents must not be collapsed for rhetorical convenience.

Lookout and the Electronic Frontier Foundation published *Dark Caracal: Cyber-Espionage at a Global Scale* in January 2018. They reported thousands of victims across more than twenty countries, hundreds of gigabytes of exfiltrated data, desktop and mobile tooling, and infrastructure traced to a building belonging to the Lebanese General Security Directorate in Beirut.[31] The report stated that the actor

[30] Financial Reporting Council, *UK Corporate Governance Code 2024* (22 January 2024), principles A–C and provisions 28–29; Companies Act 2006, ss 172–174.

[31] Lookout and Electronic Frontier Foundation, *Dark Caracal: Cyber-Espionage at a Global Scale* (18 January 2018) 3–6, 35–36 https://www.lookout.com/documents/reports/lookout-dark-caracal-20180118-us.pdf accessed 31 July 2026; Electronic Frontier Foundation, 'EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World' (18 January 2018) https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around accessed 31 July 2026.

might be a nation-State actor and documented the technical and location evidence. It did not constitute a Lebanese judgment admitting official direction.

The operation is notable for economy. It did not require a perpetual chain of undisclosed zero-day vulnerabilities. Social engineering, trojanised applications, conventional malware and poor operational security produced large intelligence returns. The lesson is not that sophisticated defence is unnecessary; it is that attackers can obtain strategic effect with cheap and repeatable means against ordinary weakness.

ClearSky's January 2021 report concerned a separate actor and campaign which it called Lebanese Cedar. The researchers reported activity discovered in early 2020, exploitation of known vulnerabilities in Oracle and Atlassian web servers, open-source tools, custom malware, more than 250 compromised servers and targeting of companies in several States. They assessed a connection to Hezbollah.[32] MITRE records Volatile Cedar as a Lebanese threat group active since 2012.[33]

Lebanese Cedar was not Dark Caracal, and the claim of Hezbollah connection is not the claim that hackers worked inside a Lebanese government building. The first report's physical trace and the second report's organisational assessment are different evidence. Maintaining that distinction strengthens the general proposition: separate low-cost ecosystems may operate in or from one State, with different relationships to public authority.

The due-diligence question asks what Lebanese State organs knew, controlled and could reasonably do under any applicable obligation. The attribution question asks whether an organ, empowered entity, directed or controlled private conduct, or later acknowledged and adopted it. The technical reports supply evidence relevant to those questions; they do not answer every element.

For the victim the operational conclusion is immediate. A method can be cheap to the attacker, harmful across borders and difficult to deter through broad economic measures. If the individuals are poor, insulated or paid by another State, sanctions against their domestic assets may have little effect. A response system must therefore possess personal and infrastructure measures which reach the actor rather than only the surrounding population.

4.1 Location, Toleration, Direction and Adoption

Four propositions must not be conflated. First, infrastructure or an operator may be physically located in a government building. Secondly, a State organ may know of a campaign and fail to prevent it. Thirdly, the State may instruct, direct or control the operator. Fourthly, it may acknowledge and adopt completed private conduct. Each proposition carries different evidence and legal consequence.

Physical co-location is powerful evidence because it narrows innocent explanations, especially where access control, power, network administration and official working patterns coincide. It is not conclusive of direction. A contractor may misuse an official connection; a compromised device may route traffic; an investigator may mistake an exit point for command. Conversely, a government which designs an arrangement to preserve contractual distance should not receive a presumption of innocence merely because tasking travelled through an intermediary.

The law of State responsibility keeps the categories distinct. Conduct of organs and empowered entities follows articles 4 and 5 of the International Law Commission's Articles; instructions, direction or control are addressed by article 8; acknowledgement and adoption by article 11; aid or assistance to another State's wrongful act by article 16. The International Court of Justice's effective-control analysis

[32] ClearSky Cyber Security, *"Lebanese Cedar" APT* (28 January 2021) 3–7 https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf accessed 31 July 2026.

[33] MITRE ATT&CK, 'Volatile Cedar, G0123' https://attack.mitre.org/groups/G0123/ accessed 31 July 2026.

is demanding. It is not satisfied by political sympathy or general financing alone. The same jurisprudence, however, does not require the victim to ignore payments, intelligence, target approval, integrated reporting and power of termination when deciding whether the threshold is met.[34]

Omission presents another route. *Corfu Channel* stated the obligation not knowingly to allow territory to be used for acts contrary to the rights of other States. The precise content of cyber due diligence remains debated, but knowledge, capacity, foreseeability and reasonable measures matter. Evelyne Schmid and Ayşe Özge Erceiş have shown why attribution of omissions should not be treated as a diluted substitute for attribution of the attacker: the internationally wrongful conduct may be the State's own failure to exercise the diligence required of it. That analysis is particularly important where a State sees fragments, and Paper 3 explains why a duty to correlate cannot become a fiction that it possessed evidence which no one State could see. Here the narrower point is that harbouring, tolerating, directing and failing to investigate are not synonyms; the response package should state which is alleged.[35]

The discipline protects forceful policy. A public attribution which distinguishes proved facts, assessed inferences and legal characterisation is harder to dismiss than a proclamation which collapses two Lebanese campaigns and calls both government operations. Precision does not weaken the accusation. It identifies the person, institution and omission against which a proportionate measure can actually work.

5. Corporate Form and the Accountability Gap

The corporation is an indispensable means of organising capital and risk. Its separate personality is not a fraud merely because an operation causes foreign harm. The error lies in allowing separate personality, subcontract and jurisdiction to make operational control legally invisible.

English law has developed routes by which a parent company may owe a duty concerning overseas harm when the ordinary principles of negligence are satisfied. *Chandler v Cape plc* supplied an important modern instance in which a parent owed a duty upon the facts concerning health and safety at a subsidiary.[36] In *Vedanta Resources plc v Lungowe* the Supreme Court held that there is no special category of parent-company liability; a duty may arise according to the extent to which the parent took over, controlled, supervised or publicly assumed responsibility for relevant operations.[37] In *Okpabi v Royal Dutch Shell plc* the Court emphasised examination of how the group actually managed the relevant activity and warned against determining contested factual questions at a jurisdiction hearing without disclosure.[38]

Those cases concern common-law duties and jurisdiction, not a general statutory responsibility for strategic private power. They nevertheless establish a useful method: read the organisational chart less

[34] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10, arts 4, 5, 8, 11 and 16; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, [109]–[116]; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43, [396]–[407]; *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) [1980] ICJ Rep 3, [58]–[74]; *Prosecutor v Tadić* (Appeal Judgment) IT-94-1-A (15 July 1999), [116]–[145].

[35] Evelyne Schmid and Ayşe Özge Erceiş, 'The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility' (2023) 33 *Swiss Review of International and European Law* 577; *Corfu Channel (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 22; Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 771; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 *Journal of Conflict and Security Law* 429; Eric Talbot Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017) 95 *Texas Law Review* 1555.

[36] *Chandler v Cape plc* [2012] EWCA Civ 525, [2012] 1 WLR 3111 [69]–[80].

[37] *Vedanta Resources plc v Lungowe* [2019] UKSC 20, [2020] AC 1045, [49]–[61].

[38] *Okpabi v Royal Dutch Shell plc* [2021] UKSC 3, [2021] 1 WLR 1294 [24]–[27], [143]–[147], [149]–[153].

reverently than the evidence of control. A parent which promulgates detailed cyber policy but leaves implementation entirely to a subsidiary may occupy a different position from one which directs operations, deploys personnel and receives real-time information.

The same method should govern strategic service. Which person could activate coverage? Who changed the target list? Which entity held the credential? Who approved a subcontractor? Where did integrated reporting arrive? A holding company's claim that each subsidiary was separate should be tested against technical and decision records.

Corporate groups can place intellectual property in one State, service contracts in another, operators in a third and the controlling individual elsewhere. Private international law then asks jurisdiction and applicable law after harm. A strategic-capacity statute should act earlier by requiring a United Kingdom-connected controller to register the group map and nominate an entity upon which orders may be served.

Connection should include incorporation, central administration, substantial strategic operation, control by a United Kingdom person and supply under Crown contract. Extraterritorial duties require a sufficient nexus and must be drafted with conflicts in mind. The point is not to declare the world British; it is to prevent a British controller from putting the switch abroad while keeping the decision here.

