The United Kingdom Economic Warfare Prevention and Response Act: An Emergency-Powers Model for Immediate Deterrence

Supplementary Paper 5

Christopher I. V. Farmer

Publication edition, August 2026

Contents

Abstract....6
Table of Authorities....8
Cases....8
Legislation....9
Treaties and International Instruments....10
Standards, Government and Technical Materials....11
Corporate, Technical and Contemporary Materials....13
1. Why Consolidation Is Necessary....14
1.1 The Threat Is Not Hypothetical....14
1.2 Cheap Aggression and the Failure of Broad Deterrence....15
1.3 The Statutory Map in August 2026....15
1.4 Legislating Before the Capability Matures....17
2. Constitutional Speed....17
2.1 The Four Clocks....18
2.2 Speed Within the Constitution....18
2.3 The Civil Contingencies Act 2004, and Why It Does Not Answer....19
3. The International Legal Envelope....20
3.1 Sovereignty, Intervention and Countermeasures....20
3.2 Use of Force and Armed Attack....21
3.3 Non-State Actors and the Territorial State....21
3.4 International Humanitarian Law....22
3.5 The International-Law Gateway....22
4. Definitions and Thresholds....23
4.1 Model Clause 1 — Economic-warfare Act....23
4.2 Model Clause 2 — Serious and Critical Acts....24
4.3 Model Clause 3 — Harm Assessment....24
4.4 Model Clause 4 — Protected Systems and Persons....25
4.5 A Label Which Does Not Decide Its Own Consequence....25
5. Institutions....26
5.1 Economic Warfare Response Authority....26
5.2 Response Group....26
5.3 Independent Commissioner....27
5.4 Interfaces, Not an Additional Silo....27
6. Reporting, Evidence and MOSAIC....28
6.1 Model Clauses 18–21 — Reporting....28
6.2 Model Clause 22 — Central Incident Register....28
6.3 Model Clause 24 — MOSAIC....29
6.4 Attribution Assessment....29
6.5 Confidence, Proof and the Decision Actually Taken....29
7. Emergency Measures....31
7.1 Model Clause 25 — Emergency Preservation....31
7.2 Model Clause 26 — Emergency Identification....32
7.3 Model Clause 30 — Temporary Protective Direction....32
7.4 Model Clause 33 — Domestic Defensive Action....33
7.5 Model Clause 34 — Emergency Asset and Transaction Hold....33
7.6 Offences and Penalties....33
7.7 The Order Must Reach the Smallest Effective Dependency....33
8. Measures Against Operators, Contractors and States....34

8.1 Level 1 — Warning and Preservation....34
8.2 Level 2 — Containment....35
8.3 Level 3 — Personal and Corporate Restraint....35
8.4 Level 4 — State and Collective Cost....35
8.5 The State Which Sees Only a Fragment....36
8.6 Direct Measures and the Operator Who Has Nothing to Freeze....36
9. Private Strategic Capacity and PMSCs....37
9.1 Model Clause 39 — Designation....37
9.2 Model Clauses 40–43 — Controller Duties....37
9.3 Model Clause 47 — PMSC and Intrusion Licensing....38
9.4 The Attribution Manifest....38
9.5 The Strategic Assistance Authorisation....39
10. Force as the Exceptional Defensive Measure....40
10.1 Model Clauses 61–62 — Domestic Decision Authority....40
10.2 The Attribution Threshold for Force....40
10.3 Maximum Harm and Necessity....41
10.4 Proportionality....41
10.5 Host-State Notice....42
10.6 Parliamentary Accountability Without Operational Paralysis....42
10.7 Model Clauses 63–64 — The Defensive Action Certificate....42
10.8 Selecting Cyber or Kinetic Means....43
10.9 Termination and Reassessment....44
10.10 The Live-Target Duty....44
10.11 Deterrence, Maximum Harm and the Limit of Punishment....45
11. Judicial Review, Remedy and Parliamentary Control....46
11.1 Designated Court....46
11.2 Automatic Review and Expiry....46
11.3 Parliamentary Instruments....47
11.4 Remedy....47
11.5 A Public Law of Classified Action....47
12. Applying the Act....48
12.1 Erasure of NHS Data....48
12.2 Winter Energy Pre-positioning....48
12.3 Theft from an Insurer....49
12.4 A Foreign-paid PMSC....49
12.5 Privately Controlled Satellite Intervention....49
12.6 What the Scenarios Prove....50
13. Principal Objections....51
13.1 Commencement, Cost and the Discipline of Use....51
14. Conclusion....53
Draft Provisions: United Kingdom Economic Warfare Prevention and Response Bill....55
Part 1 — Preliminary....55
1 Economic-warfare act....55
2 Reportable, serious and critical acts....55
3 Harm assessment....55
4 Protected systems, persons and partner States....56
5 Independent legal authority....56
6 General principles....56
7 Interpretation....56
Part 2 — Economic Warfare Response Authority....57

8 Establishment....57
9 Functions....57
10 Limits upon functions....57
11 Economic Warfare Response Group....57
12 Duty officers and readiness....57
13 Response Minister....57
14 Economic Warfare Commissioner....58
15 Codes and service standards....58
16 Devolved administrations and regulators....58
Part 3 — Reporting, Evidence and MOSAIC....58
17 Designated reporting organisations....58
18 Initial report....58
19 Further report....58
20 Single-report discharge....59
21 Reporting protection and offences....59
22 Central incident register....59
23 Correction, retention and deletion....59
24 MOSAIC....59
25 Emergency preservation notice....59
26 Emergency identification notice....60
27 Foreign service and conflict of law....60
28 Confidentiality and permitted disclosure....60
Part 4 — Emergency Protective Measures....60
29 Voluntary action and warning....60
30 Temporary protective direction....60
31 Particularity and smallest effective dependency....60
32 Duration and confirmation....60
33 Domestic defensive action....61
34 Emergency asset and transaction hold....61
35 Compensation and compliance defence....61
36 Revocation and off-ramp....61
37 Civil penalties....61
Part 5 — Strategic Private Capacity and High-Risk Services....61
38 Strategic private capacity....61
39 Designation....61
40 Responsible officers and control map....62
41 Continuity and stop capability....62
42 Strategic decision manifest....62
43 Foreign and coercive requests....62
44 Prohibition upon unauthorised strategic intervention....62
45 Strategic assistance authorisation....62
46 Humanitarian safe harbour....62
47 High-risk services licence....63
48 Prime contractor and subcontractor....63
49 Suspension, revocation and debarment....63
Part 6 — Attribution and Graduated Response....63
50 Attribution assessment....63
51 Decision-specific standard....63
52 Level 1 — warning and preservation....63
53 Level 2 — containment....63

54 Level 3 — personal and corporate restraint....63
55 Level 4 — State and collective cost....63
56 Territorial State and fragmented knowledge....63
57 Direct operator measures....64
58 International-law gateway....64
59 Assistance to partner States....64
60 Response guidance....64
Part 7 — Urgent Defensive Force....64
61 No enlargement of international right....64
62 Conditions for urgent defensive force....64
63 Defensive action certificate....64
64 Extreme urgency....65
65 Live-target verification....65
66 Host-State notice and Security Council report....65
67 Parliamentary notification and continuation....65
68 Termination, reassessment and correction....65
Part 8 — Court, Oversight and Remedy....65
69 Jurisdiction....65
70 Designated judges....65
71 Urgent application and return hearing....66
72 Protected material procedure....66
73 Powers of court....66
74 Automatic expiry....66
75 Review and appeal....66
76 Remedies....66
77 Victim support....66
78 Commissioner’s reports....66
79 Parliamentary reporting....66
80 Independent statutory review and renewal....67
Part 9 — Offences, Regulations and General....67
81 Breach of confirmed order....67
82 Destruction and falsification....67
83 Abuse of office under this Act....67
84 Corporate liability....67
85 Security researchers and whistleblowers....67
86 Regulations....67
87 Consequential coordination....67
88 Financial provision....68
89 Crown application....68
90 Territorial extent....68
91 Commencement....68
92 Transitional provision....68
93 Short title....68
Schedule 1 — Protected Functions....68
Schedule 2 — Harm and Attribution Record....68
Part 1 — Harm....68
Part 2 — Attribution....69
Schedule 3 — Defensive Action Certificate....69
Schedule 4 — Authority and Commissioner....69
Bibliography.... 70

Books, Chapters and Articles.....70

Abstract

Economic warfare is cheap to commence, difficult to attribute and capable of producing physical and societal harm after the period in which ordinary legal process can prevent it. English law divides the response amongst cybercrime, intelligence, sanctions, civil contingencies, data protection, sector regulation, corporate law, military prerogative and international law. Each instrument was drawn for a part of the problem. None provides one evidential and constitutional route by which a minister can receive an incident, preserve the disappearing fact, restrain a private controller, impose cost upon a foreign payer and, where an actual or imminent armed attack makes force necessary, defend the United Kingdom before a hospital, water system or winter grid fails.

This paper sets out the United Kingdom Economic Warfare Prevention and Response Act in model clauses. The Act defines economic-warfare acts by function and effect rather than actor or weapon; creates graduated reporting; establishes a central Authority and the federated MOSAIC evidence service; brings private strategic capacity and PMSCs under a control relationship rather than a compliance duty, through designation, a recorded control map, a registered stop capability and a strategic decision manifest; permits urgent preservation, identification, account, credential, service and asset orders; authorises targeted sanctions and coordinated countermeasures; and requires an attribution and harm assessment before serious response.

Speed is a constitutional requirement of effectiveness. The model does not make prior parliamentary debate a condition of every emergency measure. Existing law already recognises urgent executive action followed by short, automatic review: the Civil Contingencies Act 2004 requires emergency regulations to be laid and approved within seven days; the Investigatory Powers Act 2016 permits defined urgent warrants subject to later Judicial Commissioner approval; sanctions legislation employs urgent procedures; and the convention concerning military action recognises that prior Commons debate may be inappropriate in an emergency. The Act adopts that pattern whilst shortening operational decisions to minutes or hours.

The most coercive route contains the strongest conditions. Force cannot be a countermeasure under the law of State responsibility and cannot punish a completed theft. It may be considered only if the United Kingdom is subject to an actual or imminent armed attack, including a cyber operation whose scale and effects are equivalent; force is necessary to halt, repel or prevent that attack; the target is lawful; expected civilian harm is not excessive; and the action complies with international law. The United Kingdom’s published position already recognises that anticipated death, injury and physical destruction bear upon the cyber armed-attack assessment and that self-defence may extend to actual or imminent attack by non-State actors.

Proportionality must not be confined to the damage already realised. The decision maker must assess maximum reasonably credible and foreseeable harm from access, capability, target, season, persistence and replication. Erasure of NHS data or interruption of energy in winter may kill without an explosive. A keyboard which produces the scale and effects of an armed attack does not become legally gentle because the instrument lacks mass.

The model is firm against both payer and operator. A State purchasing contractor attacks may face swift attribution, sanctions, procurement and export restrictions, collective response and lawful countermeasures. A poor, off-grid or deniable operator may face direct account and infrastructure restraint, arrest, seizure, cyber isolation and, only at the armed-attack threshold, force against a lawful person or object. The Act cannot create an international right to do any of these abroad; it creates domestic power, decision discipline and immediate machinery to employ the measures which international law permits.

The safeguard is not delay. It is a named decision maker, independent evidence, legal certification, minimum necessary scope, collateral assessment, automatic expiry, rapid judicial review, parliamentary recall, correction and personal consequence for abuse. A law which demands deliberation after the attack has become irreversible supplies ceremony rather than protection.

Keywords: economic warfare; emergency powers; cyber operations; artificial intelligence; critical national infrastructure; attribution; private strategic capacity; PMSCs; self-defence; proportionality; parliamentary control

Table of Authorities

Cases

A v Secretary of State for the Home Department [2004] UKHL 56, [2005] 2 AC 68.....19

Ahmed v HM Treasury [2010] UKSC 2, [2010] 2 AC 534.....19

Al Rawi v Security Service [2011] UKSC 34, [2012] 1 AC 531.....19

Al-Skeini and Others v United Kingdom (2011) 53 EHRR 18.....41

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) [2007] ICJ Rep 43.....30

Attorney-General v De Keyser's Royal Hotel Ltd [1920] AC 508 (HL).....19

Bank Mellat v HM Treasury (No 2) [2013] UKSC 39, [2014] AC 700.....19

Big Brother Watch and Others v United Kingdom (2022) 74 EHRR 17.....47

Corfu Channel (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4.....36

Council of Civil Service Unions v Minister for the Civil Service [1985] AC 374 (HL).....46

Gabčíkovo-Nagymaros Project (Hungary/Slovakia) [1997] ICJ Rep 7.....23

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226.....41

McCann and Others v United Kingdom (1996) 21 EHRR 97.....41

Microsoft Corporation v United States 829 F 3d 197 (2d Cir 2016), vacated as moot 584 US 236 (2018).....32, 34

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14.....21

Oil Platforms (Islamic Republic of Iran v United States of America) [2003] ICJ Rep 161.....21

R (Privacy International) v Investigatory Powers Tribunal [2021] EWHC 27 (Admin), [2021] QB 936.....34

Prosecutor v Tadić (Appeal Judgment) IT-94-1-A (15 July 1999).....50

R (KBR Inc) v Director of the Serious Fraud Office [2021] UKSC 2, [2022] AC 519.....34

R (Miller) v Secretary of State for Exiting the European Union [2017] UKSC 5, [2018] AC 61.....19

R (Purdy) v Director of Public Prosecutions [2009] UKHL 45, [2010] 1 AC 345.....25

R (UNISON) v Lord Chancellor [2017] UKSC 51, [2020] AC 869.....32

R v Rimmington [2005] UKHL 63, [2006] 1 AC 459.....24–25

R v Secretary of State for the Home Department, ex p Fire Brigades Union [1995] 2 AC 513 (HL).....19

Re B (Children) (Care Proceedings: Standard of Proof) [2008] UKHL 35, [2009] 1 AC 11.....30

Shvidler v Secretary of State for Foreign, Commonwealth and Development Affairs [2025] UKSC 30.....26

Sunday Times v United Kingdom (No 1) (1979–80) 2 EHRR 245.....24

Tariq v Home Office [2011] UKSC 35, [2012] 1 AC 452.....19

United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) (Judgment) [1980] ICJ Rep 3.....50

Youssef v Secretary of State for Foreign and Commonwealth Affairs [2016] UKSC 3, [2016] AC 1457.....26

Legislation

Bribery Act 2010....33

Civil Contingencies Act 2004....14, 17, 19, 32, 37, 43, 47, 52

Civil Procedure Rules 1998....19

Companies Act 2006....38

Company Directors Disqualification Act 1986....35

Computer Misuse Act 1990....14, 33–34, 37, 49, 61

Crime and Courts Act 2013....26–27, 37

Crime (Overseas Production Orders) Act 2019....29, 32, 34

Criminal Finances Act 2017....33, 49

Criminal Justice and Police Act 2001....31

Crown Proceedings Act 1947....47

Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 32 of 2026–27 (as brought from the Commons, 17 June 2026)....16

Data Protection Act 2018....28, 33, 47

Data (Use and Access) Act 2025....16

Economic Crime and Corporate Transparency Act 2023....16, 33, 38, 49, 67

Economic Crime (Transparency and Enforcement) Act 2022....19, 33

Export Control Act 2002....35

Export Control Order 2008, SI 2008/3231....35, 38

Fraud Act 2006....49

Freedom of Information Act 2000....28, 47

Human Rights Act 1998....24–25, 46–47

Intelligence Services Act 1994....27, 47

Investigatory Powers Act 2016....14, 17, 19, 28, 32, 34, 43, 46, 52, 61

Justice and Security Act 2013....19, 46–47

National Security Act 2023....15–16, 35

National Security Act 2023 (Foreign Activities and Foreign Influence Registration Scheme: Specified Persons) (Iran) Regulations 2025, SI 2025/685....16

National Security Act 2023 (Foreign Activities and Foreign Influence Registration Scheme: Specified Persons) (Russia) Regulations 2025, SI 2025/684....16

National Security and Investment Act 2021....16, 35, 37

Network and Information Systems Regulations 2018, SI 2018/506....14, 16, 26–28, 33

Official Secrets Act 1989....28

Outer Space Act 1986....39

Police and Criminal Evidence Act 1984....31, 35, 37

Proceeds of Crime Act 2002....33, 35, 37, 49

Procurement Act 2023....35

Product Security and Telecommunications Infrastructure Act 2022....16

Protection of Trading Interests Act 1980....32

Register of People with Significant Control Regulations 2016, SI 2016/339....38

Sanctions and Anti-Money Laundering Act 2018....14, 19, 27, 30, 33, 35, 47, 52

Security Service Act 1989....27

Space Industry Act 2018....37, 39, 49

Space Industry Regulations 2021, SI 2021/792....39

Statutory Instruments Act 1946....47

Steel Industry (Special Measures) Act 2025....37

Telecommunications (Security) Act 2021....16, 37

Terrorism Prevention and Investigation Measures Act 2011....35

UK General Data Protection Regulation....28

Treaties and International Instruments

Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (signed 3 October 2019, entered into force 3 October 2022) TS No 33/2024....34

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI....21–23, 42, 45

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended); Protocol No 1....25

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....49

Council of Europe Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185....22

International Convention against the Recruitment, Use, Financing and Training of Mercenaries (adopted 4 December 1989, entered into force 20 October 2001) 2163 UNTS 75....38

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171....41

International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10....21

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3....22

Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (opened for signature 12 May 2022) CETS No 224....29

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....39

Standards, Government and Technical 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

Attorney General's Office, 'Cyber and International Law in the 21st Century' (23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century accessed 31 July 2026

Cabinet Office, *Government Cyber Security Strategy 2022–2030* (January 2022)

Cabinet Office, *Professional Standards for Government Intelligence Assessment* (November 2018)

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

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

Crown Prosecution Service, 'Cybercrime—Prosecution Guidance' https://www.cps.gov.uk/prosecution-guidance/cybercrime-prosecution-guidance accessed 6 August 2026

Cybersecurity and Infrastructure Security Agency and others, *Primary Mitigations to Reduce Cyber Threats to Operational Technology* (6 May 2025) https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology accessed 6 August 2026

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

Department for Energy Security and Net Zero, *National Emergency Plan 2023: Downstream Gas and Electricity* (July 2023) https://www.gov.uk/government/publications/national-emergency-plan-downstream-gas-and-electricity-2016 accessed 6 August 2026

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

Department for Science, Innovation and Technology, 'Cyber Security and Resilience Bill' https://www.gov.uk/government/collections/cyber-security-and-resilience-bill accessed 6 August 2026

Department for Science, Innovation and Technology, *Cyber Security and Resilience Bill: Policy Statement* (CP 1299, April 2025)

Department for Science, Innovation and Technology, *Government Cyber Action Plan* (CP 1473, January 2026) https://www.gov.uk/government/publications/government-cyber-action-plan accessed 6 August 2026

Department for Science, Innovation and Technology, 'New Cyber Action Plan to Tackle Threats and Strengthen Public Services' (6 January 2026) https://www.gov.uk/government/news/new-cyber-action-plan-to-tackle-threats-and-strengthen-public-services accessed 6 August 2026

Department for Science, Innovation and Technology, 'Summary of the Bill' (30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill accessed 6 August 2026

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

Financial Conduct Authority, *Principles for Businesses*, Principle 11

Financial Reporting Council, *UK Corporate Governance Code 2024* (22 January 2024)

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

Foreign, Commonwealth & Development Office, *Post-Legislative Scrutiny Memorandum: Sanctions and Anti-Money Laundering Act 2018* (CP 1020, March 2024)

Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (4 April 2025) https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states accessed 6 August 2026

Foreign, Commonwealth & Development Office, 'UK Holds China State-affiliated Organisations and Individuals Responsible for Malicious Cyber Activity' (25 March 2024) https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity accessed 31 July 2026

HM Government, *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK* (CP 643, December 2021)

HM Government, *National Security Strategy 2025: Security for the British People in a Dangerous World* (CP 1338, June 2025)

HM Treasury, *OFSI Guidance for the UK Financial Sanctions Regime* (December 2025)

Home Office, *Equipment Interference Code of Practice* (December 2022)

Home Office, 'Foreign Influence Registration Scheme' https://www.gov.uk/government/collections/foreign-influence-registration-scheme accessed 6 August 2026

House of Commons Library, *Military Action: Parliament's Role* (Research Briefing CBP-10001, 12 March 2026) 6–13 https://commonslibrary.parliament.uk/research-briefings/cbp-10001/ accessed 31 July 2026

House of Commons Political and Constitutional Reform Committee, *Parliament's Role in Conflict Decisions* (HC 892, 2013–14)

House of Lords Constitution Committee, *Fast-track Legislation: Constitutional Implications and Safeguards* (HL 116, 2008–09)

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

House of Lords Delegated Powers and Regulatory Reform Committee, *Democracy Denied? The Urgent Need to Rebalance Power between Parliament and the Executive* (HL 106, 2021–22)

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

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

Intelligence and Security Committee of Parliament, *Russia* (HC 632, 2019–21)

International Code of Conduct Association, *International Code of Conduct for Private Security Service Providers* (as amended 2021)

International Organization for Standardization, *ISO/IEC 27037:2012—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012)

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

Ministry of Defence, *Legal Support to Joint Operations* (Joint Doctrine Publication 3-46, 3rd edn, June 2018)

Ministry of Defence, *The Manual of the Law of Armed Conflict* (OUP 2004)

National Cyber Force, *Responsible Cyber Power in Practice* (4 April 2023) https://www.gov.uk/government/publications/responsible-cyber-power-in-practice accessed 6 August 2026

National Cyber Security Centre and others, *Guidelines for Secure AI System Development* (November 2023)

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

National Cyber Security Centre, *Cyber Assessment Framework v4.0* (6 August 2025) https://www.ncsc.gov.uk/collection/cyber-assessment-framework accessed 6 August 2026

National Cyber Security Centre, *Cyber Incident Response* https://www.ncsc.gov.uk/section/about-ncsc/incident-management accessed 6 August 2026

National Cyber Security Centre, *Mitigating Malware and Ransomware Attacks* (September 2020)

National Cyber Security Centre, ‘UK Calls Out China State-affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians’ (25 March 2024) https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians accessed 31 July 2026

National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, January 2023)

National Institute of Standards and Technology, *Computer Security Incident Handling Guide* (SP 800-61 rev 2, August 2012)

National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (NIST CSWP 29, February 2024)

National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86, August 2006)

National Institute of Standards and Technology, *Secure Software Development Framework* (SP 800-218, February 2022)

National Police Chiefs’ Council, *Good Practice Guide for Digital Evidence* (v5, 2012)

NHS England, ‘Synnovis Cyber Incident’ https://www.england.nhs.uk/synnovis-cyber-incident/ accessed 6 August 2026

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

Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights* (HR/PUB/11/04, 2011), principles 11–24

Review of Intelligence on Weapons of Mass Destruction, *Report of a Committee of Privy Counsellors* (HC 898, 2003–04)

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

UN Human Rights Committee, ‘General Comment No 36: Article 6—Right to Life’ (3 September 2019) UN Doc CCPR/C/GC/36,

United Kingdom, Letter dated 3 December 2015 from the Permanent Representative of the United Kingdom to the United Nations addressed to the President of the Security Council, UN Doc S/2015/928

United Kingdom, Letter dated 7 September 2015 from the Permanent Representative of the United Kingdom to the United Nations addressed to the President of the Security Council, UN Doc S/2015/688

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/ accessed 31 July 2026

US Department of Health and Human Services, Office for Civil Rights, ‘Cyberattack on Change Healthcare’ (Dear Colleague Letter, 13 March 2024) https://www.hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf accessed 6 August 2026

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

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

Corporate, Technical and Contemporary Materials

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

Google Threat Intelligence Group, *Adversarial Misuse of Generative AI* (January 2025) https://cloud.google.com/resources/content/adversarial-misuse-of-generative-ai accessed 6 August 2026

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

Mandiant, ‘TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping’ (10 April 2019) https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections/ accessed 6 August 2026

1. Why Consolidation Is Necessary

The United Kingdom can prosecute unauthorised access, investigate crime, obtain warrants, impose sanctions, regulate essential services, make emergency regulations, deploy intelligence capability and use armed force under the prerogative. The defect is not complete absence of power. It is the interval, fragmentation and mismatch between trigger and consequence. The inherited law of economic warfare remains predominantly organised around measures by States, even as capital, infrastructure and technical capability have escaped that institutional assumption.[1]

A local authority reports ransomware to one body, a provider sees infrastructure in another jurisdiction, intelligence identifies a contractor, the Treasury knows a payment, a regulator considers service continuity and ministers ask whether the operation is foreign policy or crime. Each acts lawfully within a separate instrument. No one owns the decision whether the events form an economic-warfare campaign and which immediate measure can preserve life and evidence.

The Sanctions and Anti-Money Laundering Act 2018 permits regulations for purposes including compliance with international obligations, national security, international peace and security and further foreign-policy objectives; it supports designation and financial restrictions.[2] Magnitsky-style sanctions address serious human-rights abuses and corruption through named persons. These are valuable powers. They do not isolate an autonomous workload in seven minutes, compel a strategic private controller to exercise a stop function, or determine whether a destructive cyber operation is an armed attack.

The Computer Misuse Act 1990 creates offences; the Investigatory Powers Act 2016 authorises specified intelligence and equipment-interference activity through its own safeguards; the Network and Information Systems Regulations 2018 regulate security and incident reporting for defined bodies; the Civil Contingencies Act 2004 addresses emergencies through broad temporary regulation.[3] None should be erased. Consolidation should provide a spine which routes to those powers, adds the missing ones and produces one accountable response record.

The Act proposed here has four constitutional purposes:

1. to recognise economic warfare as a campaign capable of crossing criminal, commercial, national-security and armed-conflict categories;
2. to preserve and aggregate facts before jurisdictional fragmentation destroys them;
3. to act rapidly against the smallest effective payer, operator, account, service or system;
4. to ensure that coercive escalation rests upon the correct domestic and international authority.

