The need for the legal regulation of economic warfare conducted by individual and State actors

Economic Warfare: The Unregulated War

Christopher I. V. Farmer

Originally submitted as an LL.M dissertation at the University of Worcester on 31 January 2024
Revised and expanded for publication, August 2026

Contents

This edition preserves the argument, voice and deliberate sentence architecture of the dissertation submitted on 31 January 2024. Legal authorities, citations, tables and factual propositions have been reverified and revised in accordance with OSCOLA fifth edition. Material first available after submission is marked where its chronology bears upon the argument; it is not presented as if it formed part of the deposited dissertation.

Abstract

Economic warfare is no longer the preserve of states. Rising individual wealth and widely available technology have put its means within reach of ultra-wealthy individuals, multinational corporations, private military and security companies and non-state actors, and have left the developed North, which has most to lose, correspondingly exposed. United Kingdom law addresses the resulting conduct only in fragments. This dissertation argues that those fragments should be consolidated into a single statute, and sets out what it would have to contain.

It begins with definition, distinguishing economic warfare from warfare as conventionally understood and identifying the actors the existing categories fail to reach. PMSCs are the clearest case: Additional Protocol I to the Geneva Conventions and the United Nations Mercenary Convention define mercenaries too narrowly to capture how such companies now operate. Case studies of the extractive industry in the Democratic Republic of Congo, the oil industry in Nigeria and the arms trade in Yemen supply the evidence.

It then tests the instruments presently doing the work—principally the Sanctions and Anti-Money Laundering Act 2018 and the United States' Sergei Magnitsky Act, with its United Kingdom and European Union analogues—and finds each drawn for a narrower problem than the one it faces, with jurisdictional reach the recurring weakness. Cyber-economic aggression falls between them; indirect perpetrators and funding sources fall outside them.

The dissertation proposes the UK Economic Warfare Prevention and Response Act: mandatory incident reporting within defined time frames, a centralised cyber-incident database, penalties for non-compliance, support, public education and provision for international collaboration. It also supplies a rapid decision structure for pre-emptive measures and, where international law independently permits it, military action. The classification problem is now live rather than hypothetical: the United Nations Security Council has held its first formal public meeting devoted to cybersecurity as a matter of international peace and security, and published State positions recognise that a cyber operation may, according to its scale and effects, constitute a use of force or an armed attack.

It closes against its own proposal, setting out where broad definitions, jurisdictional complexity, procedural safeguards and the pace of technological change would strain it.

Keywords

Economic warfare; cyber operations; private military and security companies; multinational corporations; non-state actors; sanctions; supply-chain due diligence; critical national infrastructure; attribution; use of force.

Table of Cases

United Kingdom

International Courts and Tribunals

African Commission on Human and Peoples' Rights

Netherlands

United States

Table of Legislation

United Kingdom Primary Legislation

United Kingdom Statutory Instruments

United Kingdom Bills

United States and Other Legislation

European Union Legislation

Table of Treaties and International Instruments

Table of Official and Technical Materials

United Kingdom

British Army, *Army Leadership Doctrine* (2021)

Department for Science, Innovation and Technology, ‘Incident Reporting’ (Cyber Security and Resilience (Network and Information Systems) Bill factsheet, updated 30 June 2026)

Electoral Commission, ‘Public Notification of Cyber-Attack on Electoral Commission Systems’ (8 August 2023)

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

Foreign, Commonwealth & Development Office and others, ‘UK Holds China State-Affiliated Organisations and Individuals Responsible for Malicious Cyber Activity’ (25 March 2024)

HM Government, *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World* (CP 811, 2023)

Home Office, ‘Gary McKinnon Extradition Case: Home Secretary’s Statement’ (16 October 2012)

House of Lords Constitution Committee, *Sanctions and Anti-Money Laundering Bill [HL]* (8th Report of Session 2017–19, HL Paper 39)

Information Commissioner’s Office, ‘ICO Reprimands the Electoral Commission after Cyber Attack Compromises Servers’ (30 July 2024)

Ministry of Defence, *A Soldier’s Guide to the Law of Armed Conflict* (2001)

Ministry of Defence, *The Manual of the Law of Armed Conflict* (JSP 383, OUP 2004)

National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (HC 414, Session 2017–19, 27 October 2017)

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

National Cyber Security Centre, ‘UK Calls Out China State-Affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians’ (25 March 2024)

Office for Nuclear Regulation, ‘Guardian News Article’ (4 December 2023)

Office for Nuclear Regulation, ‘Sellafield Ltd Fined £332,500 for Cyber Security Shortfalls’ (2 October 2024)

Office of Financial Sanctions Implementation, *UK Financial Sanctions: General Guidance* (HM Treasury, updated 12 May 2026)

Secretary of State for International Trade, ‘Trade Update’ (Written Statement HCWS339, 7 July 2020)

Sellafield Ltd, ‘Response to a News Report on Cyber Security at Sellafield’ (4 December 2023)

UK Parliament, ‘Cyber Security and Resilience (Network and Information Systems) Bill’ (Bill 4035)

United Kingdom Parliamentary Debates

HC Deb 16 October 2012, vol 551, cols 166–68

HC Deb 13 July 2020, vol 678, cols 1250–68

HL Deb 15 January 2018, vol 788, cols 492–93

International and Regional Materials

Council of the European Union Analysis and Research Team, *The Business of War: Growing Risks from Private Military Companies* (31 August 2023)

Court of Appeal of The Hague, 'Shell Nigeria Liable for Oil Spills in Nigeria' (29 January 2021)

European Commission, 'Report on the Functioning and Effectiveness of Regulation (EU) 2017/821' COM (2024) 415 final, 24 September 2024

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

ICRC, 'International Humanitarian Law and Private Military/Security Companies: FAQ' (10 December 2013)

ICRC, 'What Are *Jus ad Bellum* and *Jus in Bello*?' (22 January 2015)

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

ICRC, 'Cyber Operations and International Humanitarian Law' (29 November 2022)

OECD, *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas* (3rd edn, OECD Publishing 2016)

Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (HR/PUB/11/04, 2011)

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

United Nations Environment Programme, *Environmental Assessment of Ogoniland* (UNEP 2011)

United Nations Treaty Collection, 'International Convention against the Recruitment, Use, Financing and Training of Mercenaries: Status as at 31 July 2026'

UNSC, 'Final Report of the Panel of Experts on the Illegal Exploitation of Natural Resources and Other Forms of Wealth of the Democratic Republic of the Congo' (16 October 2002) UN Doc S/2002/1146

UNSC Res 1457 (24 January 2003) UN Doc S/RES/1457

UNSC, 'Final Report of the Panel of Experts on the Illegal Exploitation of Natural Resources and Other Forms of Wealth of the Democratic Republic of the Congo' (23 October 2003) UN Doc S/2003/1027

UNSC, 'Letter dated 8 June 2021 from the Permanent Representative of Estonia to the United Nations addressed to the Secretary-General' UN Doc S/2021/540

UNSC, ‘Maintenance of International Peace and Security: Cybersecurity’ (29 June 2021) UN Doc S/2021/621

United States

Commission on Security and Cooperation in Europe, *The Magnitsky Act at Five Years: Assessing Accomplishments and Challenges* (Hearing, 14 December 2017)

FBI, ‘FBI Statement on JBS Cyberattack’ (2 June 2021)

US Department of Justice, ‘Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns’ (5 March 2025)

US Department of State, ‘Promoting Accountability for Human Rights Abuse with Our Partners’ (22 March 2021)

US Department of the Treasury, ‘Treasury Targets Individuals Involved in the Sergei Magnitsky Case and Other Gross Violations of Human Rights in Russia’ (20 December 2017)

US Department of the Treasury, ‘Treasury Expands and Intensifies Sanctions against Russia’ (24 February 2023)

US House of Representatives Committee on Homeland Security, *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security* (Hearing 110-52, 20 June 2007)

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* (Inspection Report E-121-25-003-M, 11 August 2025)

Corporate and Technical Primary Materials

International Organization for Standardization, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary* (ISO/IEC 27000:2018, 5th edn, 2018)

JBS USA, ‘JBS USA Cyberattack Media Statement’ (9 June 2021)

1. Introduction

1.1 Objective

This dissertation aims to establish the necessity of a comprehensive legal framework specifically addressing economic warfare. It advocates amendment of international law, or domestic legislation capable of shaping future internationally recognised laws and directives.[1] The examination of British legislation, particularly the Sanctions and Anti-Money Laundering Act 2018 (SAMLA 2018),[2] supplies one precedent for legislating against emerging threats. Similarly, the United States' Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012 (the Sergei Magnitsky Act)[3] provides an example of how internal policy may be adopted, adapted and internationalised.[4]

This paper posits that developments in cyber warfare are instrumental in understanding the need for specific legislation against economic warfare. On 29 June 2021 the United Nations Security Council held its first formal public meeting devoted to cybersecurity as a matter of international peace and security; it did not enact a rule equating cyber operations with warfare, but the meeting placed the classification and attribution of operations capable of producing grave cross-border effects upon the Council's express agenda.[5] Published State positions have since made the legal point more precise: depending upon their scale and effects, cyber operations may cross the thresholds of prohibited force and armed attack.[6] The complexity of curtailing such acts underscores the need for a similar focus on economic warfare. Without it, indirect, third-party warfare, in which primary instigators operate within legal ambiguities, is likely to continue.[7]

This dissertation will examine elements not sufficiently included or addressed in international instruments, aiming to present a cogent argument for their analysis and enhancement. Particular attention will be paid to the actions and potential actions of both State and individual actors who conduct warfare within a legally ambiguous context.

1.2 Defining the Legal Difference between Warfare and Economic Warfare

The evolution of warfare from physical combat to sophisticated forms of conflict, like cyber and economic warfare, has witnessed a parallel evolution in international law.[8] While international law traditionally regulated physical conflicts by establishing rules to prevent unnecessary human suffering,[9] the advent of economic warfare has raised pertinent questions about the applicability and adequacy of

[1] Alan Boyle and Christine Chinkin, *The Making of International Law* (OUP 2007).

[2] Sanctions and Anti-Money Laundering Act 2018.

[3] Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012, Pub L No 112–208, title IV, 126 Stat 1496, 1502–06.

[4] Martin Russell, *Global Human Rights Sanctions* (European Parliamentary Research Service, PE 698.791, 2021) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698791/EPRS_BRI(2021)698791_EN.pdf accessed 31 July 2026.

[5] UNSC, 'Letter dated 8 June 2021 from the Permanent Representative of Estonia to the United Nations addressed to the Secretary-General' UN Doc S/2021/540; UNSC, 'Maintenance of International Peace and Security: Cybersecurity' (29 June 2021) UN Doc S/2021/621.

[6] 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.

[7] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014).

[8] National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (HC 414, Session 2017–19, 27 October 2017).

[9] Geneva Conventions of 12 August 1949, 75 UNTS 31, 85, 135 and 287; Geneva Conventions Act 1957.

existing laws.[10] This section aims to dissect the legal differences between traditional warfare and economic warfare, exploring how these distinctions vary based on the actor involved.

The case of Fraser, Trenholm & Co during the American Civil War serves as a pivotal moment in the historical development of economic warfare. The Liverpool commercial house acted as banker to the Confederate Government and financed the purchase of arms against consignments of cotton; its activities, and the litigation concerning blockade-running cargo in *The Bermuda*, materially influenced the intersection of warfare, commerce and neutrality.[11] Its involvement challenged the conventional separation between warfare and economic warfare, the boundaries of neutrality, and the extent to which economic assistance to one side could be considered participation in war.

While traditional warfare is characterised by the use of military force to achieve objectives, economic warfare employs economic strategies to exert influence or pressure. Economic warfare allows actors to engage in conflict through economic means, often obscured behind the façade of economic activities. Private military contractors, operating outside conventional state mechanisms and devoid of the stigma associated with mercenaries, have further complicated these distinctions.[12] This section will offer an in-depth analysis of the legal definitions, characteristics, and implications of both warfare types, underscoring their fundamental differences within international law and identifying legal loopholes currently exploited.