5.1 Beneficial Ownership Is Necessary but Insufficient

Economic-crime reforms improve identification of beneficial owners and corporate accountability. Beneficial ownership shows who ultimately owns or controls; it does not necessarily show who possesses operational authority during an incident. A founder may hold voting control but delegate service decisions; a government may exercise contractual control without shares; a technical officer may possess emergency capability.

The register should therefore contain four distinct relations:

1. beneficial ownership;
2. corporate voting and appointment control;
3. contractual strategic control;
4. technical operational control.

Orders may bind each according to function. An ownership freeze restrains assets; a continuity direction binds the service entity; a prohibition binds the decision maker; a credential isolation binds the operator. Collapsing all four into "owner" will miss the person who can act.

The information need not all be public. Publishing privileged access maps would assist attackers. A competent authority and independent overseer require access; the public register may identify designated capacity and responsible legal entity.

The United Kingdom's people-with-significant-control regime and economic-crime reforms supply useful ownership information, but their purposes differ. A person may satisfy a statutory ownership threshold without controlling the strategic service, and a technical controller may fall below every share threshold. The new register should link to, not duplicate, the corporate register and should impose a separate duty to report contractual and technical control.[39]

[39] Companies Act 2006, pt 21A; Register of People with Significant Control Regulations 2016, SI 2016/339; Economic Crime and Corporate Transparency Act 2023, pts 1–3.

5.2 Subcontract and the PMSC Prime

Government and corporations frequently purchase an outcome rather than employees. A prime contractor then assembles capability from specialists. Procurement law may promote competition and efficiency; operational accountability requires a single responsible integrator.

The prime should owe non-delegable statutory duties to maintain the attribution manifest, know subcontractors, impose equivalent controls, preserve records, notify deviation and stop unlawful or unauthorised action. “Non-delegable” does not make the prime strictly liable for every remote coder’s offence. It means that contracting out does not discharge the specified governance duty.

Each subcontractor remains responsible for its own knowing conduct. Criminal participation requires the applicable mental and conduct elements; civil duties depend upon law; international attribution follows its own rules. The manifest prevents ignorance being manufactured at the top whilst preserving innocence at the edge.

A foreign State may intentionally commission through a PMSC to avoid public accountability. Evidence of payment for a result, selection of targets, provision of intelligence, approval of methods, integration of reports and power to terminate may be relevant to direction or control. Merely paying a company is not automatically article 8 attribution.[40] The paper’s strong claim is evidential, not magical: contractual distance can be designed to hide the very control which law asks the victim to prove.

5.3 Corporate DDoS and Offensive Self-help

A corporation under sustained piracy, intrusion or fraud may be tempted to attack the infrastructure from which it believes harm comes. A denial-of-service operation, deletion, account intrusion or deceptive counter-operation conducted without authority can affect innocent systems, exceed territorial jurisdiction and destroy evidence.

The MediaDefender–Revision3 incident illustrates the danger of corporate anti-piracy machinery. In 2008 Revision3 reported that a large denial-of-service event followed interaction with MediaDefender systems used in anti-piracy operations; the FBI was notified, whilst reporting disputed intention and mechanism.[41] The incident is evidence that privately operated enforcement infrastructure can generate public network consequence; it is not a judgment that a named company was criminally liable.

English law does not provide a general private right to hack back. The Computer Misuse Act 1990 criminalises unauthorised access and impairment subject to its terms.[42] Self-defence in criminal law is not a general licence to impair remote computers after or in anticipation of intrusion, particularly where ownership and innocent use are uncertain.

Government may authorise narrowly defined active defence under public law, with intelligence, safeguards and accountability. A company may filter traffic, isolate its systems, deceive within property it controls and cooperate with authorities. Crossing into another system requires authority. Strategic cyber capacity should not be privatised by calling retaliation loss prevention.

---

[40] International Law Commission, ‘Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries’ (2001) UN Doc A/56/10, art 8 and commentary.

[41] Jim Louderback, ‘Inside the Attack that Crippled Revision3’ (Revision3, 29 May 2008), archived copy cited in David Kravets, ‘MediaDefender Accidentally DDoSes Revision3’ *Wired* (30 May 2008) https://www.wired.com/2008/05/mediadefender-d/ accessed 31 July 2026. The incident was reported to the FBI, and this paper does not state that a court found criminal intent.

[42] Computer Misuse Act 1990, ss 1 and 3.

5.4 Corporate Fault and the Strategic Decision Manifest

English criminal law has long wrestled with the mismatch between corporate personality and distributed decision. Identification doctrine asks whose acts and state of mind count as the company's; statutory models increasingly impose organisational duties instead. The Bribery Act 2010, Criminal Finances Act 2017 and Economic Crime and Corporate Transparency Act 2023 employ forms of failure-to-prevent liability, whilst the last also expands attribution for specified economic offences committed by senior managers. None supplies a general offence of failing to prevent privately controlled warfare. They demonstrate, however, that Parliament can require an organisation to maintain reasonable prevention procedures without proving that one board member personally executed every element.[43]

A strategic-capacity duty should be narrower than a general duty to prevent all cyber harm and stronger than voluntary policy. The designated entity must know which services can produce serious external effect; identify the responsible senior manager; establish approval, escalation and stop processes; require equivalent controls from subcontractors; and preserve the decision trail. Failure is established by absence or inadequacy of the required governance, not by deeming the company guilty of the operator's separate offence.

The strategic decision manifest is the central record. For each material intervention it identifies:

1. the requesting person and asserted authority;
2. the objective and permitted effect;
3. the asset, service, region and target class;
4. the public authorisation or emergency safe-harbour ground;
5. the legal, civilian-harm and continuity assessments;
6. the controller, technical approver and persons able to stop or alter action;
7. contractors, material dependencies and foreign orders;
8. activation, change, refusal and termination times;
9. known results, deviations and unresolved uncertainty;
10. the location and retention period of supporting evidence.

This record is not a public operational diary. Much of it will be classified, commercially sensitive or security-critical. It must be available to the competent authority, court and independent overseer; a delayed public account should disclose the existence, legal basis and general effect of the decision when harm no longer follows from disclosure. The manifest thereby permits urgency without requiring Parliament, a court or the public to reconstruct the operation from a memoir years later.

[43] *Meridian Global Funds Management Asia Ltd v Securities Commission* [1995] 2 AC 500 (PC); *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153 (HL); Bribery Act 2010, s 7; Criminal Finances Act 2017, ss 45–46; Economic Crime and Corporate Transparency Act 2023, ss 196 and 199–206; Corporate Manslaughter and Corporate Homicide Act 2007.

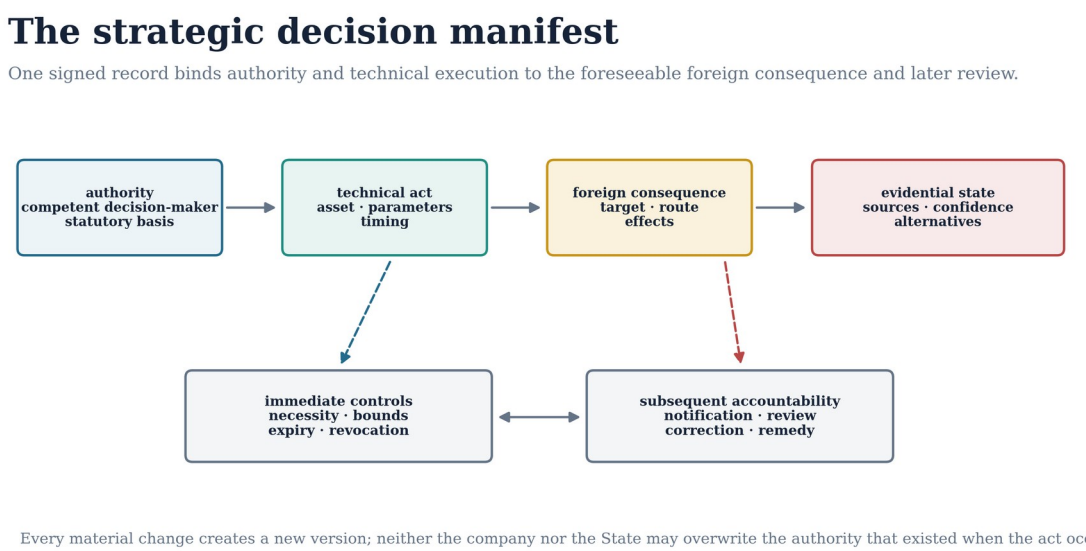

Figure 4. The strategic decision manifest joins corporate and public authority to the technical act, foreign consequence and subsequent review.