The Act is stronger than a sanctions statute because it governs the operational interval. It is narrower than permanent emergency government because powers are incident-bound, graduated and expiring.

1.1 The Threat Is Not Hypothetical

In February 2024 a joint advisory described PRC State-sponsored actors maintaining persistent access in United States communications, energy, transport, water and wastewater organisations, with the assessed intention of disruptive or destructive activity in a major crisis.[4] On 25 March 2024 the United Kingdom publicly attributed compromise of the Electoral Commission to a Chinese State-affiliated

[1] Teoman M Hagemeyer-Witzleb, *The International Law of Economic Warfare* (Springer 2021) 1–17.

[2] Sanctions and Anti-Money Laundering Act 2018, ss 1–2, 11–12 and sch 1.

[3] Computer Misuse Act 1990, ss 1–3ZA; Investigatory Powers Act 2016; Network and Information Systems Regulations 2018, SI 2018/506; Civil Contingencies Act 2004, pt 2.

[4] 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.

entity and separate reconnaissance against parliamentarians to APT31, imposing sanctions upon a company and two individuals.[5] In March 2025 United States authorities alleged a contractor ecosystem in which i-Soon personnel and others acted at public direction, sold stolen information and sometimes acted for private profit.[6]

The evidential class must be stated. The advisory contains technical observations and government assessment; the United Kingdom release is a public State attribution; the United States charges are allegations not yet proved at trial. Together they demonstrate infrastructure pre-positioning, democratic targeting and markets which mix State demand with private initiative. The architecture anticipated in the source dissertation was not an extravagant future.

Critical systems need not be novel to be dangerous. Water, health, insurance and local-government networks contain legacy services, remote access, ordinary credentials and third-party dependencies. An autonomous agent need not invent an unknown exploit if it can repeatedly search for known weakness, attempt access, adapt and persist. Speed of offence is increasingly machine time; speed of public response remains office time.

The physical consequence may arrive indirectly. Removing patient history, medication, imaging or recovery data impairs decisions and treatment. Interrupting electricity in winter disables heating, communications, fuel, water pumping and care. An attack may begin as data impairment and end as death. Classification should follow scale and effects, not whether a keyboard or gun supplied the causal energy.

1.2 Cheap Aggression and the Failure of Broad Deterrence

A wealthy State can pay contractors in currencies meaningful to them but trivial to its defence budget. An individual can rent infrastructure by the minute. A PMSC can subcontract across legal territories. An AI agent does not fear sanctions. If response consists only of a travel ban and asset freeze upon a person with no travel or assets, the law announces disapproval to no practical audience.

Broad State pressure remains necessary where public payment creates the market. The payer should face economic, diplomatic, procurement and technological consequence. Direct measures are also necessary against the operator and infrastructure. The two are complements.

Three further classes defeat the assumption on which the existing toolkit rests, which is that behind every operation there is a payer with assets and a State with a name. The first is the unaffiliated collective. In May 2024 the Cybersecurity and Infrastructure Security Agency, the National Cyber Security Centre and partner agencies published a joint fact sheet recording that pro-Russia hacktivists had compromised small-scale operational technology in water and wastewater, dams, energy and food and agriculture in North America and Europe, reaching internet-exposed human machine interfaces through remote access software, driving pumps and blower equipment beyond their normal operating parameters, disabling alarms and changing administrative passwords to lock the operators out of their own plant. A further joint advisory in December 2025 recorded the same pattern continuing against critical infrastructure more widely.[7]

---

[5] Foreign, Commonwealth & Development Office, ‘UK Holds China State-affiliated Organisations and Individuals Responsible for Malicious Cyber Activity’ (25 March 2024) https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity accessed 31 July 2026; National Cyber Security Centre, ‘UK Calls Out China State-affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians’ (25 March 2024) https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians accessed 31 July 2026.

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

That activity is the clearest available demonstration of the problem this Act exists to answer. The participants are not a State, so State-directed sanctions do not reach them. They are not a company, so procurement and export controls do not reach them. They are frequently not paid at all, so financial restriction has nothing to restrict. They are distributed across jurisdictions and membership changes weekly, so there is often no continuing legal person to designate. And what they did was not the theft of data: it was the physical manipulation of the machinery which supplies drinking water. Every instrument the United Kingdom currently holds for this is addressed either to a State or to a person with something to lose.

The second class is the operator whose capability is supplied rather than possessed. The National Cyber Security Centre assessed in January 2024 that artificial intelligence would almost certainly increase the volume and heighten the impact of cyber attacks over the following two years, and that it lowers the barrier to entry specifically for novice cyber criminals, hackers-for-hire and hacktivists, which are precisely the three categories least reachable by sanctions. Its 2025 assessment carried the analysis to 2027, concluding that artificial intelligence will almost certainly continue to make intrusion operations more effective and efficient, that frequency and intensity will rise, and that a digital divide will open between systems which keep pace and a large proportion which do not. The significance for a statute is not that machines will attack unaided. It is that the relationship between an attacker's resources and the harm he can cause is being severed, and every existing response instrument is calibrated to that relationship.[8]

The third is simultaneity. A single operation may now run through infrastructure in several jurisdictions at once, with the route selected by the system rather than by the operator, as the definition of an autonomous system in clause 7 recognises. The same operation may at the same moment be lawful where the infrastructure sits, criminal where the operator sits, and, by scale and effects, an armed attack where the consequence lands. Mutual assistance is designed for sequence rather than for concurrency, and the evidence which would establish the relation between the fragments is held by different private parties under different legal regimes, each of which will lawfully decline a request it has no duty to answer.

The response should impose expected cost without indiscriminate population harm. A precise credential suspension, equipment seizure or contract exclusion may deter more effectively than a general embargo. Where the attack meets the armed-attack threshold and lesser measures cannot stop it, force must remain legally available. Removing it in advance would tell an adversary that placing the operator outside the banking system creates immunity.

1.3 The Statutory Map in August 2026

The case for consolidation must be tested against the law which now exists, rather than against the law which existed when the dissertation was submitted. Parliament has not been idle. The National Security Act 2023 created offences concerned with espionage, foreign interference, sabotage and preparatory conduct, and Part 4 established the Foreign Activities and Foreign Influence Registration Scheme. The Scheme came into force on 1 July 2025; its enhanced tier presently applies to Russia and Iran, and it can expose a contractual or other directed relation between a foreign power and one who acts within the

[7] National Security Act 2023, pts 1–4; Home Office, 'Foreign Influence Registration Scheme' https://www.gov.uk/government/collections/foreign-influence-registration-scheme accessed 6 August 2026; National Security Act 2023 (Foreign Activities and Foreign Influence Registration Scheme: Specified Persons) (Russia) Regulations 2025, SI 2025/684; National Security Act 2023 (Foreign Activities and Foreign Influence Registration Scheme: Specified Persons) (Iran) Regulations 2025, SI 2025/685.

[8] Telecommunications (Security) Act 2021; Product Security and Telecommunications Infrastructure Act 2022, pt 1; National Security and Investment Act 2021; Economic Crime and Corporate Transparency Act 2023, pts 1–3 and ss 196, 199–206; Data (Use and Access) Act 2025.

United Kingdom.[9] This is important intelligence and a useful offence where registration was required. It is not an incident command system, nor does registration decide attribution under international law.

The Telecommunications (Security) Act 2021 strengthens duties imposed upon public electronic-communications providers; the Product Security and Telecommunications Infrastructure Act 2022 regulates defined connectable products; the National Security and Investment Act 2021 permits scrutiny of acquisitions; the Economic Crime and Corporate Transparency Act 2023 improves beneficial-ownership and corporate information and extends corporate criminal responsibility; and the Data (Use and Access) Act 2025 alters the rules governing data.[10] Each statute closes a real opening. None supplies a single route from hostile access, through rapidly vanishing evidence, to an order served upon the controller able to stop the operation.

The Network and Information Systems Regulations 2018 remain the cross-sector resilience instrument. As at 6 August 2026 the Cyber Security and Resilience (Network and Information Systems) Bill has completed its Commons stages and is in committee in the House of Lords, but has not become law. Its proposed expansion to managed-service providers, data centres and large load controllers, together with stronger reporting and regulatory powers, confirms rather than defeats the present argument: resilience duties and incident reporting are indispensable, but they govern the condition and conduct of regulated providers; they do not determine the foreign-policy, sanctions, countermeasure or self-defence consequence of the incident reported.[11] Two comparisons are worth making precisely, because a reader who knows the Bill will draw them anyway. The Bill permits designation of critical suppliers and a penalty of up to four per cent of turnover, and the model Act adopts the same ceiling deliberately so that a person is not exposed to two unrelated maxima for conduct arising from one incident. What clause 39 adds to that designation is not a further compliance duty but a control relationship: a named responsible officer, a map of who may grant, withdraw or stop the service, a registered stop capability and a manifest of strategic decisions, none of which a supplier-designation regime built for procurement assurance supplies. The reporting comparison runs the other way and is the sharper of the two. The Bill requires notification within twenty-four hours and a full report within seventy-two, which is a proportionate period in which to describe an incident to a regulator. It is not a period in which to preserve a log that an attacker is deleting, and the one-hour critical notice in clause 18 exists for that reason and for no other. The difference between the two clocks is the whole of the argument in Part 2. This paper therefore treats the Bill as a measure with which the proposed Act must be coordinated, not as an enactment already available to ministers.

The National Security Strategy 2025 describes cyber and economic security as essential to ordinary national life, records hostile pre-positioning against energy and supply chains, and places the National Cyber Force, the National Security and Investment Act and telecommunications security within a broader policy of making the United Kingdom a harder target.[12] The Government Cyber Action Plan

[9] Network and Information Systems Regulations 2018, SI 2018/506; Department for Science, Innovation and Technology, ‘Cyber Security and Resilience Bill’ https://www.gov.uk/government/collections/cyber-security-and-resilience-bill accessed 6 August 2026; Department for Science, Innovation and Technology, ‘Summary of the Bill’ (30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill accessed 6 August 2026; Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 32 of 2026–27, HL Bill 32 (as brought from the Commons, 17 June 2026).

[10] HM Government, *National Security Strategy 2025: Security for the British People in a Dangerous World* (CP 1338, June 2025) paras 12–23, 18–23 under ‘Build sovereign and asymmetric capabilities’ https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world accessed 6 August 2026; HM Government, *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK* (CP 643, December 2021).

[11] Department for Science, Innovation and Technology, ‘New Cyber Action Plan to Tackle Threats and Strengthen Public Services’ (6 January 2026) https://www.gov.uk/government/news/new-cyber-action-plan-to-tackle-threats-and-strengthen-public-services accessed 6 August 2026; Department for Science, Innovation and Technology, *Government Cyber Action Plan* (CP 1473, January 2026) https://www.gov.uk/government/publications/government-cyber-action-plan accessed 6 August 2026; Cabinet Office, *Government Cyber Security Strategy 2022–2030* (January 2022).

[12] Civil Contingencies Act 2004, ss 26–28.

announced in January 2026 adds a Government Cyber Unit and substantial resilience investment across departments and the wider public sector.[13] Those developments provide institutions with which the Authority proposed here should interlock. They do not remove the need for a legal spine. An administrative unit can coordinate only the powers it possesses; a strategy can announce resolve but cannot compel a cloud controller, freeze an account or preserve foreign evidence.

The resulting map contains four different questions which are too often treated as one. First, was the protected organisation sufficiently resilient? Secondly, has a person committed an offence? Thirdly, is conduct attributable to a State or otherwise internationally wrongful? Fourthly, which immediate measure is domestically authorised and internationally lawful? Negligent security may coexist with foreign aggression; an offence may be proved without State attribution; State responsibility may exist without proof beyond reasonable doubt against an individual; self-defence may be necessary before a prosecution can be assembled. The proposed Act does not collapse these questions. It ensures that one timed record carries each to the decision maker competent to answer it.

That distinction also prevents a politically convenient reversal of blame. The fact that an operator used an unpatched system may justify regulatory action against the operator, but does not cleanse the attacker's conduct. Conversely, the fact that the attacker was foreign does not excuse a designated controller who ignored a known, cheaply remediable danger. External aggression and domestic resilience are parallel subjects of legal judgement. A statute which uses the second to avoid the first would reward the very method by which cheap hostile power is exercised.

1.4 Legislating Before the Capability Matures

An objection follows directly from the evidence just given, and it is the objection a government is most likely to make. The May 2024 fact sheet itself records that the hacktivist activity it describes was mostly limited to unsophisticated technique producing nuisance effect. Nobody has yet died because a volunteer changed a set point on a water pump. On that view the Act legislates for a threat which has not arrived, and the constitutionally proper course is to wait until it does.

The premise is accepted. The conclusion does not follow, for two reasons which are independent of each other.

The first is that the same advisory which describes the technique as unsophisticated also records that the actors are capable of technique posing physical threat to insecure and misconfigured operational environments, and that the activity has continued from 2022 to the present. The relevant question for a legislature is not the sophistication of the last incident but the direction and rate of change, and on that the United Kingdom's own technical authority has published an assessment rather than a speculation: frequency and intensity rising, capability uplift concentrated in the least reachable actors, and a widening divide between systems which keep pace and those which do not. A statute drafted to the capability of 2026 and enacted in 2028 will be applied in 2032.[14]

The second reason is structural and matters more. Most of what this Act creates cannot be brought into existence at the moment it is needed. A duty officer rota, a bench of security-cleared judges with secure clerking, authenticated service to providers, tested contact routes to foreign hosts, an incident register with history in it, an attribution discipline which people have practised, and a control relationship with designated private capacity are all institutional facts which take years to become usable and which are worthless on the day they are first attempted. Part 2 makes the point about individual powers: a power

[13] Investigatory Powers Act 2016, ss 24–25, 109–110 and corresponding urgent-warrant provisions; Investigatory Powers Act 2016 Explanatory Notes, paras 434–35 and 553–58.

[14] Cabinet Office, *The Cabinet Manual* (1st edn, October 2011) paras 5.36–5.38 https://www.gov.uk/government/publications/cabinet-manual accessed 31 July 2026.

which can be exercised quickly in theory but requires a department to discover whom to telephone is not an emergency power. The same is true of the Act as a whole. Readiness is the component with the longest lead time and it is the component which must exist before the emergency rather than after it.

It should be said plainly that this is a precautionary argument, and that precautionary arguments are the standard justification offered for emergency legislation which later proves overbroad. What disciplines it here is the asymmetry between the two halves of the Act. The readiness components are cheap, reversible and largely invisible to the public: a register, a rota, a code, a contact list, a reporting duty. The coercive components are staged under clause 91(2) and cannot be commenced until the Secretary of State certifies readiness, are reviewed by an independent reviewer under clause 80(1), and expire under clause 80(2) and (3) with Part 7 renewable only by a further Act. A state which legislates early and turns out to have been wrong has bought a register and a rota it did not need. A state which legislates late and turns out to have been wrong discovers on the night that it holds powers it cannot exercise, because the people who would have to exercise them have never met.

That asymmetry, rather than any prediction about what attackers will do, is the case for enacting now.

2. Constitutional Speed

The objection to rapid power is constitutional abuse; the objection to delayed power is preventable harm. Both are real. The answer is not to choose one. It is to separate acts by reversibility and intrusion, permit the least irreversible emergency acts first, and make review automatic.

Preserving a named log is not producing it. Temporarily isolating a government credential is not destroying a foreign server. Freezing an asset is not confiscating it. Warning a hospital is not publicly attributing a State. Domestic legislation should permit each at the earliest evidential threshold appropriate to it.

Existing law supplies models. Under the Civil Contingencies Act emergency regulations lapse after thirty days and, once laid, after seven days unless each House approves; provision exists for parliamentary recall.[15] Under urgent warrant provisions of the Investigatory Powers Act, executive issue may precede Judicial Commissioner approval for a short period.[16] Sanctions regulations may use made-affirmative or urgent procedures under the 2018 Act. These examples prove that immediate executive action and constitutional review are not opposites.

Military action remains under prerogative power. The Cabinet Manual records a convention that the House of Commons should have an opportunity to debate before troops are committed, except where an emergency makes that inappropriate; practice has been inconsistent and Parliament has no legal approval role.[17] A 2026 Commons Library briefing confirms both the convention and its emergency exception.[18] The model Act does not require prior debate before an urgent defensive strike. It requires a contemporaneous legal and evidential certificate, notice to opposition leaders where security permits, recall or statement at the earliest feasible time, and classified scrutiny.

---

[15] House of Commons Library, *Military Action: Parliament's Role* (Research Briefing CBP-10001, 12 March 2026) 6–13 https://commonslibrary.parliament.uk/research-briefings/cbp-10001/ accessed 31 July 2026.

[16] *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] AC 508 (HL); *R v Secretary of State for the Home Department, ex p Fire Brigades Union* [1995] 2 AC 513 (HL); *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5, [2018] AC 61, [45]–[56].

[17] Civil Contingencies Act 2004, ss 26–28; Investigatory Powers Act 2016, ss 24–25 and 109–110; Sanctions and Anti-Money Laundering Act 2018, ss 11–12 and 55; Economic Crime (Transparency and Enforcement) Act 2022, ss 58–59; Foreign, Commonwealth & Development Office, *Post-Legislative Scrutiny Memorandum: Sanctions and Anti-Money Laundering Act 2018* (CP 1020, March 2024) paras 102–19.

[18] *Ahmed v HM Treasury* [2010] UKSC 2, [2010] 2 AC 534; *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 AC 68; *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700, [68]–[76].

Speed also requires readiness before crisis. Forms, thresholds, duty officers, secure communications, provider contacts, target-review teams and draft orders must exist. A power which can be exercised quickly in theory but requires a department to discover whom to telephone is not an emergency power.

2.1 The Four Clocks

The Act should operate four clocks:

- **minutes**: warning, voluntary containment, authenticated preservation, government-network defence and convening the Response Group;
- **hours**: emergency preservation orders, credential and service restraint, provisional designation, sanctions preparation, host-State notice, intelligence and legal assessment;
- **days**: judicial confirmation, parliamentary statement, fuller attribution, production process, allied coordination and correction;
- **weeks**: prosecution, compensation, licence action, treaty request, independent review and legislative approval where required.

The clocks overlap. A court may be available within an hour; a foreign host may cooperate immediately. They are maximum design assumptions, not excuses to wait.

The system should measure time from first qualifying notice, not from the moment a central department accepts the severity. Otherwise institutional delay disappears from the record. Each hand-off is signed and timed through MOSAIC.

Figure 1. Seconds and minutes serve automated containment; hours serve ministerial direction and legal certification; days serve judicial and parliamentary review; weeks serve prosecution, compensation, licensing and treaty action.

2.2 Speed Within the Constitution

Emergency power is not rendered constitutional by placing the word “emergency” before it. The executive must identify the source, subject and limit of the power which it claims. *De Keyser’s Royal Hotel* establishes that where statute occupies the field the Crown cannot select a prerogative route in order to escape the statutory terms; *Fire Brigades Union* prevents prerogative action from frustrating Parliament’s scheme; and *Miller* confirms that prerogative power cannot be used to alter domestic law

or extinguish statutory rights.[19] The proposed Act must consequently say which domestic acts it authorises, which existing enactments it routes to, and which matters—most notably the international legality of force—it cannot manufacture.

The constitutional design is a ladder of increasing intrusion. An authenticated request to preserve a particular log for twenty-four hours is less intrusive than production; temporary suspension of a compromised credential is less intrusive than seizure of an undertaking; a domestic freezing direction is less intrusive than confiscation; a covert cyber effect abroad is not rendered less serious merely because no aircraft crosses a border. The evidential threshold, office holder and period of review must rise as reversibility falls. This is not the familiar error of placing every measure behind the highest threshold. If preservation must await proof adequate for force, the evidence needed to decide force may have disappeared.

Existing legislation demonstrates three useful constitutional forms. Under section 27 of the Civil Contingencies Act 2004 emergency regulations must be laid as soon as reasonably practicable and lapse seven days after laying unless approved by each House; under section 26 they ordinarily lapse after thirty days in any event. Under the Investigatory Powers Act 2016 an urgent warrant may be issued before Judicial Commissioner approval, but the Commissioner must decide within the period ending with the third working day after issue. Section 55 of the Sanctions and Anti-Money Laundering Act 2018 uses made-affirmative procedure for specified regulations, and the Act's urgent designation machinery can operate immediately subject to a limited period and later certification.[20] The periods differ because the measures differ. Their common constitutional lesson is that immediate legal effect may precede, but must not replace, defined scrutiny.

The courts have likewise rejected the proposition that national security creates an unreviewable island. *Ahmed* invalidated asset-freezing orders made without sufficient parliamentary authority; *A v Secretary of State for the Home Department* subjected exceptional detention to legality and proportionality; and *Bank Mellat* required a rational connection, consideration of less intrusive means and a fair balance notwithstanding the security context.[21] These authorities do not require a judge to command the incident. They require Parliament to define the power and permit the court to test whether the executive used it upon the terms enacted.

For that reason the first order should carry its own review file. It must state the incident, protected interest, evidence class, confidence, contrary hypothesis, legal source, measure, scope, technical owner, expiry and route to challenge. The file is created when the order is made, not reconstructed after litigation begins. A judge who receives the contemporaneous alternatives and rejected measures can review an urgent decision; a judge who receives only a polished ministerial narrative months later can review little beyond prose.

Secrecy requires a procedure, not an exemption. Closed material, special advocates and security-cleared counsel are already known to English law, whilst *Al Rawi* warns that closed civil procedure cannot be invented by the court without statutory authority.[22] The Act should expressly permit protected-material procedure for confirmation and review, preserve the gist requirement to the extent compatible with

[19] *Al Rawi v Security Service* [2011] UKSC 34, [2012] 1 AC 531; Justice and Security Act 2013, pt 2; Civil Procedure Rules 1998, pt 82; *Tariq v Home Office* [2011] UKSC 35, [2012] 1 AC 452.

[20] Cabinet Office, *The Cabinet Manual* (n 17) paras 5.36–5.38; House of Commons Library, *Military Action: Parliament's Role* (n 18) 6–29; House of Lords Constitution Committee, *Waging War: Parliament's Role and Responsibility* (HL 236-I, 2005–06); House of Commons Political and Constitutional Reform Committee, *Parliament's Role in Conflict Decisions* (HC 892, 2013–14).

[21] 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; Attorney General's Office, 'Cyber and International Law in the 21st Century' (23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century accessed 31 July 2026.

safety, and require an open judgment stating at least the legal basis and result. The burden rests upon the State to justify what cannot be disclosed; classification is not proof of relevance.

Devolution and local responsibility do not disappear in a national incident. Health, policing, local government, water and resilience arrangements engage different settlements and operational bodies. The Authority should notify and include the affected devolved administration at the first safe opportunity, without giving any one body a veto over a measure lawfully reserved to the United Kingdom Government. Where a direction enters devolved competence or burdens a devolved public service, reasons and cost allocation should be recorded. Central speed bought by institutional blindness merely moves delay into implementation.

Nor should Parliament receive a binary choice between prior debate and ignorance. Where operations cannot safely await debate, the Prime Minister should notify the Leader of the Opposition and the Intelligence and Security Committee chair upon confidential terms if practicable; make a public statement as soon as operational safety permits; and seek Commons approval before continuing a sustained operation beyond the emergency period. The war-powers convention remains political rather than legal, and practice has varied, but emergency exception need not mean indefinite executive ownership.[23] A seven-day outer period for a parliamentary statement is appropriate; a shorter classified notification should be expected where facilities exist.

Finally, no clock should renew itself. A minister may renew only upon current evidence that the statutory conditions continue, after receiving the reviewer's account of effectiveness, collateral effect and available alternatives. A service restriction which was necessary at hour one may become punitive at day three. An operation which failed to reach the attacker may require termination rather than rhetorical escalation. Speed is constitutionally defensible when it is coupled to an equally rapid obligation to stop.

2.3 The Civil Contingencies Act 2004, and Why It Does Not Answer

An obvious objection precedes everything in this paper. Parliament has already enacted a general emergency-powers statute of very wide scope, and the case for a new Act must begin by explaining why that one will not do.

The Civil Contingencies Act 2004 is not a narrow instrument. Section 19 defines an emergency as an event or situation which threatens serious damage to human welfare, to the environment, or to the security of the United Kingdom, and expressly includes disruption of an electronic or other system of communication, of facilities for transport, and of services relating to health, money, food, water, energy and fuel.[24] A sustained attack upon the grid, upon hospital systems, or upon payment infrastructure is an emergency within that definition upon the ordinary meaning of the words, and nothing in this paper suggests otherwise. Section 21 supplies the triple lock: the emergency must have occurred, be occurring or be about to occur; the making of provision must be necessary for the purpose of preventing, controlling or mitigating an aspect or effect of it; and the need for that provision must be urgent.[25] Section 22 then confers a power of extraordinary breadth, since emergency regulations may make any provision which the person making them is satisfied is appropriate, including any provision which

[22] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10, arts 22 and 49–54.

[23] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, arts 2(4), 42 and 51; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 [191], [195]; *Oil Platforms (Islamic Republic of Iran v United States of America)* [2003] ICJ Rep 161 [51].

[24] Foreign, Commonwealth & Development Office, 'Application of International Law' (n 31) para 6.

[25] Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817, 836–58; Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) rr 69–71 and commentary.

could be made by Act of Parliament, and may confer functions, require or prohibit acts, and disapply or modify enactments.[26]

A reader may reasonably ask what is left to legislate. Four things are, and each is central to what this paper proposes.

The first is that the Act reaches the emergency and not the interval before it. Section 21(1) requires that an emergency has occurred, is occurring or is about to occur. The measures with which this paper is most concerned sit before that line and are designed to sit there: preserving a named log, asking a provider whether it controls a specified account, isolating a single credential. Those are the reversible, low-threshold acts which the constitutional method defended above places at the foot of the ladder precisely so that they may be taken early and upon modest evidence. To bring them within the 2004 Act one must first assert that a national emergency is about to occur, which is both a considerable escalation and, upon most days, untrue. An instrument available only once the position is grave is not the instrument for keeping it from becoming grave.