1.3 Definition and Characteristics of Warfare

Warfare, or traditional armed conflict, entails open hostilities between states or organised armed groups, involving the deployment of military forces and conventional weaponry. These conflicts are often driven by political, territorial, or ideological objectives. Key aspects of warfare include direct military engagement, physical violence, and the potential for substantial loss of life and property damage. The legal foundations of warfare are rooted in principles such as jus ad bellum and jus in bello,[13] as established in customary international law[14] and formalised in treaties like the Geneva Conventions[15] and the Hague Conventions.[16] These principles are designed to uphold humanitarian standards and ensure the protection of both civilians and combatants.[17]

This legal framework, entrenched in both treaty and customary international law, is significantly shaped by the United Nations Charter.[18] It regulates state use of force, permitting military action primarily for self-defence[19] or when authorised by the UN Security Council. The principles of jus in bello,[20] vital to international humanitarian law and detailed in the Geneva Conventions,[21] govern the conduct of armed conflict. They stipulate key concepts such as distinction, proportionality, and precautionary measures,

[10] Nils Ole Oermann and Hans-Jürgen Wolff, *Trade Wars: Past and Present* (OUP 2022).

[11] *The Bermuda* 70 US (3 Wall) 514 (1865).

[12] Council of the European Union Analysis and Research Team, *The Business of War: Growing Risks from Private Military Companies* (31 August 2023) https://www.consilium.europa.eu/media/66700/private-military-companies-final-31-august.pdf accessed 31 July 2026.

[13] ICRC, 'What Are *Jus ad Bellum* and *Jus in Bello*?' (22 January 2015) https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 accessed 31 July 2026.

[14] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law, vol I: Rules* (CUP 2005).

[15] Geneva Conventions of 12 August 1949 (n 9).

[16] Hague Convention (IV) Respecting the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 205 CTS 277.

[17] 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 35, 48, 51 and 57.

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

[19] Charter of the United Nations (n 18) art 51; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) (Judgment) [1986] ICJ Rep 14 [176].

[20] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, CUP 2010).

[21] Geneva Conventions of 12 August 1949 (n 9).

aiming to protect civilians and reduce human suffering. Violations of these principles can lead to international criminal liability and sanctions.[22]

In the context of UK law, these principles shape domestic policies concerning warfare. The Geneva Conventions Act 1957, subsequently amended, incorporates specified international obligations into British law and criminalises grave breaches of the Conventions and Additional Protocol I.[23] The Act exemplifies the UK's commitment to adhering to international standards in warfare.[24] Moreover, the United Kingdom's Joint Service Manual of the Law of Armed Conflict,[25] drawing upon international humanitarian law (IHL),[26] customary international law and relevant treaties, guides UK military engagements.[27] This body of law emphasises the distinction between combatants and civilians and requires proportionality and precautions in attack to minimise civilian harm.

The UK's rules of engagement (ROE),[28] reflecting the principles of jus ad bellum and jus in bello, provide operational guidelines for its armed forces. ROE ensure that the use of force in military operations is legally justified and ethically sound, demonstrating the UK's dedication to lawful conduct in warfare and its role in upholding global humanitarian standards.

Modern warfare encompasses a range of strategic, psychological, and informational elements. Command structures in military operations are characterised by complex hierarchies[29] and rules of engagement that maintain discipline and adherence to legal standards.

Psychological operations aim to impact enemy morale and decision-making, while informational warfare employs propaganda and cyber tactics. These aspects are crucial in modern conflicts, where control over information and psychological dominance can be as decisive as physical combat.[30]

Operational tactics in warfare[31] have evolved to include the use of specialised units and methods, such as special forces, guerrilla tactics,[32] and aerial bombardment—each with distinct legal implications. The advent of advanced technologies, like precision-guided munitions and drones, has transformed warfare dynamics, necessitating careful legal and ethical scrutiny under the principles of necessity and humanity.

Cyber warfare has emerged as a pivotal component of modern warfare. It entails digital attacks on a nation's information systems to disrupt critical infrastructure or gather intelligence. Such tactics, while not involving direct physical violence, can have debilitating effects on a nation's security and economy.[33] Psychological warfare, another key aspect, employs methods like propaganda and disinformation to influence public perception and morale. Additionally, economic warfare tactics,

[22] Protocol I (n 17) arts 48, 51 and 57; Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3, art 8.

[23] Geneva Conventions Act 1957, ss 1 and 1A.

[24] Andrew Clapham and Paola Gaeta (eds), *The Oxford Handbook of International Law in Armed Conflict* (OUP 2014).

[25] Ministry of Defence, *The Manual of the Law of Armed Conflict* (JSP 383, OUP 2004) https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf accessed 31 July 2026.

[26] Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.

[27] Ministry of Defence (n 25) paras 2.1–2.8, 5.22–5.36.

[28] Ministry of Defence, *A Soldier's Guide to the Law of Armed Conflict* (2001); Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (2nd edn, CUP 2016).

[29] British Army, *Army Leadership Doctrine* (2021) https://www.army.mod.uk/learn-and-explore/army-leadership-doctrine/ accessed 31 July 2026.

[30] Tilman Rodenhäuser, 'The Legal Boundaries of (Digital) Information or Psychological Operations under International Humanitarian Law' (2023) 100 *International Law Studies* 536.

[31] Benjamin Sutherland (ed), *Modern Warfare, Intelligence and Deterrence: The Technologies that Are Transforming Them* (Profile Books 2011).

[32] Charles R King, 'Revolutionary War, Guerrilla Warfare, and International Law' (1972) 4 *Case Western Reserve Journal of International Law* 91.

[33] Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015).

including sanctions, trade embargoes, and financial restrictions, aim to weaken an adversary's economy.[34] These diverse tactics, while not always fitting the traditional legal definition of warfare, play a critical role in modern strategic operations and significantly impact the outcomes of conflicts.

Economic warfare involves state or, at times, non-state actors employing economic tactics to debilitate an adversary's economy without direct military engagement. These tactics can range from economic sanctions and trade embargoes to asset freezes and other measures impacting the economic and financial stability of the targeted state.[35] The legal framework governing economic warfare is less clearly defined than that of traditional warfare, leading to ongoing debates about its legality and legitimacy.[36]

Economic warfare, characterised by its non-kinetic approach, hinges on economic leverage rather than physical force.[37] Its legality is shaped by different principles than those governing traditional warfare, with concepts of sovereignty, non-intervention, and non-interference in internal affairs playing pivotal roles in legal assessments.[38]

Complexity arises when using economic means to indirectly facilitate acts of cyber and traditional warfare. This often involves leveraging economic resources, incentives, or pressures to compel or persuade other entities to engage in cyber and traditional warfare tactics.[39] This method of engagement in warfare, while not direct, exploits the existing gaps in international law and treaty coverage.

For instance, a state or a non-state actor with substantial financial resources may invest in or provide funding to third-party groups, private military companies, or hackers.[40] This funding could be used to support cyber-attacks on rival states or entities, disrupting their critical infrastructure, stealing sensitive information, or spreading disinformation. Similarly, financial backing could be used to sponsor paramilitary groups or mercenaries[41] to conduct conventional warfare activities such as sabotage, guerrilla warfare, or direct military engagement against an adversary. These actions, while carried out by separate entities, are fuelled by the economic support and direction of the instigating actor.[42]

This form of indirect warfare is challenging to address under current international legal frameworks. The economic instigator, by maintaining a degree of separation from the actual execution of hostile activities, can operate within a realm of legal ambiguity. Current international laws and treaties focus on direct acts of aggression and have yet to catch up with the nuances of indirect, economically facilitated warfare strategies. Without specific legal provisions regarding the indirect facilitation of warfare through economic means, actors may exploit these loopholes, engaging in hostile activities while circumventing traditional legal definitions and responsibilities.

---

[34] David Nutt, 'Economic Sanctions Evolved into Tool of Modern War' *Cornell Chronicle* (11 January 2022) https://news.cornell.edu/stories/2022/01/economic-sanctions-evolved-tool-modern-war accessed 31 July 2026.

[35] Executive Order 8832, 6 Fed Reg 3825 (26 July 1941); Joy Gordon, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2010).

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

[37] Cheng Hang Teo, *The Acme of Skill: Nonkinetic Warfare* (Wright Flyer Paper No 30, Air University Press 2008).

[38] Tor Egil Førland, 'The History of Economic Warfare: International Law, Effectiveness, Strategies' (1993) 30 *Journal of Peace Research* 151.

[39] Roscini (n 7).

[40] Roscini (n 7) 17.

[41] Vladyslav Lanovoy, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 *European Journal of International Law* 563.

[42] Rodenhäuser (n 30) 543–49.

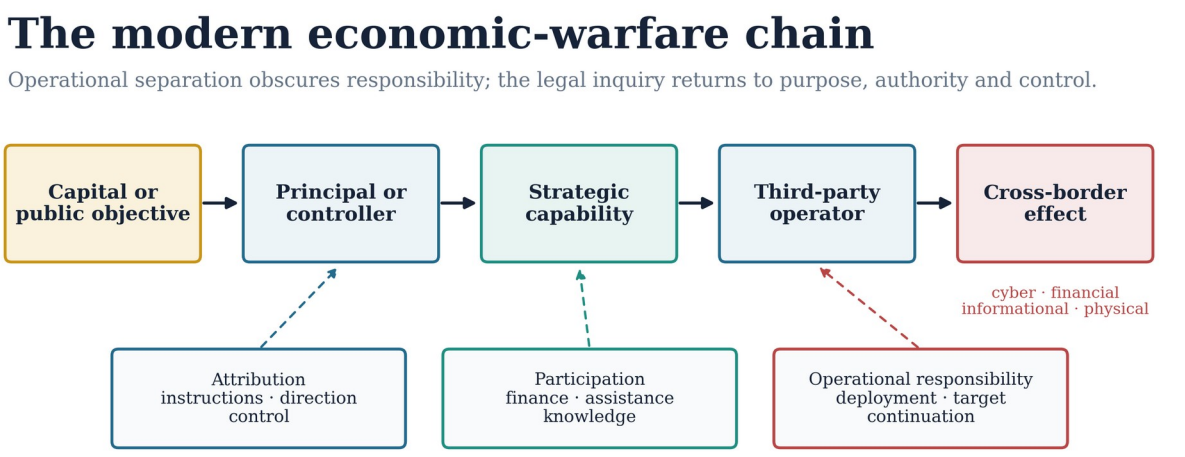

Figure 1. The modern economic-warfare chain: capital or public objective passes through a controller, strategic capability and third-party operator before producing cyber, financial, informational or physical effects. The diagram distinguishes those functions from the legal routes by which responsibility may return to the principal.

Legal ambiguity is further compounded by the difficulty in tracing and proving the source of economic support for such activities. Financial transactions can be obfuscated through complex networks, making it challenging to establish a direct link between the funding source and the warfare activities. Moreover, the international legal system's focus on state actors in warfare means non-state actors engaging in these tactics often remain beyond the scope of current legal frameworks.

In conclusion, the use of economic means to indirectly facilitate cyber and traditional warfare represents a sophisticated strategy that exploits the gaps in international law. This approach allows actors to engage in warfare by proxy, remaining legally ambiguous and often unaccountable under current international statutes.[43] Addressing this growing challenge requires an expansion and adaptation of international legal frameworks to encompass and regulate these indirect, economically driven forms of warfare.[44]

1.4 PMSCs and Their Utilisation

Third-party warfare is evident in the growing use of private military and security companies (PMSCs). PMSCs often operate in a legal grey area, raising concerns about accountability, human rights abuses, and circumvention of international humanitarian law.[45] This section explores the legal ambiguities surrounding the use of PMSCs and how states and non-state actors exploit these ambiguities.[46]

The four Geneva Conventions of 1949 set standards for humane conduct in armed conflict. Article 47 of Additional Protocol I does not prohibit mercenaries: it provides that a person satisfying each limb of its cumulative definition has no right to combatant or prisoner-of-war status.[47] The narrowness and

[43] Graham Cronogue, 'Rebels, Negligent Support, and State Accountability: Holding States Accountable for the Human Rights Violations of Non-State Actors' (2013) 23 *Duke Journal of Comparative & International Law* 365.

[44] Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817.

[45] Lou Pingeot, *Dangerous Partnership: Private Military and Security Companies and the UN* (Global Policy Forum and Rosa Luxemburg Stiftung 2012).

[46] Amy E Eckert, *Outsourcing War: The Just War Tradition in the Age of Military Privatization* (Cornell University Press 2016).

[47] Protocol I (n 17) art 47.

cumulative character of that definition exclude many private actors whose contemporary functions are nevertheless capable of affecting hostilities.