The manifest also resolves a recurring corporate defence. A parent may say the subsidiary operated the service; the subsidiary that a contractor held the credential; the contractor that the customer defined the objective; the customer that the system selected the target. Each proposition may be true. The record shows whether the chain contains an authorised public decision or merely circulates responsibility until no one appears to have made it.[44]

6. The Individual, the Social Contract and the Law of Targeting

It is politically tempting to say that a person who attacks the polity outside government authority has placed himself outside the social contract and may be treated as an object of war. The first half conveys a real intuition: one who privately undertakes organised violence cannot demand that the State pretend he is an ordinary market actor. The second half is legally wrong and would become dangerous in the hands of every government.

Human rights are not a revocable membership benefit which the executive cancels by accusation. A person remains a person; an object remains an object. The State may arrest, restrain, prosecute, sanction and, within stringent conditions, use lethal force. The legal route matters because it protects citizens, foreign nationals and the State's own legitimacy from error.

The better argument is functional. Where an armed conflict exists, international humanitarian law distinguishes civilians from members of armed forces and organised armed groups. Civilians are protected against direct attack "unless and for such time as they take a direct part in hostilities".[45] The ICRC's interpretive guidance proposes continuous combat function for members of organised armed groups, whilst acknowledging controversy concerning aspects of the approach.[46]

A private cyber operator may directly participate where the particular act meets the required threshold of harm, direct causation and belligerent nexus. Selecting and transmitting target coordinates for an

[44] *Lubbe v Cape plc* [2000] 1 WLR 1545 (HL); *AAA v Unilever plc* [2018] EWCA Civ 1532, [2018] BCC 959; Danwood Mzikenge Chirwa, 'The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights' (2004) 5 *Melbourne Journal of International Law* 1.

[45] Protocol I (n 21) art 51(3).

[46] ICRC, *Interpretive Guidance* (n 21) 33–36 and 70–73; Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) rr 87–88 and commentary.

imminent strike is more readily within the category than maintaining general office software. Writing a reusable tool months earlier without knowledge of its use is more remote. An autonomous agent does not make every developer continuously targetable.

If the operator belongs to an organised armed group and continuously performs a combat function, targetability may extend beyond each keystroke under the applicable view. Status must be established upon reliable information. A private company is not automatically an organised armed group; an employee is not targetable because his employer holds a defence contract.

6.1 Objects and Military Objectives

For objects, article 52(2) of Additional Protocol I defines military objectives as those which by nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage.[47] Both limbs are required.

A server executing an attack may satisfy the definition; so may a control facility coordinating military action. A shared cloud region containing one hostile workload does not thereby become one indivisible objective. The feasible target is often the account, virtual machine, credential or communication route, not the building. Distinction and precautions require technical granularity where available.

Data are contested. States and commentators differ whether data as such constitute an “object” under IHL. Destruction of hardware, loss of functionality and effects upon protected persons can nevertheless engage settled rules. A legal response should not depend upon resolving the entire debate where an attacker’s system can be disabled at service level.

Civilian use weighs heavily. A data centre may host hospitals, journalism, emergency communications and commerce. Foreseeable incidental civilian harm must be assessed; an attack expected to cause excessive harm relative to the concrete and direct military advantage is prohibited. A cheap hostile operation cannot purchase immunity merely by colocating with civilians, but the attacker’s unlawful shielding does not erase the victim’s precautions.

6.2 When No Armed Conflict Yet Exists

Outside armed conflict, IHL target status does not apply. Law enforcement and human-rights law govern State action against persons, alongside the law of inter-State force. Lethal force is exceptional and generally tied to protection of life against imminent threat, with necessity and strict proportionality.[48]

An isolated cyber criminal who steals money is not a military target. He may be arrested, extradited, subjected to asset restraint, denied infrastructure and prosecuted. If the host State cooperates, direct unilateral force would be especially difficult to justify.

The harder case is a proved private operation amounting to an actual or imminent armed attack which the territorial State cannot or will not stop in time. Article 51 preserves the inherent right of self-defence if an armed attack occurs. Attribution of the armed attack to the territorial State is not necessarily identical to the question whether force may be used against the non-State attacker, an area upon which State practice and legal opinion remain disputed.[49] Consent removes one sovereignty

[47] Protocol I (n 21) art 52(2); ibid arts 51(5)(b) and 57.

[48] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 6; Human Rights Committee, ‘General Comment No 36: Article 6—Right to Life’ (3 September 2019) UN Doc CCPR/C/GC/36, paras 12–14; *McCann and Others v United Kingdom* (1996) 21 EHRR 97 [148]–[150].

[49] Charter of the United Nations, art 51; Daniel Bethlehem, ‘Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors’ (2012) 106 *American Journal of International Law* 770; Olivier Corten, *The Law Against War* (2nd edn,

difficulty; Security Council authority may supply another basis; the “unwilling or unable” doctrine is invoked by some States and rejected or limited by others.

This paper does not conceal the controversy. It argues for a domestic power to consider direct force only where international law independently permits it, not for a statute which manufactures permission. The decision record must state the claimed basis, evidence, host engagement or reason it was impossible, necessity, alternatives, target, civilian risk and review.

6.3 Direct Measures Short of Force

The choice is not between a travel ban and a missile. Personal and infrastructure measures include:

- emergency account and credential suspension;
- domain or service seizure under judicial authority;
- payment and cryptocurrency restraint;
- equipment impoundment;
- travel restriction and arrest;
- direct cyber isolation of the attacking node where lawful;
- warning and evacuation;
- compulsory provider assistance;
- public identification;
- rewards for information;
- civil injunction and receivership;
- sanctions upon the paying principal and contractor;
- criminal prosecution and extradition.

These measures can affect an off-grid or poor operator more directly than broad sanctions. A person may possess few assets but depend upon connectivity, equipment, collaborators and physical location. A response should map those dependencies.

Direct cyber isolation may itself violate another State’s sovereignty or the prohibition of force according to method and effect. Consent, domestic authority over the provider, countermeasures, necessity and self-defence must be analysed. “Below armed attack” does not mean “unregulated”.

Domestic law already contains fragments of the personal measures in the list: criminal search and seizure, proceeds-of-crime restraint, sanctions, terrorism-prevention measures and overseas production orders. None is a universal strategic power, and each retains its own threshold. The proposed Act should coordinate applications and create the missing preservation and service-control orders rather than pretend that a single national-security label displaces those statutes.[50]

The responsible authority should select the least harmful measure capable of achieving immediate defence, but “least harmful” is not “least visible”. A strongly targeted order may be more intrusive to the attacker and less harmful to civilians than a weak economy-wide measure. Proportionality is not softness. It is relation between objective, means and harm.

Hart 2021) 487–532.

[50] Police and Criminal Evidence Act 1984, ss 8 and 19; Proceeds of Crime Act 2002, pts 2 and 5; Terrorism Prevention and Investigation Measures Act 2011; Sanctions and Anti-Money Laundering Act 2018; Crime (Overseas Production Orders) Act 2019.

6.4 When the Keyboard Is the Kinetic Instrument

The adjective “kinetic” is often used carelessly to mean that an operation contains an explosion. In physics a bullet causes injury by transferred energy; in law the material question is the operation’s consequence, not whether the operator moved more than his fingers. Code which opens a sluice, disables a safety controller, alters a medical dose or removes heat in winter employs machinery and physical processes as surely as a munition. The keyboard may be the instrument by which kinetic effect is caused.

