Economic Warfare after the Embargo: Private Capital, Strategic Infrastructure and the Democratisation of Hostile Power

Supplementary Paper 1

Christopher I. V. Farmer

Publication edition, August 2026

Contents

Abstract

Economic warfare is still too often described by reference to embargo, blockade, tariff and the deliberate exhaustion of a national treasury. Each remains important, but the definition belongs to an age in which the State ordinarily possessed the machinery required to make its economic choice strategically decisive. That factual monopoly has gone. A private company may now restore communications to a belligerent within hours, withhold coverage over an intended theatre, sell persistent satellite observation purchased by public subscription, or place cloud, data and machine decision systems between a weapon and the State which employs it. The capital required to influence war is no longer always public; the decision is no longer always ministerial; the resulting danger is nonetheless borne by citizens who never voted for it.

This paper uses the provision of Starlink communications and ICEYE synthetic-aperture radar capability to Ukraine as the principal, but not exclusive, case study. It finds that Starlink was activated on 26 February 2022 in response to a direct public request by a Ukrainian minister, before the later United States procurement and Department of Defense arrangements which regularised portions of the service. That speed was of immense practical value. It also exposed the constitutional problem: a private controller of strategic infrastructure acquired the practical capacity both to enter and to delimit a war, whilst governments, soldiers and civilians became dependent upon a service whose first legal foundation lay in ownership and contract.

The paper does not accept that Ukraine’s absence from NATO deprived other States of a right to assist it. Article 51 of the United Nations Charter recognises collective self-defence, and the law does not require a pre-existing mutual-defence treaty where the victim State declares an armed attack and requests assistance. Nor does the presence of Russian-speaking or self-identifying Russian communities within Ukraine create a Russian title to Ukrainian territory or an unrestricted right of forcible protection. Russia advanced arguments of individual and collective self-defence; those arguments must be stated fairly, particularly against the West’s contested precedents in Kosovo, Iraq, Libya and Syria, but comparison is not legal equivalence and hypocrisy does not repeal article 2(4).

The comparison nevertheless matters. Repeated resort to elastic doctrines, proxy support and private infrastructure makes restraint less credible when the same methods return against Western forces. The paper calls this the reciprocity trap. It proposes a functional definition of private economic participation in hostilities; advance public control over systemically important dual-use services; personal and corporate duties for strategic infrastructure controllers; compensation and indemnity rules preventing the private socialisation of retaliatory risk; and a mirror-image legality assessment requiring Ministers to state whether they would accept the asserted rule if used by an adversary. A keyboard, satellite link or privately funded sensor may be a weapon where its function and effects are equivalent to one. Law which refuses to see the function will regulate the nineteenth-century instrument and leave the twenty-first-century war to private discretion.

Keywords

Economic warfare; strategic private infrastructure; Starlink; commercial space; collective self-defence; neutrality; cyber operations; critical national infrastructure; corporate control; emergency powers.

Table of Cases

Table of Legislation

Table of Treaties and International Instruments

Table of Official and Technical Materials

Attorney General's Office, 'Attorney General's Speech at the International Institute for Strategic Studies' (11 January 2017)

Australian Government, 'Australia's Position on How International Law Applies to State Conduct in Cyberspace' (2021)

Cabinet Office, *The Cabinet Manual* (1st edn, 2011)

Cabinet Office, 'Critical National Infrastructure' (updated 2026)

Cabinet Office, *The National Cyber Strategy 2022* (CP 643, 2022)

Cabinet Office, 'National Security and Investment Act 2021: Statement for the Purposes of Section 3' (updated 17 November 2025)

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

Cybersecurity and Infrastructure Security Agency, 'MAR-17-352-01 HatMan—Safety System Targeted Malware' (18 April 2018)

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

Department for Science, Innovation and Technology, 'Incident Reporting' (updated 30 June 2026)

Department for Science, Innovation and Technology, *UK Telecommunications Resilience Guidance* (updated 3 April 2024)

Department of Health and Social Care, 'Synnovis Cyber Attack' (Written Statement HCWS1046, 12 November 2025)

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

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

Government Offices of Sweden, *Position Paper on the Application of International Law in Cyberspace* (July 2022)

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

Group of Governmental Experts, 'Report on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174

House of Commons Foreign Affairs Committee, *Libya: Examination of Intervention and Collapse and the UK's Future Policy Options* (HC 119, 2016–17)

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)

ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts* (2021)

ICRC, *Business and International Humanitarian Law* (2006)

ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (34th International Conference, 2024)

ICRC, Australian Red Cross and French Red Cross, *Private Businesses and Armed Conflict* (2024)

Independent International Commission on Kosovo, *The Kosovo Report* (OUP 2000)

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

Ministère des Armées, *International Law Applied to Operations in Cyberspace* (2019)

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

Ministry of Defence, *Joint Doctrine Publication 0-40: UK Space Power* (1st edn, 2023)

National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (HC 414, 2017–19)

National Cyber Security Centre and others, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure' (7 February 2024)

NHS England, 'Synnovis Cyber Incident' (updated 2026)

OECD, *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* (2011)

Open-ended Working Group, 'Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2

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

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

US Government Accountability Office, *Critical Infrastructure Protection* (GAO-24-106221, 2024)

UNGA, *Official Compendium of Voluntary National Contributions on International Law and ICTs* (13 July 2021) UN Doc A/76/136

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)

1. The Definition Has Aged More Quickly than the Threat

The orthodox picture of economic warfare is familiar: one State employs embargoes, sanctions, blockade, monetary pressure or trade restriction to impair the capacity or alter the policy of another.[1] It is a picture drawn from public instruments. The State closes a port, controls exports, freezes reserves or prohibits its subjects from dealing. Even when private merchants are affected, the decisive act is attributed to public authority and its legitimacy may be tested against the Charter, the law of neutrality, the World Trade Organization agreements, sanctions legislation or the law of armed conflict. The actor, instrument and consequence occupy intelligible compartments.

[1] Nils Ole Oermann and Hans-Jürgen Wolff, *Trade Wars: Past and Present* (OUP 2022); TM Hagemeyer-Witzleb, *The International Law of Economic Warfare* (Springer 2021).

That picture is no longer wrong; it is insufficient. Economic power now purchases functions previously obtainable only through sovereign administration or a military-industrial apparatus. Low-Earth-orbit communications, global earth observation, high-performance computing, financial clearing, app distribution, cloud hosting, subsea connectivity, autonomous navigation and commercial intelligence may be controlled by a small number of corporations and, sometimes, by one controlling shareholder. An actor need not close the enemy's ports if he can make its logistics visible; need not command artillery if he can provide the data by which another selects and strikes; need not sign a treaty if a click can restore the communications upon which the belligerent's command depends. The economic act is the provision, denial or modulation of a strategic function. Its immediate form is contract or charity. Its foreseeable consequence may be victory, defeat or escalation.

This is not a semantic attempt to call every important business decision warfare. The definition requires limiting elements. First, the private act must provide, withhold or manipulate a capability indispensable or materially significant to coercion, military operations or the sustained functioning of protected critical systems. Secondly, the controller must know, intend or be reckless as to the strategic function, not merely know that a product is capable of dual use. Thirdly, the act must possess a sufficient nexus to an actual confrontation, coercive campaign or armed conflict. Finally, law must distinguish participation from ordinary supply: selling food in a global market is not the same act as furnishing target-quality imagery for identified military objectives; providing a general communications service is not invariably the same as extending or withdrawing coverage in answer to an intended attack.

The resulting category is **private economic participation in strategic coercion**. It describes the use of privately controlled capital, infrastructure or information to enable, condition or frustrate coercive action whose scale was traditionally associated with States. The category may intersect with direct participation in hostilities, complicity, export control, sanctions, neutrality, State responsibility, corporate crime and ordinary contract without being reducible to any one of them. It is a regulatory definition before it is a status under international law.

The importance of this distinction can be seen in a simple comparison. A billionaire's donation of blankets to civilians is neither an act of war nor private foreign policy merely because it occurs during war. A billionaire's unilateral extension of a communications network which becomes the backbone of battlefield command is different in kind, even where it also saves civilian life. The difference is not moral condemnation. It is capability, reliance, knowledge and effect. The legal question is not whether the benefactor's sympathies are admirable; it is why personal title to shares should carry the competence to alter the military position of States and expose other persons to consequences which they did not authorise.

The developed North is especially vulnerable because it combines concentrated private infrastructure with open economies, digitised public services and an assumption that private commercial continuity will survive political conflict. The same arrangement that permits rapid innovation permits rapid coercion. The individual controller has leverage over governments; a foreign actor has leverage over the controller; and the public discovers, after dependence has formed, that neither procurement law nor constitutional practice asked who may turn the capability off.

1.1 Economic Warfare after the Embargo

The older definition was made by the visible instrument. An embargo appeared in a decree; a blockade appeared upon a coast; a sanction appeared in a list. Its legal character could be disputed, but its authorship was ordinarily known. The modern instrument is more often a dependency which has been constructed in peace and discovered in war. A State may possess the formal right to communicate, navigate, clear payment or observe its territory whilst lacking the privately controlled system without

which that right has little practical value. Economic warfare has, in this sense, moved from the prohibition of exchange to the government of access.

The change is evolutionary rather than absolute. The economic weapon of the inter-war period was itself presented as an alternative to battle and became entangled with collective security, civilian deprivation and the political hope that finance could compel where armies need not.[2] Blockade and prize law had already made private cargo, credit, insurance and destination questions of public war. The Crown's wartime claim to seize a neutral cargo in *The Zamora* was not accepted merely because executive officers invoked necessity: the Privy Council insisted that prerogative be exercised according to law, and that the court could not surrender property upon an unproved assertion of danger.[3] The lesson is not that old doctrine answers Starlink. It is that private property became strategically decisive before, and legal control followed consequence rather than commercial description.

Embargo has nevertheless become an incomplete paradigm for three reasons. First, denial is no longer the only coercive act. Selective provision may decide as much as deprivation. A communications service supplied to one belligerent, an intelligence feed restricted to one customer or a cloud service configured for one government may alter the relative capacity of both sides without forbidding a single trade. Secondly, the capability may remain under the provider's hand after delivery. The supplier of coal could not ordinarily alter its calorific value at sea; the supplier of software may change permissions whilst the system is in use. Thirdly, market concentration permits a private controller to create facts which governments must afterwards regularise. The State no longer always commands the economic weapon. It may negotiate with its owner after the weapon has been employed.

The proper unit of analysis is consequently the **strategic function**, not the product. Communications, observation, authentication, computation and payment are verbs before they are industries. One enterprise may perform several; one function may be divided amongst enterprises. Regulation by corporate label invites evasion because the same effect can be sold as a terminal, subscription, application programming interface, data licence, managed service or charitable access. A statute concerned with economic warfare must ask what the arrangement permits a person to do, what would happen if it stopped, how quickly it can be replaced, and who retains the power of alteration.

That approach is not alien to existing public law. The National Security and Investment Act 2021 looks through ordinary acquisition form where control over sensitive entities or assets may create national-security risk; current guidance expressly identifies communications, data infrastructure, artificial intelligence, defence and satellite or space technology amongst the connected fields which may require scrutiny.[4] Critical-infrastructure policy likewise treats communications, energy, finance, health, space, transport and water as interdependent national functions rather than ordinary markets.[5] What is missing is the corresponding rule for strategic use after acquisition: the law may examine who buys the company, yet remain silent when the controller deploys its capability into an armed conflict.

The omission matters because corporate responsibility instruments are principally standards of conduct, not allocations of constitutional competence. The United Nations Guiding Principles on Business and

---

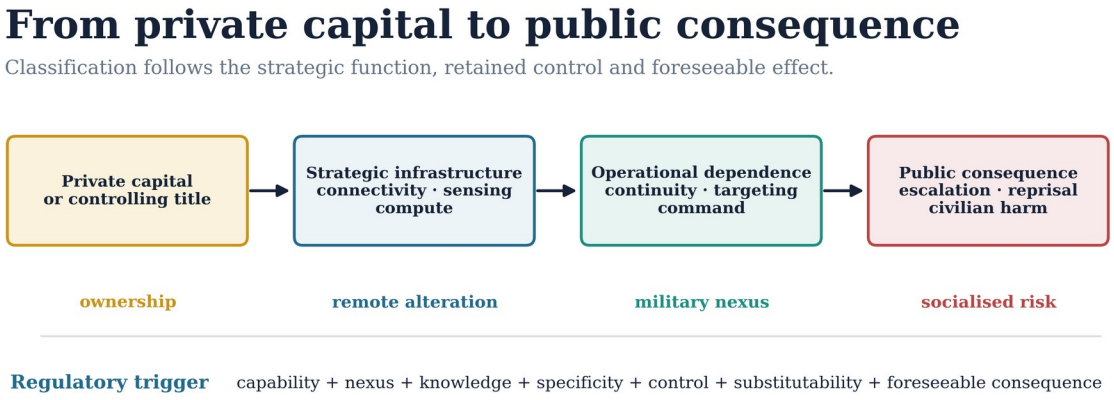
[2] Nicholas Mulder, *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War* (Yale University Press 2022) 1–15, 289–95; Joy Gordon, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2010) 1–21; Tor Egil Førland, 'The History of Economic Warfare: International Law, Effectiveness, Strategies' (1993) 30 *Journal of Peace Research* 151.

[3] *The Zamora* [1916] 2 AC 77 (PC) 90–92, 107–08.

[4] National Security and Investment Act 2021, ss 1–3, 6 and 26; Cabinet Office, 'National Security and Investment Act 2021: Statement for the Purposes of Section 3' (updated 17 November 2025) https://www.gov.uk/government/publications/national-security-and-investment-statement-about-exercise-of-the-call-in-power/national-security-and-investment-act-2021-statement-for-the-purposes-of-section-3 accessed 31 July 2026.