The United Nations Mercenary Convention, adopted in 1989, goes further by requiring its States Parties to prohibit the recruitment, use, financing and training of mercenaries.[48] Its practical reach remains limited, however, because several States materially connected with the supply or use of private force—including the United Kingdom—are not parties.[49] As at the publication revision, the Convention had thirty-eight parties; absence from it does not remove obligations arising under IHL, human-rights law, international criminal law or domestic law, but it deprives the mercenary-specific prohibition of the universality which its purpose would require.[50]

Additional Protocol I and the United Nations Mercenary Convention address mercenaries but employ definitions that do not encompass all private actors. PMSCs, offering services from logistics and intelligence to armed protection and combat support, frequently fall outside those definitions. It would, however, be inaccurate to describe them as inhabiting a complete regulatory vacuum: according to function and facts, their personnel may be members of a State's armed forces, members of an organised armed group, or civilians who lose protection against direct attack for such time as they directly participate in hostilities; ordinary rules of State attribution, superior responsibility, individual criminal liability, contract and domestic criminal law may also apply.[51] The defect is not the absence of every rule, but the fragmentation of rules, jurisdictions and evidential routes by which responsibility must be proved.

Circumventing International Obligations: States may use PMSCs to create distance between public authority and acts which the State could not lawfully undertake itself.[52] Outsourcing cannot make the deliberate targeting of civilians lawful, nor does a contract extinguish attribution where the company exercises governmental authority, acts under State instructions or direction or control, or is subsequently acknowledged and adopted by the State.[53] It may nevertheless obscure the facts necessary to establish those tests, delay proof beyond the period in which prevention was possible, and permit the hiring State to deny what it has intentionally made difficult to see.

Plausible Deniability: Employing PMSCs provides States with a practical, though not necessarily legal, means of denying responsibility for conduct that may violate international law. If a PMSC commits human-rights abuses, the hiring State may claim that the conduct was private and unauthorised; the legal enquiry then depends upon status, delegated authority, instructions, direction or control, complicity, due diligence and the facts which survive the contractual chain.

Avoiding Legal Accountability: The varied legal status of PMSCs and their employees complicates efforts to hold them accountable. Their classification is not inherently unclear—status follows the applicable legal tests—but the answer may change between personnel, operations and times, whilst the territorial State, home State, contracting State and State of nationality may each possess only part of the evidence or jurisdiction.[54]

---

[48] International Convention against the Recruitment, Use, Financing and Training of Mercenaries (adopted 4 December 1989, entered into force 20 October 2001) 2163 UNTS 75, arts 1–5.

[49] United Nations Treaty Collection, 'International Convention against the Recruitment, Use, Financing and Training of Mercenaries: Status as at 31 July 2026' https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-6&chapter=18 accessed 31 July 2026.

[50] United Nations Treaty Collection (n 49).

[51] ICRC, 'International Humanitarian Law and Private Military/Security Companies: FAQ' (10 December 2013) https://www.icrc.org/en/document/ihl-and-private-military-security-companies-faq accessed 31 July 2026.

[52] Wojciech Pałka, *The Awakening of Private Military Companies* (Warsaw Institute 2020); Eckert (n 46).

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

[54] Coalition Provisional Authority Order No 17 (Revised), *Status of the Coalition Provisional Authority, MNF–Iraq, Certain Missions and Personnel in Iraq* (27 June 2004).

In conclusion, the rise of PMSCs in warfare highlights the need to address the ambiguity in their legal status. The absence of a unified regulatory framework allows actors to circumvent international law, maintain plausible deniability, and avoid legal accountability.[55] Addressing these issues requires re-evaluation and development of comprehensive legal frameworks that recognise the evolving nature of modern warfare and the role of private actors.

1.5 The Individual and the State

When contrasting the actions of states with those of individuals or non-state actors, significant differences emerge. States hold specific rights and obligations under international law, in both warfare and economic-warfare contexts. They have the sovereign right to use force in self-defence, as outlined in Article 51 of the UN Charter, subject to necessity and proportionality constraints.[56] This right is confined to situations of armed attack, with an obligation to report such actions to the UN Security Council. Further, states are bound by international conventions like the Chemical Weapons Convention[57] and the UN Charter, which set specific restrictions on warfare conduct. Traditional economic actions, for example sanctions, taken by states also fall under legal scrutiny, requiring adherence to treaty obligations and customary international law.

These frameworks often do not extend to non-state actors in the same way, leading to a disparity in legal accountability and enforcement. A non-State actor is not a treaty party in the same manner as a State; that distinction does not, however, confer impunity. Individuals who employ chemical weapons may incur domestic criminal liability and, where the necessary contextual and jurisdictional elements are proved, international criminal responsibility.[58] Moreover, non-state entities, including guerrilla groups and terrorist organisations, may employ tactics that are strictly prohibited for States. Such actions, while equally destructive, frequently expose the weakness of enforcement and attribution rather than an absence of applicable law.

It is not to say that there are no international laws dealing directly with individuals, but these laws are often difficult to enforce. Individuals perpetrating war crimes may be criminally accountable under international criminal law,[59] as evidenced by prosecutions before the International Criminal Court and other tribunals. A publication-only update supplies a later and concrete illustration: on 6 October 2025, after submission, Trial Chamber I convicted Abd-Al-Rahman of twenty-seven counts of crimes against humanity and war crimes committed in Darfur.[60] The ICC may prosecute natural persons for genocide, crimes against humanity, war crimes and aggression where the Rome Statute's jurisdictional and admissibility requirements are met.[61] Complementarity does not impose a free-standing universal obligation upon every State to prosecute every such crime; rather, it makes a case inadmissible where a State with jurisdiction is genuinely investigating or prosecuting it, subject to the Statute's terms.[62]

The legal standards differ markedly for individuals involved in foreign conflicts. These legal distinctions are crucial in maintaining a balance between individual accountability and state responsibility, ensuring adherence to international law, and protecting human rights during conflict.[63]

---

[55] Thomas Jäger and Gerhard Kümmel (eds), *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects* (VS Verlag 2007); Eckert (n 46).

[56] UN Charter (n 18) art 51; *Nicaragua* (n 19) [176].

[57] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (adopted 13 January 1993, entered into force 29 April 1997) 1974 UNTS 45, art I.

[58] Chemical Weapons Act 1996, ss 2–3; Rome Statute (n 22) arts 8(2)(b)(xviii) and 8(2)(e)(xiii).

[59] *Prosecutor v Taylor* (Appeal Judgment) SCSL-03-01-A-1389 (26 September 2013).

[60] *Prosecutor v Abd-Al-Rahman* (Trial Judgment) ICC-02/05-01/20-1240 (6 October 2025).

[61] Rome Statute (n 22) arts 5, 12, 13, 17 and 25.

[62] Rome Statute (n 22) art 17.

[63] Vaughan Lowe and Antonios Tzanakopoulos, 'Economic Warfare' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2012).

State support for foreign rebel groups can breach international non-intervention principles and infringe upon State sovereignty, whereas individual participation rarely attracts the same level of international scrutiny. Given the intricacies of international law enforcement, an individual might engage in acts prohibited to States without facing immediate legal consequence.

In the context of international law, individuals and non-state actors often find loopholes in legal enforcement, especially in areas of weak governance or conflict. Unlike states, they are not direct signatories to treaties like the Geneva Conventions and may not face immediate international legal consequences for actions such as using chemical weapons or engaging in proxy warfare. This leads to legal ambiguities and challenges in prosecuting individuals for acts that would be clear violations if perpetrated by states. Additionally, complexity in attributing specific actions to individuals in conflict zones and navigating international and domestic legal procedures exacerbates enforcement difficulties. Political and diplomatic factors, such as diplomatic immunity or political asylum, further complicate the legal pursuit of individuals. These scenarios highlight the need for a more comprehensive international law to effectively regulate the conduct of both states and individuals in armed conflicts, considering the evolving nature of modern warfare and the role of non-state actors.[64]

[64] Nickolas Bruetsch, 'Market for Force: The Emerging Role of Private Military and Security Companies in Non-Traditional Fields' (The Security Distillery, 10 April 2021) https://thesecuritydistillery.org/all-articles/market-for-force-the-emerging-role-of-private-military-and-security-companies-in-non-traditional-fields accessed 31 July 2026.

2. The Case of Multinational Corporations and Conflict

2.1 Introduction

Economic warfare has traditionally been associated with the actions of states. However, the increasing globalisation of the world economy and the rise of powerful multinational corporations (MNCs) have blurred the lines between state and non-state actors. MNCs often operate in conflict-affected regions, where they may indirectly fuel conflicts by doing business with armed groups or governments involved in human rights abuses. This chapter examines instances where MNCs have been accused of indirectly fuelling conflicts and argues for the need to regulate economic warfare by non-state actors.

2.2 Case Studies

2.2.1 The Extractive Industry in the Democratic Republic of Congo

The DRC is rich in natural resources, including coltan, gold, diamonds, tin and tungsten; its misfortune has been that the value of those resources has repeatedly supplied both a reason and a means for violence. The proposition must, nevertheless, be drawn with care. It is not that every foreign purchaser of Congolese mineral is a belligerent, nor that a long supply chain turns every remote buyer into an accomplice. It is that commerce ceases to be politically neutral when payment, taxation, transport or protection sustains the armed control from which the commodity is obtained, and that ordinary corporate law, concerned principally with the company immediately party to the transaction, has been ill-suited to the distance deliberately placed between the final purchaser and the coercion which made its purchase possible.

The United Nations Panel of Experts' report of 16 October 2002 supplied the original public evidential foundation. It described the illegal exploitation of the DRC's natural resources as systematic, identified elite networks composed of political, military and commercial interests, and annexed lists of businesses which, in the Panel's assessment, had acted inconsistently with the OECD Guidelines for Multinational Enterprises.[65] Those were findings of an expert fact-finding body and not criminal convictions. A number of companies disputed the accusations, and the Panel's later process distinguished matters it regarded as resolved from those upon which further attention remained necessary.[66] That qualification is not an embarrassment to the argument, but part of it: a system capable only of making a politically grave accusation, inviting a private response and then leaving the consequence to dispersed national contact points possessed neither a common evidential procedure nor a proportionate ladder of legal response.

The Security Council did not treat the underlying phenomenon as conjecture. Resolution 1457 (2003) condemned the illegal exploitation of Congolese resources, stressed the link between exploitation and the continuation of conflict, urged States to investigate the Panel's findings by appropriate judicial means, and required further dialogue between the Panel, States, companies and the OECD machinery.[67] In *Armed Activities on the Territory of the Congo*, the International Court of Justice subsequently held Uganda internationally responsible for violations of the principle of non-use of force and non-intervention and, in occupied Ituri, for failing to prevent the looting, plundering and exploitation of Congolese natural resources; it also held Uganda responsible for the conduct of its armed forces in

[65] UNSC, 'Final Report of the Panel of Experts on the Illegal Exploitation of Natural Resources and Other Forms of Wealth of the Democratic Republic of the Congo' (16 October 2002) UN Doc S/2002/1146.

[66] UNSC, 'Final Report of the Panel of Experts on the Illegal Exploitation of Natural Resources and Other Forms of Wealth of the Democratic Republic of the Congo' (23 October 2003) UN Doc S/2003/1027, paras 15–25 and annex I.

[67] UNSC Res 1457 (24 January 2003) UN Doc S/RES/1457, paras 2–5, 9 and 12.

participating in such exploitation.[68] The judgment attached responsibility to a State upon the facts and rules before the Court. It did not establish a general international cause of action against every corporation in the supply chain, and therein lies the jurisdictional division which this dissertation seeks to expose: public international law may reach the occupying State, whilst the commercial actors and transactions through which value is converted into military endurance remain distributed among company, contract, customs and criminal laws.

The regulatory response has grown but has not closed that division. The OECD's five-step framework requires a company to establish management systems, identify and assess supply-chain risk, respond to that risk, obtain independent audit and report publicly; its third edition makes plain that the framework is capable of application to all minerals, but the Guidance remains voluntary and is not itself legally enforceable.[69] Regulation (EU) 2017/821 converted part of that method into binding duties for Union importers of tin, tantalum, tungsten and gold above specified volume thresholds, requiring management systems, risk management, third-party audits and disclosure.[70] The Commission's first statutory review in 2024 acknowledged both the Regulation's contribution and the difficulty created by its concentration upon importers of the minerals and metals themselves whilst much economic leverage lies further downstream.[71] Neither instrument is without value; rather, each demonstrates the central defect. A due-diligence rule manages the risk that a company may purchase through conflict, whereas an economic-warfare statute must additionally ask whether a person knowingly provides money, market access, transport, intelligence or protection which preserves a coercive enterprise, who benefits, and what immediate measure is permitted before the chain is rearranged.