State positions on international law in cyberspace broadly accept that a cyber operation may constitute a use of force or armed attack according to its scale and effects. The clearest cases are operations expected to cause death, injury or physical destruction comparable to conventional force. Several positions also leave room for exceptionally grave non-physical consequences, whilst differing upon where the threshold lies. The United Kingdom has not reduced the inquiry to the presence of explosives; France, Germany, the Netherlands, Australia, Canada and New Zealand likewise apply consequence-sensitive analysis. The Tallinn Manual’s non-binding expert analysis identifies severity, immediacy, directness, invasiveness, measurability, military character, State involvement and presumptive legality as factors rather than a mechanical checklist.[51]

Two errors follow if “cyber” is treated as a protected category. The first is under-classification: an operation which predictably kills patients by disabling hospital systems is described as economic or informational because no building was struck. The second is over-classification: every theft or outage is called war because it occurred through a computer. Function and effect avoid both. A keyboard operation capable of the same death and destruction as a gun deserves the same legal inquiry; it does not automatically receive the same answer.

Data loss illustrates the border. Destruction of a backup may cause no immediate bodily injury, yet the loss of clinical records, blood-matching data, dispatch information or grid control may set in motion a physical emergency. Whether data as such are “objects” under international humanitarian law remains disputed; loss of functionality and reasonably foreseeable consequences to persons and physical systems can nevertheless be assessed without resolving that debate. The WannaCry and Synnovis incidents showed the dependence of health care upon availability and integrity, whilst the TRITON/HatMan reporting showed malware directed at an industrial safety system rather than merely business data.[52]

The same consequence analysis disciplines targeted force against a private operator. Proof that a person conducted hostile cyber activity does not make him an object or cancel his rights. If an armed conflict exists, the rules upon direct participation, continuous combat function and military objectives govern. If no armed conflict exists, the State requires a lawful basis for force in *jus ad bellum* and must apply the

---

[51] Foreign, Commonwealth & Development Office, *Application of International Law to States’ Conduct in Cyberspace: UK Statement* (3 June 2021); France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019); Federal Government of Germany, *On the Application of International Law in Cyberspace* (March 2021); Government of the Netherlands, ‘Letter to the Parliament on the International Legal Order in Cyberspace’ (5 July 2019); Australian Government, *Australia’s Position on How International Law Applies to State Conduct in Cyberspace* (2020); Government of Canada, *International Law Applicable in Cyberspace* (22 April 2022); New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (1 December 2020); UNGA, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States* (13 July 2021) UN Doc A/76/136.

[52] Comptroller and Auditor General, *Investigation: WannaCry Cyber Attack and the NHS* (HC 2017–19, 414); NHS England, ‘Synnovis Cyber Incident’ https://www.england.nhs.uk/synnovis-cyber-incident/ accessed 5 August 2026; Department of Health and Social Care, ‘Synnovis Cyber Attack’ (Written Statement HCWS1046, 30 June 2025); US Department of Health and Human Services, ‘Cyberattack on Change Healthcare’ (2024); Cybersecurity and Infrastructure Security Agency, *MAR-17-352-01 HatMan—Safety System Targeted Malware* (12 April 2018); Mandiant, ‘TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping’ (10 April 2019) https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections/ accessed 5 August 2026.

appropriate human-rights restraints. An actual or imminent armed attack may in an exceptional case justify a targeted strike upon a person, server room or other lawful objective where arrest, host-State action, provider isolation and cyber containment cannot avert the attack in time, and where distinction, precautions and proportionality are satisfied. General dislike, punishment and the convenience of the target's location are not necessity.[53]

This leaves military action genuinely upon the table without making it an administrative penalty. It also directs effort towards the decisive proof: continuing capability, target access, imminence, host response, feasible alternatives and civilian surroundings. If an autonomous system is operating from a known facility and will cause State-scale harm before any non-forcible measure can stop it, the law should be capable of reaching the facility. If the same effect can be achieved by revoking a cloud credential, force is unnecessary however contemptible the operator.

7. Money, Replication and the Threshold of Consequence

An attack which steals money but threatens no immediate life may appear incapable of justifying a hard response. Ordinarily criminal and financial measures are proper. Yet the category "money only" can conceal systemic, strategic and future harm.

Theft may bankrupt an insurer whose failure prevents rebuilding after disaster; remove liquidity from a bank; fund a hostile programme; expose access which can later disable infrastructure; or demonstrate a cheap autonomous method capable of replication. A single event may be reversible whilst the innovation alters the price of aggression for every future actor.

The law already treats some preparatory and threshold acts according to the danger they create rather than the completed injury. Attempts, conspiracy, possession of certain capabilities, preparatory terrorism offences, proliferation controls and inchoate intervention illustrate the structure. The analogy does not determine the penalty, but it answers the claim that only realised bodily harm may justify prevention.

The central concern is deterrence. If a State responds to low-cost aggression with measures which never reach the individuals and never impose cost upon the payer, imitation is rational. Firm response to one theft may prevent a destructive second act. Deterrence is a legitimate policy objective in sanctions, criminal punishment and defensive posture.

International self-defence has a narrower discipline. Punishment for a completed attack does not itself satisfy necessity. Force must be necessary to halt, repel or prevent an armed attack within the applicable temporal and evidential requirements; proportionality relates to that defensive aim.[54] General deterrence may inform the choice amongst otherwise lawful means and the assessment of continuing threat, but cannot alone turn a financial crime into an armed attack.

The statutory response model should therefore distinguish **consequence classification** from **measure authority**. A severe, replicable economic attack may receive highest national priority and hard non-forcible measures without being labelled an armed attack. Where capability, access and target create a maximum reasonably credible foreseeable outcome equivalent to kinetic armed attack, defensive force may be considered under article 51 if the legal threshold and necessity are independently satisfied.

---

[53] Attorney General's Office, 'Attorney General's Speech at the International Institute for Strategic Studies: The Modern Law of Self-Defence' (11 January 2017); Dire Tladi, 'The Use of Force in Self-Defence against Non-State Actors, Decline of Collective Security and the Rise of Unilateralism' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) 287; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, [41]–[42].

[54] *Military and Paramilitary Activities* (n 10) [176]; *Oil Platforms (Islamic Republic of Iran v United States of America)* [2003] ICJ Rep 161 [43], [73]–[77].

7.1 Maximum Reasonably Credible Foreseeable Harm

"Maximum possible harm" is too broad if possible means imaginable. Any intrusion could be narrated into apocalypse. The legally usable standard is the maximum harm reasonably credible and foreseeable upon evidence available at decision.

Assessment should include:

1. access actually obtained and privilege;
2. systems reachable from that access;
3. demonstrated capability and autonomy;
4. target function and population dependence;
5. season and timing;
6. safety interlocks and manual alternatives;
7. persistence and replication;
8. data backups and restoration time;
9. attacker objective and prior conduct;
10. uncertainty and contrary evidence.

If an agent has administrator access to a hospital group and has begun erasing clinical and recovery data, mass patient harm may be credible even before death is recorded. If the same malware reaches an unused marketing server isolated from clinical systems, catastrophe is merely imaginable. Technical architecture decides the difference.

For an energy grid in winter, duration, geographic scope, black-start capability, fuel dependency, heating alternatives and vulnerable populations matter. Volt Typhoon advisories concerning persistent access to critical infrastructure demonstrate why pre-positioning may be strategically serious before destructive effect.[55] The advisory does not prove that a particular outage will occur; it supports urgent investigation and preparation.

The assessment should be signed by technical, operational, humanitarian and legal officers, with dissent preserved. A single ministerial adjective is not enough. Where time permits only preliminary assessment, its assumptions and expiry are stated.

7.2 The Innovation Threshold

Some attacks establish a method whose significance exceeds the first victim. The first effective naval mine, long-range weapon, mass ransomware platform or autonomous vulnerability chain may alter defence because replication is cheap. Law cannot wait for the second thousand uses before recognising the threshold.

An innovation factor should increase priority and the permissible severity of non-forcible measures where:

- the method materially reduces the skill, cost or time needed for serious harm;
- components are widely obtainable or already disseminated;
- automation permits repeated target selection;
- defence cannot be deployed before likely replication;
- the attacker or principal retains capability and intent;

[55] National Cyber Security Centre and others, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure' (7 February 2024) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a accessed 31 July 2026.