The second is that the Act cannot carry the offences. Section 23(3) restricts emergency regulations to offences triable only summarily and punishable by imprisonment not exceeding three months or a fine not exceeding level 5 upon the standard scale, and forbids any alteration of criminal procedure.[27] The offences in Part 9 of the model Act, being unlicensed provision of a high-risk service, destruction of preserved evidence and abuse of office, are indictable and carry seven and ten years. Whether those penalties are right is a fair question and Part 13 below takes it. That they cannot be made under the 2004 Act is not arguable, and any scheme resting upon them requires primary legislation.

The third is that the Act cannot build a standing architecture, because it was designed not to. Section 26 lapses emergency regulations thirty days after they are made, and section 23(4) forbids them to amend either Part 2 of the Act itself or the Human Rights Act 1998.[28] Those limits are correct and this paper would not remove them. But a duty to report within one hour, a permanent incident register, an attribution assessment discipline, a licensing regime for high-risk services and a rota of security-cleared judges are not emergency measures at all. They are the readiness which determines whether an emergency measure can be exercised in time, and Part 2 of the 2004 Act is expressly the wrong place for anything intended to outlast the emergency by more than a month.

The fourth is that the Act does not reach the decision this paper treats most carefully. Part 7 of the model Act governs the conditions upon which the United Kingdom may use force in self-defence: the standard of confidence, the certification of the Attorney General, the target review, the certificate and the parliamentary report. Nothing in sections 19 to 23 of the 2004 Act touches that decision. Emergency regulations are a domestic regulation-making power, whereas the use of force abroad rests upon the prerogative, constrained by article 51 of the Charter and by the conventions described above. A statute which cannot regulate the most consequential act in the sequence cannot be the statute which governs the sequence.

There is a fifth point, evidential rather than doctrinal. Part 2 of the 2004 Act has never been invoked. It was not used in the coronavirus pandemic, which was the largest civil emergency in the United Kingdom since the Act was passed and which fell squarely within section 19; the Government legislated afresh in the Coronavirus Act 2020 and otherwise relied upon the Public Health (Control of

[26] 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; Daniel Bethlehem, 'Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors' (2012) 106 *American Journal of International Law* 770, 775–77.

[27] Attorney General's Office, 'Attorney General's Speech' (n 36).

[28] Daniel Bethlehem (n 36) 770–77; Olivier Corten, *The Law Against War* (2nd edn, Hart 2021) 487–532.

Disease) Act 1984.[29] Two readings of that record are available and both support the argument here. If the restraint reflects the strength of the safeguards, then those safeguards are the reason the power is unsuitable for measures which must be taken in the first hour of an incident whose gravity is not yet established. If it reflects institutional reluctance, then a power which government will not reach for under any pressure so far encountered is not a power upon which a response can be planned. Either way, an Act designed to be used is worth more than an Act reserved for a category of emergency which has not yet been declared.

None of this criticises the 2004 Act, which does what it was built to do. The argument is one of fit. That Act is a residual power of last resort, general in subject matter, temporary in effect and triggered by gravity. What economic warfare requires is a specific architecture, permanent in its readiness components, triggered by function rather than by gravity, and graded so that the reversible measures are available long before anything which would satisfy section 21. The two are complements, the model Act should say so upon its face, and clause 87 accordingly provides for consequential coordination rather than displacement.

It is worth naming the tradition this method belongs to, because a reader of the emergency-powers literature will place it whether or not the paper does. The debate in that literature has largely concerned whether emergency should be governed through law at all: the extra-legal position holds that officials should act outside the legal order and answer for it afterwards, while the accommodation position holds that the crisis should be brought within the legal framework and disciplined there. This Act belongs to the second. What the accommodation literature has not settled, having been occupied with whether to legislate, is how the powers should be graded once legislated. Reversibility is the answer proposed here: not that an emergency power should be small, but that the evidential threshold for exercising it should rise with what cannot afterwards be undone, and that review should attach automatically rather than upon application.[30]

3. The International Legal Envelope

A domestic Act may authorise a minister in English law. It cannot make an act lawful internationally. Every extraterritorial measure must identify the separate international basis.

3.1 Sovereignty, Intervention and Countermeasures

Cyber operations may breach sovereignty according to the position adopted and facts; coercive interference in a State's domaine réservé may constitute prohibited intervention; operations causing effects equivalent to kinetic force may violate article 2(4). States do not agree upon every threshold or whether sovereignty is a standalone rule in cyberspace. The United Kingdom's public statements should be applied as its position, with contrary positions acknowledged.[31]

An injured State may take countermeasures against the responsible State subject to the ILC conditions: the measure responds to a prior internationally wrongful act, seeks compliance, is directed against the responsible State, is proportionate, is preceded by a call for cessation and notification where circumstances permit, and is reversible so far as possible. Countermeasures must not affect the

[29] Evelyne Schmid and Ayşe Özge Erceiş, 'The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility' (2023) 33 *Swiss Review of International and European Law* 577, 581–90.

[30] 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), 51(5)(b), 52(2) and 57; ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Nils Melzer ed, ICRC 2009).

[31] Ministry of Defence, *The Manual of the Law of Armed Conflict* (OUP 2004); Ministry of Defence, *Legal Support to Joint Operations* (Joint Doctrine Publication 3-46, 3rd edn, June 2018).

prohibition of force, fundamental human rights, humanitarian obligations prohibiting reprisals or peremptory norms.[32]

Urgency may permit immediate measures necessary to preserve rights before formal notice. That is not a general exception from conditions. The Act should require counsel to identify whether an act is retorsion, countermeasure, consent-based cooperation, domestic jurisdiction over a provider, necessity, self-defence or another basis.

Retorsion—an unfriendly but lawful act—includes some diplomatic, procurement and economic restrictions. It should ordinarily precede more controversial countermeasures where effective. Sanctions may be retorsion or implement international obligations; their legal basis and impact vary.

3.2 Use of Force and Armed Attack

Article 2(4) prohibits the threat or use of force subject principally to Security Council authority and self-defence under article 51. Not every unlawful cyber operation is force; not every use of force is an armed attack. The distinction matters because article 51 responds to armed attack.[33]

The United Kingdom's 2021 statement says that a cyber operation may constitute an armed attack where scale and effects are equivalent to a kinetic armed attack, and lists actual or anticipated physical destruction, injury and death among relevant factors.[34] The word "anticipated" is important. Law need not wait for a compromised safety controller to kill where evidence establishes the attack and outcome.

Kinetic describes physical motion; armed attack is a legal threshold of scale and effects. A gun which kills through kinetic force and a keyboard which predictably causes the same death differ in mechanism, not necessarily legal consequence. The harder cases concern severe loss of function or economic damage without physical destruction. State positions vary. The Act should not declare every systemic economic loss an armed attack, but should require a reasoned scale-and-effects assessment.[35]

An actual armed attack may consist of an operation underway though its final effect has not occurred. Anticipatory self-defence against an imminent attack is recognised by the United Kingdom, including in relation to non-State actors; imminence is assessed in context, including the last feasible opportunity to act.[36] It cannot mean force against a speculative future capability.

3.3 Non-State Actors and the Territorial State

The United Kingdom has stated that self-defence may extend to actual or imminent armed attacks by non-State actors and has supported action where the territorial State is unable or unwilling to prevent

[32] Foreign, Commonwealth & Development Office, 'Application of International Law' (n 31); International Law Commission, 'Draft Articles' (n 32) arts 20–25 and 49–54; Charter of the United Nations (n 33) arts 2(4), 39–42 and 51; Council of Europe Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185, arts 16–18 and 23–35.

[33] International Law Commission, 'Draft Articles' (n 32) arts 25, 49–54; *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)* [1997] ICJ Rep 7, [51]–[58]; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 [41]; *Oil Platforms* (n 33) [43], [73]–[77]; Protocol I (n 40) arts 51(5)(b) and 57.

[34] Charter of the United Nations (n 33) art 51; *Military and Paramilitary Activities in and against Nicaragua* (n 33) [195], [199]; Pearce Clancy, 'Neutral Arms Transfers and the Russian Invasion of Ukraine' (2023) 72 *International and Comparative Law Quarterly* 527; Alexander Wentker, 'The Armed Attack Exception to Neutrality in International Peace and Security Law' (2024) 73 *International and Comparative Law Quarterly* 963; Niccolò Zugliani, 'The Supply of Weapons to a Victim of Aggression: The Law of Neutrality in Light of the Conflict in Ukraine' (2024) 35 *European Journal of International Law* 389.

[35] *R v Rimmington* [2005] UKHL 63, [2006] 1 AC 459, [33]–[35]; *R (Purdy) v Director of Public Prosecutions* [2009] UKHL 45, [2010] 1 AC 345; Human Rights Act 1998, ss 3 and 6; *Sunday Times v United Kingdom (No 1)* (1979–80) 2 EHRR 245, [49].

[36] Human Rights Act 1998, ss 3, 6 and 8; Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221 (European Convention on Human Rights, as amended) arts 6, 8, 10 and 11 and Protocol No 1, art 1; *R v Rimmington* (n 45) [33]–[35]; *R (Purdy) (n 45)*.

them.[37] The doctrine is disputed. Some States and scholars require attribution or a more restrictive relation to the territorial State; others accept the United Kingdom's view.[38]

The Act should reflect the Government's published position whilst forcing the decision to address:

1. evidence that the non-State actor is conducting the armed attack;
2. location and target identity;
3. territorial-State consent or request;
4. notice and opportunity to act, unless impossible or dangerous;
5. capacity and willingness of the territorial State;
6. why action is confined to the attacker and not treated as force against the host population;
7. necessity and proportionality;
8. Security Council notification under article 51.

Where the host cooperates, its arrest or isolation is ordinarily preferable. Where it controls and directs the attacker, State attribution and response may follow. Where it genuinely sees only one fragment, Paper 3's due-diligence analysis applies; the victim should not punish an innocent host for the controller's sharding.[39]

3.4 International Humanitarian Law

If an armed conflict exists, target selection follows IHL. Civilians are protected unless and for such time as they directly participate; members of organised armed groups may be targetable according to status and function under the applicable analysis; objects must satisfy article 52(2)'s two limbs; distinction, proportionality and precautions apply.[40]

A private person is not an "object of war". A server is not targetable because investigators dislike its owner. A system executing military action may make an effective contribution and its neutralisation may offer definite military advantage. Shared civilian use requires feasible technical discrimination and collateral assessment.

The United Kingdom's Manual of the Law of Armed Conflict and operational legal-support doctrine already require legal advice and rules of engagement.[41] The Act should not recreate tactical law. It should ensure that the economic-warfare classification does not bypass it.

3.5 The International-Law Gateway

The model clauses should require an international-law gateway before any measure directed abroad, because identical technical conduct may stand upon different legal foundations. A provider may isolate

[37] *Bank Mellat* (n 21) [68]–[76]; *Shvidler v Secretary of State for Foreign, Commonwealth and Development Affairs* [2025] UKSC 30; *Youssef v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKSC 3, [2016] AC 1457.

[38] National Cyber Security Centre, *Cyber Incident Response* https://www.ncsc.gov.uk/section/about-ncsc/incident-management accessed 6 August 2026; Crime and Courts Act 2013, pt 1; National Cyber Force, *Responsible Cyber Power in Practice* (4 April 2023) https://www.gov.uk/government/publications/responsible-cyber-power-in-practice accessed 6 August 2026; HM Treasury, *OFSI Guidance for the UK Financial Sanctions Regime* (December 2025); Network and Information Systems Regulations 2018, SI 2018/506.

[39] National Cyber Security Centre, *Cyber Incident Response* (n 48); Crime and Courts Act 2013, pt 1; Security Service Act 1989; Intelligence Services Act 1994; National Cyber Force, *Responsible Cyber Power in Practice* (n 48); Sanctions and Anti-Money Laundering Act 2018; Network and Information Systems Regulations 2018, SI 2018/506.

[40] Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 32 of 2026–27, cls 11–18; Department for Science, Innovation and Technology, 'Summary of the Bill' (n 11); Department for Science, Innovation and Technology, *Cyber Security and Resilience Bill: Policy Statement* (CP 1299, April 2025); Regulatory Policy Committee, *Cyber Security and Resilience (Network and Information Systems) Bill Impact Assessment: RPC Opinion* (17 November 2025).

[41] Network and Information Systems Regulations 2018, regs 11, 11A and 12; UK General Data Protection Regulation, art 33; Data Protection Act 2018; Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 32 of 2026–27, cls 8–17; Financial Conduct Authority, *Principles for Businesses*, Principle 11.

its own service under contract and domestic regulation; a foreign State may consent to an operation; an injured State may take a non-forcible countermeasure against the responsible State; a hostile account may be removed as lawful retorsion; law-enforcement evidence may be obtained under treaty or overseas-production process; and force may be used only upon the much narrower Charter route. The word “cyber” does not combine these bases.[42]

The gateway is a short schedule completed by counsel. It asks: upon whose territory and infrastructure will the act operate; whose legal rights are affected; is the conduct independently lawful, consented to, a countermeasure, required by necessity, or self-defence; what prior wrong or attack is relied upon; which notification is required; what human-rights or humanitarian limits continue; and how will the act end? Where more than one basis is advanced, each must independently sustain the part attributed to it. A domestic contractual right to suspend an account cannot sustain intrusion into a foreign machine; article 51 cannot be used to justify confiscating an English bank balance when statute supplies the required domestic authority.

Necessity under article 25 of the Articles on State Responsibility must not be confused with necessity in self-defence. The former is a tightly confined circumstance precluding wrongfulness, unavailable where the act seriously impairs an essential interest of the State towards which the obligation exists or where the invoking State contributed to the situation; it is not a general power to conduct hostile operations. Necessity in article 51 asks whether force is required to halt, repel or prevent an armed attack. Countermeasure proportionality, self-defence proportionality and IHL proportionality likewise answer different questions.[43]

Collective self-defence adds a further gateway. The attacked State must declare itself attacked and request assistance; the assisting State must remain within the defensive necessity and proportionality of that request. A private corporation cannot create the request, and a commercial contract is not a substitute for it. Conversely, no defence treaty is required before a State may request lawful assistance under article 51. Treaty membership determines obligations and institutional machinery; it is not the source of the inherent right.[44]

This schedule is deliberately categorical. The danger in an emergency is not only indecision but legal drift: an operation begins as provider assistance, continues as a countermeasure and ends with effects which amount to force, whilst no official records the transition. The Authority must trigger reclassification whenever target, geography, effect or purpose changes materially. An act lawful at the first gateway does not carry a permanent legal passport.

4. Definitions and Thresholds

The legislation should avoid one definition which makes an insurance fraud “war” and a catastrophic data attack “crime” according to the attacker’s label.

4.1 Model Clause 1 — Economic-warfare Act

1 Economic-warfare act

[42] Data Protection Act 2018, pts 2–4; Freedom of Information Act 2000, ss 23–24, 31, 36 and 43; Official Secrets Act 1989; Investigatory Powers Act 2016, pt 8; *Big Brother Watch and Others v United Kingdom* (2022) 74 EHRR 17.

[43] International Organization for Standardization, *ISO/IEC 27037:2012—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (2012); National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86, August 2006); National Institute of Standards and Technology, *Computer Security Incident Handling Guide* (SP 800-61 rev 2, August 2012); UK General Data Protection Regulation, arts 5 and 25.

[44] Convention on Cybercrime (n 42) arts 16–18 and 29–30; Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (opened for signature 12 May 2022) CETS No 224; Crime (Overseas Production Orders) Act 2019; UK–US Agreement on Access to Electronic Data (signed 3 October 2019, entered into force 3 October 2022) TS No 33/2024.

1) In this Act an “economic-warfare act” is conduct, or a coordinated course of conduct, which—

1) is intended, or is reasonably capable in the circumstances, materially to impair, coerce, destabilise, appropriate or deny the economic, technological, institutional, democratic, defence or essential-service capacity of the United Kingdom, a protected person or a partner State; and

2) is carried out by or through a State, organisation, undertaking, private military or security company, autonomous system or individual.

2) Conduct may constitute an economic-warfare act whether effected by financial, commercial, cyber, informational, technological, logistical, physical or combined means.

3) Lawful competition, industrial action, journalism, academic research, protest, authorised security testing and the ordinary exercise of contractual rights do not constitute an economic-warfare act unless the conditions in subsection (1) are independently satisfied and the conduct is unlawful under an applicable rule.

4) Classification under this section does not determine whether conduct is a use of force, armed attack, act of aggression, armed conflict, offence or internationally wrongful act.

The phrase “reasonably capable” permits prevention but is tied to material impairment and circumstances. Subsection (3) prevents an executive from calling unpopular commerce war merely because it causes loss. The need for an independently applicable rule prevents the label itself creating illegality.[45]

4.2 Model Clause 2 — Serious and Critical Acts

2 Reportable, serious and critical acts

1) An act is “serious” where actual or maximum reasonably credible foreseeable harm includes—

1) material interruption of an essential service;

2) substantial danger to life or physical safety;

3) material interference with democratic institutions, national security or defence;

4) systemic financial, commercial or data-integrity harm;

5) substantial theft or destruction of strategically important property, information or capability; or

6) a material increase in the capacity for repeated serious acts.

2) An act is “critical” where—

1) serious harm is occurring or imminent;

2) delay is likely materially to reduce the ability to prevent or mitigate it; and

3) action taken within that period is capable of preventing or mitigating that harm.

Maximum harm is not fantasy. Clause 3 supplies its method.

4.3 Model Clause 3 — Harm Assessment

3 Harm assessment

1) A decision under Parts 3 to 7 must consider actual harm and the maximum harm reasonably credible and foreseeable at the time.

[45] *Re B (Children) (Care Proceedings: Standard of Proof)* [2008] UKHL 35, [2009] 1 AC 11; *Bank Mellat* (n 21); Sanctions and Anti-Money Laundering Act 2018, ss 11, 22–23 and 38–40; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43, [396]–[407]; Ministry of Defence, *Legal Support to Joint Operations* (n 41).

2) The assessment must address, so far as relevant—

1) access and privilege obtained;

2) systems and persons reachable;

3) capability, autonomy, persistence and replication;

4) target function, season, population dependency and alternatives;

5) safety controls, recovery and reversibility;

6) apparent objective and prior conduct;

7) confidence, contrary explanations and risk of deception; and

8) likely harm of the proposed response.

3) A possibility unsupported by evidence is not reasonably credible merely because its consequence would be grave.

The final subsection prevents maximum-harm analysis becoming a rhetorical permission slip.

4.4 Model Clause 4 — Protected Systems and Persons

Protected systems include NHS and social-care systems, water, energy, transport, communications, food, finance, government, democratic processes, defence, emergency services, research of strategic importance and designated supply chains. Protected persons include those within the United Kingdom and persons or partner States designated under an agreement or assistance decision.

Designation by regulation should be affirmative, with an urgent made-affirmative route where a new dependency appears. Public schedules may describe function without exposing vulnerable technical detail.

4.5 A Label Which Does Not Decide Its Own Consequence

“Economic warfare” is the organising classification of the Act, not an offence of unlimited content and not a declaration of war. The criminal law must identify prohibited conduct and mental element with sufficient certainty; compulsory orders must identify their statutory conditions; and interference with privacy, expression, property and occupation must be lawful, necessary and proportionate under the applicable rights framework.[46] Clause 1 therefore opens the coordination machinery only when material strategic effect and independent unlawfulness coincide. The executive cannot make journalism, industrial action or ordinary competition unlawful by describing its consequence as inconvenient.

Four thresholds should remain visible throughout the Act. A **reportable event** supplies information and may be reported before responsibility is known. A **serious economic-warfare act** engages coordination, assistance and proportionate preservation. A **critical act** permits short emergency restraint because delay threatens material harm. A **Charter-level attack** engages the separate use-of-force analysis. The categories may change with evidence; they do not automatically escalate. Most incidents will never enter the last.

The “maximum reasonably credible foreseeable harm” formulation is likewise a decision rule, not a substantive offence. It directs attention to access and consequence before harm is complete, but

[46] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, January 2023); National Cyber Security Centre and others, *Guidelines for Secure AI System Development* (November 2023); Department for Science, Innovation and Technology, *AI Cyber Security Code of Practice* (31 January 2025); Google Threat Intelligence Group, *Adversarial Misuse of Generative AI* (January 2025) https://cloud.google.com/resources/content/adversarial-misuse-of-generative-ai accessed 6 August 2026.

subsection 3(3) excludes unsupported possibility. Credibility should be assessed from observed privilege, reachable systems, capability, persistence, target dependency, safety architecture, season and conduct. Foreseeability concerns what a competent decision maker could reasonably apprehend at the time, not what counsel can imagine after the event.

Intent and capability must not be treated as interchangeable. A contractor may intend grave harm yet possess no means; a compromised safety controller may be capable of grave harm before motive is known. Preservation and containment may follow capability and urgency. Punishment and personal culpability require the mental element of the applicable offence. State responsibility follows its own rules. The model clauses repeatedly separate these because a law designed for prevention cannot wait for motive, whilst a law worthy of publication cannot punish capability alone.

The protected-system schedule should be functional and technology-neutral. A small supplier may be indispensable to a hospital or grid although it falls below a turnover threshold; a famous platform may be replaceable for the incident concerned. Designation should turn upon consequence, substitutability, time to recover and interdependence. Reasons may omit exploitable details, but the designated person must receive enough to challenge whether the statutory function exists. *Bank Mellat* and *Shvidler* demonstrate the continuing importance of rational connection and fair balance where targeted economic restrictions impose very substantial individual consequence.[47]

5. Institutions

5.1 Economic Warfare Response Authority

8 Establishment

1) There is established a body corporate called the Economic Warfare Response Authority.

2) The Authority shall—

1) receive and triage reports;

2) operate the United Kingdom MOSAIC node and incident register;

3) coordinate preservation, attribution and response;

4) designate and supervise strategic private capacity;

5) support ministers, courts, regulators and investigators;

6) maintain international cooperation; and

7) publish standards and reports.

3) The Authority does not exercise an investigative, intelligence, sanctions or military power except where this Act or another enactment expressly confers it.

The Authority is a conductor, not a secret department which absorbs every function. NCSC should supply technical leadership; NCA and police criminal investigation; FCDO international action; HM Treasury and the Office of Financial Sanctions Implementation financial measures; departments and regulators sector authority; intelligence agencies their statutory functions; the Ministry of Defence military planning.[48]

[47] Convention on Cybercrime (n 42) arts 16–17 and 29–30; Criminal Justice and Police Act 2001, pt 2; Police and Criminal Evidence Act 1984, ss 19–22; National Police Chiefs' Council, *Good Practice Guide for Digital Evidence* (v5, 2012).

[48] *Microsoft Corporation v United States* 829 F 3d 197 (2d Cir 2016), vacated as moot 584 US 236 (2018); *R (KBR Inc) v Director of the Serious Fraud Office* [2021] UKSC 2, [2022] AC 519; Crime (Overseas Production Orders) Act 2019; UK–US Agreement on Access to Electronic Data (n 54); Protection of Trading Interests Act 1980.

5.2 Response Group

A permanent Economic Warfare Response Group should include senior duty representatives of those bodies, the Attorney General's Office, Cabinet Office, affected devolved administrations and technical specialists. It may convene within fifteen minutes through a secure system.

The Group records one common facts table, disputed points, decision owners and deadlines. It does not decide by anonymous consensus. Each power remains with its lawful office holder.

For critical incidents a minister is designated Response Minister. For possible force, the Prime Minister or authorised senior minister, Attorney General or alternate law officer and Chief of the Defence Staff enter the separate process in Part 6.

5.3 Independent Commissioner

An Economic Warfare Commissioner, appointed through a process involving Parliament and holding security-cleared technical staff, reviews emergency orders, protected-category queries, manifest access, correction, discrimination, provider burden and the Authority's compliance.

The Commissioner may inspect systems and classified records, require information, issue recommendations and refer unlawfulness to the court or appropriate prosecutor. Operational veto belongs to courts and statutory decision makers, not a general auditor; the Commissioner's real-time access permits rapid review without becoming command.

5.4 Interfaces, Not an Additional Silo

Institutional clarity is a condition of speed. The National Cyber Security Centre is the national technical authority and incident-response lead for nationally significant cyber events; the National Crime Agency and territorial police investigate crime; the intelligence agencies operate under their statutory functions and warrants; the National Cyber Force conducts operations through the authorities applicable to GCHQ, defence and the intelligence services; OFSI implements financial sanctions; Ofcom and sector regulators supervise resilience; the Cabinet Office coordinates national-security and civil-contingencies machinery.[49] The Authority should not duplicate any of them. Its statutory function is to maintain the common incident, evidence and decision spine across them.

Every power is consequently assigned twice: first to an owner, and secondly to a dependency. The owner is the office holder legally capable of exercising it. The dependency is the evidence, provider action, diplomatic request or technical condition without which the power will be ineffective. The Response Group may see the whole dependency map; it cannot exercise a member's power by collective vote. This avoids the opposite defects of dispersed knowledge and anonymous decision.

The incident commander is not necessarily the legal decision maker. NCSC may coordinate technical containment whilst a constable seeks a warrant, a minister directs a provider, OFSI prepares a designation and the Prime Minister considers force. One person should own overall objectives, but the record must show the separate signatures. "Government decided" is constitutionally insufficient where the question is whether the designated person decided upon the statutory test.

The Cyber Security and Resilience Bill proposes stronger coordination and information sharing between NIS regulators, government and law enforcement. The Authority should receive reports through that architecture if enacted and should provide a single receipt capable of satisfying overlapping duties, but its functions extend beyond resilience regulation to attribution, private strategic

[49] *Bank Mellat* (n 21); *Ahmed* (n 21); Civil Contingencies Act 2004, ss 20–28; Investigatory Powers Act 2016, ss 24–25 and 109–110; *R (UNISON) v Lord Chancellor* [2017] UKSC 51, [2020] AC 869.

control and response.[50] A consequential-amendment power should permit routing and terminology to be conformed after the Bill's passage; it should not permit ministers to enlarge emergency powers by regulation.