The DRC therefore supplies more than a historical illustration of 'conflict minerals'. It demonstrates an economic architecture in which the mine may be controlled by one group, the local tax exacted by another, the exporter incorporated in a third State, the smelter situated in a fourth, and the final manufacturer able to say, sometimes truthfully, that it neither met nor paid the armed men. Each jurisdiction may see a lawful fragment. The aggregate may nevertheless finance territorial control. If regulation fixes only upon the final transfer, or only upon provable agency between the final purchaser and the armed group, design itself becomes a defence. The necessary answer is not automatic guilt by association, but mandatory traceability, preservation of records, a duty of heightened inquiry where conflict indicators exist, liability for deliberate or reckless circumvention, and a power to restrain the transaction whilst the evidence is tested.

2.2.2 The Oil Industry in Nigeria

The Nigerian example concerns a different conversion of private economic power. Oil operations in the Niger Delta have generated allegations of forced displacement, environmental degradation, violence against communities and corporate reliance upon public security forces. The allegations made in the *Wiwa* litigation were grave: the claimants alleged corporate complicity in abuses committed against Ogoni opponents of oil development during the 1990s.[72] The proceedings settled in 2009 for US$15.5 million without an admission of liability, Shell continuing to deny participation in the alleged violence.[73] Publication must preserve all three propositions—the allegations, the denial and the settlement—because to collapse a settlement into a conviction would be inaccurate, whilst to omit the

[68] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Judgment) [2005] ICJ Rep 168, paras 245–250 and 345(4)–(5).

[69] OECD, *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas* (3rd edn, OECD Publishing 2016) 16–20 https://doi.org/10.1787/9789264252479-en accessed 5 August 2026.

[70] Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas [2017] OJ L130/1, arts 1 and 4–7.

[71] European Commission, 'Report on the Functioning and Effectiveness of Regulation (EU) 2017/821' COM (2024) 415 final, 24 September 2024, 8–13.

[72] *Wiwa v Royal Dutch Petroleum Co* 226 F 3d 88 (2d Cir 2000).

litigation because it did not reach trial would conceal the jurisdictional obstacles which are themselves material to this inquiry.

Other authoritative findings prevent the wider subject from being dismissed as advocacy. In *SERAC and CESR v Nigeria*, the African Commission on Human and Peoples' Rights found Nigeria in violation of arts 2, 4, 14, 16, 18(1), 21 and 24 of the African Charter. Its reasoning was not confined to direct State violence: the Commission held that governments must protect rights-holders from damaging acts by private parties, criticised the State's role in oil operations and its failure to monitor them, and called for investigation, prosecution of responsible officials, compensation, environmental remediation and independent oversight.[74] This is an important precursor to the due-diligence logic relied upon later in the dissertation. A State cannot answer an externally harmful economic system merely by observing that the immediate operator possesses separate legal personality.

The physical premise has likewise been subjected to independent scientific examination. UNEP's *Environmental Assessment of Ogoniland* followed a fourteen-month inquiry involving more than 200 locations, 122 kilometres of pipeline rights of way, the review of more than 5,000 medical records and engagement with more than 23,000 people. It concluded that pollution from more than fifty years of oil operations had penetrated further and deeper than had commonly been supposed and that restoration would be an extensive, long-term undertaking.[75] That report did not determine the civil or criminal liability of each company for every spill, some of which operators attribute to sabotage or illicit refining. It did establish that the environmental system against which questions of responsibility were being litigated was neither rhetorical nor trivial.

The subsequent cases reveal, with unusual clarity, how the law divides that system. In *Kiobel v Royal Dutch Petroleum*, the United States Supreme Court applied the presumption against extraterritoriality to the Alien Tort Statute and held that the claims, concerning conduct abroad, did not sufficiently touch and concern the United States.[76] That was a ruling upon statutory reach, not a judicial finding that the alleged conduct had not occurred. English parent-company litigation has taken another route. *Vedanta Resources plc v Lungowe* rejected any special doctrine of parental liability but confirmed that an ordinary duty of care may arise where, upon the facts, a parent takes over, intervenes in, controls or publicly assumes responsibility for the relevant operations of its subsidiary.[77] In *Okpabi v Royal Dutch Shell plc*, the Supreme Court held that the claimants had an arguable case that the English parent owed a duty in relation to pollution said to have resulted from its Nigerian subsidiary's operations; again, the Court decided jurisdiction and arguability, not ultimate liability.[78]

The Court of Appeal of The Hague went further upon different spills and under Nigerian law. In January 2021 it held Shell's Nigerian subsidiary liable for damage caused by leaks at Oruma and Goi after concluding that the asserted sabotage had not been proved to the demanding standard applicable, and it required both the subsidiary and parent to secure an improved warning system for the Oruma pipeline.[79] Those judgments did not decide the historical allegations in *Wiwa*, and ought not be used as

---

[73] John Cerone, 'Wiwa v Shell: The $15.5 Million Settlement' (2009) 13(14) *ASIL Insights* https://asil.org/insights/volume-13-issue-14/ accessed 31 July 2026.

[74] *Social and Economic Rights Action Center and Center for Economic and Social Rights v Nigeria* Communication 155/96 (African Commission on Human and Peoples' Rights, 27 October 2001) paras 44–58 and disposition.

[75] United Nations Environment Programme, *Environmental Assessment of Ogoniland* (UNEP 2011) https://www.unep.org/resources/report/environmental-assessment-ogoniland accessed 5 August 2026.

[76] *Kiobel v Royal Dutch Petroleum Co* 569 US 108, 124–25 (2013).

[77] *Vedanta Resources plc v Lungowe* [2019] UKSC 20, [2020] AC 1045, paras 49–55.

[78] *Okpabi v Royal Dutch Shell plc* [2021] UKSC 3, [2021] 1 WLR 1294, paras 25, 140–53.

[79] *Milieudefensie v Royal Dutch Shell plc*, ECLI:NL:GHDHA:2021:132 and ECLI:NL:GHDHA:2021:133 (Court of Appeal of The Hague, 29 January 2021); Court of Appeal of The Hague, 'Shell Nigeria Liable for Oil Spills in Nigeria' (29 January 2021) https://www.rechtspraak.nl/organisatie-en-contact/organisatie/gerechtshoven/gerechtshof-den-haag/nieuws/2021/01/shell-nigeria-liable-for-oil-spills-in-nigeria accessed 5 August 2026.

if they did. They do, however, demonstrate that proof, corporate structure and forum may produce radically different routes to remedy even where operations form part of one economic group.

For present purposes, the Nigerian case is not offered upon the crude footing that pollution is warfare. It shows how command over an indispensable revenue source, the ability to request or benefit from coercive security, and the capacity to externalise human and environmental cost may acquire strategic effect. Where a corporation knowingly funds, directs or materially preserves coercion in order to maintain production, the fact that it does so by invoice, concession or security contract rather than uniform should not prevent inquiry into economic warfare. The proposed legislation must therefore distinguish an adverse impact from hostile or coercive economic participation, but it must not make formal corporate separation conclusive. Control, assumption of responsibility, knowledge, benefit, deliberate blindness and contribution are factual questions; they are not to be answered in advance by the place of incorporation.

2.2.3 The Arms Trade in Yemen

The conflict in Yemen supplies the clearest case in which an otherwise lawful industry may place decisive capability into a foreign war. An arms manufacturer does not ordinarily decide whether an export is lawful; the State licenses it. Nor does the issue turn merely upon profit, for States may lawfully supply weapons and recipients may lawfully use them. The question is what the legal system requires when repeated allegations of serious violations coexist with a commercial and governmental determination to preserve the supply of military capability.

The international and domestic rules already recognise that an export is not exhausted by the sale. Article 6(3) of the Arms Trade Treaty prohibits authorisation where the exporting State has knowledge, at the time of authorisation, that the arms or items would be used in genocide, crimes against humanity, grave breaches or other specified war crimes. Article 7 requires an assessment, where art 6 does not prohibit the transfer, of the potential that conventional arms or items would contribute to or undermine peace and security, or could be used to commit or facilitate serious violations of IHL or international human-rights law; an overriding risk after mitigation requires refusal.[80] The United Kingdom implements export control through the Export Control Act 2002, the Export Control Order 2008 and published licensing criteria. At the material time Criterion 2(c) required that a licence not be granted where there was a clear risk that the items might be used in the commission of a serious violation of IHL.[81]

In 2019 the Court of Appeal allowed CAAT's challenge to licensing decisions for exports to Saudi Arabia for possible use in Yemen. The Court did not decide that every allegation was true, nor that the coalition had in fact committed an identified number of IHL violations. It held the decision-making process irrational and therefore unlawful because, whilst the Secretary of State had addressed future risk, he had not made the necessary assessment of whether there had been a historic pattern of violations.[82] That distinction is central. The judgment establishes that a grave predictive decision cannot be lawfully made by refusing to decide what past conduct reveals; it is not a criminal verdict against the recipient, exporter or Minister.

The Government retook the decisions and announced on 7 July 2020 that it had identified 'possible' violations but regarded them as isolated incidents, had found no pattern and would resume the processing of applications.[83] CAAT challenged that fresh decision. On 6 June 2023 the Divisional Court dismissed the second claim, holding, upon open and closed material and according the executive the

[80] Arms Trade Treaty (adopted 2 April 2013, entered into force 24 December 2014) 3013 UNTS 269, arts 6(3) and 7.

[81] Export Control Act 2002; Export Control Order 2008, SI 2008/3231; *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2019] EWCA Civ 1020, [2020] 1 WLR 576, paras 12–20.

[82] *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2019] EWCA Civ 1020, [2020] 1 WLR 576.

latitude required by public-law review in a field of evaluative judgment, that the Secretary of State's approach was lawful.[84] Thus the 2023 judgment was not a successful appeal from the 2019 case; it concerned a new decision made after the earlier process had been held unlawful. To state otherwise would confuse both chronology and legal effect.

The two decisions expose the strength and the limit of licensing law. It can require a rational assessment of past incidents, test whether published criteria were applied, restrain exports whilst a decision is remade, and subject sensitive evidence to closed procedure. It does not supply a general account of economic participation in war. The licence remains organised by item, destination and end-use risk, whereas strategic dependence may arise from a continuing package of aircraft support, components, maintenance, software, training, finance and replenishment. Each transaction may be administratively reviewed as a unit even though the military effect lies in the continuity of the system.

This is why the case belongs in an inquiry into economic warfare. If a private enterprise, acting with State permission, provides the material without which a campaign cannot be sustained, it wields power of a different order from that of an ordinary seller. The appropriate response is not to call every defence contractor a belligerent. It is to require the regulator to examine cumulative capability, the exporter's knowledge, the foreseeable use of support services, corporate efforts to avoid end-use restrictions, and the maximum reasonably foreseeable human consequence of continuation. The same method must operate in reverse where private capital supplies communications, targeting, compute or cyber capability rather than a munition. It would be incoherent to scrutinise the aircraft component because it is tangible whilst treating an equally indispensable targeting or network service as a private commercial choice.

2.3 The Need for Regulation

The case studies above highlight the challenges of regulating economic warfare by non-state actors. MNCs often operate in a legal grey area where the lines between legitimate business activities and indirect support to armed groups or human rights abuses are blurred. There is a need for a comprehensive legal framework that regulates the actions of MNCs in conflict-affected regions.

Such a framework should include:

1. Due Diligence Requirements: MNCs should be required to conduct due diligence on their supply chains to ensure that they are not indirectly supporting armed groups or human rights abuses. This could include requirements to source minerals from certified conflict-free mines or to conduct human rights impact assessments for their operations.
2. Accountability Mechanisms: There should be clear accountability mechanisms for MNCs that indirectly support armed groups or human rights abuses. This could include judicial mechanisms, such as national or international courts, and non-judicial mechanisms, such as sanctions or reputational consequences.
3. Transparency Requirements: MNCs should be required to disclose their supply chains, business partners, and other relevant information to ensure transparency and accountability. This could include requirements to publish annual reports on their due diligence efforts, supply chain audits, or other relevant information.

These requirements must be framed according to risk and function, rather than by a list of industries which will be obsolete before it is enacted. The United Nations Guiding Principles on Business and

[83] Secretary of State for International Trade, 'Trade Update' (Written Statement HCWS339, 7 July 2020) https://questions-statements.parliament.uk/written-statements/detail/2020-07-07/HCWS339 accessed 5 August 2026; HC Deb 13 July 2020, vol 678, cols 1250–68.

[84] *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2023] EWHC 1343 (Admin).

Human Rights require human-rights due diligence to identify, prevent, mitigate and account for adverse impacts, and call for particular attention to the heightened risk of gross abuses in conflict-affected areas.[85] That structure is necessary but not sufficient. The proposed Act should add an economic-warfare inquiry which is triggered where an undertaking supplies funds, goods, services, infrastructure or information capable of materially sustaining organised coercion, territorial control, attacks upon essential services or the evasion of lawful restraints.