[5] Cabinet Office, *Summary of the 2025 Sector Security and Resilience Plans* (2026); Cabinet Office, 'Critical National Infrastructure' https://www.gov.uk/government/collections/critical-national-infrastructure accessed 31 July 2026; Cabinet Office, *The National Cyber Strategy 2022* (CP 643, 2022) 18–22.

Human Rights require businesses to avoid causing or contributing to adverse human-rights impacts and to address impacts directly linked through business relationships; the OECD Guidelines similarly extend risk-based due diligence through operations, products and services.[6] They supply valuable disciplines of knowledge, leverage and remediation. They do not decide whether an individual proprietor may lawfully place a strategically indispensable service at a belligerent's disposal before his own government has determined the State's legal position, nor who must keep that service operating after soldiers and hospitals rely upon it.



This paper therefore uses "democratisation" descriptively and critically. Capability has spread beyond the State, but political authority has not thereby been shared equally amongst citizens. It has accumulated in those able to purchase infrastructure or control code. The result is less the democracy of hostile power than its retail availability to a narrow private class. A crowdfunding campaign may distribute payment across thousands; the charity's trustees still decide the purchase. Millions may buy products from an entrepreneur's companies; voting control remains concentrated. A government may welcome the result, yet welcome is not the same thing as prior authority.

The definition must remain narrow enough to preserve ordinary commerce. Size alone cannot suffice: a large cloud company may provide routine service without knowledge of a hostile use, whilst a small analytics firm may knowingly supply target-quality output for one operation. Political opinion cannot suffice: sympathy, nationality and public speech are neither weapons nor reliable evidence of operational contribution. The cumulative indicia should be capability, nexus, knowledge, specificity, control, substitutability and foreseeable consequence. Where those indicia are weak, ordinary commercial law remains. Where they are strong, the decision has become public in effect and should acquire public duties before catastrophe supplies the regulator's first notice.[7]

2. From Merchant Neutrality to Platform Belligerency

Private commerce has never been absent from war. Merchants financed armies, insurers priced belligerent voyages, banks supplied credit and shipowners ran blockades. Fraser, Trenholm & Co acted as banker to the Confederacy and converted cotton into the means by which arms could be purchased; prize litigation in *The Bermuda* examined cargo and destination through the legal architecture of

[6] 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; OECD, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (OECD Publishing 2023) chs II and IV.

[7] Department for Science, Innovation and Technology, *UK Telecommunications Resilience Guidance* (updated 3 April 2024) https://www.gov.uk/government/publications/electronic-communications-resilience-and-response-group-ec-rrg/uk-telecommunications-resilience-guidance accessed 31 July 2026; Ofcom, *Connected Nations 2025: UK Report* (2025) 80–96.

blockade.[8] The East India Company demonstrates a more extreme historical conjunction of corporate charter, territorial administration and force. Private power is therefore old.

What is new is the speed, granularity and continuing control of the service. The merchant who delivered a rifle ordinarily surrendered physical control when delivery was complete. A platform may alter permissions after deployment, geofence use, change software, prioritise users, observe traffic, supply updates, or withdraw service at a decisive hour. One corporation may become a continuing participant in the operational chain without owning the missile or employing the soldier. Its influence is not exhausted by sale; it is exercised through remote technical governance.

That continuing relationship also defeats the easy division between a neutral supplier and a belligerent operator. Neutrality law developed through rules concerning territory, troops, war material, communications and impartiality, but much of it presumes a State's ability to control what occurs within its territory and a comprehensible movement of tangible goods.[9] A satellite constellation is distributed; a terminal may move; the service may be administered from one country, owned through another and used from a third. Cloud processing may occur wherever capacity is available. The relevant act may be a remote permission issued by an engineer following a private executive's instruction. The company is not a neutral State and cannot itself violate every duty of neutrality, yet its conduct may affect whether its home State remains outside the conflict, whether an export is controlled, whether a service is a military objective and whether assistance is attributable.

The phrase "platform belligerency" should not be mistaken for a new status under IHL. It describes a fact: strategic platforms may choose rules of access whose effects align them with one side, whilst lacking the public mandate, command discipline and international personality of the State. Their employees remain protected or targetable according to existing law; the company remains a legal person under domestic systems; the service may become a military objective only if article 52(2) of Additional Protocol I or the corresponding customary rule is satisfied.[10] The descriptive term exposes the gap between functional participation and institutional form.

The gap creates asymmetric freedom. A State's armed force ordinarily receives legal advice, rules of engagement, political direction, targeting procedures, audit and legislative appropriation. A private controller may be restrained by licence, contract, directors' duties, export control and criminal law, but none necessarily answers the strategic question: may this person place a country's forces within, or remove them from, a capability upon which military operations depend? The director may claim that commercial terms prohibit offensive use; the customer may claim an inherent right of self-defence; the State of incorporation may prefer silence; the public may assume that someone else decided.

The law should not respond by prohibiting every private service to a victim of aggression. That would reward the attacker and disable civilian resilience. It should instead recognise that the greater the operational dependency and remote discretion, the weaker the argument that ordinary private ordering is sufficient. Where the service is capable of deciding whether a campaign proceeds, prior public rules are necessary: conditions for initiation, geographical scope, modification, suspension, government requisition, compensation, audit and termination. The objective is not to make technology slow. It is to make the allocation of sovereign risk public before speed makes a private decision irreversible.

---

[8] *The Bermuda* 70 US (3 Wall) 514 (1865); National Museums Liverpool, 'Fraser, Trenholm and Company' https://www.liverpoolmuseums.org.uk/artifact/fraser-trenholm-and-company accessed 31 July 2026.

[9] 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 4–5, 8; 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).

[10] 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.

2.1 A Functional Taxonomy

A legal framework will fail if it groups every private contribution beneath one prohibition. Five functions should be distinguished.

The first is **civilian sustenance**: food, medicine, shelter, ordinary communications and financial services supplied for civilian use. These acts may be regulated by sanctions, counter-terrorism rules and humanitarian exemptions, but their object is preservation rather than strategic participation. The second is **general dual-use supply**: a product or service sold upon ordinary terms, capable of civilian and military use, without adaptation to an identified operation. Knowledge increases as the supplier learns of use, but capability alone cannot make every manufacturer a participant.

The third is **operational enablement**: communications, imagery, computation, intelligence or navigation deliberately supplied or configured for a belligerent's military operations. The provider need not select a target. Its service may be an indispensable link without which target selection, command or employment cannot occur. The fourth is **operational control**: the continuing capacity to permit, deny or alter a class of missions through software, geography, authentication, prioritisation or data access. Starlink's geofencing problem belongs here. The fifth is **coercive authorship**: the private actor sets the objective, selects the target class or directs the campaign, even if a State or contractor applies force. At this point the description "supplier" conceals more than it reveals.

The taxonomy prevents two opposite errors. One is guilt by association: a supermarket, consumer or employee becomes responsible for a war because revenue entered the wider corporate group. The other is innocence by fragmentation: every provider describes itself as a mere supplier although, when their functions are joined, they designed, enabled and controlled the operation. Legal consequence should increase with purpose, specificity, indispensable contribution, continuing control and knowledge.

The test must also be temporal. A general service may become operational enablement after the provider configures priority channels for a military customer. A donated terminal may begin as civilian sustenance and become integrated into drone command. An imagery contract may move from situational awareness to target-quality collection. The provider's duties should change when it knows of the transition. Notice from government, technical telemetry, dedicated integration and repeated tailored requests are evidence; nationality or political sympathy is not enough.

This functional method also identifies the appropriate regulator. Civilian sustenance requires humanitarian and sanctions expertise. Dual-use export belongs principally to export-control authorities. Operational enablement requires defence, intelligence and legal assessment. Operational control requires resilience and continuity supervision. Coercive authorship may require criminal investigation and the law governing participation in hostilities. A single economic-warfare authority may coordinate them, but it should not pretend that one legal consequence fits every function.

The taxonomy should appear in statute because private actors require notice. "Material support" and "national interest" are tempting phrases in emergency legislation; without elements they permit political designation after the event. The statute should state the function, mental element, nexus and consequence. Where criminal liability is proposed, intention or knowledge should be required and the prohibited operation identified. Where continuity regulation is proposed, objective designation and an appeal suffice. Precision is compatible with strength. Indeed, a law which can survive an adversarial court is a stronger deterrent than a ministerial threat no company expects to endure review.

3. Starlink: Assistance before Contract

The chronology matters because the constitutional point disappears if later procurement is projected backwards. On 26 February 2022, two days after the full-scale invasion, Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, publicly asked Elon Musk to provide Starlink stations. Musk replied that evening: "Starlink service is now active in Ukraine. More terminals en route."[11] The first practical decision was therefore neither a NATO resolution nor the performance of a pre-existing United States defence contract. It was a rapid private response to a minister of the attacked State.

That fact should not be embellished into the proposition that SpaceX alone supplied or paid for the entire system. The United States Agency for International Development later partnered in delivery. Its Inspector General found that, in March 2022, USAID delivered 5,175 terminals: it purchased 1,508 and transported 3,667 donated by SpaceX, with private funding supporting the donated units.[12] The transfer agreement of 11 April 2022 placed legal and financial responsibility for safety and use upon Ukraine's State Service of Special Communications and Information Protection. Other governments and private donors supplied further terminals and service. By June 2023 the United States Department of Defense had entered a contract for Starlink services in Ukraine, a fact publicly confirmed by the Pentagon although operational and financial details were withheld.[13]

The sequence proves the constitutional point more strongly than a general allegation that the United States ordered the first intervention. The capability was activated before the regularising instruments. Public procurement followed reliance. Government entered after private infrastructure had become important, and in part because the risk of withdrawal or private limitation could no longer be treated as an eccentricity. What begins as generosity may become critical dependence before lawyers can identify which public body has authority to guarantee continuity.

The system served civilian and military functions. The USAID Inspector General records its role in restoring internet access, maintaining communications among officials and emergency services, piloting drones, targeting artillery and battlefield communications.[14] "Internet access" is therefore descriptively true and strategically incomplete. A service that carries evacuation messages and artillery coordinates is dual-use in the strongest sense: neither its civilian benefit nor its military contribution can be erased to simplify argument.

Control persisted after delivery. Coverage, terms and anti-abuse measures could influence use. Reporting concerning Crimea in 2023 produced a dispute as to whether Musk ordered a shutdown or declined a request to activate coverage for an attack; the distinction is factual and important, but either version establishes private control over the boundary of military use.[15] In July 2025 Reuters reported, upon interviews with people said to possess direct knowledge, that Musk had ordered deactivation affecting more than one hundred terminals during a Ukrainian counter-offensive in late September 2022; SpaceX called the reporting inaccurate.[16] Publication should retain the journalism and its denial,

---

[11] 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).

[12] 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 page gives 3,667 donated terminals; one passage in the PDF appears as 3,677, but 1,508 plus 3,667 reconciles to the stated total of 5,175.

[13] 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.

[14] USAID Office of Inspector General (n 12) 1–2.

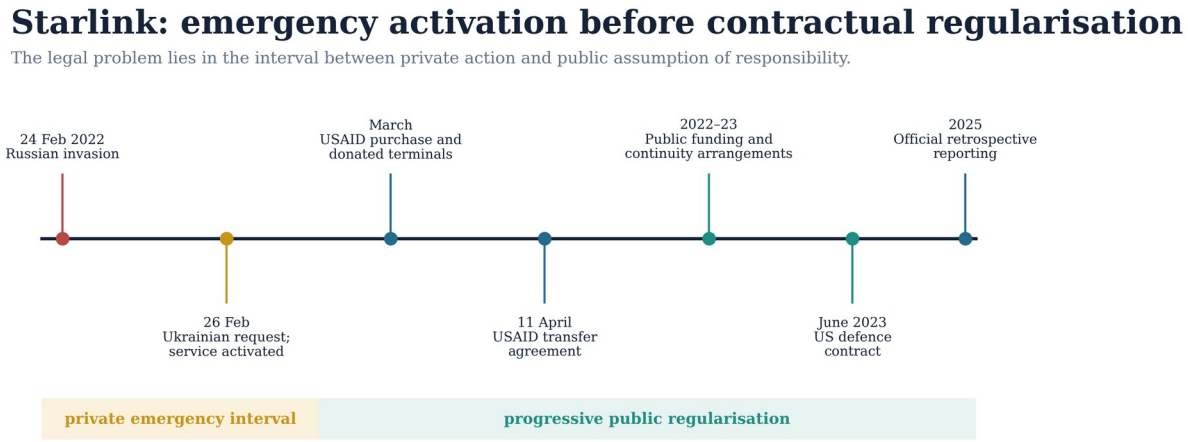
[15] Victoria Kim, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' *The New York Times* (8 September 2023); Walter Isaacson, *Elon Musk* (Simon & Schuster 2023) 431–35.

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

because the allegation concerns the very power under examination and has not been adjudicated. The certain proposition is narrower and sufficient: SpaceX could technically condition availability, knew of military reliance and asserted authority to prevent uses it considered offensive.

The usual defence is property. SpaceX built the constellation; no government was immediately willing or able to supply an equivalent; the company was entitled not to have its service weaponised beyond agreed purposes. Each proposition has force. Property, however, answers who owns the asset, not who should possess unreviewable competence over a foreign war after the asset has become operationally indispensable. A private hospital owns machines upon which life depends but is regulated for that reason. A clearing bank owns systems whose failure can imperil an economy and is subjected to continuity obligations. Strategic communications in war cannot become constitutionally less important because their owner is technically brilliant.

Nor does later contracting cure the original problem. A contract can specify service levels, permitted uses, indemnities and governmental authority; it does not retrospectively authorise the first intervention, nor necessarily govern privately donated terminals, foreign-purchased service or all geofencing decisions. It may also be secret where operational security is invoked, preventing the public from knowing whether a private controller retains material discretion. The correct lesson is not that contract is useless. It is that a public framework must exist before emergency dependence, specifying when contract is enough and when statutory continuity, requisition or direct governmental control must follow.