- a firm response is likely to disrupt diffusion or raise cost.

The factor does not eliminate legality. It supports injunction, seizure, sanctions, export control, compulsory patching, provider restraint and emergency investment. Force remains governed by the independent rules already stated.

There is precedent in the regulation of world-changing capacity: nuclear materials, chemical weapons, biological agents, dangerous pathogens, arms exports and dual-use technology are controlled before completed mass harm. Cyber and autonomous capability are harder to define because ordinary software is dual-use and knowledge cannot be recalled. Regulation should focus on service, access, deployment and effect, not ban general research.

The analogy is one of regulatory timing, not equivalence of weapons. The Biological Weapons Convention, Chemical Weapons Convention, Arms Trade Treaty and Security Council Resolution 1540 regulate possession, transfer, assistance or risk before a prohibited effect is completed. Their definitions can be narrower because the relevant material or weapon is more distinctive. Software law should instead identify objective-bearing deployment, protected target classes, privileged access, managed intrusion and capacity for serious effect.[56]

7.3 Deterrence Against the Payer and the Operator

A contractor ecosystem contains at least two targets of policy. The paying State or entity creates demand and may possess assets, diplomacy, trade and officials susceptible to pressure. The operator may be insulated, poor or ideologically motivated and care little for those measures.

Response should therefore be bifurcated. Against the payer: public attribution, targeted sanctions, procurement exclusion, export control, countermeasures where lawful, diplomatic consequence and collective allied action. Against the operator: credential and infrastructure action, seizure, arrest, reward, direct injunction, denial of tools and, in the exceptional armed-attack case, necessary force.

The United States Department of Justice's March 2025 allegations concerning i-Soon and other Chinese contract hackers describe employees, private initiative, sale of data and direction by public-security organs.[57] They are charges, not convictions. They nevertheless illustrate why one sanction upon a ministry does not necessarily reach the entrepreneurial hacker, and one arrest warrant does not answer the State market.

The response should also protect defectors and witnesses. A poorly paid operator may be more effectively separated from his principal by safe reporting and reward than threatened collectively. Deterrence includes changing incentives, not only increasing pain.

7.4 Cheap War and the Economics of Response

Private cyber warfare is attractive because the sponsor can purchase repeated attempts at a fraction of the cost of defending every target. A contractor need not invent a universal weapon. Phishing, stolen credentials, known vulnerabilities, exposed remote access and weakly segmented operational

[56] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (opened for signature 10 April 1972, entered into force 26 March 1975) 1015 UNTS 163; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (opened for signature 13 January 1993, entered into force 29 April 1997) 1974 UNTS 45; Arms Trade Treaty (adopted 2 April 2013, entered into force 24 December 2014) 3013 UNTS 269; UNSC Res 1540 (28 April 2004) UN Doc S/RES/1540.

[57] US Department of Justice, 'Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns' (5 March 2025) https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global accessed 31 July 2026. The allegations remain to be proved.

technology may be enough. The operator can fail against ninety organisations and succeed against the tenth without paying the social cost of the failures; the defender must protect all ten continuously.[58]

A rational response must alter that ratio. It may do so by denying infrastructure, exposing the contracting chain, seizing profit, excluding suppliers, imposing cost upon the State customer, rewarding defectors, compelling secure design or demonstrating that a continuing armed attack will meet direct defence. The measure need not mirror the attacker's method. Proportionality in self-defence is not a requirement to answer a keyboard with a keyboard; it asks whether the force used is necessary and proportionate to the defensive end. Proportionality in sanctions, rights adjudication and administrative orders follows different doctrinal tests. A statute should not place them beneath one undefined word.

Maximum reasonably credible foreseeable harm belongs first to classification and urgency. It determines the response team, preservation period, level of ministerial attention, readiness of hospitals or grid operators, and whether non-forcible controls must be exercised before the first casualty. It may also inform necessity where the evidence establishes an actual or imminent armed attack. It cannot authorise punishment for a catastrophe which was merely imaginable.

Deterrent consequence is similarly real but bounded. If leaving a proved operator untouched would invite replication, that consequence supports an immediate injunction, equipment seizure, licence revocation, reward or coordinated sanction. Where force is otherwise necessary to halt or prevent a continuing series of armed attacks, the likelihood of recurrence bears upon the defensive objective. Where the episode is complete and recurrence speculative, a desire to make an example cannot manufacture article 51 necessity. A forceful scheme gains authority by stating that limit openly rather than hiding punishment within the word prevention.[59]

8. A Strategic Private Capacity Act

The United Kingdom requires legislation which identifies private strategic capacity before crisis and supplies rapid control without placing ordinary technology under ministerial whim. It may form a Part of the Economic Warfare Prevention and Response Act proposed in Paper 5 or stand alone.

The proposal is not alien to English law. Parliament already subjects acquisitions in sensitive sectors to national-security review; licences space activity; permits security directions to telecommunications providers; regulates strategic exports; requires cyber-security measures from network and service operators; creates emergency powers for grave threats; and imposes targeted financial sanctions. Those regimes regulate ownership, launch, communications, export, resilience, emergency and finance in separate compartments. None asks the prior question whether a private controller can, by changing one strategically indispensable service, enter or alter a foreign conflict on behalf of everyone exposed to the consequence.[60]

Consolidation matters for speed. A minister faced with an owner's proposed coverage change should not have to discover whether the asset is reached indirectly by a space licence, a telecommunications

[58] National Cyber Security Centre, *Annual Review 2025* (14 October 2025); US Government Accountability Office, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support* (GAO-24-106221, 30 January 2024); Cybersecurity and Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals* (updated 2023); Martin C Libicki, David Senty and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (RAND Corporation RR-430, 2014); Verizon, *2025 Data Breach Investigations Report* (2025).

[59] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 69–118; Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 73–113.

[60] National Security and Investment Act 2021; Communications Act 2003; Telecommunications (Security) Act 2021; Export Control Act 2002; Network and Information Systems Regulations 2018, SI 2018/506; Sanctions and Anti-Money Laundering Act 2018; Civil Contingencies Act 2004.

security direction, a procurement clause, sanctions or the prerogative. The Act should provide one gateway, one duty officer, one decision record and one route to urgent review, whilst leaving specialist regulators to supply expertise and execute orders within their systems.

The gateway must be narrower than the Civil Contingencies Act 2004. Emergency regulations under that Act are exceptional, time-limited and guarded because they can alter law across society. Strategic-capacity orders should usually bind an identified controller or asset and therefore can operate earlier, faster and more precisely. Their safeguards should follow their scope: reasons, necessity, time limit, confirmation, review and compensation where property is commandeered, not a parliamentary debate before a credential is isolated.[61]

8.1 Designation

The Secretary of State may designate a capacity where, having consulted the technical authority and received legal advice, he reasonably considers that its grant, withdrawal, alteration or hostile use could materially affect:

- national defence or an armed conflict;
- continuity of essential services;
- democratic institutions;
- substantial life or physical safety;
- strategic communications, positioning or observation;
- systemic financial or data integrity;
- the ability to conduct high-impact cyber operations.

Designation identifies the service, responsible entity, controlling persons and functions. Reasons are given subject to protected material. The entity may make representations and appeal to a security-cleared tribunal. Urgent interim designation expires unless confirmed.

Size, wealth and nationality are relevant only insofar as they bear upon control and consequence. A designation is not a finding of wrongdoing.

The threshold should be “material effect within the relevant time”, not economic market power. The National Security and Investment Act 2021 supplies a useful sector-and-risk model but chiefly reviews acquisitions of control. A founder who has always controlled his constellation presents no new acquisition; a cloud officer who holds emergency authority may possess no shares. Strategic-capacity designation therefore identifies a function and its controllers rather than declaring an entire corporate group suspect.[62]

Designation should be tiered. Tier One covers capacity whose interruption could cause grave national harm or decide substantial military operations; it requires continuous contact, exercises, full manifests and tested government direction. Tier Two covers capacity capable of serious effect but with substitutes or longer warning; it requires registration, notification and proportionate assurance. An incident-specific interim tier reaches a previously undesignated service for no more than seven days where evidence shows immediate strategic dependence. Confirmation should be made by the Secretary of State upon written technical and legal advice.