Once triggered, the undertaking should be required to identify the beneficial recipient, preserve transactional and technical records, map material subcontractors, record the basis upon which end-use assurances were accepted, and report specified changes or suspicious circumstances to the competent authority. A company which has made an honest, evidenced and proportionate inquiry should not be punished merely because a concealed actor deceived it. A company which fragments a transaction, relies upon an intermediary it knows to be opaque, removes ordinary audit rights, or continues after credible evidence of diversion should not obtain the same protection. Liability must attach not only to actual knowledge but to deliberate blindness and reckless failure to investigate an obvious conflict indicator; otherwise the law rewards the very corporate distance which makes these operations commercially useful.

Nor should the remedy be confined to damages after the event. The proposed authority requires power to compel information, order temporary preservation of assets and records, suspend a specified service or transfer, impose licensing conditions, and coordinate sanctions, export controls, criminal investigation and civil recovery. Temporary measures would require written reasons, a defined duration and prompt access to independent review. The purpose is not to subordinate commerce to ministerial suspicion, but to prevent value or capability being irreversibly transferred during the months in which an ordinary proceeding is prepared.

The distinction between this framework and existing corporate-responsibility regulation is therefore exact. The UN Guiding Principles and OECD Guidance ask how enterprises should avoid causing, contributing to, or being directly linked to adverse impacts; export controls ask whether listed goods may lawfully be transferred; sanctions prohibit dealings with designated persons or sectors. Economic-warfare legislation must connect those fragments where the same enterprise, payment or infrastructure is serving a hostile strategic function. It should neither duplicate every existing offence nor create an unbounded moral jurisdiction. It should supply the common reporting, attribution and response structure through which the existing powers can act as one.

2.4 Conclusion

Economic warfare is not limited to the actions of States. A corporation operating in a conflict-affected region may sustain the violence around it without intending to, through supply, payment or the ordinary continuation of business with an armed group or an abusive government. Yet the conclusion is not that all harmful commerce is war. It is that private economic conduct may become strategically coercive when it supplies organised violence, preserves the means by which it is continued, or knowingly converts a conflict into revenue and revenue back into capability. The DRC shows distance within a mineral chain; Nigeria shows distance between parent, subsidiary, public force and local harm; Yemen shows distance between an export licence, a private supplier and the cumulative operation of a weapons system. In each, legal fragmentation permits every participant to describe its own act more narrowly than the system it supports.

[85] Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (HR/PUB/11/04, 2011) principles 7, 17 and 23.

There is therefore a need for a comprehensive legal framework which regulates the actions of MNCs in conflict-affected regions and ensures accountability for those which knowingly or recklessly sustain coercion or grave abuse. It must preserve lawful trade, require proof proportionate to the measure taken, and distinguish allegation from adjudication. It must equally refuse the proposition that incorporation, subcontracting or a sufficiently long invoice chain can alter the strategic character of what is done. Implementing such a framework is crucial for promoting peace, security, and respect for human rights in a globalised world.

3. Economic Cyber-warfare: The Twenty-first Century

Most of our industry, finance, infrastructure, and military are integrated through computer technology, and this is unlikely to change. Interconnection can cause major issues as actors look to find vulnerabilities and exploits in both hardware and software. An endless war ensues in cyberspace between those looking to exploit these weaknesses and those seeking to secure their systems.

Unfortunately, this new, digital battlefield is complex, with experts in the field struggling to understand and keep up with new vulnerabilities. Gene Spafford, a world-leading computer security expert from Purdue University, famously stated that "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts".[86] Hackers are individuals or groups whose job (or hobby) is to find these vulnerabilities and exploit them. Motivation may lie in the glory or thrill of the challenge, the desire to help create a more secure cyberspace, or financial or political gain. Generally, these attacks mirror traditional warfare techniques, such as sabotage, espionage, counterintelligence and (cyber) terrorism, and are conducted against individuals, companies and state bodies. The nature of the attacks and the methodologies used to conduct them differ greatly, making them very difficult to defend against. Zero-day exploits, for example, are exploits which are present at inception yet discovered much later. Additionally, many of the tools used to defend one's system, such as Virtual Private Networks (VPNs), also make it difficult to trace activity. For instance, an attack on the US originating from China could be routed through Venezuela and re-routed to a computer in Russia. Even if the US painstakingly tracked the attack from Russia to Venezuela and back to China, it would still be unsure whether the attack originated from China. Additionally, if the attacks were conducted by a third-party cyber-mercenary group, prosecution would necessitate evidentiary proof of China's involvement.

As experts struggle to keep abreast of these exploits, it is unsurprising that legislation sanctioning them has been slow to come to fruition.[87] Law may also be drawn by institutions whose technical understanding is necessarily mediated by evidence and advice, allowing defects which sophisticated organisations or individuals will pursue. Technical standards, including the ISO/IEC 27000 family, assist in defining and protecting assets but do not answer the questions of attribution, jurisdiction or permissible State response.[88] Basic practices, including timely patching of operating systems, are frequently ignored to the detriment of stakeholders.[89] Nor, however, does the use of cyber means place an operation outside the Geneva Conventions. IHL applies where there is an armed conflict and the operation possesses the necessary nexus; whether a hospital, bank or power grid is protected depends upon the object, its use, the rule engaged and the operation's reasonably foreseeable effects, not upon whether the attacker used a missile or a keyboard.[90] The Office of the ICC Prosecutor may receive information under article 15 of the Rome Statute, and an article 15 communication concerning cyber operations is evidence submitted for consideration rather than a prosecution, judgment or amendment of the Statute.[91] No separate "cyber Geneva Convention" is required before existing IHL can apply,

[86] A K Dewdney, 'Computer Recreations: Of Worms, Viruses and Core War' (1989) 260(3) *Scientific American* 110, 110.

[87] Lucas Kello, 'Cyber Legalism: Why It Fails and What to Do about It' (2021) 7(1) *Journal of Cybersecurity* tyab014.

[88] International Organization for Standardization, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary* (ISO/IEC 27000:2018, 5th edn, 2018) https://www.iso.org/standard/73906.html accessed 5 August 2026.

[89] Mary-Ann Russon, 'NHS: Millions of Medical Devices in UK Hospitals Are Completely Unprotected against Hackers' *Evening Standard* (23 June 2023) https://www.standard.co.uk/tech/nhs-medical-devices-cyber-attack-hackers-b1089559.html accessed 31 July 2026.

[90] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (position paper, November 2019) https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf accessed 5 August 2026.

[91] Rome Statute (n 22) art 15.

although serious questions remain concerning how its established rules govern data, functionality and non-physical effects.[92]

Owing to their low cost, availability and potential devastation, demand for cyber-crime services has grown. Distributed denial-of-service (DDoS) capacity may be hired for tens of dollars, a proposition established not merely by journalism but by empirical study of booter and stresser markets and repeated criminal enforcement against them.[93] At the opposite end of the market, vendors have publicly offered multi-million-dollar prices for exclusive, persistent compromise chains.[94] Individuals, organisations and States increasingly solicit or employ cyber contractors.[95] Backdoors are not conjectural: indictments and technical advisories have documented State-linked actors deploying malware that creates persistent remote access, whilst later disclosures have exposed PRC-linked contracting ecosystems in which public agencies purchase the fruits of ostensibly private intrusion.[96] It would be unsafe to turn that proof into a universal claim that Chinese companies insert hardware backdoors into every product before retail; the proved threat is stronger and more legally useful, for it shows deliberate access, persistence, contractor payment and State benefit. A new form of economic cyber-warfare is thereby emerging, in which States compete to produce advanced technologies, restrict their adversaries' access and retain exploitation capabilities within national or proxy ecosystems.[97]

3.1 Who Is Carrying Out These Attacks, and Why?

The most notorious cyber-warfare incidents have clear links to traditional confrontation.[98] The attacks upon Estonia in 2007 and Georgia in 2008 illustrated two different attribution problems. Estonia experienced sustained disruption amid political conflict with Russia; Georgia experienced cyber operations temporally coordinated with conventional hostilities. In neither case does coincidence alone prove the international-law test of State attribution. Public participation by patriotic or pro-government hackers, infrastructure overlap, advance preparation and apparent strategic benefit are evidence, but legal responsibility still requires proof connecting the relevant conduct to the State.[99] A member of the pro-Kremlin youth movement Nashi later claimed involvement in part of the Estonian campaign; that admission strengthened the case for organised private participation without, of itself, proving Russian State direction.[100] Titan Rain similarly described a series of intrusions into United States networks which officials and researchers associated with China, although the public record did not convert every technical attribution into proof of State legal responsibility.[101]

---

[92] ICRC, 'Cyber Operations and International Humanitarian Law' (29 November 2022) https://www.icrc.org/en/document/cyber-operations-and-international-humanitarian-law accessed 31 July 2026.

[93] Ali Zand and others, 'Demystifying DDoS as a Service' (2017) 55(7) *IEEE Communications Magazine* 14.

[94] Lorenzo Franceschi-Bicchierai, 'Russian Zero-Day Seller Offers $20m for Hacking Android and iPhones' *TechCrunch* (27 September 2023) https://techcrunch.com/2023/09/27/russian-zero-day-seller-offers-20m-for-hacking-android-and-iphones/ accessed 31 July 2026.

[95] Martin C Libicki, David Senty and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (RAND Corporation 2014); Jonathan Mayer, 'Government Hacking' (2018) 127 *Yale Law Journal* 570.

[96] *United States v Wu Haibo and others*, No 24 Cr 687 (SDNY, indictment unsealed 5 March 2025); US Department of Justice, 'Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns' (5 March 2025) https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global accessed 31 July 2026. The indictment contains allegations; every defendant is presumed innocent unless and until proved guilty.

[97] James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) ch 5.

[98] Green (n 97) ch 5.

[99] Alika Guchua, Thornike Zedelashvili and Gela Giorgadze, 'Geopolitics of the Russia–Ukraine War and Russian Cyber Attacks on Ukraine–Georgia and Expected Threats' (2022) 10 *Ukrainian Policymaker* 27.

[100] Natali Olovson, *Hacking for the State? The Use of Private Persons in Cyber Attacks and State Responsibility* (Master's thesis, Swedish Defence University 2020) https://www.diva-portal.org/smash/record.jsf?pid=diva2:1577790 accessed 31 July 2026.

[101] US House of Representatives Committee on Homeland Security, *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security* (Hearing 110-52, 20 June 2007) 3–4 https://www.govinfo.gov/content/pkg/CHRG-110hhrg48926/pdf/CHRG-110hhrg48926.pdf accessed 5 August 2026.

Many mercenary groups have added cyber-attacks to their repertoire, and it is often difficult to link them to their State sponsors. In the Russia–Georgia conflict, the Russian Business Network (RBN) was suspected both of participation in the attacks and of receiving State sponsorship.[102] The suspicion arose partly from the timing of 'trial' DDoS attacks occurring weeks before the conflict.[103]

Additionally, groups such as Anonymous can act in rebellion against the status quo or as a form of self-righteous vigilantism. In examining these actions, one may observe a complex interplay between perceived justice and the necessity for legal regulation. The hacker collective has demonstrated a unique blend of ideologically driven cyber activism, often perceived as a form of digital vigilantism. This was particularly evident in the wake of the 2015 Paris attacks, where it declared war on the Islamic State (IS), vowing to avenge atrocities and dismantle its online presence.[104] Leveraging its decentralised, yet formidable, network, Anonymous orchestrated a series of cyber-attacks. Its activities included identifying or reporting thousands of purportedly IS-related social-media accounts, conducting DDoS attacks on websites, leaking information said to concern IS members and launching public-awareness campaigns. Such operations, aimed at combating terrorism, were underpinned by a deeply relatable moral stance. Its actions resonated with public sentiment and built upon the good faith it had gained after the Charlie Hebdo attacks, when it targeted extremists' online platforms.[105]

However, the scope and nature of Anonymous's activities quickly evolved, raising concerns about the unregulated power of such collectives. In 2017, Operation Sacred (OpSacred), part of the larger OpIcarus, saw Anonymous conduct organised DDoS attacks against major financial institutions such as the IMF, the World Bank and the Federal Reserve.[106] More recently, in 2023, groups presenting themselves as KillNet, REvil and Anonymous Sudan announced or conducted campaigns against United States and European banking systems,[107] whilst Anonymous Sudan claimed attacks against financial institutions in the United Arab Emirates, including First Abu Dhabi Bank, RAKBANK and Mashreq Bank.[108] Contemporary reporting described service disruption, although the publicity surrounding such groups requires care when distinguishing a threat, a claim and a technically verified compromise.[109]

The capriciousness of individual and group actors, and the potentially disruptive unilateral action they may take outside legal norms, underscores the necessity of legal frameworks indifferent to perceived righteousness. Both individuals and groups leverage economic and cyber power with substantial effect. Elon Musk's deployment of Starlink in the Russia–Ukraine war supplies one example.[110]

---

[102] Andrzej Kozłowski, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan' (2014) 3 *European Scientific Journal* (special edn) 237, 241–42.