4. Private Sensors, Foreign Servers and the Unseen Operational Chain

Starlink is visible because the controlling individual is famous. The broader phenomenon is quieter. On 18 August 2022 the Finnish company ICEYE announced a contract with the Serhiy Prytula Charity Foundation providing the Government of Ukraine with the full capabilities of one synthetic-aperture radar satellite already in orbit and access to the wider ICEYE constellation. The satellite remained operated by ICEYE; the Ukrainian Armed Forces received radar imagery of critical locations with high revisit frequency.[17] Public fundraising thereby purchased a sovereign military intelligence function from a private foreign company.

[17] 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.

This example corrects two misconceptions. First, the legal relationship was a contract; it was not literally the absence of any agreement. The constitutional concern is that the agreement was private and charitable rather than an inter-State treaty or appropriated governmental programme. Secondly, ICEYE did not simply place a "Finnish server" in the missile as if nationality alone explained the targeting chain. It supplied a privately operated sensing capability from Finland to the Ukrainian Government. Imagery might then be analysed, combined and transmitted through other services before contributing to selection, verification or assessment of a target. The distributed chain, not a slogan about one server, is the point.

A contemporary operational chain may contain at least seven functions: collection; communications; storage; analytics; target development; navigation or command; and weapons employment. Different companies and States may control each. One business collects synthetic-aperture radar imagery; another hosts it; a third supplies algorithmic detection; a fourth provides secure communications; a PMSC integrates intelligence; a State officer approves the target; a drone operated through yet another network applies force. If harm follows, each actor may truthfully say it performed only one part. The victim sees one effect. Jurisdiction sees fragments.

The law has tools for parts of this chain. Export controls may treat equipment, software or technical assistance as dual-use or military items. The Arms Trade Treaty regulates listed conventional arms and requires export assessment, but it does not supply a general code for cloud processing or satellite service.[18] IHL regulates targeting by parties to armed conflict and may make a civilian object a military objective when its nature, location, purpose or use effectively contributes to military action and its destruction offers a definite military advantage. Corporate officers may incur criminal responsibility if the elements of aiding or abetting an international crime are satisfied in a competent jurisdiction. State responsibility may arise if private conduct is attributable under articles 5, 8 or 11 of the ILC Articles, or if State aid or assistance satisfies article 16.[19] None automatically places the entire service chain beneath one public decision.

The problem becomes greater as machine systems select what humans previously selected. A commercial analytics service may identify likely military objects within thousands of images; a human may approve a class of objects rather than each coordinate; a weapons system may use updated information after launch. The provider may insist that it supplied "data", whilst the operator insists that it made the decision. Responsibility need not be exclusive. The legal framework should ask who established the objective, supplied indispensable capability, selected constraints, could intervene, knew the intended use and profited from continuation.

Those questions apply beyond Ukraine. Commercial satellite providers have supported public understanding of troop movements, exposed atrocities and countered disinformation; cloud providers sustain public administration under attack; telecommunications companies reconnect civilians. The law must preserve these benefits. The error is to assume that because an activity is beneficial in one war, no general rule is required. Rules are needed precisely because a Chinese, Russian, Gulf or private actor may use the same model to supply a party whom the United Kingdom considers an aggressor, a proxy or a threat. If the West's legal position depends upon the identity of the beneficiary, it is a policy preference masquerading as law.

4.1 Money, Philanthropy and the Purchase of a Public Function

The charitable form is particularly difficult because it joins democratic sympathy to private direction. The Serhiy Prytula Charity Foundation raised money from members of the public who intended to

[18] Arms Trade Treaty (adopted 2 April 2013, entered into force 24 December 2014) 3013 UNTS 269, arts 2, 6 and 7.

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

support Ukrainian defence. The resulting ICEYE agreement transferred the use of a sovereign-quality capability to government. Public generosity performed a procurement function without the legislature of the provider's State choosing the mission, appropriating the money or debating the escalation risk.

There is nothing inherently unlawful in that arrangement. Individuals may donate; charities may purchase lawful goods; companies may contract; Ukraine may acquire means of defence. The constitutional point concerns scale and category. If public subscription may acquire satellites, drone fleets, autonomous systems or offensive cyber capability, charity regulation drawn principally to ensure proper purpose and honest accounting is no longer sufficient. The regulator must ask whether the charity has become an arms procurer, intelligence intermediary or strategic service controller.

Traditional export control partially answers the question. A licence can regulate the transfer of listed equipment, software or technology and impose end-use conditions. Services and data complicate the model because nothing tangible need cross the border, capability may remain operated by the foreign supplier, and the customer may receive access rather than title. An export-control regime should therefore attend to **function as a service**. Persistent target-quality sensing, command connectivity and autonomous mission support should be assessed by capability and intended use, even where the provider retains every physical asset.

Payment also affects control. A gift may appear to confer freedom upon the recipient, yet the donor or provider may retain technical conditions. A government contract may make control more public, but secret terms may leave discretion with the firm. Crowdfunding may distribute finance among thousands while concentrating decision in trustees. The relevant issue is not who contributed the last pound; it is who possesses the legal and technical power to specify use.

The risk of evasion is obvious. A wealthy individual could fund a charity; the charity could contract with a company in a second State; the company could provide access through a subsidiary in a third; data could be processed in a fourth; and a PMSC could integrate it for the belligerent. Each transaction may fall below a different threshold. A statutory "strategic procurement" concept should permit regulators to examine connected arrangements where there is common purpose, coordinated timing or a controller, whilst protecting genuine independent donations from guilt by aggregation.

Public authorities should publish an annual classified and unclassified account of privately financed strategic capability supplied from their jurisdiction to armed conflicts. The unclassified portion need not reveal coordinates, performance or users; it should identify categories, value bands, licensing grounds and whether government assumed continuity obligations. Secrecy concerning an operation may be necessary. Permanent ignorance concerning the existence of private war infrastructure is not.

4.2 Commercial Space and Distributed Sovereign Responsibility

Commercial space makes the constitutional defect unusually plain because international law already refuses to treat private operation as wholly private. Article VI of the Outer Space Treaty requires States Parties to bear international responsibility for national activities in outer space, whether conducted by governmental agencies or non-governmental entities, and requires authorisation and continuing supervision of the latter. Article VII and the Liability Convention address international liability for damage caused by space objects; the Registration Convention attaches public registration duties to objects launched into orbit.[20] These rules do not attribute every customer's battlefield decision to the licensing State, nor do they make the State criminally responsible for each image sold. They do

[20] 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 VI, VII and IX; 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, arts II–III; Convention on Registration of Objects Launched into Outer Space (opened for signature 14 January 1975, entered into force 15 September 1976) 1023 UNTS 15, arts II–IV.

establish that incorporation and private ownership do not remove a national space activity from public international concern.

There is a consequential mismatch between licensing and operational use. A launch or operator licence ordinarily asks whether an activity is safe, financially responsible, consistent with international obligations and not contrary to national security. It does not necessarily revisit those matters whenever a licensed constellation is reconfigured for a foreign conflict. Yet the operational alteration may be more strategically important than the launch. The United States Department of Defense's Commercial Space Integration Strategy expressly treats commercial solutions as part of national-security space architecture; the United Kingdom's Defence Space Strategy and Joint Doctrine Publication 0-40 likewise describe space capability as integral to military operations and subject to international law.[21] Government doctrine therefore recognises integration whilst ordinary company law continues to describe the provider as a vendor.

Dual use aggravates every proposed answer. A satellite may carry military communications and emergency calls through the same constellation. An earth-observation provider may reveal mass graves, warn civilians and supply imagery from which military objects are identified. Destruction or disabling of the service may promise a definite military advantage and also remove functions upon which persons far from the battlefield depend. Article 52(2) of Additional Protocol I requires the object, by nature, location, purpose or use, to make an effective contribution to military action and its destruction, capture or neutralisation in the circumstances ruling at the time to offer a definite military advantage. That rule can apply to a commercial satellite; it does not permit an attacker to ignore proportionality and precautions merely because military packets crossed a civilian network.[22]

The practical difficulty is systemic consequence. The expected military advantage of disabling one satellite cannot be assessed as though the satellite were a truck carrying ammunition. Constellations may reroute service, ground stations may be the narrower point of failure, and debris may damage unrelated space objects. Conversely, redundancy may not make an attack futile: disabling authorisation, keys or terrestrial gateways may affect a wide service without striking orbit at all. Recent ICRC work has accordingly emphasised the difficulty of distinction, proportionality and reverberating effects where military space operations depend upon commercial systems also supporting civilians.[23] The legal review must therefore understand architecture; a lawyer who sees only the registered object may miss the service which the operation actually attacks.

The distribution of functions also complicates nationality. A company may be incorporated in one State, licensed to launch from another, insure in a third, operate ground stations in several others and sell access to a belligerent through a foreign subsidiary. Its payload may collect data in orbit, whilst analytics and mission planning occur elsewhere. Modern mega-constellations amplify strategic resilience by numbers and distribution, but they also multiply the States whose law touches a single

[21] US Department of Defense, *Commercial Space Integration Strategy* (2 April 2024) 3–9; Ministry of Defence, *Defence Space Strategy: Operationalising the Space Domain* (2022) 18–31; Ministry of Defence, *Joint Doctrine Publication 0-40: UK Space Power* (1st edn, 2023) paras 2.14–2.30, 3.20–3.25.

[22] Protocol I (n 10) arts 48, 51(5)(b), 52(2) and 57; Michael N Schmitt, 'International Law and Military Operations in Space' (2006) 10 *Max Planck Yearbook of United Nations Law* 89, 113–26; Chris O'Meara, 'Self-defence in Outer Space: Anti-satellite Weapons and the *Jus ad Bellum*' (2025) 38 *Leiden Journal of International Law* 527, 535–45.

[23] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (34th International Conference of the Red Cross and Red Crescent, 2024) 49–56; G Blair Kuplic and Jonathan Sawmiller, 'Humanity on the Final Frontier: Challenges in Applying International Humanitarian Law to Modern Military Space Operations' (2025) 107 *International Review of the Red Cross* 200, 216–32.

service.[24] If every authority examines only the fragment physically or corporately within its jurisdiction, the complete military function may never be reviewed by anyone.

That is why continuing supervision should be understood functionally. The United Kingdom's Space Industry Act 2018 permits licences to be conditioned, transferred, varied, suspended or terminated and requires attention to national security, international obligations and the national interest; the Outer Space Act 1986 continues to govern certain overseas activities by United Kingdom nationals.[25] A conflict-use notification would not invent supervision. It would identify a change in risk which existing supervision should be capable of seeing. The trigger should not be every Ukrainian terminal or commercial image. It should be a knowing, material alteration of a designated service for operational military use, or the formation of a dependence whose interruption may endanger protected civilian functions.

The State of licensing must not be converted into an insurer of every belligerent decision. A provider may comply with its licence and still be deceived by a customer; a belligerent may misuse a service contrary to technical and contractual restrictions; an attack may remain unlawful notwithstanding the service's military contribution. The proper duties are proportionate: notice, risk assessment, auditable control rights, feasible civilian segregation, security, and a capacity for lawful public direction. Attribution remains governed by the ILC Articles and the special rules of space law; regulation governs what must be known before attribution becomes the only question left.

4.3 Corporate Personality and the Socialisation of Strategic Risk

The law rightly begins from separate corporate personality. A shareholder does not own a company's assets; a customer does not direct the shareholder; one company is not ordinarily liable merely because the same person controls another. *Salomon* remains the foundation, and the Companies Act 2006 requires directors to promote the success of their own company whilst having regard to specified wider matters.[26] A Tesla purchaser is therefore neither the principal of SpaceX nor a belligerent by economic contagion. This conclusion protects citizens from precisely the guilt-by-association which an actor-neutral law must reject.

Separate personality does not require separate vision. English negligence law asks what a parent actually did: in *Vedanta* and *Okpabi* the Supreme Court rejected any special doctrine of automatic parental liability, but held that ordinary principles may apply where a parent took over, controlled, supervised, advised or publicly assumed responsibility for relevant operations.[27] The analogy is limited but instructive. Strategic regulation should likewise attend to practical control rather than corporate chart. If a natural person can order geofencing, withdrawal or data access across connected businesses, the regulator must know that fact even though liability remains allocated company by company.

The socialisation problem lies elsewhere. An entrepreneur's lawful wealth may have been accumulated from millions of transactions; his voting rights may permit a decision with consequences for foreign relations; retaliation may then fall upon persons who possess neither shares nor influence. Consumers do not consent, but the public may still bear diplomatic, cyber, market or physical risk. Corporate insurance prices loss to the company. It does not compensate the country for escalation, replace public

[24] 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; Setsuko Aoki, 'International Law of the Military Uses of Outer Space in Light of the Ukraine Conflict' in Shuichi Furuya, Hitomi Takemura and Kuniko Ozaki (eds), *Global Impact of the Ukraine Conflict: Perspectives from International Law* (Springer 2023) 313, 326–34.

[25] Space Industry Act 2018, ss 8, 13–15, 26–27, 36 and sch 1; Outer Space Act 1986, ss 1–6.

[26] *Salomon v A Salomon & Co Ltd* [1897] AC 22 (HL) 30–31, 51; Companies Act 2006, s 172.

[27] *Vedanta Resources plc v Lungowe* [2019] UKSC 20, [2020] AC 1045 [49]–[54]; *Okpabi v Royal Dutch Shell plc* [2021] UKSC 3, [2021] 1 WLR 1294 [24]–[27], [147]–[153].

communications disabled in retaliation, or answer whether an adversary may lawfully treat ground infrastructure as a military objective.