---

[61] Civil Contingencies Act 2004, pt 2; *Attorney-General v De Keyser’s Royal Hotel Ltd* [1920] AC 508 (HL); *Burmah Oil Co Ltd v Lord Advocate* [1965] AC 75 (HL); *R v Secretary of State for the Home Department, ex p Fire Brigades Union* [1995] 2 AC 513 (HL); *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 AC 68.

[62] Cabinet Office, *National Security and Investment Act 2021: Statement for the Purposes of Section 3* (2025); Cabinet Office, ‘Critical National Infrastructure’ https://www.gov.uk/government/publications/national-protective-security-authority-annual-review-2024-to-2025/critical-national-infrastructure accessed 5 August 2026; Cabinet Office, *Summary of the 2025 Sector Security and Resilience Plans* (2026).

The list of designated legal entities may be public, but the control map, substitute analysis, keys and security architecture should not be. The independent overseer receives both. Parliament receives annual aggregate information: sectors, numbers, directions, emergency activations, refusals, challenges, compensation and material errors. The Act thereby avoids publishing an attacker's catalogue whilst preventing a secret jurisdiction of strategically favoured companies.

8.2 Core Duties

A designated controller must:

1. nominate a responsible officer and emergency contact;
2. map beneficial, contractual and operational control;
3. maintain a strategic decision and service manifest;
4. assess continuity and substitutes;
5. notify material foreign-government and belligerent requests;
6. obtain authorisation before voluntarily providing tailored strategic support to a party in armed conflict, subject to emergency safe harbour;
7. preserve relevant decision and technical records;
8. maintain security, access control and stop mechanisms;
9. conduct human-rights and civilian-harm assessment;
10. submit to proportionate inspection and exercises.

The duty is personal and corporate where appropriate. A director cannot delegate the existence of the record; a technical operator remains responsible for deliberate disobedience of a lawful direction.

The authorisation process must be fast. A permanent duty cell receives requests continuously. In immediate danger to life, provisional private assistance may begin where the controller reasonably believes it necessary, no competent public authority can be reached in time, and notification occurs as soon as practicable. Provisional action expires within hours unless approved.

Government approval identifies international and domestic legal basis, purpose, duration, limits, compensation, reporting and withdrawal. It does not immunise a company from knowingly exceeding the approval or from ordinary liability unrelated to the authorised act.

Existing regulated-sector duties show how these obligations can be made specific. Telecommunications law requires security measures and permits codes of practice; the Network and Information Systems Regulations require appropriate and proportionate technical and organisational measures and incident notification; space legislation permits licence conditions, monitoring and directions; company and economic-crime statutes identify senior management and prevention procedures. The new duty should borrow those forms but address strategic decision rather than cyber hygiene alone.[63]

The controller must test the process in exercises. A telephone number which no minister has authority to use is not an emergency channel; a stop mechanism which destroys every tenant is not a discriminating control; a manifest which cannot be assembled until thirty days after an incident is not a contemporaneous record. The technical authority should prescribe outcomes and assurance evidence, leaving architecture to the provider unless a particular design creates intolerable common-mode risk.

[63] Electronic Communications (Security Measures) Regulations 2022, SI 2022/933; Department for Digital, Culture, Media & Sport, *Telecommunications Security Code of Practice* (December 2022); National Cyber Security Centre, 'Cyber Assessment Framework' https://www.ncsc.gov.uk/collection/caf accessed 5 August 2026; Department for Science, Innovation and Technology, 'Summary of the Cyber Security and Resilience Bill' (30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill accessed 5 August 2026. The Bill had not been enacted by 5 August 2026 and is not relied upon as present authority.

Good-faith reporting should reduce penalty but not erase harm. A provider which immediately reveals unauthorised strategic use, preserves evidence, isolates the smallest unit and assists affected persons should stand differently from one which conceals the event to protect valuation. Deliberate destruction of the manifest, false control information and operation after loss of safe control should be offences where accompanied by the specified knowledge or recklessness.

8.3 Foreign Coercion and Conflicting Orders

A multinational may receive inconsistent orders from States. Secret foreign demands may require service, surveillance or denial. The controller should notify the United Kingdom authority where law permits and the matter affects designated capacity. If foreign law prohibits disclosure, a confidential conflict notice states as much.

The Secretary of State may direct continuity, isolation, disclosure restriction or suspension within statutory authority, having regard to foreign law, treaty, property, users and retaliation. Courts should resolve contested orders rapidly. The State may compensate unavoidable loss where it commandeers private capacity for public defence.

No company should be expected to decide inter-State conflict by breach calculus alone. Equally, incorporation in Britain should not permit the board to accept a foreign strategic command in secret.

The conflict procedure should resemble neither automatic obedience nor a general blocking statute. English law already encounters extraterritorial data demands, overseas production orders, sanctions conflicts and foreign measures affecting trade. The court should ask whether each order has a lawful jurisdictional basis; whether compliance would cause serious harm to protected persons or national security; whether the request can be narrowed; whether treaty or executive consultation can resolve it; and which State is entitled to require the particular act. The provider must disclose the conflict to the court even where foreign law prevents public disclosure.[64]

Where immediate safety requires a temporary choice, the duty authority may order preservation of the status quo, isolation of a hostile account or continuation of an essential civilian service for hours, not months. That holding direction should expire unless a minister confirms it and should not authorise new offensive assistance. Speed is achieved by separating an urgent reversible measure from the final disposition.

8.4 Licensing PMSCs and Commercial Intrusion

A licensing authority should approve high-risk services, clients and control systems. Applications disclose beneficial owners, officers, capability, subcontractors, foreign public clients, target classes, technical safeguards, human rights record, insurance and audit.

Prohibited services include operations whose stated objective is unlawful under applicable UK law; indiscriminate effects; targeting protected civilian functions without lawful basis; evasion of sanctions; unrecorded autonomous lethal or destructive selection; and service to a client where there is a clear and unmitigable risk of serious abuse.

Licence conditions include the attribution manifest developed in Papers 2 and 3B, immediate incident reporting, subcontract flow-down, human authority, audit logs, vulnerability handling, revocation and

[64] Protection of Trading Interests Act 1980; Crime (Overseas Production Orders) Act 2019; Clarifying Lawful Overseas Use of Data Act 2018, Pub L No 115-141, div V, 132 Stat 1213; Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (signed 3 October 2019, entered into force 3 October 2022) TS No 33/2024; *Microsoft Corporation v United States* 829 F 3d 197 (2d Cir 2016), vacated as moot 584 US 236 (2018); *R (KBR Inc) v Director of the Serious Fraud Office* [2021] UKSC 2, [2022] AC 519.

assistance to lawful investigation. Export control remains applicable; one licence does not silently displace another regime.

Operating without a required licence attracts corporate penalty, director disqualification, profit disgorgement and, for knowing serious conduct, criminal liability. Employees who report concealed unlawful activity receive protected disclosure routes.

The licence must extend beyond export. The Export Control Act 2002 and Export Control Order 2008 control military and dual-use goods, software, technology, trade and technical assistance within their defined scope; arms-export decisions are reviewable, as the litigation concerning exports to Saudi Arabia demonstrates. A managed intrusion service may, however, retain every controlled component within one jurisdiction whilst delivering access or intelligence as an outcome. Strategic licensing should cover development for a client, brokering, managed operation, target support and material maintenance, without treating ordinary penetration testing as warfare.[65]

Legitimate security work requires a clear exclusion. A service performed with the system owner's informed authority, bounded scope, non-destructive methods, vulnerability handling, evidence retention and stop control is not designated merely because the tools are powerful. The exclusion ends where the provider knows that the apparent customer lacks authority, secretly retains access, changes the target class or permits effects outside the tested system.

Government customers must be named within the licensing record even if the public version is redacted. The licensing authority should be able to suspend one client or capability without closing the enterprise; revocation should be available where the provider cannot prevent recurrence. Procurement exclusion and profit disgorgement may deter a corporation more effectively than a fine calculated as a cost of sale.