[103] Kozłowski (n 102) 241.

[104] 'Anonymous Hackers Declare War on Islamic State' *Sky News* (16 November 2015) https://news.sky.com/story/anonymous-hackers-declare-war-on-islamic-state-10339388 accessed 31 July 2026; John Zorabedian, 'Anonymous Declares War on Islamic State after Paris Attacks' (Sophos News, 16 November 2015) https://news.sophos.com/en-us/2015/11/16/anonymous-declares-war-on-islamic-state-after-paris-attacks/ accessed 31 July 2026.

[105] Alex Hern, 'Anonymous Claims Victory over Jihadi Twitter Accounts in #OpIsis' *The Guardian* (10 February 2015) https://www.theguardian.com/technology/2015/feb/10/anonymous-claims-victory-over-jihadi-twitter-accounts-in-opisis accessed 31 July 2026.

[106] 'OpSacred 2017: Financial Institutions to Face Anonymous-Driven DDoS Attacks' (Data Foundry, 12 June 2017) https://www.datafoundry.com/blog/opsacred-ddos-attacks-anonymous-2017 accessed 31 July 2026.

[107] Trustwave SpiderLabs, 'KillNet, Anonymous Sudan, and REvil Unveil Plans for Attacks on US and European Banking Systems' (15 June 2023) https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/killnet-anonymous-sudan-and-revil-unveil-plans-for-attacks-on-us-and-european-banking-systems/ accessed 31 July 2026.

[108] Ashish Khaitan, 'Anonymous Sudan Attacks UAE Banks: Cybersecurity Breach Raises Concerns' *The Cyber Express* (12 May 2023) https://thecyberexpress.com/uae-banks-cyber-attack-by-anonymous-sudan/ accessed 31 July 2026.

[109] Karl Greenberg, 'Anonymous Sudan's Attack on European Investment Bank: Money, Politics and PR' *TechRepublic* (26 June 2023) https://www.techrepublic.com/article/anonymous-sudan-attacks-european-investment-bank/ accessed 31 July 2026.

[110] Christopher Miller, Mark Scott and Bryan Bender, 'How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare' *Politico* (9 June 2022) https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039

Similarly, examples of individual cyber power include Gary ‘Solo’ McKinnon and Jonathan James. McKinnon was accused of obtaining unauthorised access to 97 United States Government computers between February 2001 and March 2002.[111] The United States further alleged that deletion of critical files caused the United States Army’s Military District of Washington network, comprising more than 2,000 computers, to shut down for twenty-four hours, and that remedial costs exceeded $700,000. Likewise, in 1999, James, then a teenager, penetrated systems belonging to NASA and the United States Department of Defense.[112] In McKinnon’s case, the Home Secretary’s refusal to order extradition illustrates the legal and ethical complexities of prosecuting cybercrime across jurisdictions. The House of Lords had rejected McKinnon’s appeal in 2008, but in 2012 the Home Secretary prevented extradition upon human-rights grounds relating to the severe risk that he would end his life.[113]

Finally, large businesses may be motivated by their own growth or by the hindrance of competition. The MediaDefender disclosures provide a properly bounded example. The anti-piracy contractor worked for major motion-picture and recording interests, reportedly including Universal and Sony; leaked communications described a proposal to hire hackers to disrupt The Pirate Bay, and The Pirate Bay filed complaints naming entertainment companies, though no judgment established that Sony or Universal had ordered that particular DDoS operation.[114] A separate and technically documented episode is less equivocal: Revision3’s chief executive reported that MediaDefender’s automated system flooded the company with SYN packets and disabled its service after its tracker ceased returning the response expected by MediaDefender’s software.[115] The evidential distinction matters. Journalism and leaked material prove that corporate clients purchased an offensive anti-piracy ecosystem; the leaked correspondence proves that the contractor contemplated disruptive methods; and the Revision3 incident proves that infrastructure operated by the contractor caused a denial of service. What has not been adjudicated should not be invented, but neither should proved corporate cyber-disruption be written out of the account.

3.2 When the Keyboard Becomes a Weapon: Scale and Effects

It is necessary to distinguish categories which political speech too often compresses into the phrase “cyber-attack”. Unauthorised access may be a domestic crime without being an internationally wrongful act. A coercive operation interfering with matters which international law reserves to a State may be a prohibited intervention. A graver operation may constitute a use of force contrary to article 2(4) of the Charter; only an operation reaching the further threshold of an armed attack engages the inherent right of self-defence under article 51. If an armed conflict already exists, IHL may govern a cyber operation because of its nexus to that conflict even though the same operation did not begin it. War crimes, in turn, require the elements of the particular offence and cannot be inferred merely from the adjective “cyber”.[116]

---

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* (Inspection Report E-121-25-003-M, 11 August 2025) https://oig.usaid.gov/node/7845 accessed 5 August 2026.

[111] *McKinnon v Government of the United States of America* [2008] UKHL 59, [2008] 1 WLR 1739 [4]–[5].

[112] Kevin Poulsen, ‘Former Teen Hacker’s Suicide Linked to TJX Probe’ *Wired* (9 July 2009) https://www.wired.com/2009/07/hacker-3/ accessed 31 July 2026.

[113] *McKinnon* (n 111); HC Deb 16 October 2012, vol 551, cols 166–68; Home Office, ‘Gary McKinnon Extradition Case: Home Secretary’s Statement’ (16 October 2012) https://www.gov.uk/government/speeches/gary-mckinnon-extradition-case-home-secretarys-statement accessed 31 July 2026.

[114] Ryan Singel, ‘MediaDefender Emails Reveal Secret Government Project’ *Wired* (18 September 2007) https://www.wired.com/2007/09/mediadefender-emails-reveal-secret-government-project/ accessed 31 July 2026; ‘The Pirate Bay Files Charges against Media Companies’ *TorrentFreak* (24 September 2007) https://torrentfreak.com/the-pirate-bay-files-charges-against-media-companies-070924/ accessed 31 July 2026.

[115] Jim Louderback, ‘Inside the Attack that Crippled Revision3’ (Revision3, 29 May 2008); Ryan Singel, ‘MediaDefender DDoS Attack Took Down Revision3’ *Wired* (29 May 2008) https://www.wired.com/2008/05/mediadefender-d/ accessed 31 July 2026.

[116] Roscini (n 7) chs 2–4; Hathaway and others (n 44) 836–58.

The absence of gunpowder cannot decide the matter. A gun is legally significant because of what its employment does, not because metal and propellant possess a peculiar moral status. If commands delivered through a keyboard foreseeably open a dam, disable a hospital's life-support systems or produce a prolonged winter failure of an electricity grid, the fact that the causal chain proceeds through code does not make the deaths, destruction or deprivation less physical. The United Kingdom's published position accordingly accepts that cyber operations may amount to a use of force and that an operation of sufficient scale and effects may constitute an armed attack; it also rejects the proposition that only operations causing physical damage can ever engage the prohibition of force.[117] France, Australia, the United States and other States have expressed positions which, though not identical, likewise examine severity, immediacy, directness, invasiveness, military character and measurable effects.[118]

"Scale and effects" is therefore a threshold analysis rather than a verbal licence. In *Nicaragua* the International Court of Justice distinguished the "most grave" forms of force, constituting armed attack, from less grave forms; in *Oil Platforms* and *Armed Activities* it insisted upon necessity, proportionality and proof.[119] A single theft of money does not become an armed attack because the sum is large, nor does every outage permit missiles. Yet an operation must be assessed by its reasonably foreseeable consequences, including the systems upon which life depends, the duration and geographical spread of disruption, the attacker's persistence, the vulnerability of those affected and the prospect of cascading failure. Where defenders interrupt an operation before its intended effects mature, successful defence should not perversely erase the nature of what was attempted. The appropriate measure is the maximum reasonably credible and foreseeable harm disclosed by the capability, target, preparation and course of conduct—not an unbounded theoretical catastrophe which could be imagined after any intrusion.

Attribution remains separate. Technical confidence that infrastructure or malware is associated with a group is not, by itself, proof that conduct is attributable to a State under the law of State responsibility. Articles 4, 5, 8 and 11 of the International Law Commission's Articles describe different routes: conduct of State organs; entities exercising governmental authority; persons acting upon State instructions or under its direction or control; and conduct acknowledged and adopted as the State's own.[120] Financing, shelter, intelligence and operational benefit may be compelling evidence without satisfying every route in every case. The law's demand for connection is justified where force may follow; the vice exposed by this dissertation is that the instigator may intentionally distribute money, personnel, code and infrastructure so that no investigating State holds the whole proof.

Finally, the legal response cannot be selected by the label alone. Retorsion, criminal investigation, sanctions, disruption with territorial consent and otherwise lawful defensive cyber measures occupy a different legal field from countermeasures; countermeasures are constrained, temporary and may not involve force.[121] Force in self-defence requires an actual or imminent armed attack, attribution or another legally sufficient basis, necessity and proportionality; any attack must then comply with distinction, proportionality in attack and precautions under IHL where that body of law applies. Deterrence may guide which lawful and necessary measure is chosen, but punishment of past conduct cannot manufacture article 51 necessity. This separation is carried into the proposed Act in Chapter 6.

---

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

[118] UNGA, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States' (13 July 2021) UN Doc A/76/136 https://digitallibrary.un.org/record/3933543 accessed 5 August 2026.

[119] *Nicaragua* (n 19) [191]; *Oil Platforms (Islamic Republic of Iran v United States of America)* (Judgment) [2003] ICJ Rep 161 [51], [73]–[78]; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Judgment) [2005] ICJ Rep 168 [146]–[147].

[120] International Law Commission (n 53) arts 4, 5, 8 and 11.

[121] International Law Commission (n 53) arts 49–54, especially art 50(1)(a).

3.3 Economic Cyber-warfare: Urgency and Danger

The scariest parts of cyber warfare are its simplicity, minimal required manpower or infrastructure and potential for harm. For example, in June 2021, JBS SA, the world's largest meat processing company, was hit by a REvil ransomware attack. JBS paid $11 million in Bitcoin to resolve the incident.[122]

This paper focuses upon economic costs, but cyber operations may produce physical consequences, including the disruption of safety systems at nuclear, water and energy facilities, at a cost far below that of conventional attack. The Guardian reported in December 2023 that Sellafield had been compromised by groups linked to Russia and China; Sellafield Ltd and the Office for Nuclear Regulation stated that they had no evidence of a successful State-linked hack.[123] Publication requires both parts of that record. It also requires the later fact that Sellafield Ltd pleaded guilty to offences concerning information-technology security between 2019 and 2023 and was fined in October 2024: the official denial rebuts the particular attribution, whilst the conviction proves serious security failings at the nuclear site.[124] The wider infrastructure warning has, moreover, been officially confirmed. In February 2024 the NCSC and allied agencies assessed that Volt Typhoon, a PRC State-sponsored group, had compromised United States critical-infrastructure organisations and sought persistent access which could be used to disrupt operational technology during a crisis.[125] The authorities described pre-positioning and capability, not a proved nationwide outage; that distinction leaves the threat no less grave. An operation coordinated across power, communications, water or health systems could devastate an economy and cause deaths without an explosive device ever crossing a border.

3.4 Post-submission Confirmation: APT31 and the Proxy Ecosystem

Publication-revision note. The dissertation was submitted on 31 January 2024. The official attributions in this section were published afterwards and are identified as such so that they confirm, rather than silently rewrite, the historical argument.

On 25 March 2024—fifty-four days, or just under eight weeks, after submission—the Foreign, Commonwealth and Development Office and the National Cyber Security Centre publicly identified two Chinese State-affiliated campaigns against British democratic institutions.[126] First, the NCSC assessed that the Electoral Commission's systems were highly likely compromised by a Chinese State-affiliated entity between 2021 and 2022. The hostile actors first obtained access in August 2021 and remained capable of accessing Commission systems until the intrusion was detected in October 2022. The accessible material included Commission email and electoral-register data; the Information Commissioner's Office later described the servers as containing the personal information of

[122] JBS USA, 'JBS USA Cyberattack Media Statement' (9 June 2021) https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9 accessed 31 July 2026; FBI, 'FBI Statement on JBS Cyberattack' (2 June 2021) https://www.fbi.gov/news/press-releases/fbi-statement-on-jbs-cyberattack accessed 31 July 2026.