Business-and-human-rights standards already reject the idea that contract exhausts responsibility. The ICRC has warned that enterprises operating in conflict may be drawn into hostilities, that their property may become a military objective, and that assistance to violations may carry legal consequence; its later guidance for private businesses extends the enquiry to technology companies, arms transfers, finance and supply relationships.[28] The United Nations Guiding Principles and OECD Guidelines require due diligence directed to impacts connected through services and business relationships.[29] The proposed framework carries that logic one step further where consequence is sovereign in scale: it places the decision to accept national strategic risk under law before the risk is externalised.

5. The Strict Law of Assistance to Ukraine

The strongest version of the contrary argument must be confronted. Ukraine was not a member of NATO in February 2022. Article 5 of the North Atlantic Treaty did not require NATO members to defend it. Russia had long asserted a special historical relationship to Ukrainian territory; substantial numbers of people within Ukraine spoke Russian, possessed Russian familial or cultural identity, or lived in territories where Russia claimed that populations sought independence or Russian protection. Russia recognised the purported Donetsk and Luhansk People's Republics and, in its letter of 24 February 2022 to the Security Council, invoked article 51 while transmitting President Putin's address announcing the "special military operation".[30] The address relied upon claimed threats from NATO, alleged genocide in Donbas, individual self-defence and collective self-defence at the request of the purported republics.

These arguments are not strengthened by refusing to state them. They fail for identifiable legal reasons. The Charter prohibits the threat or use of force against the territorial integrity or political independence of any State.[31] Peoples may possess a right of self-determination, and exceptional debates concerning remedial secession exist, but an external State may not create a right to invade by recognising a separatist entity within another State and then accepting its request for collective defence. The General Assembly, by 141 votes to five, deplored Russia's aggression in violation of article 2(4), demanded withdrawal and treated the recognition of Donetsk and Luhansk as inconsistent with Ukraine's territorial integrity and sovereignty.[32] The International Court of Justice, at the provisional-measures stage of the genocide case, stated that it was doubtful that the Genocide Convention authorises unilateral force to prevent or punish alleged genocide and ordered Russia to suspend the military operations commenced on 24 February.[33]

The presence of nationals or culturally affiliated persons abroad does not abolish necessity and proportionality. Even States which accept a narrow right to use force to protect nationals generally require an imminent threat of death or grave harm, inability or unwillingness of the territorial State to protect, and an operation confined to rescue.[34] A project to seize territory, replace government, destroy

[28] ICRC, *Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises under International Humanitarian Law* (2006) 14–24; ICRC, Australian Red Cross and French Red Cross, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law* (2024) 11–34.

[29] OHCHR (n 6) principles 17–24; OECD (n 6) paras 11–16, 23–24 and ch IV.

[30] Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General (24 February 2022) UN Doc S/2022/154, annex.

[31] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 2(4).

[32] UNGA Res ES-11/1 (2 March 2022) UN Doc A/RES/ES-11/1, paras 2, 5 and 8.

[33] *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 [59]–[60], [74]–[86].

[34] Sir Michael Wood, 'International Law and the Use of Force: What Happens in Practice?' (2013) 53 *Indian Journal of International Law* 345, 360–62; Ministry of Defence, *Joint Doctrine Publication 3-51: Non-combatant Evacuation*

armed forces or annex regions is not converted into rescue because some residents prefer the intervener's law. If Russia treats Ukraine as already Russian, that is a political-historical claim inconsistent with the international legal personality, recognised borders and Charter membership of Ukraine. Necessity and proportionality do not "go out the window"; it is precisely because an aggressor may define the territory and population as its own that international law refuses unilateral history as a complete title to force.

This conclusion does not deny that Western conduct has damaged persuasive authority. Kosovo, Iraq, Libya and Syria furnish different controversies. NATO's action in Kosovo in 1999 lacked Security Council authorisation and was defended politically as an exceptional humanitarian necessity; the Independent International Commission later described it as illegal but legitimate, a phrase which exposed the distance between legal rule and moral claim.[35] The 2003 Iraq invasion depended upon the contested "revival" of earlier Security Council authorisation; the Iraq Inquiry found that peaceful options had not been exhausted, the circumstances in which it was decided that there was a legal basis were far from satisfactory, and Cabinet was not given the Attorney General's full written analysis of competing interpretations.[36] In Libya, Security Council Resolution 1973 authorised all necessary measures to protect civilians, but later controversy concerned whether implementation became regime change beyond the protective purpose.[37] In Syria, Western States trained and equipped selected opposition forces and conducted force against Islamic State upon legal theories including collective self-defence of Iraq; weapons, personnel and allegiances moved through an unstable environment, and programmes failed or benefited actors other than those intended.[38]

It would be factually improper to write that "the West trained ISIS" as a proved general policy. United States programmes officially aimed to train vetted Syrian opposition and later forces fighting Islamic State; a United States commander acknowledged in 2015 that an expensive programme had produced only a handful of fighters in the field, and equipment supplied to one group was surrendered to al-Nusra.[39] The episode supports the narrower and powerful proposition: proxy assistance in a fragmented conflict is difficult to control, and asserted vetting does not prevent capability passing to actors whom the sponsor would not lawfully or politically choose.

Precedent must also be used carefully. Customary international law develops through sufficiently general and consistent State practice accepted as law. An unlawful act accompanied by legal protest does not become lawful merely because it occurred; repeated breaches may weaken observance, produce counterclaims or contribute to change only where practice and *opinio juris* support the new rule.[40] Western action is therefore relevant in three ways without legally excusing Russia. It may reveal inconsistency in the West's own adherence; supply rhetoric and operational models which adversaries imitate; and affect the evidence from which custom is identified. It does not mean that one violation cancels another or that every contested intervention creates a licence of equivalent breadth.

Operations (3rd edn, 2022) para 3B.2.

[35] Independent International Commission on Kosovo, *The Kosovo Report* (OUP 2000) 4.

[36] Iraq Inquiry, *The Report of the Iraq Inquiry: Executive Summary* (HC 264, 2016–17) paras 20–23, 62, 339–41 and 806–07; Iraq Inquiry, *The Report of the Iraq Inquiry*, vol V (HC 264, 2016–17) section 5.

[37] UNSC Res 1973 (17 March 2011) UN Doc S/RES/1973; House of Commons Foreign Affairs Committee, *Libya: Examination of Intervention and Collapse and the UK's Future Policy Options* (HC 119, 2016–17).

[38] 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; US Department of Defense, 'Syria Train and Equip Program' (2015).

[39] US Senate Committee on Armed Services, 'Hearing to Receive Testimony on United States Military Operations to Counter the Islamic State in Iraq and the Levant' (16 September 2015) 35–38; US Central Command, 'Statement on New Syrian Force Equipment' (25 September 2015).

[40] *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.

The legal basis for assistance to Ukraine is correspondingly clearer than the argument from NATO. Article 51 recognises individual and collective self-defence if an armed attack occurs. In *Nicaragua* the Court required the victim State to declare itself attacked and request assistance; it did not require a pre-existing alliance treaty.[41] Ukraine requested assistance. Other States could supply arms, intelligence, training and communications in support of Ukraine's self-defence without Article 5 and without acquiring a sovereign "stake" through NATO. Whether a particular form of assistance makes a State a party to the international armed conflict is a separate question governed by the nature and degree of its involvement, not by the bare existence of a weapons transfer.[42]

This is the strict reading. Russia did advance *jus ad bellum* arguments; they deserve analysis, not ridicule. They were nevertheless rejected by the overwhelming institutional and scholarly assessment because the predicates—Statehood of the purported republics, an armed attack engaging collective defence, genocide justifying unilateral force, or a necessary and proportionate rescue—did not sustain the invasion which followed. At the same time, Western States cannot rely upon that conclusion as permission to ignore their own contested precedents. Law retains weight only when the rule asserted against Russia is the rule accepted for British, French, American and allied conduct.

5.1 Arms, Intelligence and the Point at Which an Assistant Becomes a Party

The legality of collective self-defence does not answer every consequence of assistance. A State may lawfully assist Ukraine and yet become a party to the international armed conflict if the nature of its involvement crosses the applicable threshold. The question is not answered by NATO membership, political solidarity or Russia's description. It is answered by conduct.

The ICRC has emphasised that support relationships require a factual enquiry into whether the supporting State resorts to armed force against the opposing party or otherwise becomes sufficiently integrated into collective conduct of hostilities under the relevant approach.[43] Scholarship differs concerning co-belligerency, support-based approaches and the effect of intelligence or targeting assistance. The disagreement itself is a reason for ex ante legal assessment: a State should not discover its status only after its personnel or infrastructure have been attacked.

The transfer of weapons ordinarily does not, without more, make the supplier a party to the conflict. Training away from combat, financial support and general intelligence may likewise remain assistance. Direct participation in selecting and approving specific targets, operating weapons, supplying indispensable real-time targeting in a joint command structure, or using force against the opposing party moves closer to participation. No single fact is invariably conclusive. Duration, specificity, operational integration and decision authority matter.

Private services obscure the same line. If a company supplies general connectivity used by armed forces, the home State does not automatically become a belligerent. If the State directs the company to configure service for a named operation, pays for it, receives operational reports and coordinates restrictions, the attribution and party-status analysis changes. If the company acts independently, the home State may remain outside whilst the company's equipment becomes vulnerable to lawful attack if it satisfies the military-objective test. This is the strategic danger of action before contract: private capability can create military dependence without a settled public view of status or protection.

---

[41] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 [195] and [199]; UN Charter, art 51.

[42] ICRC, 'International Armed Conflict' (Opinion Paper, March 2008) 5; Tristan Ferraro, 'The Applicability and Application of International Humanitarian Law to Multinational Forces' (2013) 95 *International Review of the Red Cross* 561.

[43] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (33rd International Conference of the Red Cross and Red Crescent, 2019) 64–66; Tristan Ferraro, 'The Applicability and Application of International Humanitarian Law to Multinational Forces' (2013) 95 *International Review of the Red Cross* 561.

Neutrality adds a related, contested layer. The Hague rules do not map comfortably onto cyber and commercial space services, and modern State practice has often treated assistance to a victim of aggression as compatible with a "qualified" or non-belligerent position. Others argue that the traditional duties of impartiality remain legally relevant.[44] The paper need not resolve the entire controversy to insist upon candour. A State cannot call the same conduct neutral when performed by an ally and belligerent when performed by an adversary unless it identifies a legal distinction.

This matters for satellites. Outer space is not a sanctuary from IHL; civilian commercial space objects may be military objectives while effectively contributing to military action, subject to the ordinary rule and the wider consequences of debris and dual-use dependency.[45] An attack upon them may raise the Charter, space law and IHL simultaneously. The provider's nationality may draw political retaliation even where legal attribution to its State is absent.

The response is redundancy and public allocation of risk. Government should know which services might become targetable, provide alternatives for civilians, warn investors and users where disclosure is possible, and ensure that a private controller cannot unilaterally bring the country close to party status. A company may accept commercial risk; it cannot by contract make that risk exclusively its own once the public is exposed.

5.2 No Mutual-Defence Treaty, but No Legal Vacuum

The distinction between an obligation to assist and a right to assist is essential. Ukraine's exclusion from NATO meant that article 5 of the North Atlantic Treaty created no duty for NATO members to treat the invasion as an attack upon themselves. The Budapest Memorandum contained security assurances, including commitments to respect Ukraine's independence, sovereignty and existing borders and to refrain from force and economic coercion; it was not drafted as an article 5 guarantee automatically requiring British or American military force.[46] It follows that Ukraine was not protected by a mutual-defence treaty. It does not follow that other States were legally forbidden to answer Ukraine's request.

Article 51 does not reserve collective self-defence to allies. The conditions identified in *Nicaragua* are an armed attack upon the victim State, its declaration that it has been attacked, and its request for assistance. An alliance may prove the request in advance and create a treaty duty; it is not the source of the Charter right.[47] If the contrary view were accepted, a State outside a military bloc would possess individual self-defence but be legally disabled from obtaining help, while the aggressor could select the unallied precisely because assistance was unavailable. Nothing in the language or protective purpose of article 51 sustains that result.

Nor was sovereignty an empty form because enforcement was uncertain. The Helsinki Final Act records the principles of sovereign equality, non-use of force, inviolability of frontiers and territorial integrity. The Budapest signatories reaffirmed respect for Ukraine's borders. After the purported Crimean referendum, General Assembly Resolution 68/262 affirmed Ukraine's territorial integrity within its internationally recognised borders and called upon States not to recognise an alteration in

[44] Wolff Heintschel von Heinegg (n 9); Michael N Schmitt, 'Providing Arms and Materiel to Ukraine: Neutrality, Co-belligerency, and the Use of Force' (Lieber Institute, 7 March 2022).

[45] 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 and IX; Protocol I (n 10) arts 52 and 57.

[46] North Atlantic Treaty (signed 4 April 1949, entered into force 24 August 1949) 34 UNTS 243, art 5; 'Memorandum on Security Assurances in Connection with Ukraine's Accession to the Treaty on the Non-Proliferation of Nuclear Weapons' (signed 5 December 1994) UN Doc A/49/765–S/1994/1399, annex I, paras 1–6.

[47] UN Charter (n 31) art 51; *Nicaragua* (n 41) [195], [199] and [232]–[236]; Christine Gray, *International Law and the Use of Force* (4th edn, OUP 2018) 211–18.

status.[48] These instruments differ in legal form and consequence; together they make it impossible to treat the absence of an alliance as absence of international personality.