Resourcing must follow the clock. A nominal twenty-four-hour court with no secure clerk, a ministerial duty rota without technical advice, or a foreign contact list last tested two years earlier is not readiness. The Authority should publish service standards; conduct annual cross-government and provider exercises; report missed clocks; and commission red-team tests in which false attribution, provider refusal, devolved-system failure and allied disagreement are introduced deliberately. Performance data may be classified in detail, but failure itself should not disappear from public account.

6. Reporting, Evidence and MOSAIC

6.1 Model Clauses 18–21 — Reporting

A designated organisation must report a critical act within one hour of reasonable confirmation, a serious act within six hours and a fuller report within seventy-two hours. The first report states what is known; attribution is not required.[51]

The Authority may adjust a period for technical impossibility or overriding life-safety work. Good-faith preliminary error is not penalised. Knowing concealment, reckless material misstatement and unjustified failure attract graduated civil penalties; intentional destruction after preservation may be criminal.

One submission should satisfy overlapping cyber-reporting duties where the Authority has agreed routing with the relevant regulator. The receipt identifies each obligation satisfied. This avoids asking a hospital to report the same emergency in five formats.

Confidentiality protects personal, commercial, security, legal and intelligence information. Disclosure is permitted for defence, investigation, court, regulation, warning, oversight and lawful international cooperation. Public-interest and subject-access questions remain governed by applicable law and specific exemptions.[52]

6.2 Model Clause 22 — Central Incident Register

The original dissertation proposed a central cyber-incident database. The stronger model is central coordination with federated custody. The Authority maintains case metadata, source classification, receipts, decisions and public lessons; raw evidence remains with the lawful custodian or accredited repository unless produced.[53]

The register distinguishes direct observation, custodian record, forensic finding, intelligence assessment, model analysis, State attribution, allegation and legal finding. A public release cannot silently convert one into another.

---

[50] Computer Misuse Act 1990, ss 1–3ZA; National Cyber Force, *Responsible Cyber Power in Practice* (n 49); Michael N Schmitt (ed), *Tallinn Manual 2.0* (n 35) rr 4, 6–7 and 20–21; Foreign, Commonwealth & Development Office, 'Application of International Law' (n 31).

[51] Proceeds of Crime Act 2002, pts 2 and 5; Criminal Finances Act 2017, ss 1–16; Sanctions and Anti-Money Laundering Act 2018, ss 3–9 and 11–17; Economic Crime (Transparency and Enforcement) Act 2022, pts 2–3.

[52] Economic Crime and Corporate Transparency Act 2023, ss 196 and 199–206; Bribery Act 2010, s 7; Criminal Finances Act 2017, ss 45–46; Network and Information Systems Regulations 2018, regs 18–20; Data Protection Act 2018, ss 155–158.

[53] Investigatory Powers Act 2016, pts 5 and 9; Home Office, *Equipment Interference Code of Practice* (December 2022); Computer Misuse Act 1990, ss 1–3ZA; *R (Privacy International) v Investigatory Powers Tribunal* [2021] EWHC 27 (Admin), [2021] QB 936.

Access is role-, case- and purpose-bound, continuously logged and independently reviewable. Correction propagates to every recipient. Retention follows purpose and legal hold; a deletion tombstone may preserve the audit fact without the personal content.

6.3 Model Clause 24 — MOSAIC

The Authority operates the Multijurisdictional Operation Signal Attribution and Integrity Correlation service specified in Paper 3B. The statutory purposes are authenticated discovery, rapid preservation, source integrity, lawful evidence routing and controller-manifest custody.

MOSAIC does not itself authorise production, interception, equipment interference, sanction or force. Each request identifies its independent basis. Foreign nodes receive no general search of British data.[54]

Regulations prescribe common schemas, cryptographic assurance, trust tiers, protected categories, refusal, correction, transparency and accreditation. Technical specifications may be updated by the Authority after consultation, but cannot enlarge statutory power.

6.4 Attribution Assessment

Before a Level 4 or 5 response, the Authority produces an attribution assessment separating:

1. operation and campaign linkage;
2. infrastructure and account control;
3. human or organisational identity;
4. financing and benefit;
5. State-organ status or governmental authority;
6. instructions, direction or control;
7. acknowledgement or adoption;
8. host knowledge and due diligence;
9. confidence and contrary hypotheses;
10. evidential class and disclosure.

The assessment applies the relevant legal route. Payment supports an inference; it does not automatically prove article 8 control. A State may bear responsibility for its own omission without the attacker's conduct becoming its act. A domestic minister may impose some sanctions on a lower evidential standard than a criminal court; the difference is stated.

Intentional fragmentation, failure to maintain a required manifest and destruction may support an adverse inference in the proceedings for which Parliament permits it, subject to burden and fairness. They do not conclusively establish foreign State responsibility.

6.5 Confidence, Proof and the Decision Actually Taken

There is no single "attribution standard" for every response. A criminal conviction demands proof beyond reasonable doubt; a civil order ordinarily follows the civil standard, adjusted in its application to the seriousness and inherent probability of the allegation; a sanctions designation depends upon its statutory test and remains reviewable; a public diplomatic attribution is an executive act with political and legal consequence; State responsibility asks whether the conduct and relation satisfy the applicable international rule; operational self-defence is judged upon the information reasonably available to the

[54] Crime (Overseas Production Orders) Act 2019; Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (n 54); *Microsoft Corporation v United States* (n 58); *R (KBR Inc)*.

State when action was necessary.[55] The Act should require the decision maker to name the standard or test used, not conceal it behind a percentage.

Confidence nevertheless requires structure. The assessment should distinguish direct fact, technical inference, identity inference, organisational inference and legal conclusion. It should record source independence, access, chain of custody, time, alternative explanation, deception opportunity and what additional fact would change the result. Two reports derived from the same telemetry are one evidential root, not corroboration. A government statement repeating a contractor report does not create an independent source merely by changing the letterhead.

For irreversible action the statute should require a high degree of confidence in the proposition necessary to the target. That proposition may be narrower than complete campaign attribution. If a particular controller is certainly issuing destructive commands, it may be possible to stop that controller whilst sponsorship remains uncertain. If the individual is uncertain but a workload can be isolated without injury, the order may follow the workload. Force against a payer, by contrast, cannot be inferred merely from evidence that money passed somewhere within the contractor market.

The Authority should maintain an attribution matrix rather than a single score. The rows are campaign, infrastructure, operator, integrator, payer, State organ, territorial host and protected target; the columns are identity, conduct, knowledge, control, location, capability, timing and confidence. The legal adviser then identifies which cells are essential to the proposed measure. This prevents a strong technical link to infrastructure from lending unearned confidence to State direction, and it makes disagreement intelligible.

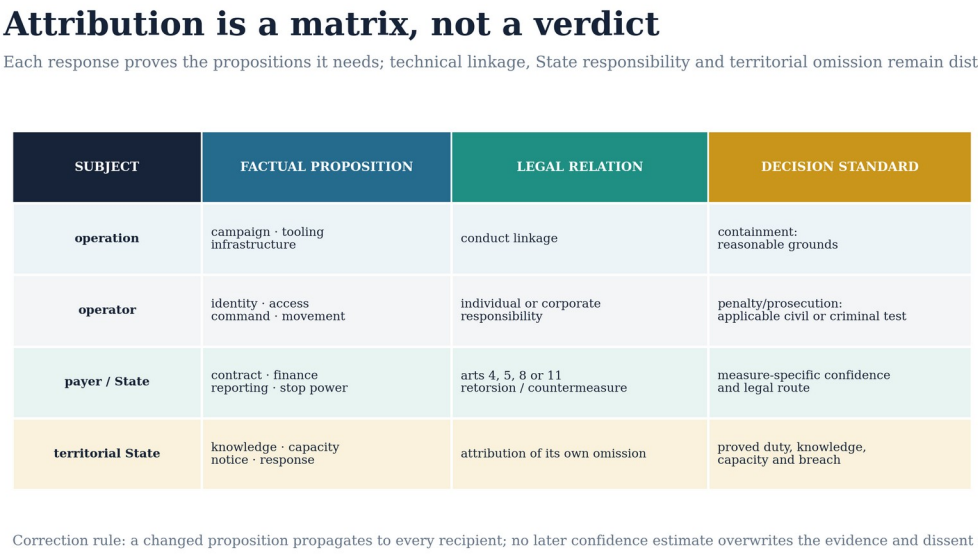

Figure 2. The attribution matrix separates factual propositions, legal relations and the evidential threshold required by the particular response.

Artificial intelligence may assist clustering, translation, anomaly detection and hypothesis generation; it must not be represented as an eyewitness. The model, version, prompt or task, data boundary, validation and material output should be preserved where it influenced the decision. Known model error, poisoned telemetry and adversarial manipulation belong in the deception assessment. An unexplained model score cannot discharge a minister’s duty to be satisfied.[56]

[55] Police and Criminal Evidence Act 1984, ss 8 and 19; Proceeds of Crime Act 2002; Company Directors Disqualification Act 1986; Procurement Act 2023, ss 57–59 and schs 6–7; National Security Act 2023, pts 1–3; Terrorism Prevention and Investigation Measures Act 2011.

Public attribution should state evidential class without exposing operational detail. “The Government assesses”, “forensic evidence demonstrates”, “an indictment alleges” and “a court found” are not stylistic variants. They tell the reader what has happened. Where confidence later falls materially, the correction should identify which link failed and which consequences have been withdrawn. An attribution regime worthy of coercive power must be able to retreat from error as quickly as it advances upon evidence.

7. Emergency Measures

Emergency powers should be ordered by reversibility. The Authority may warn and seek voluntary action; a duty officer may preserve; a minister may impose brief restraint; a court confirms continued intrusion; Parliament reviews the larger regime.

7.1 Model Clause 25 — Emergency Preservation

25 Emergency preservation notice

1) A designated officer may issue an emergency preservation notice where he reasonably believes that—

1) specified data are likely to be relevant to a serious economic-warfare act;

2) the data are at material risk of alteration, loss or destruction; and

3) preservation is necessary and proportionate.

2) The notice must identify, so far as practicable, the data, custodian, period, purpose, officer, issue time, expiry and means of challenge.

3) A notice requires preservation and prohibits intentional destruction; it does not authorise disclosure.

4) An emergency notice expires after seven days unless confirmed by a judge or other authority specified for the applicable data.

5) The custodian shall return a signed receipt or a reasoned inability or refusal.

Seven days is a backstop, not a service target. The recipient should acknowledge in minutes for a critical case. Production proceeds through existing or expressly created authority. The distinction permits speed without treating seizure of content as preservation.[57]

The notice may be served through a foreign MOSAIC node only where an agreement or foreign law permits. A British signature proves origin, not foreign jurisdiction.

7.2 Model Clause 26 — Emergency Identification

An identification notice may require a provider subject to United Kingdom jurisdiction to state whether it controls a specified account, domain, service, workload or payment identifier and to provide the competent contact for lawful process. It does not require content.

---

[56] Sanctions and Anti-Money Laundering Act 2018; Export Control Act 2002; Export Control Order 2008, SI 2008/3231; National Security and Investment Act 2021; International Law Commission, ‘Draft Articles’ (n 32) arts 30–31 and 49–54; *Bank Mellat* (n 21).

[57] *Corfu Channel (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 22; *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) [1980] ICJ Rep 3, [58]–[74]; Evelyne Schmid and Ayşe Özge Erceiş (n 39); Antonio Coco and Talita de Souza Dias, ‘Cyber Due Diligence: A Patchwork of Protective Obligations in International Law’ (2021) 32 *European Journal of International Law* 771; Russell Buchan, ‘Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm’ (2016) 21 *Journal of Conflict and Security Law* 429.

The notice requires reasonable grounds and particularity. Bulk enumeration is prohibited. Protected professions and political activity receive enhanced approval. Results are retained only for the case.

Foreign providers offering relevant services in the United Kingdom may be required to appoint a legal representative for notices, consistently with international obligations. Conflict of law is recorded and brought before the designated court.[58]

7.3 Model Clause 30 — Temporary Protective Direction

30 Temporary protective direction

1) The Response Minister may direct a person within United Kingdom jurisdiction to take specified action where—

1) a critical economic-warfare act is occurring or imminent;

2) the person controls a service, account, credential, system or capability materially enabling the act or necessary to mitigate it;

3) the direction is necessary and proportionate; and

4) judicial approval cannot reasonably be obtained without materially increasing harm.

2) A direction may require preservation, isolation, suspension, credential revocation, traffic filtering, warning, continuity, exercise of a registered stop function or supply of technical assistance within the person's capability.

3) A direction may not require—

1) indiscriminate weakening of security;

2) disclosure beyond an independent lawful power;

3) force against a person; or

4) action manifestly contrary to international law.

4) The direction expires after twenty-four hours unless approved by a designated judge and may in no case continue under emergency authority beyond seventy-two hours.

The court may continue, narrow or discharge the direction under a separate protective order. The person receives compensation for exceptional reasonable cost where the direction chiefly serves public defence rather than correcting his own breach. Good-faith compliance with a facially valid direction is protected; negligent collateral disclosure and deliberate excess are not.

Twenty-four hours is long for a credential and short for court preparation. A rota of security-cleared judges should make review possible sooner. The statutory maximum prevents convenience becoming emergency.[59]

7.4 Model Clause 33 — Domestic Defensive Action

The Authority, NCSC and public bodies may take proportionate technical action upon systems they lawfully control to detect, isolate, deceive, rate-limit, redirect or remove hostile activity. They may share indicators and warnings under the Act.

[58] Police and Criminal Evidence Act 1984, ss 8 and 19; Proceeds of Crime Act 2002, pts 2 and 5; Computer Misuse Act 1990; Crime and Courts Act 2013, pt 1; National Cyber Force, *Responsible Cyber Power in Practice* (n 49).

[59] National Security and Investment Act 2021; Telecommunications (Security) Act 2021; Space Industry Act 2018; Steel Industry (Special Measures) Act 2025; Civil Contingencies Act 2004, pt 2; HM Government, *National Security Strategy 2025* (n 12) paras 17–23 under 'Build sovereign and asymmetric capabilities'.

Action upon a third party's system requires consent, direction, warrant, court order or another lawful basis. The phrase "active defence" does not erase the Computer Misuse Act or foreign sovereignty.[60]

A sinkhole, honeypot or token may collect personal data. The authorisation records purpose, scope, retention and access. Technical defence remains law.

7.5 Model Clause 34 — Emergency Asset and Transaction Hold

Where funds or economic resources are reasonably believed to finance, constitute proceeds of, or be necessary to a critical act, a minister or authorised court may impose a temporary hold for forty-eight hours pending a sanctions designation, restraint order or discharge.

The order may reach cryptocurrency and payment intermediaries within jurisdiction. It is particularised; ordinary customers of an exchange are not frozen because one account is suspect. Financial institutions receive a defence for compliance and a route for essential expenses.

The lower emergency threshold is justified by short duration and reversibility. Confiscation requires ordinary process.[61]

7.6 Offences and Penalties

Intentional breach of a confirmed protective order, destruction of preserved evidence, concealment of a designated strategic controller, unlicensed high-risk PMSC operation and knowing supply of materially false manifest information are offences. Corporate liability follows the applicable directing-mind or failure-to-prevent provisions enacted; individual guilt still requires the specified mental element.

Civil penalties consider harm, culpability, cooperation, turnover, benefit, remediation and ability to pay. A maximum percentage of worldwide turnover may be necessary for global providers; a fixed fine may be absorbed as a fee. Penalty cannot substitute for a technically useful order.[62]

Whistleblowers and security researchers require protected reporting. A researcher who discovers an exposed strategic system and reports responsibly should not be treated as the attacker. Authorised testing remains outside the definition.

7.7 The Order Must Reach the Smallest Effective Dependency

The emergency hierarchy begins with the smallest dependency capable of stopping the act. It may be a token, credential, model endpoint, payment instruction, domain, account, virtual machine, physical port, named item of equipment or human operator. An order directed to the entire company or population when the effective dependency is known is not merely clumsy; it may be disproportionate and may increase the very service failure the Act exists to prevent.

---

[60] Companies Act 2006, ss 171–174; Financial Reporting Council, *UK Corporate Governance Code 2024* (22 January 2024); 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, *Guidelines for Multinational Enterprises on Responsible Business Conduct* (2023).

[61] Swiss Federal Department of Foreign Affairs and ICRC, *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (17 September 2008); International Code of Conduct Association, *International Code of Conduct for Private Security Service Providers* (as amended 2021); International Convention against the Recruitment, Use, Financing and Training of Mercenaries (adopted 4 December 1989, entered into force 20 October 2001) 2163 UNTS 75, art 1; Export Control Order 2008, SI 2008/3231; Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (4 April 2025) https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states accessed 6 August 2026.

[62] Companies Act 2006, pt 21A; Register of People with Significant Control Regulations 2016, SI 2016/339; Economic Crime and Corporate Transparency Act 2023, pts 1–2; Financial Reporting Council, *UK Corporate Governance Code 2024* (n 71); National Institute of Standards and Technology, *Secure Software Development Framework* (SP 800-218, February 2022); National Institute of Standards and Technology, *Cybersecurity Framework 2.0* (NIST CSWP 29, February 2024).

Particularity is therefore technical as well as legal. The notice should contain machine-readable identifiers, confidence and exclusions, an authenticated official signature, a human contact and a revocation channel. The recipient returns whether the identifier exists, whether action was taken, collateral services affected and whether migration is observed. The Authority should maintain pre-agreed secure interfaces with designated providers, whilst retaining a manual channel for a small operator who cannot build one.

No order should require a universal vulnerability or indiscriminate weakening of encryption. Assistance must be capability-bound and incident-specific. The Investigatory Powers Act contains its own equipment-interference and technical-capability regimes; the proposed Act should not reproduce them through an undefined duty to help.[63] Where the desired act is interception, equipment interference or compelled disclosure, the responsible authority must use the independent statutory route.

Conflicting foreign law is neither an automatic defence nor an instruction to violate it. The provider identifies the conflict promptly; the court considers nationality, place of service, place of control, data and system location, comity, protective provisions and available treaty or executive-agreement route. An emergency preservation direction may maintain the status quo whilst the conflict is resolved, provided it does not purport to command conduct which English law cannot reach. The Crime (Overseas Production Orders) Act 2019 and the UK–US Agreement illustrate an expedited production route founded upon agreement rather than unilateral assertion.[64]

Each order must contain an off-ramp. Compliance, changed evidence, migration, judicial refusal, host action, technical failure and unacceptable collateral effect are separate termination events. The Authority sends revocation through the same authenticated route and confirms receipt. A power designed only to begin is not rapid law; it is rapid loss of control.

8. Measures Against Operators, Contractors and States

The response ladder should be statutory guidance, not an automatic escalator. Evidence, urgency, objective and collateral consequence decide the measure. The ladder's value is to make government explain why it skipped a less harmful effective step or persisted with one which could not work.

8.1 Level 1 — Warning and Preservation

Warning may prevent harm where a provider or host is unaware. It also supplies notice relevant to later due-diligence assessment. A warning states confidence and avoids public accusation before evidence.

Preservation ensures later process has an object. Allied queries discover whether fragments form one campaign. The Authority supplies technical assistance to vulnerable public bodies rather than punishing initial weakness.

[63] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205, arts III, VI and IX; Space Industry Act 2018, ss 7, 26–33 and 62; Outer Space Act 1986; Space Industry Regulations 2021, SI 2021/792.

[64] 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); 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; 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/ accessed 31 July 2026; Walter Isaacson, *Elon Musk* (Simon & Schuster 2023) 431–35.

8.2 Level 2 — Containment

Containment acts upon access: credential reset, account suspension, domain control, network filtering, workload isolation, patch, segmentation and continuity. A service provider may act voluntarily or under direction.

The measure should be technically precise. Disabling a shared service may harm more civilians than the attack. Where the hostile agent migrates, the controller's stop function and manifest become important. The Authority may coordinate simultaneous action among providers so isolation in one State does not merely move the operation.

8.3 Level 3 — Personal and Corporate Restraint

This level identifies the operator, integrator, payer and beneficial controller. Measures include arrest, search, seizure, injunction, licence suspension, director disqualification, asset restraint, travel restriction, domain seizure, procurement exclusion and disclosure to partners.[65]

The poor or off-grid operator may have no bank account worth freezing. Equipment, connectivity, credentials, physical movement and collaborators remain dependencies. A reward and protected defection route may divide him from the payer more effectively than a broad sanction.

Courts may impose a Cyber Operations Prevention Order upon conviction or, for a civil order, upon clear statutory criteria and evidence, restricting possession of specified credentials, provision of high-risk services or access to named systems. Restrictions must be tailored, time-limited and reviewable; ordinary computer use cannot be forbidden for life merely because it is easy to draft.

8.4 Level 4 — State and Collective Cost

Where evidence supports foreign State responsibility, assistance or knowing tolerance under the applicable law, measures may include:[66]

- public attribution;
- targeted financial, director, travel and service sanctions;
- export and technology restrictions;
- exclusion from public procurement and research access;
- diplomatic protest and reduction of cooperation;
- allied coordinated designations;
- lawful countermeasures seeking cessation and reparation;
- civil claims or international proceedings;
- defensive disclosure of tools and infrastructure;
- support for victims and capacity building in transit States.

Sanctions should reach the contractor market, public payer and enabling entity. Designations require reasons sufficient for challenge subject to protected evidence. Periodic review asks whether the measure still serves its purpose.

Collective response raises expected cost and reduces migration. It also multiplies error if attribution is wrong. MOSAIC correction must reach every partner; the United Kingdom should request review when its source conclusion changes.

---

[65] Ministry of Defence, *The Manual of the Law of Armed Conflict* (n 41); Ministry of Defence, *Legal Support to Joint Operations* (n 41); Protocol I (n 40), arts 48, 51, 52 and 57; ICRC, *Interpretive Guidance* (n 40).

[66] Christopher Greenwood, 'International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida, and Iraq' (2003) 4 *San Diego International Law Journal* 7, 13–23; Attorney General's Office, 'Attorney General's Speech' (n 36).

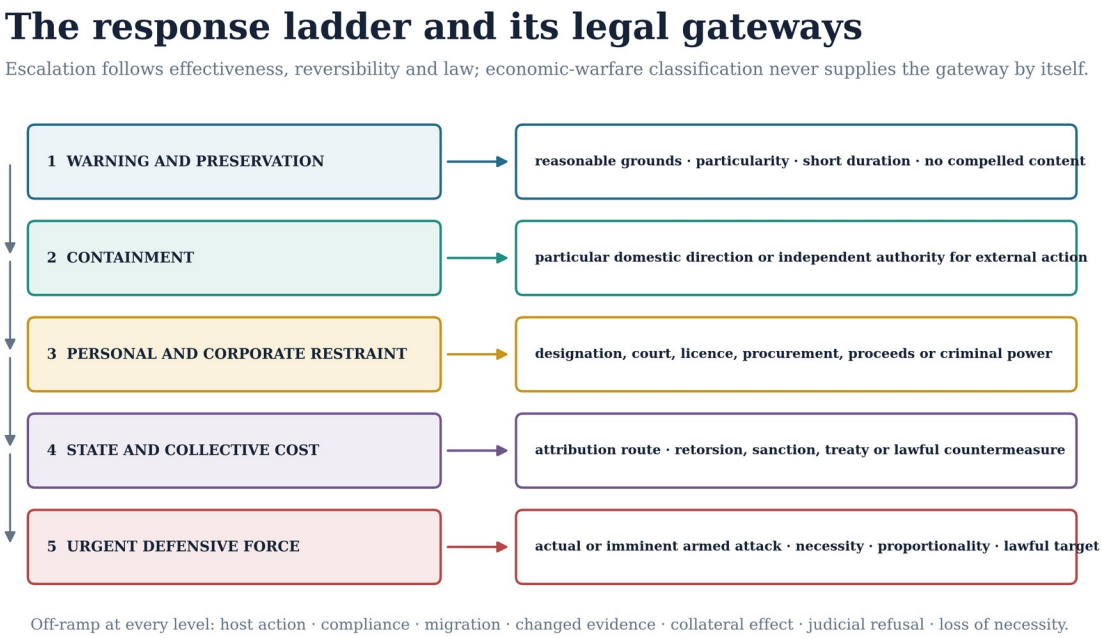

Figure 3. The response ladder moves from warning and preservation through containment, personal restraint and collective State cost to force at the actual-or-imminent armed-attack threshold; every rung has an independent legal gateway.

8.5 The State Which Sees Only a Fragment

A provider in State A may execute one encrypted model inference without target identity. The controller in State B holds the objective; the payer is State C. It is unjust and strategically foolish to treat A as the attacker because the workload happened there.

The first request to A should preserve, explain the campaign and seek feasible cooperation. After authenticated notice, refusal to take a reasonable measure may support a separate due-diligence enquiry. Responsibility for omission is not attribution of attack.[67]

If the controller intentionally selected A for weak retention and A genuinely lacked knowledge, the controller bears the designed opacity. The response should target control and payment. This distinction makes international cooperation more likely because innocent hosts need not fear that helping confirms guilt.

8.6 Direct Measures and the Operator Who Has Nothing to Freeze

The response ladder fails if every measure assumes that the operator values access to British banks, travel or reputation. A low-paid contractor, militia technician or autonomous workload may possess none of them. Direct response means acting upon the dependencies by which the attack continues: equipment, power, connectivity, credentials, domains, command channels, physical location, prime contract and receipt of task or reward. Search, seizure, arrest, injunction, service suspension and narrowly directed defensive cyber action are not “soft” merely because they are not explosive.[68]

[67] Iraq Inquiry, *The Report of the Iraq Inquiry: Executive Summary* (HC 264, 2016–17) paras 20–82 and 630–807; Review of Intelligence on Weapons of Mass Destruction, *Report of a Committee of Privy Counsellors* (HC 898, 2003–04); Intelligence and Security Committee of Parliament, *Russia* (HC 632, 2019–21); Cabinet Office, *Professional Standards for Government Intelligence Assessment* (November 2018).