[123] Anna Isaac and Alex Lawson, 'Sellafield Nuclear Site Hacked by Groups Linked to Russia and China' *The Guardian* (4 December 2023) https://www.theguardian.com/business/2023/dec/04/sellafield-nuclear-site-hacked-groups-russia-china accessed 31 July 2026; Sellafield Ltd, 'Response to a News Report on Cyber Security at Sellafield' (4 December 2023) https://www.gov.uk/government/news/response-to-a-news-report-on-cyber-security-at-sellafield accessed 31 July 2026; Office for Nuclear Regulation, 'Guardian News Article' (4 December 2023) https://www.onr.org.uk/news/all-news/2023/12/guardian-news-article accessed 31 July 2026.

[124] Office for Nuclear Regulation, 'Sellafield Ltd Fined £332,500 for Cyber Security Shortfalls' (2 October 2024) https://www.onr.org.uk/news/all-news/2024/10/sellafield-ltd-fined-332-500-for-cyber-security-shortfalls accessed 31 July 2026.

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

[126] Foreign, Commonwealth & Development Office and others, '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; NCSC, '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.

approximately forty million people.[127] The NCSC assessed that the actors highly likely accessed and exfiltrated email and register data, capable of combination with other sources for large-scale espionage and transnational repression.

Secondly, and separately, the NCSC assessed that APT31 was almost certainly responsible for online reconnaissance against the email accounts of United Kingdom parliamentarians in 2021. Parliamentary security prevented successful compromise, but prevention of the final intrusion does not turn State-linked reconnaissance of legislators into an imaginary event. The Government sanctioned Wuhan Xiaoruizhi Science and Technology Company Limited—a front company associated with APT31 and operating on behalf of the Chinese Ministry of State Security—together with APT31 members Zhao Guangzong and Ni Gaobin.[128] The precision is important: the Electoral Commission compromise was attributed to a Chinese State-affiliated entity; the parliamentary reconnaissance was attributed to APT31. The Government announced them together as parts of a pattern, not as one incident or upon the fiction that every Chinese operation has one technical operator.

Further confirmation arrived on 5 March 2025, when the United States Department of Justice charged twelve Chinese contract hackers and law-enforcement officers in campaigns said to have operated as a private-hacker-for-hire ecosystem. According to the indictments and the Department's account, some defendants worked through the company i-Soon, public-security organs paid for stolen information, and freelance hackers conducted intrusions both at official direction and upon their own initiative before selling useful data to State agencies.[129] An indictment is an allegation to be proved, not a judgment; a formal British attribution is an executive assessment, not a criminal conviction. Yet evidential classification must not be confused with timidity. The later material exposes exactly the institutional machinery which the submitted dissertation said was both possible and dangerous: public power purchasing from private intrusion, actors operating with mixed motives, and a State receiving strategic benefit whilst contractual and technical layers burden attribution. The later evidence did not create the vulnerability diagnosed on 31 January 2024; it revealed, within eight weeks and then in greater contractual detail, the machinery by which that vulnerability was being exploited.

[127] Electoral Commission, 'Public Notification of Cyber-Attack on Electoral Commission Systems' (8 August 2023) https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems accessed 31 July 2026; Information Commissioner's Office, 'ICO Reprimands the Electoral Commission after Cyber Attack Compromises Servers' (30 July 2024) https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/ico-reprimands-the-electoral-commission-after-cyber-attack-compromises-servers/ accessed 31 July 2026.

[128] Foreign, Commonwealth & Development Office and others (n 126).

[129] US Department of Justice (n 96).

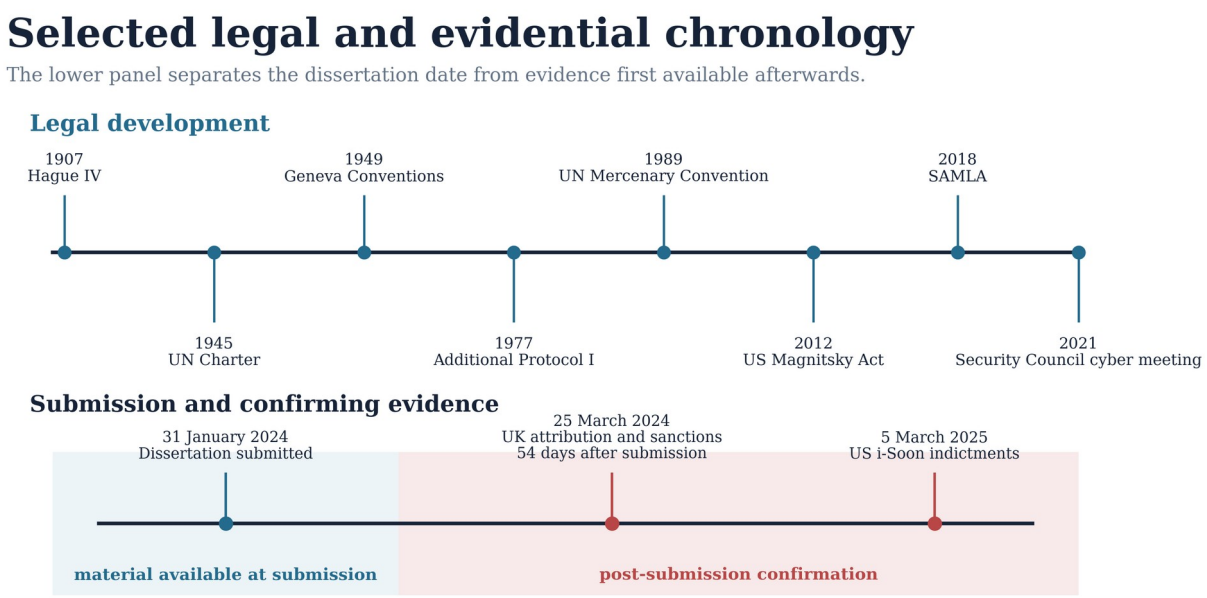

Figure 2. Selected legal and evidential chronology: the Charter and law of armed conflict; mercenary regulation; sanctions statutes; the 2021 Security Council cybersecurity meeting; the 31 January 2024 dissertation submission; and the official APT31 and i-Soon material which followed. Post-submission events are visually distinguished.

3.5 Conclusion

An intricate network of actors—state-sponsored groups, cyber-mercenaries, ideologically motivated collectives, individual hackers, and even corporate entities—has demonstrated a capability to wage war in the digital realm with significant real-world consequences. The cases of Russian-Georgian and Russian-Estonian conflicts, the activities of Anonymous, and the exploits of individuals like Gary McKinnon and Jonathan James exemplify the diverse motivations and capabilities of these actors. This multifaceted threat landscape has rendered traditional legal and security frameworks inadequate, struggling to keep pace with the rapid evolution of cyber warfare tactics and technologies.

The economic implications of these cyber-attacks range from direct financial damage to strategic impacts on national security. The ease of orchestrating these attacks, coupled with the low cost and minimal infrastructure requirements, has made cyber warfare an attractive tool for actors seeking to advance their interests, exert influence, or simply cause disruption. The targeting of critical infrastructure, such as power plants, financial institutions, and military installations, has challenged national and international security architectures.

The next chapter analyses the limitations of current UK policy in addressing these challenges. Specific legislation on economic cyber warfare is imperative, not only to deter attacks but to establish a legal framework that can adapt to evolving threats.

4. Establishing Precedent: Internal Legislation of Note

4.1 The Sanctions and Anti-Money Laundering Act 2018

The Sanctions and Anti-Money Laundering Act 2018 (SAMLA 2018)[130] is a cornerstone of the United Kingdom's autonomous sanctions system after withdrawal from the European Union. It empowers an appropriate Minister to make sanctions regulations for the purposes set out in section 1, including compliance with United Nations obligations or other international obligations, furthering the prevention of terrorism, national or international peace and security, foreign-policy objectives and respect for democracy, human rights and the rule of law.[131] It was not enacted as a comprehensive economic-warfare code; its importance here is analogical, because Parliament accepted a flexible delegated structure capable of imposing substantial restrictions against fast-changing external threats.

Sections 1(1) and 1(2), correctly read, establish the power and permitted purposes; section 1(5) concerns the meaning of a human-rights purpose and is not a catalogue of cyber or economic threats. Section 3 identifies the types of sanction which regulations may impose, including financial, immigration, trade, aircraft, shipping and other sanctions. The Act therefore supplies wide regulatory machinery, but the economic-warfare analysis must not pretend that Parliament placed every act examined in this dissertation within section 1.

Description-based designation is authorised by section 12, which permits sanctions regulations to designate persons by description where stated statutory conditions are met; it is not created loosely by sections 1(2) and 9.[132] Section 3 identifies types of sanctions rather than itself freezing a particular person's funds. These distinctions matter because the strength of a legislative analogy depends upon describing the legislation which exists, not a more convenient statute which does not.

Section 15 concerns exceptions and licences. Information, record-keeping, reporting and information-sharing powers arise under section 16 and the regulations made beneath the Act; enforcement provisions appear in sections 17 and 17A, whilst section 21 supplies extra-territorial application to United Kingdom persons abroad.[133] There were no "2017 amendments" to a 2018 Act establishing the reporting extension alleged in the submitted text. The substantive burden remains real—financial institutions, professionals and other regulated actors bear significant screening, reporting and licensing costs—but it must be proved from the enacted regime and the regulations applicable to them, not attached to the wrong section.[134]

4.1.1 Speed, Severity and the Constitutional Limit

The principal lesson for an economic-warfare statute is not that decisive restraint must await an ordinary trial. It is that Parliament must itself state the purpose, threshold, available measures and route of challenge. In *HM Treasury v Ahmed*, the Supreme Court quashed asset-freezing provisions made under the United Nations Act 1946 where the executive had imposed severe restraints without the Parliamentary authority which interference with fundamental rights required, and where the relevant scheme denied an effective judicial remedy.[135] The defect was not that freezing assets could never be

[130] Sanctions and Anti-Money Laundering Act 2018.

[131] Sanctions and Anti-Money Laundering Act 2018, s 1.

[132] Sanctions and Anti-Money Laundering Act 2018, s 12.

[133] Sanctions and Anti-Money Laundering Act 2018, ss 15–17A and 21.

[134] Office of Financial Sanctions Implementation, *UK Financial Sanctions: General Guidance* (HM Treasury, updated 12 May 2026) https://www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance accessed 5 August 2026.

[135] *HM Treasury v Ahmed* [2010] UKSC 2, [2010] 2 AC 534, paras 45–61, 75–82.

urgent or necessary. It was that general words were treated as authority for an intrusive regime which Parliament had not squarely enacted.

Bank Mellat v HM Treasury (No 2) supplies the corresponding discipline once Parliament has authorised action. Proportionality asks whether the objective is sufficiently important, whether the measure is rationally connected to it, whether a less intrusive measure could have been used without unacceptably compromising the objective, and whether a fair balance has been struck between individual and community interests.[136] These questions do not demand leisurely decision-making before an emergency restraint. They demand that the decision-maker possesses evidence addressed to each question, records the necessity for acting at once, and submits the measure to review before temporary necessity hardens into indefinite punishment.

SAMLA 2018 now contains more particular safeguards than the instruments considered in *Ahmed*. Section 11 requires reasonable grounds to suspect that a named person is involved in or connected with the specified activity and requires the Minister to consider designation appropriate, having regard to the regime's purpose and, so far as known, the likely significant effects upon that person. Section 38 permits a court to review specified decisions by applying judicial-review principles.[137] The Act consequently demonstrates that rapid executive designation and legal control can occupy the same statute. It does not establish that every designation will be correct, nor that judicial review will disclose every item of intelligence, but it denies the false choice between immediate action and law.

The point has been strengthened, after the submission of this dissertation, by *Shvidler*. In 2025 the Supreme Court majority upheld a designation under the Russia sanctions regime and the detention of the yacht *Phi*, emphasising that the effectiveness of a sanctions regime may depend upon the cumulative effect of measures and that sanctions may need to be severe and open-ended. Lord Leggatt's dissent in relation to Mr Shvidler disputed the rational connection and the majority's degree of deference, thereby exposing rather than eliminating the hard constitutional question.[138] The decision assists the present proposal in two respects. First, it confirms that severity is not a legal vice where evidence, statutory purpose and proportionality support it. Secondly, the division in the Court demonstrates why an economic-warfare Act must identify the connection between target and threat more exactly than a power which merely invites the executive to select a person whose designation may add to aggregate pressure.