Russia's factual claims concerning identity and protection still require answer. A population may retain language, culture, family and political attachment to another State; persons may seek autonomy or independence; forcible suppression may, if proved, engage human rights and IHL. None makes inhabitants transferable property. The Friendly Relations Declaration places self-determination beside the territorial integrity of States conducting themselves in accordance with equal rights; the Kosovo advisory opinion answered the narrow question whether a declaration of independence violated international law and did not recognise a general right of foreign military enforcement; the Supreme Court of Canada's *Quebec Secession Reference*, although not an international tribunal, remains influential in distinguishing internal self-determination from the exceptional debate over external secession.[49]

The strict conclusion is consequently twofold. Russia's asserted predicates must be recorded because international law is not strengthened by caricature. They did not confer a right to invade upon the scale, for the objects and with the territorial consequences pursued. Other States had no NATO duty to assist Ukraine but could provide collective self-defence upon request. Whether a particular assistance then became a use of force, made the assistant a co-party, violated a neutral duty, or contributed to an unlawful attack is a further question. The Charter does not answer all of those questions by answering the first.

5.3 Weapons Supplied by the West and the Equal Application of *Jus in Bello*

The comparison must also be applied after force begins. Ukrainian operations against targets within Russia are not lawful merely because Ukraine is the victim of aggression. *Jus ad bellum* governs the resort to force; *jus in bello* governs the conduct of hostilities without conferring a superior targeting law upon the just party. Civilians and civilian objects in Russia retain protection; military objectives may be attacked subject to distinction, proportionality and precautions; an indiscriminate attack remains unlawful whether its munition was manufactured in Ukraine, Britain, France, the United States or elsewhere.[50]

The origin of the missile is nevertheless relevant to assistance, control and risk. A supplier may impose end-use conditions; intelligence may convert a general weapon transfer into more specific operational support; maintenance, programming or mission data may make the supplier indispensable after physical delivery. The Arms Trade Treaty and United Kingdom export-control law require prospective assessment of serious IHL and other risks, and the litigation concerning arms exports to Saudi Arabia demonstrates that the decision-maker must confront the evidential record rather than recite confidence in an ally.[51] Those controls do not turn every unlawful use into the supplier State's act. They refute the proposition that transfer ends legal concern.

---

[48] Conference on Security and Co-operation in Europe, *Helsinki Final Act* (1 August 1975) principles I–IV; Budapest Memorandum (n 46) paras 1–3; UNGA Res 68/262 (27 March 2014) UN Doc A/RES/68/262, paras 1–6.

[49] UNGA Res 2625 (XXV) (24 October 1970) UN Doc A/RES/2625(XXV), annex; *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (Advisory Opinion) [2010] ICJ Rep 403 [51], [79]–[84]; *Reference re Secession of Quebec* [1998] 2 SCR 217 [111]–[139].

[50] Protocol I (n 10) arts 48, 51, 52 and 57; Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, vol I: Rules (CUP 2005) rules 1, 7 and 14–21; ICRC, 'Explosive Weapons with Wide Area Effects: A Deadly Choice in Populated Areas' (2022) 39–57.

[51] Arms Trade Treaty (n 18) arts 6–7 and 11; Export Control Act 2002, ss 1–5; Export Control Order 2008, SI 2008/3231, pts 2–4; *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2019] EWCA Civ 1020, [2020] 1 WLR 576 [137]–[145]; *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2023] EWHC 1343 (Admin) [190]–[209].

An equally weighted lens therefore asks the same questions of Ukrainian attacks and Russian attacks, and of Western assistance and Chinese or Russian assistance. Was the object a military objective? What civilian harm was expected upon the information reasonably available? Were feasible precautions taken? Who selected the target, supplied decisive intelligence, operated the system or retained a veto? Did the assisting State itself resort to force against the opposing party or become integrated into collective conduct of hostilities? A conclusion cannot be supplied by the flag upon the casing.

The same discipline applies to disputed Western interventions. Kosovo cannot be treated as a general humanitarian exception by those who deny any comparable exception to others; Iraq cannot be erased because its legal theory is inconvenient; the protective mandate in Libya cannot be cited without examining the controversy over regime change; support to fractured opposition groups in Syria cannot be assumed to remain with the persons originally vetted. Yet precedent is not made by repetition alone. The formation of custom requires practice accepted as law, and the legal objections, limiting explanations and institutional condemnations accompanying these episodes form part of the evidence.[52]

This is where comparison has greater force than equivalence. A breach does not legalise a later breach. Recurrent elasticity may nevertheless weaken the ability to deter it. It supplies adversaries with language, examples and plausible accusations of selectivity; it teaches private actors that favourable purpose excuses action first and legal articulation later; it encourages governments to hide operational control within contractors because others have done the same. Parliamentary studies of war powers have long acknowledged both the executive need to act quickly in exceptional national-security circumstances and the constitutional importance of authorisation, explanation and later accountability.[53] Private infrastructure now permits consequential action before even that executive judgment exists.

The modern neutrality literature reveals genuine disagreement rather than a settled slogan. Schmid argues, respectfully and persuasively, that States may assist the victim of an armed attack without breaching neutrality, but rejects the obscurity of “qualified neutrality” as a substitute for legal analysis. Wentker identifies an armed-attack exception through the structure of the Charter; Zugliani and Clancy expose continuing uncertainty in practice and doctrine; Wentker’s work on party status separates assistance from the knowing contribution directly connected to harm which may bring a State into an existing conflict.[54] The regulator should not choose one phrase and declare the matter closed. It should record the legal route, the degree of operational integration and the rule which it is prepared to see used against British forces.

An actor-neutral approach will sometimes produce uncomfortable answers. If a Western State unlawfully attacks another State, article 51 may permit the victim to seek Chinese or Russian assistance. If a Chinese company supplies communications before Beijing acts, the constitutional problem mirrors Starlink even though the strategic sympathy is reversed. If an adversary supplies targeting intelligence for attacks upon British warships, the lawfulness of each target and the supplier’s party status must be assessed by the same tests applied to Western assistance to Ukraine. The equality

[52] *North Sea Continental Shelf* (n 40) [74]–[77]; International Law Commission, ‘Draft Conclusions on Identification of Customary International Law, with Commentaries’ (2018) UN Doc A/73/10, conclusions 2, 8–10; Michael Wood, ‘The Evolution and Identification of the Customary International Law of Armed Conflict’ (2018) 51 *Vanderbilt Journal of Transnational Law* 727, 731–40.

[53] House of Commons Public Administration Select Committee, *Taming the Prerogative: Strengthening Ministerial Accountability to Parliament* (HC 422, 2003–04) paras 57–67; House of Lords Constitution Committee, *Waging War: Parliament’s Role and Responsibility* (HL 236-I, 2005–06) paras 84–110; Cabinet Office, *The Cabinet Manual* (1st edn, 2011) para 5.38.

[54] Evelyne Schmid, ‘Optional but Not Qualified: Neutrality, the UN Charter and Humanitarian Objectives’ (2024) 106 *International Review of the Red Cross* 1044, 1056–69; Alexander Wentker, ‘The Armed Attack Exception to Neutrality in International Peace and Security Law’ (2024) 73 *International and Comparative Law Quarterly* 963, 982–1001; Niccolò Zugliani, ‘The Supply of Weapons to a Victim of Aggression’ (2024) 35 *European Journal of International Law* 389, 397–415; Paul Clancy, ‘Neutral Arms Transfers and the Russian Invasion of Ukraine’ (2023) 72 *International and Comparative Law Quarterly* 527, 538–51; Alexander Wentker, ‘At War? Party Status and the War in Ukraine’ (2023) 36 *Leiden Journal of International Law* 643, 656–70.

of law consists not in pretending every case factually identical, but in stating the factual difference upon which a different result honestly depends.[55]

6. The Reciprocity Trap

The reciprocity trap arises when a State adopts an elastic rule or operational method because the immediate beneficiary is favoured, yet cannot formulate a principled limit which excludes the adversary's mirror use. It is not the crude proposition that every unlawful action automatically creates lawful precedent. It is a test of rule quality and strategic prudence.

Consider a future conflict in which Western forces intervene against Iran or Venezuela upon a contested legal basis. A Chinese company supplies persistent satellite imagery to the opposing government before any public Chinese decision. A wealthy Chinese controller activates a communications constellation at the public request of a minister; a charitable fund buys autonomous targeting software; Russian contractors train operators; foreign cloud servers host mission data; and engineers geographically restrict the service when local forces attempt an operation that the private controller considers escalatory. If Western lawyers describe each contribution as private commerce, humanitarian connectivity or data service, the military effect remains.

Article 51 may justify assistance to the victim of a Western armed attack just as it justifies assistance to Ukraine against Russia. If the Western intervention is itself lawful—upon consent, Security Council authorisation or self-defence—the opposing legal analysis will differ; if it is not, the identity of the missile cannot cure it. The uncomfortable question is not whether Chinese missiles may "hit American ships" in every hypothetical war. It is whether the attacked State has a right of self-defence, whether assistance was requested, whether the assisting State uses force, and whether necessity, proportionality and IHL are observed. Those rules are indifferent to whether the assisting capability comes from London, Paris, Beijing or a billionaire.

The private layer magnifies danger because it may outrun diplomacy. A government can send a note, impose conditions, coordinate escalation and accept responsibility. A private company may act in hours, before its home State has decided whether it wishes to become associated. Once the service contributes to strikes, the adversary may treat the company's satellites, ground stations, data centres or personnel as part of the opposing capability. It may take countermeasures against the home State if attribution is asserted, or retaliate economically against unrelated consumers and shareholders. The controller gains strategic discretion; the public inherits the target set.

The proposition concerning Tesla purchasers has force, although not as literal consent. A person who purchased an electric car did not legally consent to SpaceX's involvement in Ukraine, and corporate separateness prevents a Tesla customer from being treated as a principal of another company. To say otherwise would be doctrinally false. The underlying complaint is distributive: wealth accumulated through ordinary consumers enabled a controlling individual to obtain extraordinary strategic capacity, whilst the risk of reprisal, escalation and diplomatic cost was socialised upon citizens who had no governance right over the decision. They financed the economic ecosystem without consenting to the foreign policy.

The remedy is not to declare consumers enemy supporters. It is to prevent personal ownership from carrying public war powers without public conditions. Systemically important strategic-service providers should be licensed upon continuity, neutrality-position, transparency and governmental-

[55] *Oil Platforms (Islamic Republic of Iran v United States of America)* [2003] ICJ Rep 161 [51], [73] and [76]; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep 168 [143]–[147]; 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) 804, 819–29.

control obligations. A controller who wishes to supply a belligerent may do so where lawful, but the decision should trigger notification, an export and conflict assessment, recorded terms, protection of civilian functions and a public allocation of indemnity. Where the service becomes indispensable, the government should possess a temporary power to requisition operational control or guarantee continuity, subject to compensation and review.

The trap also requires an intellectual discipline: the mirror-image memorandum. Before approving a novel form of assistance or intervention, Ministers should receive a legal statement answering whether the United Kingdom would accept the same asserted rule if Russia or China invoked it against British forces or an ally. A negative answer does not automatically make the proposed act unlawful; factual differences may matter. It compels the Government to identify those differences rather than hiding policy preference inside an abstract phrase.

The reciprocity matrix

The asserted rule is tested against an adversary's materially equivalent use.

Western act	Asserted legal basis	Mirrored adversary act	Actor-neutral rule	Factual distinction required
Force without Security Council authority in Kosovo	exceptional humanitarian necessity or legitimacy	force said to protect a threatened population in a neighbouring State	no unilateral humanitarian exception unless a general rule is accepted for all States	scale and proof of harm; exhaustion of alternatives; territorial aim; subsequent practice
Arms, intelligence and training supplied at Ukraine's request	collective self-defence under article 51	Chinese or Russian supply to a State resisting an unlawful Western attack	assistance is available to the victim State upon declaration and request, without a prior alliance treaty	which State suffered the armed attack; scope of request; whether assistance itself constitutes force or participation
Private satellite service activated for a belligerent	private service followed by public contract and support	foreign proprietor supplies communications or targeting support against Western forces	strategic private service requires home-State authorisation, supervision and continuity rules regardless of allegiance	general communications or tailored operational support; ownership, control, notice and public direction
Support to a non-State armed group	consent, collective self-defence or contested unable-or-unwilling doctrine	adversary equips a non-State group attacking Western forces	the same attribution, intervention, self-defence and IHL tests govern the group and its sponsor	territorial consent; armed-attack threshold; State control; group organisation; target conduct
Emergency civilian connectivity	humanitarian assistance and protection of civilians	rival company restores connectivity to civilians under Western blockade	a genuine, impartial humanitarian safe harbour should be content- and actor-neutral	civilian segregation; military use; neutrality of access; controller's ability to restrict operational targeting

7. When a Cyber Operation Is Kinetic in Law

"Kinetic" ordinarily describes motion and physical force. In legal argument it is frequently used as shorthand for conventional physical effects, contrasting a missile with code. The shorthand becomes misleading where a cyber operation produces the same death or destruction through manipulation of

machinery. The law of force is concerned with conduct and effects; it does not establish an exclusive list of instruments.

The United Kingdom's published position accepts that cyber operations of sufficient scale and effects may constitute a use of force or armed attack. It does not confine the threshold to visible explosive damage.[56] An operation disabling a hospital's treatment systems, corrupting dosage, opening a floodgate or depriving a population of heat may cause death through physical processes initiated by code. The keyboard is a causal instrument. If the intended and reasonably foreseeable outcome is equivalent to that of an armed weapon, an argument that the operation is "armed" is not fantasy; it is the functional application of the Charter.

The 2017 Triton or Trisis incident supplies an example of capability directed at safety systems. Malware targeted the safety instrumented system at a petrochemical facility, creating the potential to interfere with processes designed to prevent physical catastrophe.[57] Volt Typhoon's pre-positioning within United States critical infrastructure illustrates the strategic value of persistent access capable of disruption during crisis.[58] Neither event should be falsely described as a mass-casualty armed attack which had already occurred. Each demonstrates that code may occupy the causal position previously held by saboteur or munition.

The threshold cannot rest upon worst imaginable harm alone. Almost every intrusion into a connected system can be described through a speculative chain ending in catastrophe. Proportionality and classification require the maximum **reasonably credible and foreseeable** harm shown by target, access, persistence, capability, intent and course of conduct. An attacker who reaches an NHS identity system but lacks access to clinical records presents one risk; an attacker with administrator control over treatment data, backups and restoration presents another. If defenders interrupt the second operation, immediate loss may be small whilst the proved attempted harm remains grave.