[68] Comptroller and Auditor General, *Investigation: WannaCry Cyber Attack and the NHS* (HC 2017–19, 414); NHS England, ‘Synnovis Cyber Incident’ https://www.england.nhs.uk/synnovis-cyber-incident/ accessed 6 August 2026; Department of Health and Social Care, ‘Synnovis Cyber Attack’ (Written Statement HCWS1046, 30 June 2025); Cybersecurity and Infrastructure Security Agency, *MAR-17-352-01 HatMan —Safety System Targeted Malware* (12 April 2018); National Cyber Security Centre and others, ‘PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure’ (n 4).

The State which paid for the operation remains a separate object of policy. Procurement exclusion, export restriction, sanctions upon the contracting entity, disclosure of the market, allied action and lawful countermeasures raise the cost of purchasing deniability. Direct action against the operator stops the present act; consequence for the payer alters the market which will produce the next. Either without the other leaves an obvious adaptation.

Where investigators know the attacking location but the host is unable to act, the first question is which non-forcible dependency can be reached lawfully. Where none can stop an actual or imminent armed attack, location becomes relevant to necessity and target verification; it does not itself supply article 51 authority. The same room may contain an attacker, innocent staff, shared power and unrelated servers. “Known location” begins the target review; it does not finish it.

The Act should permit rewards, protected surrender and contractor debarment alongside compulsion. A subcontractor may hold the credential which proves the State relation whilst having little loyalty to the prime. Protection and lawful immigration or witness arrangements may create an exit more effective than a threat which cannot reach him. Conversely, one who continues after authenticated warning supplies stronger evidence of knowledge and may narrow the remaining alternatives.

The decisive principle is personal and functional rather than theatrical. The response should reach the person or thing maintaining the hostile function, upon the independent legal authority applicable to it, and should cease when that function ceases. Poverty does not immunise hostile action; nor does it remove the operator’s rights. Precision permits firmness without converting frustration into collective punishment.

9. Private Strategic Capacity and PMSCs

This is the Part which does something the literature has not attempted. That some private firms now exercise control of a kind previously reserved to States is well established and well described: they have been called digital Switzerlands, mapped as proxies and analysed as chokepoints. [69]The description is not in dispute. What has not been done is to convert it into a power. Designation under clause 39 does not impose a further compliance duty upon a supplier; it creates a control relationship. A named responsible officer, a map recording who may grant, withdraw, alter or stop the service, a registered stop capability which the state may require to be exercised, and a manifest of strategic decisions together give a government something it presently lacks entirely, which is a route to the switch. Paper 4 supplies the theory. This Part supplies the clauses.

9.1 Model Clause 39 — Designation

The Secretary of State may designate a service or capability where its grant, withdrawal, alteration or hostile use could materially affect defence, armed conflict, essential services, democratic institutions, life, systemic finance, strategic communications, positioning, observation or high-impact cyber operations.[70]

An interim designation may take immediate effect for seventy-two hours in a critical incident. Confirmation requires reasons and a right of appeal to a security-cleared tribunal. Designation is preventive, not a finding of fault.

---

[69] *Legality of the Threat or Use of Nuclear Weapons* (n 43) [41]; *Oil Platforms* (n 33) [43], [73]–[77]; Protocol I (n 40) arts 51(5)(b) and 57.

[70] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 6; UN Human Rights Committee, ‘General Comment No 36: Article 6—Right to Life’ (3 September 2019) UN Doc CCPR/C/GC/36, paras 12–14; *McCann and Others v United Kingdom* (1996) 21 EHRR 97 [148]–[150]; *Al-Skeini and Others v United Kingdom* (2011) 53 EHRR 18 [138]–[150].

9.2 Model Clauses 40–43 — Controller Duties

The controller must nominate responsible officers; record beneficial, contractual and operational control; maintain a continuity and strategic-decision plan; notify defined foreign or belligerent requests; preserve records; maintain secure stop and recovery capability; conduct civilian and human-rights assessment; and participate in exercises.[71]

A private controller must obtain authorisation before supplying tailored strategic assistance to a party to armed conflict, unless an emergency safe harbour applies. The safe harbour permits immediately necessary action to protect life where public authority cannot be reached, followed by notification and review within hours.

Consumers and minority shareholders are not treated as consenting participants. Orders bind control, not the population which purchased unrelated goods.

9.3 Model Clause 47 — PMSC and Intrusion Licensing

High-risk services require a licence: offensive cyber access, target generation, autonomous effect, operation of weapons or destructive systems, detention, strategic intelligence and command of armed personnel. The licence identifies clients, jurisdictions, target restrictions, model and tool governance, subcontractors, insurance, audit and incident duties.[72]

The prime contractor remains responsible for the specified governance duties throughout the chain. Each person remains liable only according to his own conduct and mental element for substantive offences. The model prevents responsibility being contractually diluted without manufacturing guilt at the edge.

Government procurement is within the regime. Public secrecy may alter disclosure, not record and oversight. A State cannot demand accountability from foreign PMSCs whilst purchasing deniability from its own.

9.4 The Attribution Manifest

The controller records objective, human authority, target class, prohibited targets, software and model versions, infrastructure, subcontractors, credentials, autonomous discretion, stop conditions, changes and incidents. A sealed manifest may protect legitimate covert action; split custody prevents unilateral deletion.[73]

Opening triggers include serious harm, credible unlawfulness, court order, inspector demand and applicable foreign request. A verified answer may disclose only the proposition needed, preserving unrelated secrecy.

Failure to create or intentional destruction is a regulatory offence and may support a permitted adverse inference. The manifest is not conclusive proof that the operation stayed within it; event logs and effects remain necessary.

---

[71] Charter of the United Nations (n 33) art 51; Attorney General's Office, 'Attorney General's Speech' (n 36); Daniel Bethlehem (n 36) principles 10–12; United Kingdom, Letter dated 7 September 2015 from the Permanent Representative of the United Kingdom to the United Nations addressed to the President of the Security Council, UN Doc S/2015/688; United Kingdom, Letter dated 3 December 2015 from the Permanent Representative of the United Kingdom to the United Nations addressed to the President of the Security Council, UN Doc S/2015/928.

[72] Cabinet Office, *The Cabinet Manual* (n 17) paras 5.36–5.38; House of Commons Library, *Military Action: Parliament's Role* (n 18); House of Lords Constitution Committee, *Waging War* (n 23); House of Commons Political and Constitutional Reform Committee, *Parliament's Role in Conflict Decisions* (n 23).

[73] Iraq Inquiry, *Executive Summary* (n 78); Cabinet Office, *The Cabinet Manual* (n 17); Civil Contingencies Act 2004, ss 20–28; Investigatory Powers Act 2016, urgent-warrant provisions.

9.5 The Strategic Assistance Authorisation

The authorisation required from a private strategic controller should be short enough to obtain and detailed enough to transfer political responsibility. The application identifies the requesting party, legal position asserted, service or capability, intended function, target or target class, territorial reach, expected civilian dependence, duration, technical discretion retained by the company, foreign subcontractors, stop condition and consequence of refusal. Government returns approval, refusal or bounded provisional approval through a permanent duty cell.

Tailored assistance to military targeting requires the highest private-capacity scrutiny because it may alter the conduct of hostilities whilst leaving the decision in a proprietor's hands. General communications supplied upon ordinary terms stand differently from configuration, geofencing, priority, sensing or analysis adapted to a belligerent operation. The Outer Space Treaty places responsibility upon States for national activities in outer space and requires authorisation and continuing supervision of non-governmental activities; domestic space legislation already employs licensing and directions.[74] The proposed Act adds the foreign-conflict decision which ordinary launch and safety licensing does not answer.

The authorisation neither declares the requesting State's entire cause lawful nor guarantees every later use. It states the basis upon which the United Kingdom permits the specified British-controlled intervention and the limits which the controller must enforce. Material change in target class, geographic boundary, belligerent, autonomy or expected civilian use requires renewal. Humanitarian continuity may be protected separately from targeting support.

Starlink illustrates why sequence matters. Service was publicly activated for Ukraine on 26 February 2022; later United States procurement and reimbursement arrangements regularised parts of the relationship, whilst later reporting exposed the strategic significance of private service boundaries and decisions.[75] The legal point does not depend upon condemning assistance to Ukraine. It is that a proprietor's initial power to incur foreign consequence did not arise from a treaty, public office or consumer consent. The Act ensures that a future Chinese, Russian, British or American proprietor meets the same public-authority rule.

Where life is immediately endangered the controller may act within a humanitarian safe harbour, but must notify at once, preserve the decision and seek continuation. The safe harbour cannot be used to provide open-ended targeting on the assertion that victory will ultimately save life. The line is the act which could not safely await government, confined by time and purpose. Public authority then assumes, limits or ends the intervention.

Refusal also requires discipline. Government cannot compel manifestly unlawful or technically unsafe operation; the controller cannot refuse merely because its owner disagrees with lawful policy after accepting designation and continuity duties. Urgent judicial review should be available to either. The two-key rule thereby prevents private foreign policy without treating the corporation as equipment without legal responsibility.

[74] National Cyber Force, *Responsible Cyber Power in Practice* (n 49); ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Position Paper, November 2019); Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 73–113; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 69–118.

[75] *Military and Paramilitary Activities in and against Nicaragua* (n 33) [176], [194]–[201]; *Oil Platforms* (n 33) [43], [73]–[77]; *Legality of the Threat or Use of Nuclear Weapons* (n 43) [41]; International Law Commission, 'Draft Articles' (n 32) art 53.

10. Force as the Exceptional Defensive Measure

The proposed Act must not pretend that force is unthinkable. It must make force difficult to misuse and possible to employ before an armed attack completes its harm.

10.1 Model Clauses 61–62 — Domestic Decision Authority

61 No enlargement of international right; 62 Conditions for urgent defensive force

1) Nothing in this Part creates or enlarges a right to use force under international law or alters the law applicable to armed forces.

2) The Prime Minister, or a Secretary of State expressly authorised where the Prime Minister is unable to act, may direct the use of force in response to a critical economic-warfare act only where satisfied that—

1) an actual or imminent armed attack against the United Kingdom or a State requesting collective self-defence exists;

2) the proposed force is necessary to halt, repel or prevent that armed attack;

3) the force is proportionate to the defensive purpose;

4) each person or object to be attacked is a lawful target under applicable law;

5) feasible precautions have been taken and expected incidental civilian harm is not excessive;

6) the territorial State has consented, is responsible upon the applicable law, or the Government has a lawful basis for action without consent;

7) the Attorney General has certified the legal basis or, if unavailable in an extreme emergency, a qualified alternate Law Officer has done so; and

8) the Chief of the Defence Staff has certified operational feasibility and target review.

3) The direction must state the defensive objective, target, duration or mission limit, factual confidence, international legal basis, alternatives considered, civilian-risk assessment and review time.

4) Force may not be directed solely to punish a completed act or produce general deterrence.

The clause does not grant soldiers tactical power or displace command. It specifies the domestic apex decision and record. Rules of engagement, target verification and operational law remain applicable.[76]

The word “pre-emptive” should be avoided if it suggests force against a non-imminent future threat. Anticipatory self-defence, on the United Kingdom’s position, addresses imminence and the last feasible opportunity. Clause 62 permits that, not preventive war against a capability which might someday be used.[77]

10.2 The Attribution Threshold for Force

Criminal proof beyond reasonable doubt is not a universal precondition of self-defence; States often act upon intelligence and operational evidence. The standard cannot be “minister believes”. The decision should require a high degree of confidence commensurate with irreversibility, corroborated by independent sources where feasible, and a documented deception analysis.

[76] Protocol I (n 40) arts 51–52 and 57; ICRC, *Interpretive Guidance* (n 40) 33–36 and 70–73; Michael N Schmitt (ed), *Tallinn Manual 2.0* (n 35) rr 92–100; National Institute of Standards and Technology, *AI RMF 1.0* (n 56).

[77] Charter of the United Nations (n 33) art 51; *Military and Paramilitary Activities in and against Nicaragua* (n 33) [176], [194]–[201]; *Oil Platforms* (n 33) [43], [73]–[77]; Daniel Bethlehem (n 36) 770–77; Christopher Greenwood (n 77) 13–23.

Identity, control and target must be separated. It may be highly certain that a server is executing the attack whilst uncertain who paid for it. Necessary force might lawfully stop the server without justifying force against the suspected payer. Conversely, evidence of State sponsorship does not make every system in that State a target.

If time permits, the Attorney General should appoint a devil's-advocate team with access to intelligence to test attribution, imminence, alternatives and civilian effect. Where time does not permit, the independent review occurs immediately after. Dissent is preserved.[78]

10.3 Maximum Harm and Necessity

An NHS data attack may cause death through clinical uncertainty and delay. A winter-grid attack may cause hypothermia, fire, interruption of care and water failure. The attack need not have completed those consequences if access, action and trajectory make them reasonably credible and imminent.[79]

Necessity asks whether force is needed to halt, repel or prevent the armed attack. If the hostile virtual machine can be suspended by its cooperative provider in two minutes, a strike is unnecessary. If the node is hardened, continuing, beyond effective local process and the last opportunity to prevent mass harm is closing, direct force may become necessary.

The scale of possible harm affects the urgency and the force reasonably required. It does not erase target verification. High consequence may demand action upon less complete information, but the greater risk of mistake must be acknowledged and mitigated through narrow target, reversible cyber effect where feasible and rapid reassessment.

10.4 Proportionality

Proportionality in self-defence relates force to the defensive objective; IHL proportionality, where applicable, compares expected incidental civilian harm with the concrete and direct military advantage. The Act should require both rather than use one word to conceal two tests.[80]

Deterrence may bear upon whether an attacker's campaign is continuing and whether a measure will prevent repetition within that attack. Punitive exemplary destruction after the threat has ended is not self-defence. Criminal sentence, sanction and retorsion have their own deterrent functions.

Direct force against an individual requires lawful status and targetability. In armed conflict, direct participation or continuous combat function may be relevant. Outside armed conflict, human-rights and law-enforcement constraints apply alongside article 51. The executive cannot make a person an "object of war" by certificate.[81]

---

[78] Comptroller and Auditor General, *Investigation: WannaCry (n 79)*; NHS England, 'Synnovis Cyber Incident' (n 79); Cybersecurity and Infrastructure Security Agency, *MAR-17-352-01 HatMan* (n 79); Mandiant, 'TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping' (10 April 2019) https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections/ accessed 6 August 2026.

[79] *Council of Civil Service Unions v Minister for the Civil Service* [1985] AC 374 (HL); *R (Miller)* (n 19); *Al Rawi* (n 22); Justice and Security Act 2013, pt 2; *Privacy International* (n 63).

[80] Investigatory Powers Act 2016, ss 24–25 and 109–110; *Ahmed* (n 21); *Bank Mellat* (n 21); Human Rights Act 1998, s 8; *R (UNISON)* (n 59).

[81] Civil Contingencies Act 2004, s 27; Sanctions and Anti-Money Laundering Act 2018, s 55; Statutory Instruments Act 1946; House of Lords Constitution Committee, *Fast-track Legislation: Constitutional Implications and Safeguards* (HL 116, 2008–09); House of Lords Delegated Powers and Regulatory Reform Committee, *Democracy Denied? The Urgent Need to Rebalance Power between Parliament and the Executive* (HL 106, 2021–22).

10.5 Host-State Notice

Where feasible, the United Kingdom should give the territorial State a specific request: identify the attacker, location, threat, action sought and response time. The time may be minutes in an attack upon life. A refusal, inability or silence is recorded.

Notice may be omitted where it would reveal the target, enable migration or consume the last opportunity to act. The reasons are certified. After action the territorial State receives an explanation consistent with security and the United Kingdom reports to the Security Council under article 51.[82]

10.6 Parliamentary Accountability Without Operational Paralysis

Prior Commons debate should occur where circumstances permit, especially sustained or discretionary campaigns. It should not be a statutory condition which an attacker can defeat by operating during recess or within minutes.

Where force occurs without prior debate:

1. the Prime Minister informs the Leader of the Opposition and designated security-cleared parliamentarians before action where feasible;
2. the Speaker is notified and recall considered immediately;
3. a statement is made to the Commons at the earliest feasible time;
4. a public legal summary is issued, with a classified annex to the Intelligence and Security Committee and relevant select committee;
5. continued operations beyond seven days require a Commons resolution unless disclosure would cause a specified immediate operational danger, in which case a short extension is certified and reviewed;
6. completion receives an independent lessons report.

This adopts the logic of existing emergency convention whilst giving it more definite consequence. Parliament does not choose the target in real time; it controls sustained policy and examines the emergency claim.[83]

10.7 Model Clauses 63–64 — The Defensive Action Certificate

The certificate should be a statutory document completed before force where time permits and contemporaneously in the most extreme case. It is not a public recital of intelligence. It is the irreducible record against which Cabinet, Parliament, a court and later inquiry can test what the decision maker believed.

63 Defensive action certificate; 64 Extreme urgency

1) A direction under section 62 has no effect unless a certificate records the matters set out in Schedule 3, of which the principal items are—

1) the armed attack and whether it is actual or imminent;

2) the person or State against which defence is directed and the evidential confidence;

3) the legal basis under the Charter and any relevant request for collective self-defence;

4) the defensive objective and why non-forcible alternatives cannot achieve it in time;

[82] Human Rights Act 1998, s 8; European Convention on Human Rights (n 46), arts 6, 8 and 13 and Protocol No 1, art 1; Crown Proceedings Act 1947; Data Protection Act 2018, ss 165–169; Sanctions and Anti-Money Laundering Act 2018, ss 38–40.

[83] Justice and Security Act 2013, pt 2; Intelligence Services Act 1994, ss 10 and 10A and sch 3; Sanctions and Anti-Money Laundering Act 2018, s 40; Freedom of Information Act 2000, ss 23–24; *Al Rawi* (n 22); *Big Brother Watch (n 52)*.

5) the target's status and, for an object, each limb of the military-objective test where applicable;

6) expected direct and incidental effects, including protected services and shared infrastructure;

7) territorial-State consent, responsibility, inability or unwillingness and any notice;

8) mission limit, reassessment interval and termination condition;

9) the advice of the Attorney General and Chief of the Defence Staff; and

10) material dissent or uncertainty.

2) If delay necessary to complete the certificate would probably forfeit the last feasible opportunity to prevent death or serious physical harm, an oral direction may be given and recorded by two officials; the certificate must be completed as soon as practicable and in any event within six hours.

3) Failure to comply with subsection (2) terminates authority for continuing action and must be reported immediately to the Commissioner and the Prime Minister.

The certificate prevents later accounts from combining facts learned after action with those available before. A supplementary record may explain new evidence; it must not overwrite the original.[84]

Six hours is not permission to invent reasons after the event. The two-official record should state target, objective and emergency basis at the moment of direction. Where even that is impossible, ordinary command self-defence may apply under existing law, but the strategic Clause 62 procedure should not be treated as complete.

10.8 Selecting Cyber or Kinetic Means

The law should not prefer a cyber effect because it sounds bloodless. A cyber operation may propagate, erase civilian data, disable safety systems or remain undiscovered; a precise physical seizure may be safer. The decision compares expected consequence.[85]

A reversible cyber action is preferred where it can reliably stop the attack with less civilian harm. Reversibility includes the ability to restore function, not merely the intention to do so. If the hostile system automatically migrates or retaliates upon interference, the assessment records that behaviour.

Kinetic force may be instrumental where equipment is isolated, the attacking function cannot otherwise be stopped and the legal tests are met. The target package should identify physical boundary, civilian presence, shared utilities, timing, warning and feasible lower-yield means. Describing a location as a "server farm" does not complete distinction.

Capture or seizure may offer intelligence and reduce uncertainty but expose personnel and host sovereignty. Remote cyber action may preserve life but destroy evidence. The decision is operational and legal, not a hierarchy in which the modern tool is presumed proportionate.

---

[84] Comptroller and Auditor General, *Investigation: WannaCry* (n 79); NHS England, 'Synnovis Cyber Incident' (n 79); US Department of Health and Human Services, Office for Civil Rights, 'Cyberattack on Change Healthcare' (Dear Colleague Letter, 13 March 2024) https://www.hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf accessed 6 August 2026; National Cyber Security Centre, *Mitigating Malware and Ransomware Attacks* (September 2020).

[85] National Cyber Security Centre and others, 'PRC State-Sponsored Actors' (n 4); Cybersecurity and Infrastructure Security Agency and others, *Primary Mitigations to Reduce Cyber Threats to Operational Technology* (6 May 2025) https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology accessed 6 August 2026; Department for Energy Security and Net Zero, *National Emergency Plan 2023: Downstream Gas and Electricity* (July 2023) https://www.gov.uk/government/publications/national-emergency-plan-downstream-gas-and-electricity-2016 accessed 6 August 2026; National Cyber Security Centre, *Cyber Assessment Framework v4.0* (6 August 2025) https://www.ncsc.gov.uk/collection/cyber-assessment-framework accessed 6 August 2026.

10.9 Termination and Reassessment

Self-defence ends when necessity ends. A direction should identify measurable termination conditions: hostile traffic ceased and persistence removed; control equipment disabled; attacking unit surrendered; provider isolation confirmed; or threat no longer imminent.[86]

Reassessment intervals should be short for an autonomous system because target and infrastructure can change without human order. A target lawful at authorisation may migrate into civilian shared infrastructure. Continuing automation must receive updated constraints or stop.

Every strike or destructive cyber effect returns battle-damage and service-impact information to the decision record. Unexpected civilian consequence triggers pause where operationally feasible and immediate legal review. Deterrent desire cannot keep an operation alive after its defensive objective has been achieved.

Where evidence later shows attribution was wrong, the United Kingdom must investigate, correct, compensate where legally due and disclose enough to restore trust. The prospect of error is not a reason to abandon defence; the refusal to plan for correction would be.

These duties also discipline allies: intelligence supplied by a partner must retain its source class, caveat and uncertainty, notwithstanding the political convenience of collective confidence.

10.10 The Live-Target Duty

The certificate authorises a defensive purpose and a bounded target; it does not convert yesterday's intelligence into a continuing permission. Before force or a destructive cyber operation is executed, the responsible commander must confirm, so far as the time and means reasonably permit, that the target still performs the function upon which necessity depended, that the anticipated civilian use has not materially changed and that no less harmful effective measure has become available.

This duty is especially important where the object is virtual. A credential may be revoked, a workload may migrate and an autonomous process may reproduce itself between authorisation and execution. The lawful object cannot be defined merely by an IP address, domain name or building if the hostile function has moved. The operational order may follow a migrating process only by criteria fixed in advance: authenticated code or model identity, behaviour, command relationship, bounded infrastructure, time, exclusions and stop condition. It may not authorise force against every system through which an adversary has passed.[87]

Where verification fails because time has expired, evidence conflicts or civilian co-use has become materially greater, execution pauses unless the delay itself would expose persons to an imminent and graver harm. That exception is recorded contemporaneously and reviewed afterwards; it is not a phrase inserted later to rescue an indefensible act. Automated engagement must fail closed when identity, geography or exclusion data fall outside the certified bounds.

The same machinery must receive cancellation as reliably as authorisation. Revocation by the decision authority, loss of necessity, host-State containment, surrender, mistaken identity or completion of the defensive object must propagate to every contractor, platform and autonomous component. A fast

[86] Computer Misuse Act 1990; Fraud Act 2006; Proceeds of Crime Act 2002; Economic Crime and Corporate Transparency Act 2023; Criminal Finances Act 2017; Crown Prosecution Service, 'Cybercrime—Prosecution Guidance' https://www.cps.gov.uk/prosecution-guidance/cybercrime-prosecution-guidance accessed 6 August 2026.

[87] Montreux Document (n 72); Deborah D Avant, *The Market for Force: The Consequences of Privatizing Security* (CUP 2005); Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018); International Law Commission, 'Draft Articles' (n 32) arts 4, 5, 8 and 11; *Application of the Genocide Convention* (n 55) [396]–[407].

power which cannot stop is not an emergency power but an abdication. Speed is preserved by designing verification and revocation into the operation before the emergency arises.

10.11 Deterrence, Maximum Harm and the Limit of Punishment

Deterrence belongs in the statute, but in its correct place. The whole architecture is intended to alter expected cost: mandatory reporting reduces secrecy; manifests reduce contractual deniability; provider interfaces make cheap infrastructure less dependable; personal and corporate orders reach the operator; sanctions, procurement and export measures reach the payer; and collective response denies easy migration. These consequences may be swift and deliberately communicated. None requires pretending that a completed theft is an armed attack.

Force has a different gateway. It may produce a deterrent consequence, as almost any successful defence may, but its legal object under article 51 remains halting, repelling or preventing the actual or imminent armed attack. Punishment of past conduct, exemplary destruction and general intimidation cannot be relabelled necessity. The clause should therefore require the decision maker to state which continuing or imminent attack the target's neutralisation will affect, how, and for how long.[88]

Maximum reasonably credible foreseeable harm enters before that conclusion. A destructive command against a winter grid is not assessed only by the substations already lost; privileged access, reachable load, safety systems, temperature, repair time, hospitals, water pumping and cascading failure define the attack underway. An operation erasing health records is not valued at the price of storage media; clinical dependency, backup integrity, medication and diagnostic consequence matter. CISA's reporting upon the TRITON/HatMan safety-system malware, the official account of WannaCry's effect upon the NHS and subsequent health-sector incidents demonstrate that digital interference can cross into physical safety without adopting the appearance of a bomb.[89]

The assessment must also include replication. Code, credentials and autonomous tasking may permit parallel attacks at negligible marginal cost. Replication can affect scale, imminence and the adequacy of a narrow defence. It does not make every copy a lawful target. The Authority must identify which integrator, command service, root credential or distribution mechanism controls the repetition and whether its neutralisation will actually stop it.

There is an important asymmetry between defensive urgency and collateral prediction. The State may be forced to decide before final harm is known, but it must still examine the harm its own action may cause. A strike upon a building which hosts the command system and a hospital service cannot be justified by placing catastrophic hostile possibilities in one column and refusing to investigate civilian use in the other. Maximum-harm analysis disciplines both sides of the decision.