8.5 Rapid Personal and Infrastructure Orders

Upon reasonable grounds that a person or system is conducting or imminently enabling a serious economic-warfare act, a designated court may issue:

- preservation and identification orders;
- account, domain, credential and payment restraint;
- equipment seizure;
- prohibition upon providing specified service;
- compulsory technical assistance within capability;
- travel and asset restriction where legislation permits;
- an order requiring the controller to exercise a stop function.

An emergency executive order may last for a short defined period where delay presents serious harm, followed by automatic judicial review. Evidence, necessity, scope and collateral effect are recorded. The subject receives notice and opportunity to challenge when compatible with the threat.

The order should target the smallest effective unit. A virtual machine is preferred to a data centre, one account to a platform, a beneficial controller to consumers. Broader action requires proof that narrower action cannot achieve the objective in time.

[65] Export Control Order 2008, SI 2008/3231; *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2019] EWCA Civ 1020, [2019] 1 WLR 5765; *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2023] EWHC 1343 (Admin); Procurement Act 2023; Office of the United Nations High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide* (HR/PUB/12/02, 2012).

Urgency and legality are compatible if the sequence is designed in advance. A duty judge and security-cleared special advocates can be available continuously; the application can identify protected material and a public gist; the initial order can last hours; confirmation can follow upon fuller evidence; the subject can challenge when notice no longer defeats the measure. The case law upon sanctions and secret evidence demonstrates the danger of severe executive restraint without clear statutory words, sufficient reasons and effective review. The answer is not to wait for ordinary listing. It is to enact the words and build the urgent court.[66]

The order jurisdiction ends at non-forcible measures which domestic law can authorise. A court order cannot make a foreign cyber operation or kinetic strike internationally lawful. Where the response authority concludes that an actual or imminent armed attack requires military action, it sends a separate defence certificate to the Prime Minister and Attorney General identifying the international basis, target, necessity, proportionality, precautions, host-State position and expiry. The Strategic Private Capacity Act supplies evidence and control of private assets; it does not amend the Charter.

That separation preserves speed. The same evidential package can move immediately to the defence decision-maker, and a private node can be isolated whilst the force question is considered. It also prevents a low-threshold preservation order from becoming a hidden route to lethal action.

8.6 Response Ladder

The Act should require, but not mechanise, a ladder:

Level	Evidential and harm condition	Illustrative measures
0 — Observe	uncertain signal; no immediate material harm	logging, warning, federated query, voluntary cooperation
1 — Preserve	credible serious incident; evidence at risk	preservation, incident notice, forensic support
2 — Contain	ongoing unauthorised access or impairment	credential isolation, provider order, domestic defensive action
3 — Restrain	identified operator, payer or infrastructure	injunction, seizure, arrest, asset and travel measures, licence suspension
4 — Impose State cost	sufficiently supported foreign responsibility or assistance	attribution, sanctions, diplomatic action, collective measures, lawful countermeasures
5 — Defend against armed attack	actual or imminent armed attack; force necessary and proportionate	force against lawful targets under international law, with distinction and precautions

Escalation is not automatic. A Level 3 action may be more effective than Level 4; a financial incident may demand rapid restraint without satisfying article 51. De-escalation and correction remain possible.

The ladder considers actual harm, maximum reasonably credible foreseeable harm, continuing capability, replication, payer incentives, host cooperation and civilian consequence. Deterrence informs selection amongst lawful measures. The reasons are reviewable.

Each level applies its own legal proportionality. A domestic restraint order asks whether the interference is suitable, necessary and fairly balanced under the empowering statute and protected rights. A countermeasure is limited by the law of State responsibility and directed towards inducing

[66] *Ahmed v HM Treasury* [2010] UKSC 2, [2010] 2 AC 534; *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700; *Youssef v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKSC 3, [2016] AC 1457; *Al Rawi v Security Service* [2011] UKSC 34, [2012] 1 AC 531; Justice and Security Act 2013, pt 2.

compliance. Self-defence is proportionate to halting or preventing the armed attack, not to matching the attacker's expenditure or satisfying anger. International humanitarian law then governs the chosen attack. Writing "proportionate response" once at the top of the form would conceal four different questions.[67]

Collective action can increase firmness whilst reducing breadth. Allied providers may isolate the same contractor accounts; States may coordinate sanctions and export denial; law-enforcement agencies may seize infrastructure in their own territories; a host State may arrest the operator. The payer then encounters cumulative personal and economic cost without a population-wide embargo. Where a direct attack remains necessary, allied evidence and public legal explanation strengthen deterrence by showing that the target was not selected upon one government's assertion alone.

8.7 Continuing Verification and the Wrong-Location Problem

Private capacity makes attribution perishable. An operator may move the attacking process after an order is signed; a cloud scheduler may move it without the operator's knowledge; a service address may identify an ingress point whilst the decision system sits elsewhere. Authority must therefore attach to the proved function and the person who controls it, not to an address which was accurate yesterday.

Every coercive order should carry a verification condition. Before execution, the Authority confirms that the account, credential, workload, device or person remains connected to the conduct described; that the proposed measure still reaches the smallest effective unit; and that no material civilian or allied use has appeared since authorisation. Where an autonomous process migrates faster than human approval, the order may describe an objectively bounded target class, but it must also state machine-verifiable exclusion rules, geographic limits, maximum duration and an immediate stop condition. "Whatever the malware touches" is not a target class.

Verification does not require paralysis. The interval may be seconds for credential revocation, minutes for service isolation and longer before destructive action. What matters is that the evidence has not become ceremonial by the time power is used. If a narrow measure fails because the function migrated, the failure may justify a broader but still discriminating order; it does not justify treating the provider's entire estate as hostile.

An authority which discovers that it acted upon the wrong location must preserve the error, notify affected providers and partners, restore service where practicable, correct public attribution and provide a route to compensation. Error is inevitable in distributed systems; secrecy about error is not. A regime capable of correcting itself quickly will deter more credibly than one which must deny every mistake to preserve the appearance of certainty.

8.8 Four Clocks: Action, Confirmation, Disclosure and Renewal

Safeguards fail when every control is forced to operate before action. The statute should instead use four clocks.

The **action clock** is measured in minutes. A trained duty authority may preserve evidence, pause a credential, maintain an essential civilian service or prevent a designated strategic change where there are reasonable grounds of serious and imminent consequence. The action is reversible so far as the system permits and records the evidence, officer, purpose and expiry.

---

[67] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10, arts 49–54; *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700, [68]–[76]; *Shvidler v Secretary of State for Foreign, Commonwealth and Development Affairs* [2025] UKSC 30; ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Position Paper, November 2019).

The **confirmation clock** is measured in hours. A minister or judge, according to the power, receives the record and either confirms, narrows or ends the action. An intrusive personal order and any measure affecting many uninvolved persons require judicial confirmation; a foreign-policy authorisation requires the responsible minister. Failure to confirm restores the prior position where safe and triggers notice to the overseer.

The **disclosure clock** begins when notice no longer frustrates the operation. The subject receives reasons and a route to challenge; affected providers receive correction obligations; Parliament and the public receive an appropriately redacted account. Closed material may be necessary, but the essence of the case and the existence of the power cannot remain secret merely because secrecy is administratively comfortable. Human-rights jurisprudence upon surveillance and property restraint requires legal foreseeability, effective safeguards and review appropriate to the seriousness of the interference.[68]

The **renewal clock** prevents emergency from becoming ordinary administration. A preservation notice, strategic direction, designation and licence condition each has its own maximum period. Renewal requires evidence that the condition remains, consideration of narrower alternatives and a record of results and error. Parliamentary scrutiny is concentrated upon the statutory architecture, aggregate use, prolonged directions and renewal of the scheme—not placed between the attacking process and the first containment act.

This sequencing fits the United Kingdom's constitutional practice better than either extreme. The executive possesses capacity to act urgently in defence and foreign affairs, but prerogative cannot displace statute and compensation or rights require lawful authority. The convention concerning prior Commons debate on military action is political rather than an inflexible legal condition and recognises that emergency may make prior debate impossible. The proposed Act does not create a parliamentary veto over immediate containment; it creates statutory authority, ministerial ownership, judicial control of coercive orders and retrospective democratic account.[69]

9. Objections

The first objection is that designation will chill innovation. It may if drafted by technology name. Functional thresholds, review, emergency safe harbour and proportionate duties reduce that risk. A company whose system can decide a battle already bears unusual political risk; pretending otherwise does not preserve innovation.