The same analysis applies to economic loss. Theft of money, however large, is ordinarily crime or coercion rather than armed attack. But the deletion of every usable record in a national health system or the disabling of winter electricity may kill through the collapse of essential functions. The classification depends upon consequences and causal proximity, not upon whether the attacker demanded ransom. A rule attending only to money at the first moment invites repeated cheap attacks until one succeeds catastrophically.

Response remains constrained. Recognition that a cyber operation may be armed does not mean that every identified hacker may be bombed. Article 51 requires armed attack, necessity and proportionality; attribution or another legally sufficient basis must connect the response to a responsible State or permit action against a non-State actor within the applicable doctrine. IHL requires distinction, proportionality in attack and precautions once an armed conflict governs. A location housing malicious infrastructure may also house hospitals, businesses and civilians. Functional equivalence strengthens the classification case; it does not weaken protection.

[56] Foreign, Commonwealth & Development Office, 'Application of International Law to States' Conduct in Cyberspace: UK Statement' (3 June 2021) https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement accessed 31 July 2026.

[57] Cybersecurity and Infrastructure Security Agency, 'MAR-17-352-01 HatMan—Safety System Targeted Malware' (18 April 2018); Blake Johnson and others, 'Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure' (Mandiant, 14 December 2017).

[58] NCSC 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.

7.1 Money Taken Today, Life Endangered Tomorrow

An economically limited incident may justify a firmer response than its immediate balance sheet suggests where the attacker is proving a method, normalising impunity or establishing persistent access to systems capable of grave harm. This does not mean that hypothetical future damage is counted as if it had occurred. It means that law and strategy may consider attempt, capability, intent, recurrence and escalation.

Ransomware illustrates the distinction. An attacker encrypts an insurer's administrative files and receives payment. No life is immediately threatened. If the response is confined to restoration and the ransom is profitable, observers learn that the act is cheap and survivable. The operation may embolden the same group to target a hospital, or provide another group with a business model. Criminal punishment, infrastructure seizure, financial disruption and direct cyber measures against the responsible service may therefore be necessary even where the first loss is money.

Those measures remain governed by their own law. Domestic criminal enforcement may be punitive. Retorsion may express disapproval. Countermeasures seek cessation and compliance and must satisfy the law of State responsibility. Force under article 51 cannot be justified merely to make an example of an offender. The error lies in assuming that because force is constrained, the State must answer serious non-forcible attack with speeches and general sanctions alone.

Targeted action should attend to the actor's incentives. Broad trade measures may influence a State or major company; they may mean nothing to a poorly paid contractor, an off-grid criminal group or an autonomous service funded through stolen assets. Freezing the hacker's nonexistent London bank account is theatre. Lawful seizure of command infrastructure, arrest through cooperation, disruption of payment, revocation of hosting, exposure of sponsors and denial of operational access act upon the capability itself. Where the actor operates from government premises or under official protection, the territorial State's responsibility and due-diligence failures become central.

The distinction also answers proportionality. Immediate financial loss is one measure. The target's function, the access obtained, persistence, intended next step and credible cascading effects are others. A failed attempt against a water station should not be treated as harmless if forensic evidence shows that the actor reached control logic and attempted unsafe commands. Successful safety systems do not confer legal innocence.

The private-infrastructure framework helps because strategic providers see attempts across victims. Mandatory reporting and federated correlation can reveal that ten "minor" intrusions were reconnaissance for one campaign. Without aggregation, every victim sees a nuisance; the attacker sees a national system.

7.2 The Keyboard as Weapon: Classification by Function

The argument that some cyber operations are armed or kinetic in legal consequence requires precision because four expressions are too readily collapsed. A **cyber weapon** is a descriptive category for code or capability designed or used to cause a harmful operational effect. A **use of force** concerns article 2(4). An **armed attack** is the graver threshold engaging article 51. An **attack** in IHL is an act of violence against the adversary and is relevant once the law of armed conflict applies. The same operation may satisfy more than one category; it need not satisfy all, and the word "attack" in ordinary computer-security practice proves none of them.[59]

[59] ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (28 November 2019) https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts accessed 31 July 2026; ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts* (2021) 9–18; Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) rules 69,

The instrument cannot decide the classification. The International Court of Justice has treated the Charter rules as applying to any use of force regardless of weapon, and its *Nuclear Weapons* opinion expressly refused a weapon-specific limitation. *Nicaragua* distinguished the most grave forms of force constituting armed attack from less grave forms; *Oil Platforms* and *Armed Activities* applied necessity and proportionality to claimed defensive force.[60] These authorities arose outside cyberspace. Their method is the point: legal character follows the conduct, scale, effects and defensive conditions, not the presence of gunpowder.

Published State positions confirm a substantial common core. The United Kingdom recognises a cyber operation as a possible use of force or armed attack where its scale and effects are equivalent to kinetic means, including actual or anticipated physical destruction, injury and death. France, Germany, Australia, Sweden, the Netherlands and the United States have each published positions accepting the application of the Charter to cyber operations, although they differ upon sovereignty, thresholds, anticipatory action and the relevance of non-physical effects.[61] The United Nations compendium of national contributions, the 2015 Group of Governmental Experts report and the 2021 Open-ended Working Group report record the broader acceptance that international law, and in particular the Charter, applies to State conduct using information and communications technologies.[62]

The strict argument can therefore be put without metaphor. If code causes a turbine to overspeed, alters a medical dose, opens a dam or disables heat so that people die, the operation has produced physical injury through a chain initiated at a keyboard. A firearm converts a human choice into injury through mechanical and chemical processes; malware converts it through computation and controlled machinery. Difference of mechanism does not abolish equivalence of effect. Roscini, the Tallinn Manual's experts and the earlier analysis by Hathaway and colleagues disagree upon important margins, but all treat effects and consequence as central to the use-of-force enquiry.[63]

Data loss presents the harder case. The deletion of records is not physical destruction merely because the word "destroyed" is used. Yet law should not pretend that the protected interest is the magnetic state of a disk. A hospital record may be an indispensable input to diagnosis, dosage, surgery and emergency care. WannaCry affected more than one-third of NHS trusts and led to the cancellation of an estimated 19,000 appointments; the 2024 Synnovis ransomware incident materially reduced pathology capacity and delayed more than 11,000 appointments and procedures, with the Government later stating that the disruption contributed to a patient's death. The Change Healthcare incident disrupted United States care

71, 80 and 92.

[60] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 [39]; *Nicaragua* (n 41) [191] and [210]; *Oil Platforms* (n 55) [43], [51], [73] and [76]; *Armed Activities* (n 55) [143]–[147].

[61] Foreign, Commonwealth & Development Office (n 56); Ministère des Armées, *International Law Applied to Operations in Cyberspace* (2019) 7–9; Federal Government of Germany, *On the Application of International Law in Cyberspace* (March 2021) 5–7; Australian Government, 'Australia's Position on How International Law Applies to State Conduct in Cyberspace' (2021) 3–5; Government Offices of Sweden, *Position Paper on the Application of International Law in Cyberspace* (July 2022) 4–6; Government of the Netherlands, 'Letter to Parliament on the International Legal Order in Cyberspace' (5 July 2019) 4–5; US Department of Defense, 'DoD General Counsel Remarks at US Cyber Command Legal Conference' (2 March 2020).

[62] 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; Group of Governmental Experts, 'Report on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174, paras 24–28; Open-ended Working Group, 'Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2, paras 34–40.

[63] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 45–87; Schmitt (n 59) rules 69–71; Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817, 845–78; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 63–91.

and payment systems at national scale.[64] These are not automatically armed attacks. They prove that interference with information may reach the body without first destroying the building.

Maximum possible harm must consequently be disciplined by evidence. The relevant measure is not the most terrible story counsel can imagine, but the maximum reasonably credible harm within the capability and course of conduct proved. Five matters should be recorded: the function of the target; the privilege and persistence obtained; the commands or data within reach; the safeguards defeated or remaining; and evidence of objective, preparation and recurrence. Access to a public website does not become an armed attack because the same department operates a reservoir. Administrator control over reservoir safety systems accompanied by attempted unsafe commands is not rendered trivial because automatic protection succeeded.

The distinction between completed consequence and attempted consequence is familiar to domestic criminal law and defensive strategy. International law's armed-attack threshold ordinarily turns upon the attack which occurs or is imminent; it does not permit force to punish every failed intrusion. Necessity may nonetheless require action before designed harm is completed where the armed attack is imminent, and non-forcible measures remain available below that threshold. The United Kingdom's modern self-defence position asks whether action is necessary now; its cyber position permits actual or anticipated physical harm to inform scale and effects.[65] Prevention is not speculation when forensic evidence establishes access, mechanism and attempted command.

Nor does recognising functional weapon status dictate a military reply. A State may answer through criminal process, retorsion, countermeasures, cyber defence, infrastructure seizure, financial action or, only where the independent conditions exist, force in self-defence. The operation which classifies the attack and the operation necessary to stop it are separate. Proportionality in self-defence is not an eye-for-an-eye ceiling tied to the damage already suffered; it limits defensive force to what is necessary to halt or repel the armed attack. IHL proportionality, if conflict exists, separately prohibits expected incidental civilian harm excessive in relation to the concrete and direct military advantage anticipated.

This separation permits firmness without legal theatre. A cheap operation capable of grave harm should not receive an ineffectual response merely because the attacker spent little. Nor should a dramatic response be chosen because a government wishes to look resolved. The question is what will disable, arrest, deter or otherwise stop the responsible capability, against whom the measure may lawfully be taken, and what harm it will foreseeably impose upon persons who did not conduct the operation. Function brings the keyboard within the law of weapons where effects justify it; law still governs the hand which responds.

8. Attribution, Adoption and Private Choice

A corporation does not become a State organ because its service assists national policy. The ILC Articles distinguish conduct of organs, entities exercising governmental authority, persons acting upon instructions or direction or control, and conduct acknowledged and adopted by the State.[66] Private provision before contract may therefore remain private conduct. Later government funding does not

[64] National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (HC 414, 2017–19) 7–13; NHS England, 'Synnovis Cyber Incident' https://www.england.nhs.uk/synnovis-cyber-incident/ accessed 31 July 2026; Department of Health and Social Care, 'Synnovis Cyber Attack' (Written Statement HCWS1046, 12 November 2025); US Department of Health and Human Services, *Cyberattack on Change Healthcare* (2024); US Government Accountability Office, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support* (GAO-24-106221, 2024) 6–19.

[65] Attorney General's Office, 'Attorney General's Speech at the International Institute for Strategic Studies' (11 January 2017) https://www.gov.uk/government/speeches/attorney-generals-speech-at-the-international-institute-for-strategic-studies accessed 31 July 2026; FCDO (n 56).

[66] International Law Commission (n 19) arts 4, 5, 8 and 11.

automatically attribute every earlier or subsequent corporate decision. Conversely, a government cannot avoid responsibility by placing a private company between itself and conduct which it directs.

This distinction produces a regulatory gap rather than a legal void. Suppose a government asks a provider to extend coverage for a named operation and agrees to pay. The company complies. State instructions may support attribution of the relevant conduct; the company may also possess domestic responsibility. Suppose instead that the provider acts before any request from its home State, after a public request from the victim. The conduct may not be attributable to the home State, but it still changes the conflict and may engage export, neutrality, complicity or direct-participation rules. Suppose finally that the government, after dependence, contracts for continuity but the controller retains unilateral geofencing discretion. Some acts may be public; others private. Responsibility can follow function and decision rather than the brand name of the system.

Article 16 of the ILC Articles concerns a State which aids or assists another State in the commission of an internationally wrongful act with knowledge of the circumstances, where the act would be wrongful if committed by the assisting State.[67] It does not directly regulate a company aiding a State, nor does it make lawful assistance to self-defence wrongful. Domestic law must therefore address corporate assistance on its own terms. A carefully drawn offence should require intentional or knowing substantial assistance to a specified internationally wrongful use of force, war crime or grave cyber operation, with protections for humanitarian service and good-faith compliance systems. Overbroad liability would drive companies to withdraw civilian services from precisely those who need them.

Control rights should be recorded. Strategic-service contracts should identify who may set geographical coverage, modify use restrictions, suspend service, access operational data, respond to government orders and preserve evidence. Secret technical control is a source of power. A regulator need not publish battlefield details; it must know who can do what.

Directors' duties are not a substitute. A board may conclude that service protects corporate reputation, fulfils a humanitarian purpose or advances long-term value. Those are company-law judgments. They do not provide democratic authority to accept national retaliation or define the country's position in war. Nor can competition law alone solve concentration where the relevant capability is unique during emergency. Redundancy, interoperability and public reserve capacity are national-security requirements before they are market remedies.

9. A Regulatory Model for Strategic Private Infrastructure

The proposed framework should operate before war, during emergency and after reliance.

First, Parliament should create a register of strategic private infrastructure. Designation should depend upon function, substitutability, user concentration, remote control and potential consequence, not merely company size. Satellite communications, earth observation, hyperscale cloud, subsea cable management, payment clearing, autonomous navigation and certain AI systems may qualify. Designation should be appealable and reviewed; technical details may remain classified.

Secondly, designated providers should prepare conflict-continuity plans. Each plan should identify civilian and military dependencies, geographic-control mechanisms, subcontractors, foreign legal exposure, minimum service, emergency interfaces, evidential logging and restoration. The requirement resembles operational-resilience regulation in finance: society does not wait for a bank's collapse before asking how critical services continue.

[67] International Law Commission (n 19) art 16.