Where the attack has ceased, direct forcible defence ceases with it. The remaining response may still be severe: prosecution, seizure, sanction, expulsion, public attribution, licence loss, civil recovery, countermeasure where conditions remain, and collective restriction upon the contractor market. The Act is more credible, not less, when it places these measures upon their proper bases. It does not tiptoe around hostile action; it refuses to make an unlawful response the attacker's strategic gift.

---

[88] Outer Space Treaty (n 74) arts III, VI and IX; Space Industry Act 2018; Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat 2310, arts 8–9; Michael N Schmitt, 'International Law and Military Operations in Space' (2006) 10 *Max Planck Yearbook of United Nations Law* 89; 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 accessed 6 August 2026; Pearce Clancy (n 44).

[89] Comptroller and Auditor General, *Investigation: WannaCry* (n 79); NHS England, 'Synnovis Cyber Incident' (n 79); Department of Health and Social Care, 'Synnovis Cyber Attack' (n 79); Cybersecurity and Infrastructure Security Agency, *MAR-17-352-01 HatMan* (n 79).

11. Judicial Review, Remedy and Parliamentary Control

11.1 Designated Court

A small rota of High Court judges with appropriate clearance should hear protective, manifest, conflict and compensation applications continuously. Remote secure procedure allows review within hours.

Urgent without-notice orders are permitted where notice would prejudice the objective; a return hearing follows promptly. Special advocates or closed material procedures should be used only under existing or carefully enacted authority, with open reasons to the greatest extent possible.

The court may discharge, narrow, continue, correct, order compensation and refer abuse. It cannot adjudicate the legality of battlefield tactics prospectively beyond justiciable issues, but executive assertions of national security do not exclude all review.[90]

11.2 Automatic Review and Expiry

Every emergency measure has a clock visible in MOSAIC. Expiry occurs automatically unless the approving act is recorded. Reissuing an identical order to evade review is prohibited.

Preservation expires or converts to lawful hold; protective direction expires within twenty-four hours without court; asset hold within forty-eight; interim designation within seventy-two; emergency regulations follow parliamentary approval; sustained force follows the seven-day Commons rule proposed above.

Acts lawfully completed before a later refusal are not automatically void, but continuation stops and the reviewer considers deletion, return, compensation, notification and disciplinary action. This follows the workable logic of urgent warrant review without making illegality consequence-free.[91]

[90] International Law Commission, ‘Draft Articles’ (n 32) arts 4, 5, 8 and 11; *Application of the Genocide Convention* (n 55) [396]–[407]; *United States Diplomatic and Consular Staff in Tehran* (n 67) [58]–[74]; *Prosecutor v Tadić* (Appeal Judgment) IT-94-1-A (15 July 1999), [116]–[145]; Evelyne Schmid and Ayşe Özge Erceiş (n 39) 581–90.

[91] Department for Science, Innovation and Technology, *Cyber Security and Resilience (Network and Information Systems) Bill: Impact Assessment* (12 November 2025); Regulatory Policy Committee, *RPC Opinion* (n 50); Department for Science, Innovation and Technology, ‘Summary of the Bill’ (n 11).

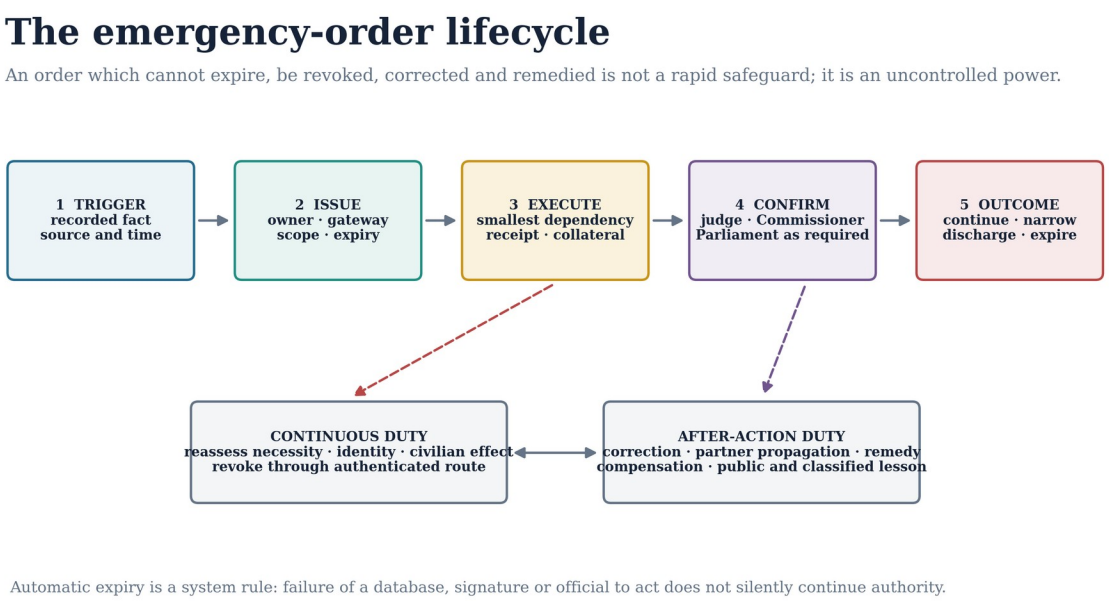

Figure 4. Every emergency order travels from a recorded trigger through narrow execution and independent confirmation to renewal, correction, remedy or automatic expiry.

11.3 Parliamentary Instruments

Technical standards and designated protected-system lists may use negative or affirmative regulations according to impact. New offence, class of compulsory participant, intrusive power or material expansion requires affirmative procedure.

In an urgent case a made-affirmative instrument may take effect immediately but lapse after seven or twenty-eight days according to category unless approved. The shorter period applies to broad emergency restrictions; the longer to targeted sanctions. Parliament may amend or revoke without invalidating completed lawful acts.[92]

The Government publishes an annual report containing use, response time, error, correction, penalty, international cooperation, civilian impact, cost and examples. Classified details go to the Intelligence and Security Committee and designated select committees.

11.4 Remedy

A person unlawfully subjected to restraint may obtain discharge, correction, declaration, return, compensation and costs. A provider complying in good faith may be compensated for exceptional burden. Victims may obtain support and, where law permits, recovery from confiscated assets.[93]

Where public attribution is materially wrong, the Government corrects with prominence reasonably equivalent to the original and notifies partners. National dignity is not a ground for preserving error.

Officials who knowingly fabricate evidence, conceal material contrary information or use the Act for political or commercial favour commit offences and misconduct. Good-faith urgent judgement is not criminalised because later information differs. The line is dishonesty, recklessness and abuse.

---

[92] Civil Contingencies Act 2004, ss 26–28; Investigatory Powers Act 2016, ss 234–239 and 260; House of Lords Constitution Committee, *Fast-track Legislation* (n 92); House of Lords Delegated Powers and Regulatory Reform Committee, *Democracy Denied? (n 92)*.

[93] House of Lords Constitution Committee, *Fast-track Legislation* (n 92); House of Lords Delegated Powers and Regulatory Reform Committee, *Democracy Denied?* (n 92); Civil Contingencies Act 2004, s 27; Sanctions and Anti-Money Laundering Act 2018, s 55.

11.5 A Public Law of Classified Action

The legitimacy of the scheme will depend upon what can be known about acts which cannot be described in operational detail. The statute should require an open legal framework, published codes, annual aggregate data, reasons for designation, notice of error and a public legal summary after any use of force. Classified annexes should be available to the designated court, Commissioner and Intelligence and Security Committee. Secrecy should protect capability, source and current target; it should not conceal which power was used or whether its statutory clock expired.[94]

The minimum public account after a critical incident should state the classification of the event, principal domestic powers used, whether an international-law basis was relied upon, the broad category of target, the duration of emergency measures, material civilian or service effect, whether review found error and whether correction or compensation followed. Delay may be necessary; permanent silence should require a fresh, reasoned certificate reviewed annually.

Standing must be practical. A person named, restrained or materially affected may challenge; a provider may challenge burden and legality; the Commissioner may refer systemic unlawfulness; and Parliament may require a special report. Victims should not depend upon proving the attacker's identity before obtaining support. Public-interest organisations may seek ordinary judicial review where the established standing test is met, but the Act need not create a roving merits appeal for strangers to the incident.

Remedy must correspond to the wrong. Wrongful preservation may require deletion; wrongful production return and exclusion; wrongful restraint discharge and compensation; wrongful public attribution correction of equal prominence; unlawful designation removal and consequential relief; unlawful force the remedies available under domestic and international law. A declaration alone may be sufficient for some procedural failure, but it should not become the universal price of an expired order whose effects remain.

The Commissioner's annual report should identify median response and confirmation times, lapsed orders, refusals, false positives, corrected attributions, provider burden, use against journalists or protected professions, international requests, autonomous-system incidents, compensation and disciplinary referrals. A classified supplement may explain causes. Parliament cannot scrutinise a system which reports only how often it succeeded according to itself.

12. Applying the Act

12.1 Erasure of NHS Data

An autonomous agent obtains privileged access to a hospital group, encrypts primary records and begins deleting backups. Technical evidence shows lateral reach to pharmacy and diagnostic systems. The ordinary ransomware demand does not determine classification.

Within minutes the hospital files a critical notice. NCSC assists containment; MOSAIC sends preservation and exact-match queries; providers isolate identified credentials; the Authority assesses maximum credible harm from treatment delay, medication error, restoration and spread. If access can be removed through providers, force is unnecessary.[95]

Suppose instead the agent operates from dedicated equipment in a lawless area, continues destructive commands, defeats cyber isolation and presents imminent lethal consequence. The United Kingdom

[94] Civil Contingencies Act 2004, s 19(1)–(2). See generally Clive Walker and Jim Broderick, *The Civil Contingencies Act 2004: Risk, Resilience and the Law in the United Kingdom* (OUP 2006).

[95] Civil Contingencies Act 2004, s 21(1)–(5).

seeks host action if feasible. If evidence establishes an armed attack by scale and effects, the last effective opportunity is closing and international law permits self-defence against the actor, Clause 62 allows force against the lawful target after legal and operational certification. The presence of a ransom demand does not turn an armed attack into mere theft.

12.2 Winter Energy Pre-positioning

Investigators discover persistent access across power operators resembling public advisories but no destructive command. The harm assessment considers privilege, safety systems, geography, winter timing, redundancy and apparent crisis preparation. Pre-positioning demands urgent containment and State response; it is not automatically an occurring armed attack.

The Authority coordinates simultaneous credential replacement, segments networks, preserves evidence, warns allies and targets the contractor and payer with sanctions and countermeasures where lawful. If a command sequence begins and physical or lethal effects become imminent, the legal classification is revisited. The Act permits the threshold to change with facts.[96]

12.3 Theft from an Insurer

A group steals funds from an insurer without immediate danger to life. The amount is substantial, the method automated and code offered to others. Police, asset restraint, exchange orders, domain seizure, provider action and contractor sanctions apply. Innovation and replication raise priority and severity; they do not by themselves create article 51 force.[97]

If the theft is one stage in a campaign intended to collapse systemic insurance and prevent disaster recovery, the campaign is assessed as a whole. Maximum harm must still be technically and economically credible. “Money only” does not end analysis; “economic warfare” does not begin missiles.

12.4 A Foreign-paid PMSC

State A pays a PMSC to cause the United Kingdom to abandon a policy. The prime sets an objective; subcontractors in several time zones build modules; an agent selects local authorities and water systems. Evidence links payment, reporting and stop authority to State A but criminal proof concerning particular officials remains incomplete.

MOSAIC preserves fragments; the PMSC’s manifest, where within reach, identifies integration; the Authority separates contractor identity, State direction, host omission and infrastructure. Operators face direct restraint; the PMSC loses licence and assets; State A faces public attribution and coordinated measures upon the standard applicable to each.[98]

If one subcontractor wrote a generic scheduler without knowing the objective, he is not made guilty by architecture. If the prime deliberately prevented him knowing, that ignorance does not pass upward. The Act follows knowledge and control.

12.5 Privately Controlled Satellite Intervention

A British-controlled constellation is asked by a belligerent to provide targeting support. The controller cannot decide merely because he owns it. He seeks rapid authorisation; government assesses the

[96] Civil Contingencies Act 2004, s 22(1)–(3).

[97] Civil Contingencies Act 2004, s 23(1) and (3).

[98] Civil Contingencies Act 2004, ss 23(4) and 26(1).

requesting State's legal position, neutrality, space obligations, civilian use, retaliation and public interest. Approval records responsibility and limits.[99]

In immediate danger to civilians the controller may invoke safe harbour, notify and confine action to what cannot await decision. Military targeting does not hide within humanitarian continuity. The board's approval is necessary corporate governance, not a sovereign mandate.

12.6 What the Scenarios Prove

The five scenarios are deliberately unequal. They prevent the Act becoming an escalator in which the same label supplies the same response. The hospital case combines immediate life dependency, destructive access and a potentially autonomous operator; the energy case begins with pre-positioning and uncertain timing; the insurer begins with property loss and replication; the PMSC case tests payment, designed ignorance and State relation; the satellite case concerns a British private controller whose chosen assistance may expose the public to foreign consequence.

Across them, the first common act is preservation and service defence. That does not mean the legal character is identical. The hospital and energy operators also engage sector-resilience duties; the theft engages criminal and proceeds machinery; the PMSC engages licence, corporate and foreign-State questions; the satellite controller engages space supervision, company duty and the public-authority condition. Consolidation means one clock and evidence spine, not one substantive rule.

The cases also show why actual monetary loss is an incomplete measure. Official investigation of WannaCry recorded disruption across the NHS and the cancellation of thousands of appointments; the Synnovis incident again demonstrated pathology and blood-service dependency; industrial-control reporting concerning TRITON/HatMan showed malicious code directed at a safety instrumented system.[100] A system may be attacked through data and injure through service. The harm assessment follows the causal chain.

Yet the insurer scenario shows the opposite discipline. A large theft may be serious economic warfare, particularly where automated replication threatens systemic effect, without becoming armed attack. The Act responds firmly through seizure, restraint, provider action, prosecution, sanction and prevention orders. Force remains unavailable unless a distinct actual or imminent armed attack and its remaining tests are established. A doctrine which needs every important wrong to become war has impoverished the civil and economic powers it should instead strengthen.

The PMSC scenario proves that "the State did it" may contain several propositions. Article 4 organ status, article 5 governmental authority, article 8 instruction, direction or control, and article 11 acknowledgement and adoption are different routes; financing may evidence one without completing it. A territorial State may separately breach a due-diligence obligation after knowledge and capacity arise. The manifest and MOSAIC preserve the facts, but the legal conclusion must name its route.[101]

Finally, the satellite scenario proves reciprocity. A rule invented because the present intervention is sympathetic will remain when the proprietor supports the other side or a rival intervenes in a Western conflict. Published corporate governance, consumer choice and wealth do not supply a sovereign right. The statute places authority where retaliation and public consequence will fall, whilst leaving the company responsible for technical safety and legal compliance.

---

[99] Coronavirus Act 2020; Public Health (Control of Disease) Act 1984, s 45C; House of Lords Library, *Coronavirus: Emergency Legislation* (LLN-2020-0084, 23 March 2020).

[100] John Ferejohn and Pasquale Pasquino, 'The Law of the Exception: A Typology of Emergency Powers' (2004) 2 International Journal of Constitutional Law 210, 210–39.

[101] Veronika Fikfak and Hayley J Hooper, *Parliament's Secret War* (Hart 2018); Rosara Joseph, *The War Prerogative: History, Reform, and Constitutional Design* (OUP 2013).

The comparative result can be stated shortly: act first upon reversible dependencies; increase proof with irreversibility; separate operator, payer, host and State; reassess when scale and effects change; and never allow the economic-warfare classification to do the work of the independent legal gateway. This is the model's answer to both impotence and excess.

13. Principal Objections

The first objection is definitional breadth, and it is the objection which decides whether anything else in the Act is safe. Economic life is coercive by design. A supplier who withdraws credit, a union which strikes, a newspaper which publishes a leak and a State which raises a tariff all impair capacity, and each has at some point been described by a government as an attack upon the national interest. A statute which permits a minister to apply the label decides who is treated as an enemy, and the history of emergency legislation is that definitions widen under pressure rather than narrow.

The definition in clause 1(1) is broad and deliberately so, because a definition tied to instruments would be obsolete within a year of enactment. That concession has to be made plainly rather than managed.

What answers the objection is that the label carries no consequence of its own. Clause 1(5) provides expressly that classification determines nothing about offence, wrongful act, intervention, use of force, armed attack, aggression or armed conflict, so calling conduct economic warfare authorises no measure whatever. Every measure requires its own further findings: the thresholds in clause 2, the harm assessment in clause 3, the attribution assessment and decision-specific standard in clauses 50 and 51, the international-law gateway in clause 58, and for force the conditions in clause 62 and the certificate in clause 63. Clause 1(3) puts competition, industrial action, journalism, academic research, protest, authorised security testing and the ordinary exercise of contractual rights beyond the definition unless the conduct is independently unlawful. Clause 2(5) permits the Secretary of State to amend the descriptions of serious harm but forbids alteration of the critical threshold and forbids the creation of any use-of-force threshold by regulation.

What that does not reach is reputation. A person may be publicly described as the subject of an economic-warfare assessment before any measure is taken against him and before any court has seen the evidence, and neither judicial review nor the correction duty in clause 68 undoes the description. The Act should be understood as leaving that harm unremedied.

The second objection is executive overreach, and it is not answered by pointing at safeguards. Speed is precisely what makes a power dangerous. Under clause 30 a minister may require a private person to suspend a service upon the minister's own view of necessity, before any judge has seen the material, and the person must comply first and argue afterwards. Emergency powers enacted for the exceptional case become the ordinary case: Ferejohn and Pasquino's typology of emergency regimes describes that migration as the characteristic pathology rather than as an accident[102], and the objection is that this Act supplies a well-drafted vehicle for it.

The concession is that the risk is inherent and cannot be drafted away. A power which can be exercised in an hour can be misused in an hour.

The design answer is not delay but expiry, and expiry which operates without anyone having to apply for it. A temporary protective direction lapses after twenty-four hours without judicial approval and can never continue under emergency authority beyond seventy-two, an asset hold lapses after forty-eight, an

[102] Oren Gross and Fionnuala Ní Aoláin, *Law in Times of Crisis: Emergency Powers in Theory and Practice* (CUP 2006); David Dyzenhaus, *The Constitution of Law: Legality in a Time of Emergency* (CUP 2006); Clive Walker and Jim Broderick, *The Civil Contingencies Act 2004: Risk, Resilience and the Law in the United Kingdom* (OUP 2006); Adam Tomkins, 'Justice and Security in the United Kingdom' (2014) 47 Israel Law Review 305.

interim designation after seventy-two, and clause 74 provides that authority ends automatically where the conditions are not satisfied, with clause 74(2) stating that system failure does not extend authority. Clause 32(4) forbids reissue of a substantially similar direction to evade review, which is the ordinary route by which short powers become long ones. Accountability is personal rather than institutional: clause 83 makes it an offence for an official knowingly to use a power under the Act for political, personal or commercial favour, and the Commissioner sees the classified record under clause 78.

The residual difficulty is one of frequency rather than of drafting. A power used twice a year is reviewed carefully; a power used twice a week is reviewed by a form. Nothing in the Act prevents that erosion. The five-year expiry of Parts 4 and 7 in clause 80 is the only structural answer, and it is the weakest safeguard here because expiry invites renewal on a departmental account of how useful the power has been.

The third objection is duplication. The National Cyber Security Centre, the National Crime Agency, the National Cyber Force, the Office of Financial Sanctions Implementation, the sectoral regulators, the Investigatory Powers Commissioner and, if the Cyber Security and Resilience Bill passes, a further set of regulatory relationships already occupy this ground. Creating an Authority means one more body which must be consulted in the first hour, which is the opposite of the speed the Act is for.

That is a fair description of the risk and the Act cannot claim otherwise. Coordination bodies are frequently proposed and frequently become an additional layer.

The answer is that the Authority holds three things none of those bodies holds. It holds one timed record opened by a single report, running from first qualifying notice rather than from the moment a department accepts the severity, so that institutional delay appears in the record instead of disappearing from it. It holds a preservation power which operates across jurisdictions before any production process, which is the gap no existing body can close because preservation is not any regulator’s function. And it holds the control relationship over designated strategic capacity under Part 5, which is a relationship rather than a duty and has no existing holder at all. Clause 10 limits the Authority’s functions expressly so that it does not absorb police, intelligence, courts or armed forces; clause 16 requires notification of the devolved administrations and regulators; and clause 87 permits routing and terminology to be conformed to later cyber-resilience legislation rather than competing with it.

Whether that works is an appropriations question rather than a legal one. An Authority which cannot answer at three in the morning is an additional layer, exactly as the objection says, and the certification of readiness required by clause 91(2) before commencement is the only honest protection against it.

The fourth objection is the militarisation of cybercrime. Placing ransomware against a district council and self-defence against an armed attack within one statute invites a government to reach for the higher rung, because the higher rung is now in the same book. The Act’s name makes the invitation worse.

The concession is that a statute cannot prevent a government from arguing that a criminal intrusion is an armed attack. No drafting achieves that.

What the Act does is make the argument expensive and visible. Clause 1(5) separates the categories on the face of the definition. Part 7 is commenced separately under clause 91(2), expires separately under clause 80(3), and may be renewed only by an Act of Parliament rather than by regulations, which is a deliberately higher bar than the affirmative renewal available for Part 4. The international-law gateway in clause 58 is a separate finding which must be made and recorded, and the certificate under clause 63 and Schedule 3 requires the armed attack, its actual or imminent character, the evidential confidence and the reasons why non-forcible alternatives cannot achieve the objective in time. The overwhelming majority of incidents never leave Part 4 and the Act is designed so that they do not.

The residual point is real and should be stated rather than buried: by drafting conditions for the use of force in response to a cyber operation, the Act makes that possibility look more ordinary than it is. That is a cost of drafting anything, and it is accepted here on the view that an unregulated possibility is worse than a regulated one.

The fifth objection is escalation, and it is the objection this paper answers least well. Firm action invites reprisal. Publishing the legal basis for a measure tells an adversary where the thresholds sit and permits deliberate operation beneath them. Targeting the paying State for conduct carried out by a contractor converts a criminal matter into a State-to-State dispute. And a graduated ladder, which is the Act's central device, is by its nature an invitation to climb: each rung establishes that the previous rung was insufficient.

No claim is made here that the Act reduces escalation. Such a claim could not be tested and would not deserve belief.

Three features bear upon it. Clause 31 requires a direction to act upon the smallest dependency reasonably capable of achieving the purpose, which is a rule about the size of the first move rather than about whether to move. Clause 36 requires mandatory termination events, so that the ladder has defined points at which descent is compulsory rather than discretionary. And the publication of legal basis, though double-edged, is less dangerous than the alternative: unexplained action forfeits allied coordination, and the international thresholds are in any event already public, so what the Act publishes is the domestic route rather than the international rule.

The sub-threshold problem survives all of that. A patient adversary who reads the ladder can calibrate indefinitely to the rung below the one that bites, which is the characteristic form of contemporary economic coercion and the reason it is difficult to answer at all. The Act's response is clause 2(2)(f), which treats a material increase in the capacity for repeated serious acts as itself serious harm and so permits a campaign to be assessed as a campaign rather than as a series of incidents. That is a partial answer. It requires the Authority to hold and correlate a record over years, which is a capability the Act creates but which nothing guarantees will be used that way.

The sixth objection is attribution error. The Act attaches consequences to a determination which is technically uncertain, sometimes politically convenient, and occasionally wrong. Infrastructure is shared, tooling is stolen and reused, false flags are constructed precisely because analysts complete familiar patterns, and the record of public attribution by governments contains errors which were not corrected as loudly as they were made.

Irreversibility compounds the problem rather than sitting alongside it. A mistaken sanction can be lifted; a mistaken use of force cannot.

The Act's answer is to make the confidence structure explicit. Clause 50 requires an attribution assessment; clause 51(1) requires the decision maker to state the statutory test and the evidential standard applicable to the particular response; clause 51(2) forbids criminal, civil, sanctions, diplomatic, State-responsibility and self-defence conclusions from being represented as interchangeable, which is the single commonest error in this field; and clause 51(3) requires a high degree of confidence in each proposition essential to an irreversible response, so that the standard rises with what cannot be undone. Schedule 2, Part 2 records the material. Clause 56 addresses the territorial State which sees only a fragment, so that an innocent host is not made responsible by proximity. Clause 68 requires termination, reassessment and correction when the assessment changes.

What none of that reaches is the difference between the number of sources and their independence. Ten reports derived from one vendor's telemetry are one evidential root, and a decision maker under time pressure will not reliably notice. The Act requires the distinction to be recorded, which makes the error

reviewable afterwards rather than preventable at the time, and that is a smaller claim than the objection deserves.

The seventh objection is that Parliament should always approve the use of force, and in its strongest form it is not the objection that the Act gives Parliament too little. It is that clause 67 gives Parliament something worse than nothing. Fikfak and Hooper's study of the war-powers convention concludes that parliamentary involvement has operated as executive legitimation rather than as control: the House votes upon the Government's framing, at the Government's chosen moment, upon the Government's information, and a vote so constrained confers authority without exercising judgement. Joseph, arguing for a substantive parliamentary role, adds a constitutional back-stop for the courts precisely because a vote alone does not discipline the executive.[103] A statutory requirement of a Commons resolution to continue operations beyond seven days may therefore entrench the defect it appears to cure, by converting a convention which can at least be criticised into a statutory box which has been ticked.

That is the strongest objection in this Part and it is conceded that clause 67(3) may reproduce the very asymmetry Fikfak and Hooper identify.