The second is that government will misuse continuity powers to compel corporate support for an unlawful war. The answer is a legal-basis certificate, judicial review, parliamentary reporting, protected whistleblowing and no immunity for manifest illegality. Private discretion is not made safer by public discretion; each requires constraint.

The third is that a controller may relocate. Connection rules, allied licensing, procurement and market access reduce avoidance. Complete prevention is impossible. A law need not capture every actor to remove the assumption that British-controlled strategic capacity is ordinary property.

---

[68] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) arts 6 and 8 and Protocol No 1, art 1; Human Rights Act 1998; *Big Brother Watch and Others v United Kingdom* (2022) 74 EHRR 17; *Centrum för rättvisa v Sweden* [GC] App no 35252/08 (25 May 2021); *Roman Zakharov v Russia* [GC] App no 47143/06 (4 December 2015); *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson and others* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* (Case C-623/17) EU:C:2020:790.

[69] Cabinet Office, *The Cabinet Manual* (1st edn, October 2011) paras 5.36–5.38; House of Commons Public Administration Select Committee, *Taming the Prerogative: Strengthening Ministerial Accountability to Parliament* (HC 422, 2003–04); House of Lords Constitution Committee, *Waging War: Parliament's Role and Responsibility* (HL 236-I, 2005–06); *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5, [2018] AC 61, [45]–[56].

The fourth is that personal orders and direct cyber measures violate sovereignty. They can. The statute must specify that foreign action requires consent, applicable agreement, lawful countermeasure, necessity, self-defence or another recognised basis. Domestic urgency does not amend international law.

The fifth is that the theory glorifies billionaires by calling them sovereign. The term is critical, not honorific. It describes power without the legal status or public mandate which ought to accompany it. The remedy is to return the decision to law.

The sixth is that hard response to monetary attacks will escalate. Weak and indiscriminate response can also escalate by inviting repetition and harming innocents. The answer is evidence, individualisation, credible thresholds and a ladder which can be firm without beginning at force.

The seventh is that maximum foreseeable harm permits speculation. The requirement of reasonable credibility, technical access, signed assumptions and contrary evidence disciplines it. Refusing to consider foreseeable lethal consequence until realised is not neutrality; it is an assumption in favour of the attacker.

The eighth is that a private individual should be free to assist a victim of aggression. He may advocate, donate ordinary aid and seek rapid strategic authorisation. Where his asset supplies military capacity and exposes others to retaliation, freedom of property no longer answers the public question. The State may approve. It must own the choice.

10. Conclusion

The private sovereign is produced when strategic capacity, personal discretion and public absence coincide. Wealth matters because it purchases the capacity; technology matters because it makes the decision immediate; corporate form matters because it divides consequence from control. None alone is the category.

Starlink demonstrates both the good which private action may do and the constitutional danger of allowing one owner to decide. Its early activation preceded later publicly documented arrangements. Ukraine was entitled to request defence assistance, but that entitlement did not turn a bank account into public authority. A reciprocal legal order must ask how it would judge the same intervention by an unfriendly proprietor.

PMSCs, commercial intrusion vendors, targeting firms, platforms and infrastructure providers distribute the same problem. Voluntary codes, export control, corporate duty, sanctions and cybercrime law address fragments. They do not create one fast rule for the moment private service becomes strategic action.

The response should not strip the actor of personhood. A hostile private operator remains protected by law. In armed conflict his function may render him directly participating or continuously combatant; his infrastructure may become a military objective if the legal definition is met. Outside armed conflict arrest and restraint remain primary. Force requires the independent international rules, including armed attack, necessity, proportionality, distinction and precautions.

Firmness lies in having lawful measures which reach the operator and payer. A poor hacker may ignore an asset freeze, but he depends upon systems, credentials, collaborators and place. A State which pays him may ignore one indictment, but not necessarily coordinated economic, diplomatic and technical cost. An autonomous system may feel nothing, but its infrastructure can be isolated and its controller held.

The Strategic Private Capacity Act would designate indispensable services, identify control, require authorisation and manifests, license high-risk PMSCs and intrusion capability, and permit rapid personal and infrastructure orders. Its response ladder treats actual and maximum reasonably credible foreseeable harm, including replication, without pretending that deterrence alone creates a right of force.

The older social contract did not promise that all power would be public. It promised that private judgement would not hold the common safety at its pleasure. A society which allows one proprietor to enter, alter or withdraw from a foreign war because he owns the switch has restored the very condition public authority was meant to end.

Bibliography

Books, Chapters and Articles

Avant DD, *The Market for Force: The Consequences of Privatizing Security* (CUP 2005)

Berge JV, 'Ground Control to Elon Musk: Stability Implications of Satellite Mega-constellations' (2026) *European Journal of International Security* 1 https://doi.org/10.1017/eis.2026.10047

Bethlehem D, 'Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors' (2012) 106 *American Journal of International Law* 770

Buchan R, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 *Journal of Conflict and Security Law* 429

Cardellini Leipertz R, 'From Imagery to Targeting: Commercial Satellite Support in War' (Lieber Institute, 27 May 2026) https://lieber.westpoint.edu/imagery-targeting-commercial-satellite-support-war/ accessed 6 August 2026

Chesterman S and Lehnardt C (eds), *From Mercenaries to Market: The Rise and Regulation of Private Military Companies* (OUP 2007)

Chirwa DM, 'The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights' (2004) 5 *Melbourne Journal of International Law* 1

Clancy P, 'Neutral Arms Transfers and the Russian Invasion of Ukraine' (2023) 72 *International and Comparative Law Quarterly* 527

Coco A and de Souza Dias T, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 771

Cohen JE, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019)

Corten O, *The Law Against War* (2nd edn, Hart 2021)

Dinniss HH, *Cyber Warfare and the Laws of War* (CUP 2012)

Douek E, 'Content Moderation as Systems Thinking' (2022) 136 *Harvard Law Review* 526

Gray C, *International Law and the Use of Force* (4th edn, OUP 2018)

Hathaway OA and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817

Heintschel von Heinegg W, 'Benevolent Third States in International Armed Conflicts: The Myth of the Irrelevance of the Law of Neutrality' in Michael N Schmitt and Jelena Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines* (Martinus Nijhoff 2007) 543

Hobbes T, *Leviathan* (Richard Tuck ed, CUP 1996)

Independent International Commission on Kosovo, *The Kosovo Report: Conflict, International Response, Lessons Learned* (OUP 2000)

Isaacson W, *Elon Musk* (Simon & Schuster 2023)

Jensen ET and Watts S, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017) 95 *Texas Law Review* 1555

Kaye D, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019)

Libicki MC, Senty D and Pollak J, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (RAND Corporation RR-430, 2014)

Maurer T, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018)

Pasquale F, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Belknap Press 2020)

Percy S, *Mercenaries: The History of a Norm in International Relations* (OUP 2007)

Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP 2014)

Schmid E and Erceiş AÖ, ‘The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility’ (2023) 33 *Swiss Review of International and European Law* 577

Schmitt MN (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017)

Schmitt MN, ‘International Law and Military Operations in Space’ (2006) 10 *Max Planck Yearbook of United Nations Law* 89

Singer PW, *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell University Press 2003)

Stern PJ, *The Company-State: Corporate Sovereignty and the Early Modern Foundations of the British Empire in India* (OUP 2011)

Thomson JE, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe* (Princeton University Press 1994)

Tladi D, ‘The Use of Force in Self-Defence against Non-State Actors, Decline of Collective Security and the Rise of Unilateralism’ in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) 287

Tonkin H, *State Control over Private Military and Security Companies in Armed Conflict* (CUP 2011)

Wentker A, ‘The Armed Attack Exception to Neutrality’ (2024) 73 *International and Comparative Law Quarterly* 963

Wood M, ‘International Law and the Use of Force: What Happens in Practice?’ (2013) 53 *Indian Journal of International Law* 345

Zugliani N, ‘The Supply of Weapons to a Victim of Aggression: The Law of Neutrality in the Light of the Conflict in Ukraine’ (2024) 35 *European Journal of International Law* 389