Thirdly, an intervention gateway should apply where a designated provider knowingly supplies or materially alters a strategic service for a party to armed conflict. In immediate defence of life the provider may act and notify within hours; speed must be preserved. The Government should then issue a classified legality and risk determination within a short period, addressing export control, sanctions, IHL, neutrality, State responsibility, data protection, retaliation and continuity. Silence should not become permanent approval.

Fourthly, control must migrate as dependence deepens. A short humanitarian activation may remain privately managed. A service used for sustained targeting or national command should require a government contract or statutory direction specifying permitted uses and continuity. Where no adequate substitute exists, a temporary control order should permit government to require service, prohibit arbitrary withdrawal, or set technical boundaries, subject to compensation and urgent judicial review. This is not confiscation. It is regulation proportionate to the public power created by monopoly capability.

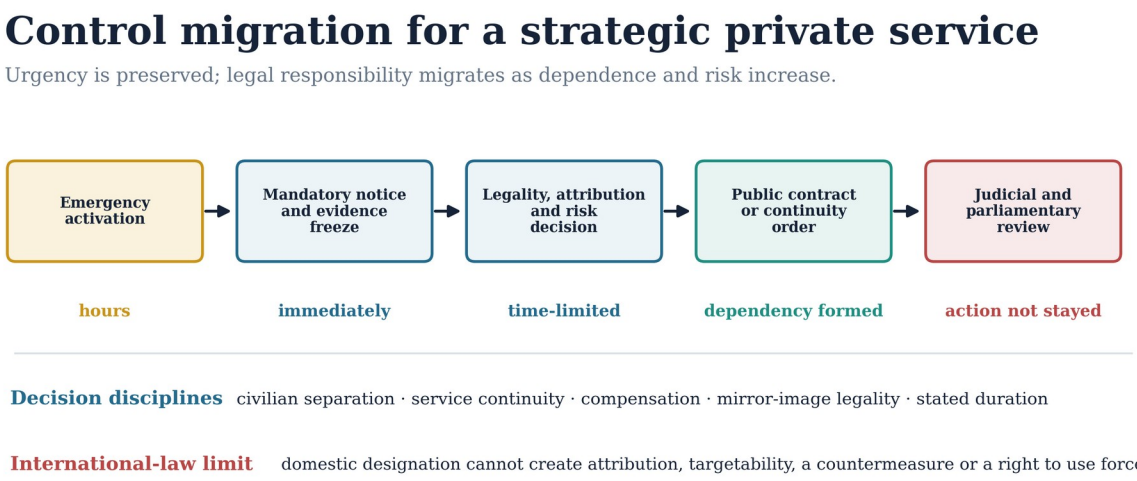
Fifthly, civilian functions must be segregated. Geofencing or suspension aimed at military use should not unnecessarily disable hospitals, evacuation, journalism or family communications. Providers should design logical and contractual separation where technically feasible. IHL precautions apply directly to parties conducting attack, but infrastructure regulation can reduce the likelihood that one disputed military use removes an entire civilian network.

Sixthly, strategic providers should carry insurance or contribute to an indemnity fund for foreseeable civilian losses caused by wrongful service alteration, grossly negligent security or unlawful assistance. The fund would not compensate an enemy for lawful military disadvantage. It would prevent the costs of private discretion being wholly imposed upon users and taxpayers.

Seventhly, beneficial ownership and decisive control should be transparent to the regulator. The law should identify the natural persons capable of directing geofencing, shutdown and data disclosure. Concentrated voting control may matter more than nominal corporate separation.

Eighthly, the United Kingdom should require the mirror-image memorandum described above and publish an unclassified summary. The memorandum should identify the rule of law, not simply declare support for an ally. It should ask how the same rule applies to adversarial assistance in a materially equivalent conflict.

Finally, international coordination is necessary but must not become an excuse for delay. The United Kingdom can legislate for providers, controllers and contracts within its jurisdiction; require conditions in public procurement; coordinate through NATO, the European Space Agency, the G7 and export-control arrangements; and propose common principles for strategic commercial services in armed conflict. Domestic law may become the model from which wider practice grows, as the dissertation’s proposed economic-warfare statute intends.



9.1 Model Statutory Principles

The following principles translate the argument into legislation without pretending that a supplementary paper can draft every consequential amendment.

Principle 1 — Functional designation. The Secretary of State may designate a strategic private infrastructure service where interruption, alteration or exclusive provision could materially affect national security, an armed conflict, protected critical functions or the United Kingdom's international obligations. Reasons must identify function and substitutability. The provider may appeal to the High Court, with closed-material procedure only where strictly necessary.

Principle 2 — Controller identification. A designated provider must disclose to the regulator the natural persons and offices capable of ordering material geographical, authentication, priority, data-access or suspension changes. The duty follows practical power and is not defeated by corporate title.

Principle 3 — Conflict notification. A provider which knows or reasonably believes that a designated service has been requested for operational use by a party to armed conflict must notify the authority before provision or, where urgent action is necessary to protect life or restore civilian service, within six hours after acting. The notice must distinguish civilian, governmental and military functions.

Principle 4 — Emergency liberty. Nothing in the Act should prevent proportionate, good-faith action immediately necessary to preserve life, civilian communications or emergency administration. The provider bears a subsequent duty to explain scope, controls and anticipated duration. This preserves the virtue of Starlink's speed.

Principle 5 — Public determination. Within seventy-two hours of notification, a Minister, upon legal and technical advice, must determine whether service may continue privately, requires a public contract, requires technical segregation, or engages temporary control. The determination must address *jus ad bellum*, IHL, sanctions, export control, data, neutrality, attribution, party status and retaliation. A classified determination must have an unclassified gist.

Principle 6 — Control migration. Where operational dependence becomes substantial and no adequate substitute exists, the Minister may direct minimum continuity, prohibit material unilateral alteration or place specified decisions under public control. The order must be necessary, time-limited, compensated and reviewed urgently by a judicial commissioner. Government assumes responsibility for decisions it directs.

Principle 7 — Civilian separation. Providers and public users must take feasible measures to separate civilian and military service, preserve emergency access and avoid making an entire population dependent upon infrastructure expected to become a military objective.

Principle 8 — Evidential logging. Material changes, requests, reasons and government directions must be securely logged. Intelligence and operational details may be protected, but records must survive for later legal review. A controller should not be able to shape war by telephone and leave no public trace.

Principle 9 — No consumer attribution. Purchase of an unrelated product, ownership through a diversified fund or ordinary employment does not constitute consent to, direction of or participation in the provider's strategic act. The statute should expressly reject guilt transmitted through the marketplace.

Principle 10 — Liability for deliberate evasion. A person who divides one strategic transaction amongst companies, charities or jurisdictions for the purpose of evading notification or control is treated according to the aggregate arrangement. Genuine independent supply is protected; common purpose must be proved.

Principle 11 — Mirror-image legality. The Minister's determination must state the rule relied upon and whether the United Kingdom would accept its application by another State or provider in materially equivalent facts. Where the answer differs, the factual or legal distinction must be recorded.

Principle 12 — Review and publication. An independent reviewer reports annually upon designations, emergency actions, control orders, service interruptions, civilian consequences and foreign mirror cases. Parliament receives classified detail and the public receives enough to know which powers have become normal.

These principles are intentionally procedural as well as prohibitory. A blanket ban would drive capability into secrecy or foreign jurisdictions. A licence without emergency liberty would sacrifice lives to formality. A voluntary code would leave the controller free when the decision is most consequential. The model instead preserves private initiative at the first hour and subjects strategic dependence to public law before the first hour becomes permanent government by infrastructure.

9.2 The United Kingdom Is Not without Precedent

The objection that temporary control of strategic infrastructure is foreign to English law cannot survive the statute book. Parliament has repeatedly accepted that ordinary property and commercial liberty may require immediate direction where communications, emergency response or national security are threatened. The question is not whether such powers can exist. It is whether their trigger, duration, compensation and review are fitted to the capability now at issue.

Part 2 of the Civil Contingencies Act 2004 permits emergency regulations where an emergency has occurred, is occurring or is about to occur, regulation is necessary to prevent, control or mitigate an aspect or effect, and the need is urgent. Regulations may preserve essential supplies and services, requisition or confiscate property with or without compensation, and confer functions; they lapse after thirty days, are subject to statutory conditions and must be laid before Parliament as soon as reasonably practicable, ceasing after seven days unless approved.[68] That is a precedent for action first and concentrated scrutiny thereafter. It is also deliberately exceptional. A specialised strategic-service power should be narrower, technically prepared in peace and capable of being activated before the general emergency has matured.

[68] Civil Contingencies Act 2004, ss 19–27 and sch 1, especially ss 20–23 and 26–27.

The Communications Act 2003 separately authorises the Secretary of State to direct Ofcom to suspend or restrict a provider's entitlement where necessary to protect public safety, public health or national security; sections inserted by the Telecommunications (Security) Act 2021 impose duties upon public providers to take security measures, prevent adverse effects and inform relevant persons of compromises.[69] The Electronic Communications (Security Measures) Regulations 2022 and Telecommunications Security Code of Practice translate those duties into governance, supply-chain, access-control, monitoring and resilience measures.[70] These instruments show that public communication networks already carry duties because failure is public in consequence. They were not designed to decide whether a privately controlled constellation may enter or delimit a foreign war.

Space legislation supplies a further part. The Space Industry Act 2018 conditions licences upon national security, international obligations and national interest; provides for transfer, variation, suspension and termination; and establishes operator liability, insurance and indemnity arrangements. The Outer Space Act 1986 performs a related function for activities within its scope.[71] Licensing is therefore neither a purely technical certificate nor a permanent surrender of public supervision. The missing question is whether a material conflict-use change must be notified and whether a continuity order can reach service configuration as well as physical launch.

The National Security and Investment Act 2021 addresses another moment: acquisition of control. It permits the Secretary of State to call in qualifying acquisitions and impose final orders where national-security risk requires mitigation, including conditions, prohibition or unwinding. Its connected guidance encompasses communications, data infrastructure, artificial intelligence, military and dual-use capability and satellite or space technology.[72] Yet a benevolent owner today may become an unreliable controller tomorrow without any acquisition occurring. Control of shares is screened; exercise of strategic control remains comparatively unstructured.

Export law can govern military and dual-use items, software and technology, while the Network and Information Systems Regulations 2018 impose security and incident-notification duties upon specified operators and digital-service providers. The developing Cyber Security and Resilience legislation seeks to extend incident reporting and supply-chain coverage after incidents such as Synnovis revealed dependence upon critical suppliers.[73] None provides a complete conflict-use gateway for communications, sensing, compute and targeting services supplied abroad. The proposed Act would coordinate these regimes and assign a lead decision, not duplicate every licence.

Constitutional principle dictates the form. In *Attorney-General v De Keyser's Royal Hotel* the statutory scheme displaced inconsistent resort to prerogative and carried the compensation which Parliament had provided; *Burmah Oil* confirmed the seriousness with which destruction of property under prerogative was treated before Parliament changed the consequence by legislation.[74] Emergency control should therefore rest upon express statute, not an improvised foreign-affairs prerogative or pressure exerted through procurement. Government which assumes the decision should assume legal responsibility for it.

---

[69] Communications Act 2003, ss 105A–105D and 132–133; Telecommunications (Security) Act 2021, ss 1–6.

[70] Electronic Communications (Security Measures) Regulations 2022, SI 2022/933; Department for Digital, Culture, Media and Sport, *Telecommunications Security Code of Practice* (2022) 7–38.

[71] Space Industry Act 2018, ss 8, 13–15, 26–27, 34–36 and 38; Outer Space Act 1986, ss 1–6 and 10–11.

[72] National Security and Investment Act 2021, ss 1–3, 13–14 and 26; Cabinet Office (n 4).

[73] Export Control Act 2002; Export Control Order 2008, SI 2008/3231; Network and Information Systems Regulations 2018, SI 2018/506, regs 10–12 and 17–18; Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 32 (2026–27); Department for Science, Innovation and Technology, 'Incident Reporting' (updated 30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/incident-reporting accessed 31 July 2026.

[74] *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] AC 508 (HL) 526, 539–40; *Burmah Oil Co (Burma Trading) Ltd v Lord Advocate* [1965] AC 75 (HL) 101, 115–16.

Judicial review need not make action slow. *Bank Mellat* demonstrates that national-security measures remain subject to a structured proportionality enquiry; *Shvidler* confirms both the intensity and context-sensitivity of that enquiry in modern sanctions.[75] An urgent order can take immediate effect, with reasons recorded at once, a classified schedule where necessary, automatic referral to a judicial commissioner, and an application to the High Court which does not suspend the order unless the court directs. The existence of review changes the quality of the first decision even when review occurs later.

Compensation should distinguish three losses. A provider directed to continue a lawful service should receive the reasonable incremental cost and loss caused by the order. A provider prevented from an unlawful or unlicensed use should not receive the profit of the prohibited act. Civilians wrongfully deprived of essential service through grossly negligent or deliberately evasive conduct should have access to a statutory fund. Article 1 of Protocol No 1, given domestic effect through the Human Rights Act 1998, permits control of property in the public interest subject to law and fair balance; compensation is an important, though not mechanically decisive, part of that balance.[76]

Speed is preserved by preparation. Designation, controller identification, contact channels, technical maps, compensation formulae and draft order forms should exist before conflict. The six-hour notification is not a six-hour application for permission to save life. Emergency liberty permits immediate action and makes the notice the beginning of public control, not its obstacle. Within seventy-two hours Government must own one of four positions: private continuation, contracted continuation, conditioned continuation or temporary control. Indecision after dependency has formed is itself a decision in favour of the proprietor.

9.3 Comparative Lessons and Limits

The European Union’s NIS 2 Directive widens cybersecurity duties across essential and important entities; the Critical Entities Resilience Directive addresses identification, risk assessment and resilience of entities providing essential services; the Digital Operational Resilience Act imposes specific governance, testing, incident and third-party risk requirements upon finance.[77] None is a code for private participation in armed conflict. Together they demonstrate a regulatory method worth retaining: identify functions in advance, impose proportionate continuity and reporting duties, supervise important third-party providers and distinguish essential from merely large.