Three things distinguish clause 67 from the convention as they describe it. The trigger is fixed rather than discretionary, so the Government cannot choose whether the moment has arrived. The material is prescribed: what Parliament votes upon is the continuation of an operation for which a certificate under clause 63 and Schedule 3 already exists, recording the armed attack, the evidential confidence, the legal basis, the rejected alternatives, the expected incidental effects, the advice of the Attorney General and the Chief of the Defence Staff, and any material dissent, with the original preserved under clause 63(2) and incapable of being overwritten by later information. That is a direct attack upon the information asymmetry, because the House is no longer dependent upon a ministerial narrative composed after the fact. And clause 68 makes termination, reassessment and correction obligations which operate independently of the vote, so that a favourable resolution does not validate a continuing operation whose factual basis has failed.

None of that answers the legitimation point, and it should not be presented as though it does. If the House votes upon a certificate the executive has written, the executive still frames the question, and a resolution obtained under those conditions will be cited afterwards as approval. The honest position is that clause 67 improves the information available to Parliament and does not alter the politics of how Parliament uses it. A reader who regards the politics as the whole of the problem should treat clause 67 as an improvement in the record rather than as a control, and should press for the judicial back-stop Joseph proposes in addition.

The eighth objection is that force directed at a named private individual is assassination however it is drafted. Article 51 addresses the permission of one State to defend itself against another; invoking it against an individual outside an armed conflict is a category error, and the unable-or-unwilling doctrine upon which action without host consent depends is contested rather than settled.

The Act does not assert that the doctrine is settled and clause 62(1)(f) requires the lawful basis for acting without consent to be identified rather than assumed.

The structural answer is that the Act creates no international permission at all. Clause 61 provides that nothing in Part 7 creates or enlarges a right to use force under international law or alters the law applicable to armed forces, and clause 5 requires any decision authorising conduct outside the United Kingdom to identify its independent basis in both domestic and international law. Outside armed conflict the law-enforcement standard and the right to life continue to apply with full force, and within

[103] Kristen E Eichensehr, 'Digital Switzerlands' (2019) 167 University of Pennsylvania Law Review 665; Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018); Henry Farrell and Abraham L Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44 International Security 42.

armed conflict status and conduct govern targeting under clause 62(1)(d) and the military-objective limb of the certificate. The Act cannot designate a person out of protection, and clause 1(5) prevents the classification from doing so by implication.

The residual cost is one of appearance rather than of doctrine. By setting out conditions under which force against an individual might lawfully be directed, the Act lends the contested doctrine the appearance of settlement. That is accepted, on the view that the alternative is not the absence of the practice but the absence of the record.

The ninth objection is that maximum reasonably credible foreseeable harm is speculative and converts precaution into permission. Any harm can be made to sound credible given enough hypotheticals, and a standard which licenses action upon harm that has not occurred licenses action upon harm that will not occur.

That is right wherever the exclusion in clause 3(3) is not enforced, and the standard stands or falls upon it.

Clause 3(2) directs the assessment to eight evidential matters rather than to imagination: access and privilege obtained, systems and persons reachable, capability and autonomy and persistence and replication, target function and season and population dependency and alternatives, safety controls and recovery and reversibility, apparent objective and prior conduct, confidence and contrary explanations and risk of deception, and the likely harm of the proposed response. Clause 3(3) then provides that a possibility unsupported by evidence is not reasonably credible merely because its consequence would be grave, which is the operative restraint. Schedule 2, Part 1 requires the assessment to be recorded. The alternative standard, which confines proportionality to harm already realised, is not neutral: it systematically rewards the attacker who is stopped seconds before consequence and penalises the defender who acts in time.

The residual weakness is that the standard is only as good as the record, and the record is written by the person who wants the power. The Commissioner’s access to the classified material under clause 78 and the independent reviewer under clause 80(1) are the checks; whether they are exercised with rigour is a question about institutions rather than about drafting.

The tenth objection is cost, and it should not be answered with rhetoric. Paper 3B estimates the core MOSAIC programme at £61.2 million over three years following a £10.61 million pilot, and that figure covers the evidence layer alone. The Authority, a rota of security-cleared judges with secure clerking, twenty-four-hour legal and technical staffing, special-advocate readiness, Commissioner capacity, provider interfaces, compensation, exercises, secure facilities and devolved participation all sit outside it. This is proposed to a government which has not fully resourced the regime it already operates, and the benefit is a counterfactual which cannot be measured.

The unmeasurability is conceded. A claim that the Act would have prevented a particular incident is unprovable and should not be made.

Two things bear upon the appraisal. Commencement is staged under clause 91(2) and conditional upon the Secretary of State certifying readiness, so the expensive components need not be bought before the cheap ones have demonstrated their value: definitions, appointments, codes and voluntary reporting first; preservation and identification once authenticated service and the judicial rota have been tested; strategic-capacity designation with an implementation period. And a large part of the cost is shared rather than additional, because the judicial rota, the special-advocate capacity and the twenty-four-hour legal function already exist in fragments across the national security estate and are duplicated precisely because nothing coordinates them. The Government should publish a business case separating capital

build, recurring operation, provider burden and contingent incident cost, and should model benefits as reduced consequence and reduced time rather than as invented revenue.

The comparison usually offered, that a single severe critical-infrastructure incident can exceed the programme cost, is true and close to worthless as an argument, because it assumes the thing to be proved. It is offered here only as an order of magnitude. The point which does carry weight runs the other way: an under-funded Act is worse than no Act, because it creates duties which cannot be discharged, a record which cannot be kept and a rota which cannot be staffed, and the certification of readiness in clause 91(2) exists so that a government which cannot fund Part 4 is obliged to say so before commencing it rather than afterwards.

13.1 Commencement, Cost and the Discipline of Use

The Act should commence in stages. Definitions, institutional appointments, codes and voluntary reporting may begin first; preservation and identification should follow once authenticated service and judicial rota have been tested; strategic-capacity designation should allow an implementation period except for an immediate interim designation; and the most intrusive directions should not commence until Parliament has approved the code governing evidence, review and provider compensation. Force provisions principally discipline an existing prerogative decision and can commence with the certificate machinery, but exercises must test the process before reliance.

Paper 3B's cost model supplies the evidence layer rather than the whole Authority. Additional costs include twenty-four-hour legal and technical staff, court and special-advocate readiness, Commissioner capacity, provider interfaces, compensation, exercises, secure facilities and devolved participation. The Government should publish a business case separating capital build, recurring operation, provider burden and contingent incident cost; benefits should be modelled as reduced consequence and time, not invented revenue. The Cyber Security and Resilience Bill's impact assessment estimates substantial economy-wide regulatory cost, which is a useful warning that apparently simple reporting duties can transfer a large operational burden.[104]

Cost cannot be assessed from the Authority's budget alone. Duplicate reports, uncoordinated warrants, delayed restoration, mistaken sanctions and broad service interruption are public and private costs of the present fragmentation. Conversely, a central body may create its own duplication if it requires data already held by a competent regulator or builds forensic capacity which NCSC, police or the private sector already provides. The statutory duty to accept an agreed single report and route it to each competent body is therefore a cost control, not an administrative courtesy.

Parliament should require an independent review after two years of substantive operation and a five-year renewal vote for the emergency-order Parts. Ordinary reporting, victim support, manifests and institutional provisions may continue; the power to impose rapid protective and asset directions should lapse unless renewed after evidence of use, error, burden and benefit. A sunset is not appropriate for every definition or offence, but is appropriate where exceptional speed reduces ordinary prior process.[105]

Parliamentary scrutiny should thus be moved to the point at which it can improve the system without consuming the moment in which the system must act. Before commencement, Parliament approves the

[104] Cybersecurity and Infrastructure Security Agency and others, *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity* (Fact Sheet, 1 May 2024) https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity accessed 7 August 2026; Cybersecurity and Infrastructure Security Agency and others, 'Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure' (AA25-343A, 9 December 2025).

[105] National Cyber Security Centre, *The Near-Term Impact of AI on the Cyber Threat* (24 January 2024) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat accessed 7 August 2026; National Cyber Security Centre, *Impact of AI on Cyber Threat from Now to 2027* (May 2025) https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027 accessed 7 August 2026.

threshold, the protected classes, the maximum duration, the remedial jurisdiction and the code governing each intrusive power. After use, the court tests the individual order, the Commissioner tests the classified record and Parliament receives aggregate and exceptional-incident reporting. At renewal, Parliament sees error, refusal, lapse, collateral effect, compensation and time-to-action. That division is not a diminution of parliamentary authority. It distinguishes the legislative question—what power may exist and upon what conditions—from the operational question—whether a named dependency must be stopped at 02.17 tomorrow morning.

The distinction should also govern delegated legislation. A minister may update a technical interface, reporting format or class of provider by instrument, because obsolescence would otherwise be rapid. A minister should not, by the same route, create a new offence, enlarge the use-of-force gateway or revive an expired power of urgent defensive force. Made-affirmative procedure is defensible where immediate effect is itself protective, provided lapse is automatic and short; it is not a substitute for primary legislation where the constitutional character of the power changes. The Bill accordingly permits a five-year renewal of Part 4 by affirmative instrument only after independent review, whilst requiring primary legislation to renew Part 7. The executive therefore receives speed in the incident, not permanent control over the legal perimeter.[106]

The review should ask not only how many orders were made but how many incidents were stopped sooner, how often a narrower dependency became available, whether evidence survived, how many orders lapsed without confirmation, how often protected activity was affected, whether operators migrated, whether foreign partners corrected records, and whether the response deterred the payer or merely displaced the contractor. A power unused may be unnecessary or may deter; a power frequently used may be essential or drafted too broadly. Numbers require case examination.

Implementation should conclude with a national exercise in which government is denied convenient facts. One provider should be foreign and cooperative, one domestic and resistant, one compromised; attribution should contain a persuasive false flag; the autonomous workload should migrate; Parliament should be in recess; the host State should see only a fragment; and civilian services should share the suspected infrastructure. If the Act works only when every institution agrees and the attacker remains still, it has been tested as ceremony rather than law.

14. Conclusion

Economic warfare is no longer contained by the categories in which English law looks for it. A criminal intrusion may be one fragment of State coercion; a commercial service may decide a battlefield; an autonomous agent may select the jurisdiction through which it attacks; a poor operator may cause State-scale harm; a State may purchase deniability more cheaply than a weapon.

The proposed Act does not abolish the existing law. It makes it move together. One report opens one timed record. Evidence is preserved before production. Fragments are correlated without universal central collection. Controllers keep manifests. Strategic private capacity comes under rapid public authority. Measures reach payer, operator, account and infrastructure.

Its constitutional method is immediate action followed by immediate accountability. Preservation, identification and short restraint occur upon lower but defined thresholds because they are reversible. Courts confirm continuation. Parliament controls broad regulation and sustained force. The Commissioner sees the classified record. Error propagates as correction rather than institutional memory.

[106] National Cyber Security Centre, *Impact of AI on Cyber Threat from Now to 2027* (n 8); Cybersecurity and Infrastructure Security Agency and others, *Defending OT Operations* (n 7).

The Act is deliberately more powerful than Magnitsky-style designation. Sanctions name and constrain; they do not alone stop a destructive workload. The response ladder includes criminal, civil, financial, technical, diplomatic and military measures. It selects according to law and effect, not institutional habit.

Military force remains exceptional and real. A cyber operation may be an armed attack when its scale and effects equal kinetic attack. Anticipated death, injury and physical destruction are part of the United Kingdom's published position. If a keyboard is causing the consequence of a weapon, the law should examine the consequence. If, and only if, an actual or imminent armed attack exists, force is necessary and proportionate, the target lawful, precautions taken and the international basis certified, Clause 62 permits the executive to act before delay turns prediction into casualty.

This is not a licence to punish theft with missiles. Deterrence alone does not create article 51 necessity; countermeasures cannot use force; broad possibility is not credible maximum harm; private attackers retain rights; innocent host States are not responsible merely because they see one fragment. Those are legal boundaries, not apologies.

The greater danger is a system which is most scrupulous at the point where scrutiny can no longer protect. The law should be strongest before the hospital loses its only record and before winter power failure makes every minute irreversible. Speed and restraint are reconciled when the first act is narrow, the evidence preserved, the authority named and the review already waiting.

The measure is therefore neither a declaration that every cyber offence is war nor a promise that sanctions will suffice. It is a constitutional allocation of time. The first minute belongs to warning, preservation and defence; the first hours to the named minister, legal gateway and narrow dependency; the first days to the court, Parliament, correction and allies; the later period to prosecution, compensation, licence and institutional learning. At no stage does one label replace the rule applicable to the act proposed.

Its deterrent is strongest because it is executable. The foreign payer knows that the market and procurement relation may be exposed; the operator that credentials, equipment and movement may be reached; the infrastructure provider that an authenticated, particular order is already prepared; the private sovereign that political authority cannot be purchased with the asset; and the armed attacker that placing a cheap agent between itself and consequence will not remove lawful defence. A power which is both swift and bounded is more credible than a threat so broad that ministers dare not use it.

Draft Provisions: United Kingdom Economic Warfare Prevention and Response Bill

A Bill to prevent, identify and respond to economic-warfare acts; to establish an Economic Warfare Response Authority; to provide for reporting, preservation, protective directions, strategic private capacity and high-risk security services; to regulate urgent defensive decisions; and for connected purposes

Be it enacted by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows—

Part 1 — Preliminary

1 Economic-warfare act

1. In this Act an "economic-warfare act" is conduct, or a coordinated course of conduct, which—
    a. is intended, or is reasonably capable in the circumstances, materially to impair, coerce, destabilise, appropriate or deny the economic, technological, institutional, democratic, defence or essential-service capacity of the United Kingdom, a protected person or a partner State; and
    b. is carried out by or through a State, organisation, undertaking, private military or security company, autonomous system or individual.
2. Conduct may constitute an economic-warfare act whether effected by financial, commercial, cyber, informational, technological, logistical, physical or combined means.
3. Lawful competition, industrial action, journalism, academic research, protest, authorised security testing and the ordinary exercise of contractual rights do not constitute an economic-warfare act unless the conditions in subsection (1) are independently satisfied and the conduct is unlawful under an applicable rule.
4. Classification under this section does not determine whether conduct is an offence, internationally wrongful act, prohibited intervention, use of force, armed attack, act of aggression or conduct occurring in armed conflict.

2 Reportable, serious and critical acts

1. A "reportable act" is an event which a designated person reasonably suspects may constitute a serious economic-warfare act.
2. An act is "serious" where actual or maximum reasonably credible foreseeable harm includes—
    a. material interruption of an essential service;
    b. substantial danger to life or physical safety;
    c. material interference with democratic institutions, national security or defence;
    d. systemic financial, commercial or data-integrity harm;
    e. substantial theft or destruction of strategically important property, information or capability; or
    f. a material increase in the capacity for repeated serious acts.
3. An act is "critical" where—
    a. serious harm is occurring or imminent;
    b. delay is likely materially to reduce the ability to prevent or mitigate it; and
    c. action taken within that period is capable of preventing or mitigating that harm.
4. The Secretary of State may by affirmative regulations amend descriptions in subsection (2), but may not alter subsection (3) or create a use-of-force threshold.

3 Harm assessment

1. A decision under Parts 3 to 7 must consider actual harm and maximum harm reasonably credible and foreseeable at the time.
2. The assessment must address, so far as relevant—
    a. access and privilege obtained;
    b. systems and persons reachable;
    c. capability, autonomy, persistence and replication;

d. target function, season, population dependency and alternatives;

e. safety controls, recovery and reversibility;

f. apparent objective and prior conduct;

g. confidence, contrary explanations and risk of deception; and

h. likely harm of the proposed response.

3. A possibility unsupported by evidence is not reasonably credible merely because its consequence would be grave.

4. Schedule 2 makes further provision concerning harm and attribution assessments.

4 Protected systems, persons and partner States

1. Schedule 1 specifies protected functions, and the Secretary of State may by affirmative regulations add a function to that Schedule.

2. The Secretary of State may designate a person, system, service, supply chain or partner State where protection is necessary in the interests of national security, defence, life, essential services or the performance of an international obligation.

3. A designation must describe the protected function sufficiently to permit compliance and challenge, but may place security-sensitive technical detail in a protected annex.

4. An urgent designation may take effect immediately and expires after seven days unless approved by resolution of each House of Parliament.

5 Independent legal authority

1. Nothing in this Act—

   a. except as expressly provided by this Act, makes conduct lawful which is unlawful under another enactment;

   b. authorises interception, equipment interference, acquisition of communications data, search, production, confiscation or force except where expressly provided; or

   c. determines State responsibility or the existence of an armed conflict.

2. A decision authorising conduct outside the United Kingdom must identify its independent basis in domestic and international law.

3. A material change in target, geography, effect or purpose requires the basis to be reconsidered and recorded.

6 General principles

1. A person exercising a function under this Act must act lawfully, necessarily, proportionately and for a statutory purpose.

2. Where two effective measures are available, the person must prefer the measure reasonably expected to be less intrusive or harmful.

3. Emergency action must be particular, time-limited, reviewable and capable of revocation so far as technically practicable.

4. The fact that an act is cheap, privately conducted or technically remote does not reduce its assessment by consequence.

5. The fact that conduct is classified under section 1 does not reduce the rights of an individual or the protection of a civilian or civilian object.

7 Interpretation

In this Act—

- “the Authority” means the Economic Warfare Response Authority;
- “autonomous system” means a computational system capable, after activation, of selecting or materially adapting targets, techniques, timing, infrastructure or jurisdictional route without approval of each material decision by a natural person;
- “controller” means a person with legal or practical power to grant, withdraw, alter, direct or stop a service or capability;
- “designated judge” means a judge assigned under section 70;
- “designated organisation” means a person prescribed under section 17 or designated under Part 5;
- “MOSAIC” means the Multijurisdictional Operation Signal Attribution and Integrity Correlation service;
- “protected material” means material whose disclosure would be likely to damage national security, defence, intelligence capability, an investigation, legal privilege, personal safety or the security of a protected system;

- “Response Minister” means the minister designated under section 13;
- “strategic assistance” has the meaning in section 45.

Part 2 — Economic Warfare Response Authority

8 Establishment

1. There is established a body corporate called the Economic Warfare Response Authority.
2. The Authority is not to be regarded as the servant or agent of the Crown except in the exercise of a function expressly conferred upon it as such.
3. Schedule 4 makes provision concerning appointment, staff, finance and accounts.

9 Functions

The Authority must—

1. receive and triage reports;
2. operate the United Kingdom MOSAIC node and central incident register;
3. coordinate preservation, attribution and response;
4. designate and supervise strategic private capacity as directed by the Secretary of State;
5. support ministers, courts, regulators, investigators and victims;
6. maintain international cooperation and tested contact routes;
7. publish standards, codes and reports; and
8. conduct exercises and measure response time.

10 Limits upon functions

1. The Authority may not exercise an investigative, intelligence, sanctions, regulatory or military power vested in another person except where this Act or another enactment expressly confers it.
2. Coordination by the Authority does not transfer the legal responsibility of the office holder exercising a power.
3. The Authority must maintain a public map of institutional responsibilities, subject to omission of protected operational detail.

11 Economic Warfare Response Group

1. The Authority must maintain a continuously available Response Group comprising duty representatives of—
    a. the National Cyber Security Centre;
    b. the National Crime Agency and territorial policing;
    c. the Foreign, Commonwealth and Development Office;
    d. His Majesty’s Treasury and the Office of Financial Sanctions Implementation;
    e. the Cabinet Office;
    f. the Ministry of Defence;
    g. the Attorney General’s Office;
    h. affected regulators and devolved administrations; and
    i. such other bodies as the Authority considers necessary.
2. The Group must be capable of secure assembly within fifteen minutes of a critical notice.
3. It must record facts, disputed propositions, owners, dependencies, decisions and deadlines.
4. The Group does not exercise a member’s statutory power by consensus.

12 Duty officers and readiness

1. The Authority must maintain duty officers authorised to issue notices under sections 25 and 26.
2. The Secretary of State must ensure that ministerial, legal, judicial and technical duty arrangements are continuously available.
3. The Authority must test provider contacts, secure channels, revocation routes and foreign-node contacts at least every six months.

13 Response Minister

1. Upon a critical notice the Prime Minister or a Secretary of State must designate a Response Minister.
2. The Response Minister owns the protective objective and coordination of ministerial decisions.
3. Subsection (2) does not authorise the Response Minister to exercise a power vested in another person.
4. The designation and every substitution must be recorded in MOSAIC.

14 Economic Warfare Commissioner

1. There is to be an Economic Warfare Commissioner appointed by the King upon an address of the House of Commons.
2. The Commissioner holds office for a single term of six years and may be removed only upon an address of each House.
3. The Commissioner may—
    a. inspect any record, system or protected material held for a function under this Act;
    b. require information from the Authority or a designated controller;
    c. attend the Response Group without exercising command;
    d. refer a matter to a designated judge, prosecutor, regulator or Parliament; and
    e. issue recommendations and reports.

15 Codes and service standards

1. The Authority must issue codes concerning reporting, preservation, source classification, protected categories, provider interfaces, strategic manifests, correction and revocation.
2. A code affecting an intrusive power has no effect until approved by resolution of each House.
3. Departure from a code does not of itself create civil or criminal liability, but the code is admissible in proceedings and reasons for material departure must be recorded.

16 Devolved administrations and regulators

1. The Authority must notify and involve an affected devolved administration and competent regulator at the earliest time compatible with safety.
2. The absence or delay of notification does not invalidate a reserved measure urgently required to protect life or national security, but reasons must be recorded.
3. The Authority must agree single-report and information-routing arrangements with regulators.

Part 3 — Reporting, Evidence and MOSAIC

17 Designated reporting organisations

1. The Secretary of State may by affirmative regulations designate a class of organisation which provides or materially supports a protected function.
2. Regulations may apply by function, dependency, scale, substitutability or risk and need not depend upon turnover.
3. Before making regulations the Secretary of State must consult the Authority, affected regulators and representatives of persons likely to be designated.
4. An urgent interim designation expires after seven days unless approved by each House.

18 Initial report

1. A designated organisation must notify the Authority—
    a. within one hour after reasonable confirmation of a critical act; or
    b. within six hours after reasonable confirmation of a serious act.
2. The report must state what is known concerning incident, affected function, observed access, action taken, immediate dependency and responsible contact.
3. Attribution is not required in an initial report.
4. The Authority may extend time where technical impossibility or immediate life-safety work reasonably prevented reporting.

19 Further report

1. A designated organisation must provide a fuller report within seventy-two hours.

2. The report must address chronology, systems, data, service effect, indicators, provider dependencies, recovery, evidence preserved and material uncertainty.

3. A materially changed fact must be notified without waiting for the further report.

20 Single-report discharge

1. Where the Authority has an agreement with a competent regulator, a report submitted through the prescribed interface discharges each identified overlapping duty to the extent stated in the receipt.

2. The Authority must route the report promptly and record delivery.

3. Nothing in this section reduces a duty to make an emergency call or undertake life-safety action.

21 Reporting protection and offences

1. A person is not liable for a good-faith preliminary error made in an urgent report.

2. A person commits an offence if, without reasonable excuse, the person—

    a. intentionally conceals a critical act;

    b. knowingly or recklessly makes a materially false report.

3. A person guilty under subsection (2) is liable on conviction on indictment to imprisonment not exceeding five years, a fine, or both, and on summary conviction to imprisonment not exceeding twelve months, a fine, or both.

4. Protected disclosure and responsible security research are to be provided for by code and regulations.

22 Central incident register

1. The Authority must maintain a register of case metadata, source class, preservation receipt, decision, expiry, correction and public lesson.

2. Raw evidence must remain with its lawful custodian or accredited repository unless produced under independent lawful authority.

3. The register must distinguish observation, custodian record, forensic finding, intelligence assessment, model analysis, allegation, State attribution and legal finding.

4. Access must be role-, case- and purpose-bound and continuously logged.

23 Correction, retention and deletion

1. A material correction must be propagated to every recorded recipient.

2. Personal and confidential material may be retained only for a statutory purpose, legal hold or period prescribed by regulations.

3. Deletion may preserve a tombstone recording source, authority, time and fact of deletion without retaining the deleted content.

4. A person may apply to the Commissioner or designated court for correction or deletion.

24 MOSAIC

1. The Authority must operate the United Kingdom MOSAIC node for authenticated discovery, rapid preservation, source integrity, lawful evidence routing and manifest custody.

2. MOSAIC does not itself authorise production, interception, equipment interference, designation, sanction, countermeasure or force.

3. Every request must state its independent legal basis, purpose, scope, retention and recipient.

4. A foreign participant may search no British content generally; discovery is limited to signed, particular queries and locally evaluated match assertions.

25 Emergency preservation notice

1. A designated officer may issue an emergency preservation notice where the officer reasonably believes that—

    a. specified data are likely to be relevant to a serious act;

    b. the data are at material risk of alteration, loss or destruction; and

    c. preservation is necessary and proportionate.

2. The notice must identify, so far as practicable, the data, custodian, period, purpose, officer, issue time, expiry and means of challenge.

3. The notice requires preservation and prohibits intentional destruction; it does not authorise disclosure.

4. A notice expires after seven days unless confirmed by a designated judge or the authority competent for the applicable data.

5. The custodian must return a signed receipt or a reasoned inability or refusal.

26 Emergency identification notice

1. A designated officer may require a provider within United Kingdom jurisdiction to state whether it controls a specified account, domain, service, workload, credential or payment identifier and to identify the competent contact for lawful process.
2. The notice may not require content or bulk enumeration.
3. A notice concerning legally privileged, journalistic, parliamentary, medical or political material requires approval of the Commissioner or a designated judge, save where delay presents an imminent danger to life.
4. Results may be retained only for the incident and applicable legal hold.

27 Foreign service and conflict of law

1. A provider offering a designated service in the United Kingdom may be required to appoint a representative for service.
2. Service abroad must comply with an applicable treaty, agreement, foreign law or other lawful basis.
3. A recipient claiming conflict of law must notify the Authority promptly and identify the conflict so far as lawful.
4. A designated judge may preserve the status quo, vary the notice or direct use of a treaty or agreed production route.

28 Confidentiality and permitted disclosure

1. Information obtained under this Part is confidential.
2. It may be disclosed where necessary and proportionate for protection, investigation, legal proceedings, regulation, warning, oversight, victim support or lawful international cooperation.
3. Legal privilege is not displaced except by express enactment.
4. The Authority must maintain and publish a disclosure code.

Part 4 — Emergency Protective Measures

29 Voluntary action and warning

1. Before issuing a compulsory direction the Authority must consider whether authenticated warning or voluntary action can achieve the protective purpose in time.
2. Failure to warn does not invalidate action where warning would increase harm, reveal the target or consume the last effective opportunity.
3. Reasons must be recorded.

30 Temporary protective direction

1. The Response Minister may direct a person within United Kingdom jurisdiction to take specified action where—
    a. a critical act is occurring or imminent;
    b. the person controls a service, account, credential, system or capability materially enabling the act or necessary to mitigate it;
    c. the direction is necessary and proportionate; and
    d. judicial approval cannot reasonably be obtained without materially increasing harm.
2. A direction may require preservation, isolation, suspension, credential revocation, traffic filtering, warning, continuity, exercise of a registered stop function or technical assistance within the person’s existing capability.
3. It may not require indiscriminate weakening of security, disclosure beyond an independent power, force against a person or conduct manifestly contrary to international law.

31 Particularity and smallest effective dependency

1. A direction must act upon the smallest dependency reasonably capable of achieving the purpose.
2. It must state machine-readable identifiers where available, exclusions, authorised action, collateral service, issue time, expiry, human contact and revocation route.
3. The recipient must report action, material collateral effect and observed migration.

32 Duration and confirmation

1. A temporary protective direction expires twenty-four hours after issue unless approved by a designated judge.
2. It may in no case continue under emergency authority beyond seventy-two hours.

3. The judge may continue, narrow, substitute or discharge the direction.

4. An identical or substantially similar direction may not be reissued to evade review.

33 Domestic defensive action

1. The Authority, the National Cyber Security Centre and a public authority may take necessary and proportionate action upon a system it lawfully controls to detect, isolate, deceive, rate-limit, redirect or remove hostile activity.

2. Action upon another person's system requires consent, direction, warrant, court order or another lawful basis.

3. Collection through a sinkhole, honeypot or token must identify purpose, scope, retention and access.

4. This section does not amend the Computer Misuse Act 1990 or Investigatory Powers Act 2016.

34 Emergency asset and transaction hold

1. A minister authorised by the Treasury or a designated judge may impose a hold where funds or economic resources are reasonably believed to finance, constitute proceeds of, or be necessary to a critical act.

2. The hold expires after forty-eight hours unless converted to a sanctions designation, restraint order or other lawful order.

3. It must be particular and must not restrain unrelated customers merely because they use the same intermediary.

4. Provision must be made for essential expenses, challenge and good-faith compliance.

35 Compensation and compliance defence

1. A person complying in good faith with a facially valid direction is not liable for the act required, save for negligence, bad faith or conduct outside the direction.

2. The Authority must compensate exceptional reasonable cost where compliance chiefly serves public defence rather than remediation of the person's own breach.

3. Dispute concerning compensation is determined by a designated judge.

36 Revocation and off-ramp

1. Every direction must specify termination events.

2. Compliance, changed evidence, host action, migration, unacceptable collateral effect, judicial refusal and loss of necessity must be assessed continuously.

3. Revocation must be sent through the authenticated issue route and receipt confirmed.

4. Failure of a recipient to stop after confirmed revocation is an offence unless technically impossible despite reasonable preparation.

37 Civil penalties

1. The Authority may impose a civil penalty for unjustified reporting failure, failure to preserve, non-compliance with a confirmed direction or breach of a designation duty.

2. In determining amount it must consider harm, culpability, cooperation, turnover, benefit, remediation and ability to pay.

3. Regulations may prescribe a maximum not exceeding four per cent of the person's worldwide annual turnover, including that of any group of which the person is a member, or £25 million, whichever is greater.

4. A person may appeal upon fact, law and amount to the designated court.

Part 5 — Strategic Private Capacity and High-Risk Services

38 Strategic private capacity

1. A service or capability is strategic private capacity where its grant, withdrawal, alteration or hostile use could materially affect defence, armed conflict, life, essential services, democratic institutions, systemic finance, strategic communications, positioning, observation, compute or high-impact cyber operation.

2. Designation attaches to the function and control, not merely to size or market share.

39 Designation

1. The Secretary of State may designate strategic private capacity by notice stating function, controller, reasons, duties and review date.

2. An interim designation may take immediate effect and expires after seventy-two hours unless confirmed.

3. Confirmation requires consultation with the Authority and notice sufficient for challenge.

4. A designated person may appeal to the designated court.

40 Responsible officers and control map

1. A controller must nominate a board-level responsible officer and continuously available operational officer.
2. It must record beneficial ownership, contracting entity, technical operator, credentials, infrastructure, subcontractors and persons able to stop or materially alter the function.
3. A material change must be notified within twenty-four hours or sooner during a critical incident.

41 Continuity and stop capability

1. A controller must maintain a tested continuity, recovery and strategic-decision plan.
2. Where technically feasible for a capability capable of serious autonomous or destructive effect, the controller must maintain a secure revocable root credential or equivalent stop facility.
3. The facility must fail closed for destructive action when command integrity or certified bounds are lost, subject to life-safety requirements.
4. The Authority may approve an alternative where a stop facility would create greater risk.

42 Strategic decision manifest

1. The controller must preserve a signed, versioned manifest recording objective, human authority, target class, prohibited targets, software and model versions, infrastructure, subcontractors, credentials, autonomous discretion, stop conditions, changes and incidents.
2. A sealed manifest may be held in split custody.
3. It may be opened upon serious harm, credible unlawfulness, court order, Commissioner demand or lawful foreign request.
4. The manifest is evidence but not conclusive proof of conduct or attribution.

43 Foreign and coercive requests

1. A controller must notify the Authority of a request by or on behalf of a foreign power or party to armed conflict for strategic assistance.
2. It must also notify coercion, conflicting legal demand or material attempt to obtain undisclosed control.
3. The notice must identify the requested act, time, legal basis asserted and person able to approve or refuse.

44 Prohibition upon unauthorised strategic intervention

1. A controller of designated strategic private capacity must not provide tailored strategic assistance to a party to armed conflict without authorisation under section 45.
2. General service on ordinary and non-discriminatory terms is not tailored assistance unless configuration, priority, geofencing, sensing, analysis, target support or continuity is materially adapted to the operation.
3. This section does not prohibit action required by another enactment or immediate humanitarian action under section 46.

45 Strategic assistance authorisation

1. The Response Minister may authorise strategic assistance after considering—
    a. the requesting party and legal position asserted;
    b. the function, target class and territorial reach;
    c. civilian dependence and retaliation risk;
    d. neutrality, space, human-rights and humanitarian obligations;
    e. technical discretion retained by the controller;
    f. duration, stop condition and consequence of refusal; and
    g. the United Kingdom’s public interest.
2. Authorisation must be bounded, signed, time-limited and recorded.
3. Material change requires renewal.

46 Humanitarian safe harbour

1. A controller may take immediately necessary action to protect life where public authority cannot be reached in time.
2. The action must be confined to the purpose and period which cannot safely await decision.
3. The controller must notify the Authority immediately and seek continuation within six hours.
4. Tailored military targeting is not humanitarian merely because success may ultimately protect life.

47 High-risk services licence

1. A person must not provide a high-risk service from the United Kingdom, by a United Kingdom person, or through designated British-controlled capacity without a licence.
2. High-risk service means offensive cyber access, commercial intrusion, target generation, autonomous effect, operation of weapons or destructive systems, strategic intelligence, detention and command of armed personnel.
3. A licence must identify clients, jurisdictions, target restrictions, model and tool governance, subcontractors, insurance, audit, reporting and manifest duties.

48 Prime contractor and subcontractor

1. A licensed prime contractor remains responsible for governance, manifest, client, target and reporting duties throughout its chain.
2. Subsection (1) does not make a subcontractor guilty of a substantive offence without the conduct and mental element required for that offence.
3. Deliberate fragmentation intended to prevent subcontractors identifying the whole does not permit the prime to rely upon their ignorance as its own.

49 Suspension, revocation and debarment

1. The Authority may suspend a licence for seventy-two hours where a critical risk exists.
2. Continued suspension, revocation or debarment requires notice and determination by the designated court or licensing tribunal.
3. Government procurement of high-risk services is subject to this Part; protected procurement may alter disclosure but not record or oversight.

Part 6 — Attribution and Graduated Response

50 Attribution assessment

Before a Level 4 or Part 7 response the Authority must assess operation, infrastructure, identity, integration, financing, benefit, State relation, host knowledge, confidence, contrary hypothesis and evidential class in accordance with Schedule 2.

51 Decision-specific standard

1. The decision maker must state the statutory test and evidential standard applicable to the response.
2. Criminal, civil, sanctions, diplomatic, State-responsibility and self-defence conclusions must not be represented as interchangeable.
3. A high degree of confidence is required in each proposition essential to an irreversible response.

52 Level 1 — warning and preservation

The Authority may warn, request voluntary action, supply technical assistance, issue preservation and identification notices and query partner nodes.

53 Level 2 — containment

Upon the authority applicable to the act, containment may include credential reset, account suspension, domain control, filtering, workload isolation, patching, segmentation, sinkholing and continuity action.

54 Level 3 — personal and corporate restraint

1. The responsible authority may seek arrest, search, seizure, injunction, licence action, director disqualification, asset restraint, travel restriction, domain seizure, procurement exclusion, reward or protected cooperation.
2. Each measure requires its independent statutory basis.

55 Level 4 — State and collective cost

1. Where the applicable evidential and legal conditions are met, ministers may employ public attribution, targeted sanction, export and procurement restriction, diplomatic measure, allied designation, lawful countermeasure, international proceeding, defensive disclosure and victim support.
2. Countermeasures must comply with international law and may not involve force.
3. A material correction must be transmitted to every partner requested to act.

56 Territorial State and fragmented knowledge

1. The Authority must distinguish conduct attribution from responsibility for an omission.

2. Location of a fragment is not proof that the territorial State conducted or knew of the operation.
3. Where feasible the United Kingdom must give authenticated notice, sufficient information and a reasonable opportunity to act.
4. Deliberate jurisdictional fragmentation by the controller must be recorded in attribution and response.

57 Direct operator measures

1. Measures should reach the smallest effective dependency of the operator, including equipment, connectivity, credentials, command, payment and movement.
2. Lack of attachable assets does not immunise the operator.
3. Poverty, nationality or location does not reduce legal rights or remove the requirement for necessity and proportionality.

58 International-law gateway

1. Counsel must classify each material external act as consent-based cooperation, retorsion, countermeasure, treaty process, necessity, self-defence or other specified basis.
2. The record must state territory, affected right, prior wrong or attack, notification, limit and termination.
3. Where the basis changes, fresh authority is required.

59 Assistance to partner States

1. The United Kingdom may provide assistance at the request of a partner State in accordance with domestic and international law.
2. Collective self-defence requires a request by the attacked State and compliance with article 51 of the Charter.
3. A private request or commercial contract is not a request for collective self-defence.

60 Response guidance

The Secretary of State must publish guidance requiring decision makers to explain why a less harmful effective measure was unavailable, why an ineffective measure was not continued and how escalation and civilian consequence were assessed.

Part 7 — Urgent Defensive Force

61 No enlargement of international right

Nothing in this Part creates or enlarges a right to use force under international law or alters the law applicable to armed forces.

62 Conditions for urgent defensive force

1. The Prime Minister, or a Secretary of State expressly authorised where the Prime Minister is unable to act, may direct force concerning a critical act only where satisfied, to the standard required by section 51(3), that—
    a. an actual or imminent armed attack against the United Kingdom or a State requesting collective self-defence exists;
    b. force is necessary to halt, repel or prevent that attack;
    c. force is proportionate to the defensive purpose;
    d. each person or object to be attacked is a lawful target;
    e. feasible precautions have been taken and expected incidental civilian harm is not excessive;
    f. the territorial State has consented, bears responsibility upon the applicable law, or action without consent has another lawful basis;
    g. the Attorney General or qualified alternate Law Officer has certified the legal basis; and
    h. the Chief of the Defence Staff has certified operational feasibility and target review.
2. Force may not be directed solely to punish a completed act or produce general deterrence.

63 Defensive action certificate

1. Except where section 64 applies, a direction under section 62 has no effect unless a certificate records the matters in Schedule 3.
2. The original certificate must be preserved and may not be overwritten by later information.
3. Supplementary information must identify its time and source.

64 Extreme urgency

1. Where completion of the certificate would probably forfeit the last feasible opportunity to prevent death or serious physical harm, an oral direction may be given and recorded by two officials.
2. The record must identify target, objective, attack, legal basis and decision maker.
3. The certificate must be completed as soon as practicable and in any event within six hours.
4. Failure terminates authority for continuing action and must be reported immediately to the Commissioner.

65 Live-target verification

1. Immediately before execution the responsible commander must confirm, so far as time and means reasonably permit, that—
    a. the target still performs the hostile function;
    b. civilian use has not materially changed;
    c. necessity continues; and
    d. no less harmful effective measure has become available.
2. A migrating virtual target may be followed only by pre-authorised identity, behaviour, geography, time, exclusion and stop criteria.
3. Failure of identity or exclusion data must cause automated engagement to fail closed.

66 Host-State notice and Security Council report

1. Where feasible the United Kingdom must request territorial-State action, identifying threat, location, action sought and response time.
2. Notice may be omitted only where it would reveal the target, enable migration or consume the last effective opportunity; reasons must be certified.
3. Action in self-defence must be reported to the Security Council in accordance with article 51.

67 Parliamentary notification and continuation

1. Prior Commons debate must occur where circumstances permit.
2. Where action cannot await debate, the Prime Minister must—
    a. notify the Leader of the Opposition and designated security-cleared parliamentarians where feasible;
    b. consider recall immediately;
    c. make a statement at the earliest safe time; and
    d. provide an open legal summary and classified annex.
3. Continued operations beyond seven days require a Commons resolution.
4. A single extension not exceeding seven days may be certified where disclosure would cause specified immediate operational danger.

68 Termination, reassessment and correction

1. Force must cease when necessity ceases.
2. The direction must specify reassessment interval and measurable termination conditions.
3. Unexpected civilian consequence, failed target verification or material contrary evidence requires pause where operationally feasible and immediate legal review.
4. Material error requires investigation, correction and compensation where legally due.

Part 8 — Court, Oversight and Remedy

69 Jurisdiction

The High Court in England and Wales, the Court of Session and the High Court of Justice in Northern Ireland have jurisdiction according to ordinary territorial and subject-matter rules, with transfer and common procedural provision made by rules of court.

70 Designated judges

1. The Lord Chief Justice of England and Wales, the Lord President of the Court of Session and the Lady Chief Justice of Northern Ireland must maintain a rota of judges with appropriate clearance and technical support.
2. Secure remote application must be continuously available.

3. Judicial independence is not affected by participation in the rota.

71 Urgent application and return hearing

1. An application may be made without notice where notice would materially prejudice the protective purpose.
2. The court must give such notice, gist and opportunity to be heard as safety permits.
3. A return hearing must occur as soon as practicable and ordinarily within seventy-two hours.

72 Protected material procedure

1. Rules of court may provide for closed material and special advocates where necessary in the interests of national security and consistent with a fair hearing.
2. The court must give open reasons to the greatest extent possible.
3. Protected procedure may not be created by executive direction.

73 Powers of court

The court may confirm, continue, narrow, substitute, discharge, correct, order deletion or return, award compensation and costs, and refer apparent offence or misconduct.

74 Automatic expiry

1. Every emergency measure expires automatically unless confirmation or renewal is signed and entered in MOSAIC before expiry.
2. System failure does not extend authority.
3. The Authority must notify recipient and affected person of expiry so far as lawful and practicable.

75 Review and appeal

1. A person named, directed, restrained or materially affected may apply for review.
2. A provider may challenge jurisdiction, burden, conflict of law and compensation.
3. Appeals lie on a point of law with permission.
4. The Commissioner may refer systemic unlawfulness without displacing an affected person’s rights.

76 Remedies

1. Remedy may include declaration, discharge, correction, deletion, return, compensation, costs and notification to partners.
2. Wrongful public attribution must be corrected with prominence reasonably equivalent to the original.
3. National security does not by itself exclude compensation, but the court may protect the calculation and source of evidence.

77 Victim support

1. The Authority must maintain assistance for restoration, legal process, notification and recovery.
2. Support does not depend upon final attribution.
3. Regulations may provide for recovery from confiscated assets consistently with existing proceeds legislation and third-party rights.

78 Commissioner’s reports

1. The Commissioner must report annually upon use, time, lapse, refusal, error, correction, protected categories, international requests, autonomous incidents, civilian effect, compensation and referral.
2. A public report and classified annex must be laid before Parliament.
3. The Commissioner may issue a special report at any time.

79 Parliamentary reporting

1. The Secretary of State must publish annual aggregate data and a response to the Commissioner.
2. The Intelligence and Security Committee and relevant select committees must receive protected information necessary for their functions.
3. Permanent withholding of a critical incident’s existence requires annual ministerial certification and Commissioner review.

80 Independent statutory review and renewal

1. An independent reviewer must report after two years of substantive operation.
2. Part 4 expires five years after the commencement of that Part unless renewed, after the report under subsection (1), by affirmative regulations for a period not exceeding five years.
3. Part 7 expires five years after the commencement of that Part unless renewed by an Act of Parliament passed after the report under subsection (1).
4. Expiry does not invalidate completed lawful acts or continuing ordinary proceedings.

Part 9 — Offences, Regulations and General

81 Breach of confirmed order

A person who intentionally and without reasonable excuse contravenes section 44, provides a service which section 47 requires to be licensed without such a licence, or breaches a confirmed protective, manifest, licensing or court order commits an offence and is liable on conviction on indictment to imprisonment not exceeding seven years, a fine, or both, and on summary conviction to imprisonment not exceeding twelve months, a fine, or both.

82 Destruction and falsification

A person who intentionally destroys preserved evidence or a required manifest, fabricates material evidence, conceals material contrary information or supplies knowingly false manifest information commits an offence and is liable on conviction on indictment to imprisonment not exceeding ten years, a fine, or both, and on summary conviction to imprisonment not exceeding twelve months, a fine, or both.

83 Abuse of office under this Act

An official who knowingly uses a power under this Act for political, personal or commercial favour, or knowingly directs action upon fabricated evidence, commits an offence and is liable on conviction on indictment to imprisonment not exceeding ten years, a fine, or both, and on summary conviction to imprisonment not exceeding twelve months, a fine, or both.

84 Corporate liability

1. A body corporate or partnership is guilty of an offence under section 21, 81 or 82 where the offence is committed by a senior manager acting within the actual or apparent scope of the manager’s authority.
2. A relevant body is guilty of an offence where a person associated with it (“the associate”) commits an offence under section 81 or 82 intending to benefit, whether directly or indirectly, the relevant body or any person to whom, or to whose subsidiary undertaking, the associate provides services on behalf of the relevant body.
3. It is a defence under subsection (2) for the relevant body to prove that, when the offence was committed, it had reasonable procedures to prevent the conduct or that it was not reasonable in all the circumstances to expect such procedures.
4. “Senior manager”, “relevant body” and “associate” have the meanings given by sections 196 and 199 respectively of the Economic Crime and Corporate Transparency Act 2023, save that the condition that a relevant body be a large organisation does not apply.
5. No individual is guilty merely because the individual is employed within the chain.

85 Security researchers and whistleblowers

1. The Secretary of State must make regulations protecting good-faith, proportionate research and reporting conducted to prevent or disclose harm.
2. Protection does not extend to extortion, reckless harm, persistence beyond what is reasonably necessary to verify, or disclosure creating an unjustified danger.
3. Existing protected-disclosure law continues to apply.

86 Regulations

1. Regulations under this Act are made by statutory instrument.
2. Regulations creating an offence, compulsory class, intrusive power, protected function or material expansion are subject to affirmative procedure.
3. Technical and administrative regulations are subject to negative procedure unless this Act provides otherwise.
4. An urgent made-affirmative instrument may take effect immediately and lapses after seven days for a broad emergency restriction or twenty-eight days for a targeted regulation unless approved; and for this purpose a broad emergency restriction is one applying generally to a class of person, service or activity, and a targeted regulation is one applying only to a person, system or service identified in the instrument.

87 Consequential coordination

1. Regulations may amend references, routing and terminology in subordinate legislation to coordinate this Act with later cyber-resilience legislation.
2. Regulations under subsection (1) may not create or enlarge an emergency power, offence, use-of-force authority or class of protected material.

88 Financial provision

Parliament is to provide money for the Authority, Commissioner, court readiness, provider compensation, victim support, international nodes, exercises and secure infrastructure.

89 Crown application

1. This Act binds the Crown.
2. Criminal proceedings against the Crown are excluded, but declaratory, injunctive and compensation relief remains available as provided by law.
3. Crown servants remain individually liable for offences.

90 Territorial extent

1. This Act extends to England and Wales, Scotland and Northern Ireland.
2. The provisions concerning United Kingdom persons and designated British-controlled capacity apply outside the United Kingdom to the extent stated.
3. An Order in Council may extend appropriate provisions to a Crown Dependency or Overseas Territory with its consent and modifications.

91 Commencement

1. Sections 1–16, 78–80 and 86–93 commence on Royal Assent.
2. Other provisions commence by regulations after the Secretary of State has certified readiness of the relevant court, code, secure service and duty arrangements.
3. Sections 30, 34, 47 and Part 7 may not commence before approval of their governing codes.

92 Transitional provision

Regulations may provide for existing reports, licences, designations and proceedings to be treated as complying where equivalent safeguards and information exist, but may not retrospectively criminalise conduct.

93 Short title

This Act may be cited as the Economic Warfare Prevention and Response Act 2027.

Schedule 1 — Protected Functions

The protected functions are—

1. health and social care, including clinical records, diagnostics, blood, pharmacy, dispatch and medical devices;
2. drinking water, wastewater, flood control and environmental safety;
3. energy generation, transmission, distribution, fuel, heat and safety systems;
4. transport, traffic management, ports, aviation, rail, road and maritime navigation;
5. communications, cloud, data centres, managed services, identity, domain name, positioning and time;
6. finance, payment, insurance, clearing, settlement and systemic market infrastructure;
7. food, medicines, strategic materials and designated supply chains;
8. government, Parliament, elections, courts, emergency services and public administration;
9. defence, intelligence, research, space, compute and technology designated as strategically important; and
10. a function added by regulations under section 4(1).

Schedule 2 — Harm and Attribution Record

Part 1 — Harm

The record must state—

1. actual harm;
2. maximum reasonably credible foreseeable harm;
3. technical access and reach;
4. capability, autonomy, persistence and replication;
5. population, season, dependency and recovery;
6. contrary explanation and deception risk;
7. confidence and source class;
8. expected harm of each response; and
9. the fact which would materially change the assessment.

Part 2 — Attribution

The record must distinguish—

1. campaign linkage;
2. infrastructure and account control;
3. operator and integrator identity;
4. financing, benefit and prime contract;
5. State-organ status or governmental authority;
6. instruction, direction, control, acknowledgement or adoption;
7. territorial-State knowledge, capacity and omission;
8. evidential standard for the proposed decision;
9. material dissent; and
10. correction and recipient propagation.

Schedule 3 — Defensive Action Certificate

The certificate under section 63 must state—

1. the armed attack and whether actual or imminent;
2. the person or State against which defence is directed and confidence;
3. the Charter basis and request for collective self-defence, if any;
4. the defensive objective;
5. why non-forcible alternatives cannot achieve it in time;
6. each target’s status and current hostile function;
7. for an object in armed conflict, each limb of the military-objective test;
8. expected direct and incidental effects, protected services and shared infrastructure;
9. territorial-State consent, responsibility, inability or unwillingness and notice;
10. mission limit, reassessment interval and termination condition;
11. the advice of the Attorney General and Chief of the Defence Staff;
12. material dissent, uncertainty and deception analysis;
13. the live-target verification route; and
14. the time and method of parliamentary and Security Council notification.

Schedule 4 — Authority and Commissioner

1. The chair and non-executive members of the Authority are appointed by the Secretary of State following fair and open competition and a pre-appointment hearing for the chair.
2. Operational members must include expertise in public law, international law, cyber security, critical infrastructure, intelligence assessment, privacy, human rights, finance and devolved administration.
3. The Authority must maintain accounts audited by the Comptroller and Auditor General.
4. The Authority may employ staff, enter agreements, procure secure services and establish accredited foreign nodes within appropriated funds.

5. The Commissioner appoints staff independently and controls the Commissioner's investigative programme.

6. Neither the Authority nor Commissioner may receive direction as to the conclusion of an individual review, attribution or judicial referral, save that lawful ministerial direction may set the Government's response objective.

Bibliography

Books, Chapters and Articles

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

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

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

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

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

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

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

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

Dyzenhaus D, *The Constitution of Law: Legality in a Time of Emergency* (CUP 2006)

Eichensehr KE, 'Digital Switzerlands' (2019) 167 University of Pennsylvania Law Review 665

Farrell H and Newman AL, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44 International Security 42

Ferejohn J and Pasquino P, 'The Law of the Exception: A Typology of Emergency Powers' (2004) 2 International Journal of Constitutional Law 210

Fikfak V and Hooper HJ, *Parliament's Secret War* (Hart 2018)

Greenwood C, 'International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida, and Iraq' (2003) 4 *San Diego International Law Journal* 7

Gross O and Ní Aoláin F, *Law in Times of Crisis: Emergency Powers in Theory and Practice* (CUP 2006)

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

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

Joseph R, *The War Prerogative: History, Reform, and Constitutional Design* (OUP 2013)

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

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

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

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

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

Tomkins A, 'Justice and Security in the United Kingdom' (2014) 47 Israel Law Review 305

Walker C and Broderick J, *The Civil Contingencies Act 2004: Risk, Resilience and the Law in the United Kingdom* (OUP 2006)

Wentker A, 'The Armed Attack Exception to Neutrality in International Peace and Security Law' (2024) 73 *International and Comparative Law Quarterly* 963

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