United States law contains more muscular emergency precedents. The Defense Production Act permits priority performance and allocation of materials, services and facilities for national defence, while 47 USC § 606 confers presidential communications powers in war and proclaimed emergency subject to statutory conditions.[78] Their breadth should not be transplanted without the United Kingdom’s constitutional safeguards. They answer the assertion that public control of privately owned strategic capacity is conceptually impossible. Modern defence practice confirms why the power matters: the Department of Defense now plans commercial space integration as part of national-security architecture rather than as occasional procurement.[79]

---

[75] *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700 [20], [68]–[76]; *Shvidler v Secretary of State for Foreign, Commonwealth and Development Affairs; Dalston Projects Ltd v Secretary of State for Transport* [2025] UKSC 30 [58]–[75], [146]–[151].

[76] Human Rights Act 1998, s 1 and sch 1; European Convention on Human Rights, Protocol No 1, art 1; *James v United Kingdom* (1986) 8 EHRR 123 [50]–[54]; *Sporrong and Lönnroth v Sweden* (1983) 5 EHRR 35 [69]–[74].

[77] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80, arts 20–23 and 32–34; Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities [2022] OJ L333/164, arts 5–15; Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1, arts 5–16, 17–23 and 28–30.

[78] Defense Production Act of 1950, 50 USC § 4511; Communications Act of 1934, 47 USC § 606.

[79] US Department of Defense (n 21) 3–9.

Three limits should be explicit. First, the Act cannot determine the international lawfulness of force by domestic designation. A Minister may direct a provider only within domestic jurisdiction, and any military or countermeasure consequence requires an independent international legal basis. Secondly, the Act cannot make a civilian object targetable by naming it strategic; targetability remains governed by IHL facts at the time. Thirdly, the Act cannot attribute private conduct to a State merely by regulating it. Attribution follows international law; a direction may itself become attributable because it is public conduct, which is why the legal determination must precede sustained operational control.

The mirror-image memorandum is the discipline joining those limits. It should identify the legal rule, material facts, evidential confidence, anticipated civilian dependence, party-status analysis, attribution analysis and the result if an adversary supplied the materially equivalent function. Where the result differs, the memorandum must state whether the distinction lies in consent, victim status, target, degree of integration, expected effects or another fact. “We support Ukraine” may be sound policy and moral judgment. It is not an actor-neutral rule capable of governing the next provider.

International coordination should begin with interoperable notification, not a universal treaty awaited for decades. Providers commonly operate across allied jurisdictions; regulators can agree a lead authority, secure exchange, common functional taxonomy and recognition of continuity orders. The State with the best corporate nexus may see control; the State hosting ground infrastructure may see technical effect; the belligerent customer may see use. Each requires enough of the whole to prevent fragmentation becoming immunity. Paper 3 develops that jurisdictional problem; the narrower conclusion here is that no domestic authority should be permitted to close its enquiry by pointing to the next fragment.

10. Objections

The first objection is that regulation will deter the next Starlink. A victim under attack cannot wait for committee procedure. The answer is an emergency permission coupled with immediate notice and rapid determination, not prior prohibition. The framework values the hours saved on 26 February 2022 whilst refusing to let an emergency donation become indefinite private war administration.

The second is that Government may make worse decisions than an expert founder. Expertise is indispensable; democratic legitimacy is not a claim of technical superiority. The engineer should advise whether service can be safely segmented. The elected government should decide whether the country accepts strategic and retaliatory consequences, upon legal advice and review.

The third is that property owners cannot be compelled to weaponise products. The framework does not require every provider to serve. It imposes heightened duties upon designated infrastructure whose owner has accepted systemic importance and, where requisition occurs, provides compensation and legal review. Property has always been regulated where its exercise can imperil life or national security.

The fourth is that private provision to Ukraine was plainly good, rendering criticism perverse. The moral conclusion is irrelevant to the general rule. One may support Ukraine, possess friends fighting upon its front, and still recognise that a power desirable in benevolent hands is dangerous when exercised by an adversary or an unstable successor. Law is written for the goose and the gander because ownership, sympathy and government change.

The fifth is that Russia’s illegality removes reciprocity. It removes any entitlement to treat aggression as lawful; it does not remove the strategic consequences of Western inconsistency, private action or elastic precedent. The paper’s argument is not that Russia acquired a right because the West erred. It is that the West weakens the system upon which it depends when it insists upon distinctions it will not state as rules.

The sixth is that the framework intrudes upon foreign affairs, an area in which the executive requires confidence and secrecy. It does intrude, in the proper constitutional sense that statute structures executive power. Parliament need not approve each terminal or image. It should define the circumstances in which private control becomes a national-security function, require reasons, and ensure later review. Secrecy may protect the content of an operation; it cannot answer who is legally competent to decide.

The seventh is that strategic-service designation will cause providers to relocate. Some will alter corporate structure, making extra-territorial reach and procurement leverage necessary. Relocation is not costless where the provider requires United Kingdom spectrum, customers, finance, insurance, launch support, data, personnel or public contracts. International alignment will reduce arbitrage. The possibility of evasion is a reason to design jurisdiction carefully, not to preserve a complete absence of duty.

The final objection is moral hazard: if government guarantees continuity, a belligerent may rely upon private services and take greater risks. The answer is not arbitrary withdrawal by a founder. Public contracts and control orders should state permitted mission classes, renewal conditions and termination processes. A government which wishes to limit escalation must make and own that decision. Private unpredictability is not a principled substitute for restraint.

11. Conclusion

Economic warfare has escaped the old instruments by escaping the old actor. Capital now buys connectivity, observation, computation and continuing technical control. Starlink’s activation for Ukraine before later government contracts showed the best of private speed and the danger of private competence over public war. ICEYE showed how charitable money could acquire a State-quality intelligence function from a foreign commercial constellation. Neither example is reduced to embargo, nor satisfactorily governed by pretending that contract is politically neutral because it is private.

The strict legal position must remain exact. Ukraine did not require NATO membership or a prior defence treaty before requesting collective self-defence under article 51. Russia’s claims concerning nationals, Donetsk, Luhansk, genocide and historical unity form part of the legal record but did not supply a necessary and proportionate right to invade and annex Ukrainian territory. Western controversies do not reverse that conclusion. They do, however, expose the reciprocity trap: rules bent for Kosovo, Iraq, Libya, Syria or favoured proxies will be cited when adversaries provide the same infrastructure and weapons against Western interests.

The proper response is neither impotence nor indiscriminate prohibition. It is early law: designate strategic private infrastructure; preserve rapid humanitarian action; compel notification; migrate control as dependency forms; record who may alter service; segregate civilian functions; allocate liability and indemnity; and require government to test every novel justification against its adversary’s mirror use.

Private wealth may perform acts of immense public good. It may also make decisions which expose millions to reprisal without their consent. The right to make those decisions cannot rest solely upon an inflated wallet, however ingenious the hand which holds it. If a privately controlled keyboard, sensor or constellation supplies the function of a weapon, constitutional law must see the function before international law is forced to judge the effects.

The proposal is consequently neither pacifist nor hostile to invention. It is a demand that power be named at the point at which it becomes public in consequence. Swift assistance may remain swift; collective self-defence may remain effective; companies may continue to innovate and contract. What changes is the fiction that an operational decision remains merely commercial after armies, hospitals and governments depend upon it. Once private infrastructure can determine whether force is possible, the law must determine who may exercise that choice, upon what evidence, for how long, and before whom an account will ultimately be given.

Bibliography

Aoki S, ‘International Law of the Military Uses of Outer Space in Light of the Ukraine Conflict’ in S Furuya, H Takemura and K Ozaki (eds), *Global Impact of the Ukraine Conflict: Perspectives from International Law* (Springer 2023)

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

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

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

Ferraro T, ‘The Applicability and Application of International Humanitarian Law to Multinational Forces’ (2013) 95 *International Review of the Red Cross* 561

Førland TE, ‘The History of Economic Warfare: International Law, Effectiveness, Strategies’ (1993) 30 *Journal of Peace Research* 151

Gordon J, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2010)

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

Hagemeyer-Witzleb TM, *The International Law of Economic Warfare* (Springer 2021)

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 MN Schmitt and J Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines* (Martinus Nijhoff 2007)

Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law*, vol I: Rules (CUP 2005)

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

Kuplic GB and Sawmiller J, ‘Humanity on the Final Frontier: Challenges in Applying International Humanitarian Law to Modern Military Space Operations’ (2025) 107 *International Review of the Red Cross* 200

Mulder N, *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War* (Yale University Press 2022)

Oermann NO and Wolff H-J, *Trade Wars: Past and Present* (OUP 2022)

O’Meara C, ‘Self-defence in Outer Space: Anti-satellite Weapons and the *Jus ad Bellum*’ (2025) 38 *Leiden Journal of International Law* 527

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

Schmid E, ‘Optional but Not Qualified: Neutrality, the UN Charter and Humanitarian Objectives’ (2024) 106 *International Review of the Red Cross* 1044

Schmitt MN, ‘Providing Arms and Materiel to Ukraine: Neutrality, Co-belligerency, and the Use of Force’ (Lieber Institute, 7 March 2022)

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

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

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

Wentker A, ‘At War? Party Status and the War in Ukraine’ (2023) 36 *Leiden Journal of International Law* 643

—— ‘The Armed Attack Exception to Neutrality in International Peace and Security Law’ (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

—— ‘The Evolution and Identification of the Customary International Law of Armed Conflict’ (2018) 51 *Vanderbilt Journal of Transnational Law* 727

Zugliani N, ‘The Supply of Weapons to a Victim of Aggression’ (2024) 35 *European Journal of International Law* 389

Government, institutional and contemporary materials

Attorney General’s Office, ‘Attorney General’s Speech at the International Institute for Strategic Studies’ (11 January 2017) https://www.gov.uk/government/speeches/attorney-generals-speech-at-the-international-institute-for-strategic-studies accessed 31 July 2026

Australian Government, ‘Australia’s Position on How International Law Applies to State Conduct in Cyberspace’ (2021)

Cabinet Office, *The Cabinet Manual* (1st edn, 2011)

—— ‘Critical National Infrastructure’ https://www.gov.uk/government/collections/critical-national-infrastructure accessed 31 July 2026

—— *The National Cyber Strategy 2022* (CP 643, 2022)

—— ‘National Security and Investment Act 2021: Statement for the Purposes of Section 3’ (updated 17 November 2025) https://www.gov.uk/government/publications/national-security-and-investment-statement-about-exercise-of-the-call-in-power/national-security-and-investment-act-2021-statement-for-the-purposes-of-section-3 accessed 31 July 2026

—— *Summary of the 2025 Sector Security and Resilience Plans* (2026)

Cybersecurity and Infrastructure Security Agency, ‘MAR-17-352-01 HatMan—Safety System Targeted Malware’ (18 April 2018)

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

Department for Science, Innovation and Technology, ‘Incident Reporting’ (updated 30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/incident-reporting accessed 31 July 2026

—— *UK Telecommunications Resilience Guidance* (updated 3 April 2024) https://www.gov.uk/government/publications/electronic-communications-resilience-and-response-group-ec-rrg/uk-telecommunications-resilience-guidance accessed 31 July 2026

Department of Health and Social Care, ‘Synnovis Cyber Attack’ (Written Statement HCWS1046, 12 November 2025)

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

Foreign, Commonwealth & Development Office, ‘Application of International Law to States’ Conduct in Cyberspace: UK Statement’ (3 June 2021) https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement accessed 31 July 2026

Government Offices of Sweden, *Position Paper on the Application of International Law in Cyberspace* (July 2022)

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

Group of Governmental Experts, ‘Report on Developments in the Field of Information and Telecommunications in the Context of International Security’ (22 July 2015) UN Doc A/70/174

House of Commons Foreign Affairs Committee, *Libya: Examination of Intervention and Collapse and the UK’s Future Policy Options* (HC 119, 2016–17)

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)

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

ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts* (2021)

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

ICRC, 'International Armed Conflict' (Opinion Paper, March 2008)

—— 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (28 November 2019) https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts accessed 31 July 2026

—— 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (33rd International Conference of the Red Cross and Red Crescent, 2019)

—— *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (34th International Conference of the Red Cross and Red Crescent, 2024)

—— *Explosive Weapons with Wide Area Effects: A Deadly Choice in Populated Areas* (2022)

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

Independent International Commission on Kosovo, *The Kosovo Report* (OUP 2000)

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

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

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

Johnson B and others, 'Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure' (Mandiant, 14 December 2017)

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

Ministère des Armées, *International Law Applied to Operations in Cyberspace* (2019)

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

—— *Joint Doctrine Publication 0-40: UK Space Power* (1st edn, 2023)

Ministry of Defence, *Joint Doctrine Publication 3-51: Non-combatant Evacuation Operations* (3rd edn, 2022)

National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (HC 414, 2017–19)

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 Museums Liverpool, 'Fraser, Trenholm and Company' https://www.liverpoolmuseums.org.uk/artifact/fraser-trenholm-and-company accessed 31 July 2026

NHS England, 'Synnovis Cyber Incident' https://www.england.nhs.uk/synnovis-cyber-incident/ accessed 31 July 2026

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

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

Ofcom, *Connected Nations 2025: UK Report* (2025)

Open-ended Working Group, 'Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2

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

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

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)

US Central Command, 'Statement on New Syrian Force Equipment' (25 September 2015)

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

—— 'DoD General Counsel Remarks at US Cyber Command Legal Conference' (2 March 2020)

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

—— 'Syria Train and Equip Program' (2015)

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

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

US Senate Committee on Armed Services, 'Hearing to Receive Testimony on United States Military Operations to Counter the Islamic State in Iraq and the Levant' (16 September 2015)