Despite these strengths, SAMLA 2018 is not without its limitations. The Bill's broad discretionary powers raised concerns about potential overreach and inadequate oversight; during its passage Lord McNally warned that, unless Parliament restrained the delegated power then under consideration, it risked a 'constitutional car crash'.[139] Its complexity, especially in the implementation of description-based sanctions, can pose challenges in identifying appropriate targets, and for those targets to seek the lifting of sanctions. Exacerbated by the challenges in international coordination, SAMLA 2018's unilateral framework can lead to discrepancies with sanctions imposed by other nations or bodies like the EU.

Moreover, the Act's enforcement can strain diplomatic relations, because extraterritorial reach may be perceived as an infringement of sovereignty. SAMLA 2018's effectiveness against non-state actors, specifically terrorist groups or transnational criminal organisations, can also be limited by their decentralised networks. Human-rights concerns arise where sanctions inadvertently disrupt civilian populations or hinder humanitarian efforts. Description-based sanctions are innovative but introduce

[136] *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39, [2014] AC 700, paras 20 and 74.

[137] Sanctions and Anti-Money Laundering Act 2018, ss 11 and 38.

[138] *Shvidler v Secretary of State for Foreign, Commonwealth and Development Affairs; Dalston Projects Ltd v Secretary of State for Transport* [2025] UKSC 30, paras 6–7, 105–26, 203–05 and 233–83.

[139] HL Deb 15 January 2018, vol 788, cols 492–93.

further complexity into compliance and enforcement, potentially affecting a broader class of individuals and entities than intended. Asset freezes and travel bans might also affect family members of sanctioned individuals who are not themselves involved in the sanctioned activities. Sophisticated actors may employ nominees, layered ownership and other methods of evasion, presenting a need for continual revision of sanctions mechanisms and strategies.

In conclusion, SAMLA 2018 marks a pivotal step in confronting economic warfare, yet its broad discretionary scope, human-rights implications and potential enforcement difficulties reveal a pressing need for more refined legislation. Parliamentary scrutiny of the Bill identified the significance of its combined legislative and administrative powers and insisted upon procedural fairness, disclosure of the essence of the case and effective review.[140] Ambiguity may cause businesses and individuals to violate sanctions inadvertently, whilst unclear routes to variation or revocation aggravate the burden upon a wrongly designated person. One fear is that insufficiently confined powers may facilitate arbitrary or politically motivated decisions. These concerns highlight the necessity for a targeted enactment that unambiguously delineates the parameters of economic warfare and clearly defines the role of third-party actors. It should not be a vague, catch-all instrument prone to indiscriminate application by government. It must instead be a precise, comprehensible statute, serving both as a deterrent against economic aggression and as a remedy for deficiencies in current international law. Such legislation would reinforce the legal framework against economic threats whilst preserving the civil liberties upon which its legitimacy depends.

4.2 The Magnitsky Legislation

The Magnitsky legislation supplies a critical legislative analogy, but it was not enacted as a response to economic warfare. The United States' Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act 2012 responded to the detention and death of Sergei Magnitsky and to specified gross violations of internationally recognised human rights.[141] The later Global Magnitsky Human Rights Accountability Act and Executive Order 13818 broadened the United States framework to serious human-rights abuse and corruption.[142] Its relevance to this dissertation lies in legislative technique: personal designation, asset restraint and travel consequences aimed beyond the territorial criminal trial may be adapted to a different, carefully defined problem.

The United Kingdom's Global Human Rights Sanctions Regulations 2020 and Global Anti-Corruption Sanctions Regulations 2021, and the European Union's global human-rights sanctions regime, are analogous but distinct instruments. They share an emphasis upon individual or entity accountability, asset freezes and travel restrictions; none converts "economic warfare" into an existing designation ground merely because the present dissertation considers the technique useful.[143] The argument is thus for a new statutory purpose and evidential gateway, not for tendentious use of a human-rights power outside its terms.

These regimes have frozen assets and barred entry to designated persons, presenting a strong message against serious abuse and corruption. They nevertheless face familiar criticisms concerning the evidential basis for designation, disclosure, procedural fairness, diplomatic repercussions and the risk of

[140] House of Lords Constitution Committee, *Sanctions and Anti-Money Laundering Bill [HL]* (8th Report of Session 2017–19, HL Paper 39) paras 4, 27–29.

[141] Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012 (n 3), §§ 404–06.

[142] Global Magnitsky Human Rights Accountability Act, Pub L No 114–328, subtitle F, §§ 1261–65, 130 Stat 2000, 2533–37; Executive Order 13818, 82 Fed Reg 60839 (20 December 2017).

[143] Global Human Rights Sanctions Regulations 2020, SI 2020/680; Global Anti-Corruption Sanctions Regulations 2021, SI 2021/488; Council Decision (CFSP) 2020/1999 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses [2020] OJ L410I/13; Council Regulation (EU) 2020/1998 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses [2020] OJ L410I/1.

use as a political expedient. Those objections do not defeat individually targeted sanctions; they establish the safeguards which a more powerful economic-warfare statute must contain.

The influence of Magnitsky-style sanctions upon international relations is noteworthy. Targeted States may regard them as an infringement of sovereignty or unjust interference, and may answer them with reciprocal measures.[144] This underscores the balance between enforcing public norms and preserving diplomatic relations, but it also discloses a virtue: where a particular financier, contractor or controller bears responsibility, an individual measure avoids visiting the first response upon an entire civilian economy.

Like SAMLA, Magnitsky-style legislation imposes consequences and reinforces a public commitment to fundamental rights. Its efficacy requires continuous monitoring and adaptation of enforcement mechanisms against evasion through complex financial structures, nominees and proxy entities.[145]

For present purposes, the Act supplies a legislative technique rather than an existing economic-warfare power. Its combination of individual designation, asset restraint and travel restriction demonstrates how law can address the financial underpinnings of illicit activity; the statutory grounds themselves remain directed to the wrong legal object. Economic-warfare tactics, including covert financial manipulation and cyber-attack, pose complex challenges to security and stability.[146] A new enactment may borrow the Magnitsky architecture to restrain the resources of those orchestrating economic aggression, but it must do so under an express economic-warfare purpose and an evidential test drafted for that conduct.[147]

The effectiveness of Magnitsky-style measures when adapted to economic warfare, however, depends upon international cooperation and coordination. Economic warfare often involves activities spanning multiple jurisdictions, making the transnational enforcement of sanctions a complex endeavour. The success of such a model in deterring economic aggression[148] is thus significantly influenced by the willingness of other States to recognise and enforce the imposed sanctions.[149]

Looking forward, the Magnitsky Act's framework can serve as a model for developing comprehensive international regulations aimed at addressing the multifaceted challenges of economic warfare. Its focus on individual and entity-level accountability, combined with its extraterritorial purview, provides a robust template for future legal instruments in this domain. However, to enhance its efficacy, there is a need for continuous evolution and improvement of the Act. This includes addressing challenges related to the identification of sanction targets, ensuring the fair and transparent application of sanctions, and mitigating potential diplomatic frictions that may arise from their implementation.

[144] Gordon (n 35).

[145] Commission on Security and Cooperation in Europe, *The Magnitsky Act at Five Years: Assessing Accomplishments and Challenges* (Hearing, 14 December 2017) https://www.govinfo.gov/content/pkg/CHRG-115jhrg28314/html/CHRG-115jhrg28314.htm accessed 5 August 2026.

[146] HM Government, *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World* (CP 811, 2023).

[147] US Department of the Treasury, 'Treasury Expands and Intensifies Sanctions against Russia' (24 February 2023) https://home.treasury.gov/news/press-releases/jy1296 accessed 31 July 2026.

[148] Franklin De Vrieze, *The Magnitsky Sanctions and the Politics of Individual Accountability* (Westminster Foundation for Democracy 2020).

[149] Antony J Blinken, 'Promoting Accountability for Human Rights Abuse with Our Partners' (US Department of State, 22 March 2021) https://2021-2025.state.gov/promoting-accountability-for-human-rights-abuse-with-our-partners/ accessed 31 July 2026.

In conclusion, while the Magnitsky Act represents a significant stride in countering gross human-rights violations, its usefulness against economic warfare is circumscribed by notable limitations. Economic warfare tactics, particularly those leveraging digital platforms and transnational financial networks, require a legal response that transcends national boundaries and individual cases. This necessitates a legal framework that is both globally cohesive and adaptable to the evolving landscape of economic threats; the Act is neither. Furthermore, the Act's current framework, primarily tailored to address gross human-rights violations and corruption,[150] only partially intersects with the broader spectrum of economic warfare. Additional legislation must specifically target the complex mechanisms of economic warfare. Such legislation must act, not as a vague overarching tool subject to arbitrary application, but as a precise, well-defined instrument. It should serve the dual purpose of deterring economic aggression and filling the gaps left by outdated international laws, thereby reinforcing the global legal architecture against the nuanced and evolving forms of economic threats. A new legislative act, complementary to the Magnitsky Act, yet distinct in its focus on the intricacies of economic warfare, is crucial for an effective and holistic legal response in the international arena.

[150] US Department of the Treasury, 'Treasury Targets Individuals Involved in the Sergei Magnitsky Case and Other Gross Violations of Human Rights in Russia' (20 December 2017) https://home.treasury.gov/news/press-releases/sm0243 accessed 31 July 2026.

5. Limitations of Current Policy: Reasons for Specific Legislation on Economic Warfare

5.1 Introduction

In contemporary international relations, the lines between traditional warfare and economic warfare are increasingly blurred. While the Sanctions and Anti-Money Laundering Act 2018 (SAMLA 2018)[151] and the Sergei Magnitsky Rule of Law Accountability Act of 2012 (Magnitsky Act)[152] represent significant strides in addressing aspects of economic warfare, they also underscore the limitations of existing legal frameworks in effectively managing the complex dynamics of modern economic conflicts. This chapter examines those limitations against the corporate, cyber and jurisdictional forms identified above, and asks which defects require specific legislation rather than the further extension of a sanctions instrument drawn for another purpose.

The evolving dynamics of global conflict, with a growing emphasis on economic and cyber warfare, necessitate a critical reassessment of the UK's legal framework. While SAMLA 2018 marks a significant stride in sanctioning capabilities post-Brexit, its limitations are evident when contrasted with the challenges of modern economic warfare. Additionally, the Global Human Rights Sanctions Regulations 2020,[153] which are the UK's adaptation of Magnitsky-style sanctions, target individuals involved in human rights abuses but do not specifically address the broader complexities of economic warfare. The Magnitsky Act of 2012 itself, while significant, also reveals critical gaps in its legal framework upon inspection, with these acts, primarily focused on sanctions and human rights violations, not comprehensively addressing the multifaceted nature of economic warfare. This chapter critically examines these gaps and proposes a tailored legal approach for the UK, emphasising the need for a dynamic and inclusive legal policy.

5.2 Limitations of Current Frameworks

5.2.1 Scope and Jurisdictional Reach

SAMLA 2018 and the Magnitsky Act, while instrumental in their respective domains, are limited by their jurisdictional and thematic focus. SAMLA 2018, which primarily addresses the UK's sanctioning capabilities post-Brexit, and the Global Human Rights Sanctions Regulations 2020 are limited in jurisdictional scope, failing to address the transnational nature of economic warfare effectively. Similarly, the Magnitsky Act, although impactful, is narrowly tailored to address human rights violations and corruption associated with specific cases, rather than the broader spectrum of economic warfare tactics.

5.2.2 The Nuances of Economic Warfare

Economic warfare encompasses a wide array of tactics, from sanctions and trade embargoes to cyber-attacks and currency manipulation. The existing legal frameworks, as delineated by SAMLA 2018 and the Magnitsky Act, are not sufficiently equipped to address the entirety of this spectrum. For instance, while these acts allow for the imposition of sanctions and address financial crimes, they offer limited tools for confronting indirect economic warfare tactics, such as cyber-attacks on critical financial infrastructure, currency manipulation, and the use of third-party proxies; tactics increasingly employed in economic warfare.

[151] Sanctions and Anti-Money Laundering Act 2018.

[152] Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012 (n 3).

[153] Global Human Rights Sanctions Regulations 2020, SI 2020/680.

5.2.3 Political and Diplomatic Implications

The use of economic warfare tools, such as sanctions, can have significant political and diplomatic repercussions.[154] While intended to exert pressure on target states or entities, they can also strain international relations and provoke retaliation. The unilateral nature of these tools, as evidenced in SAMLA 2018, can lead to conflicts with international allies and complicate multilateral efforts to address global security threats. In some instances, it may be wise for a country to ignore the acts of another sovereign nation to preserve order or if clandestine retaliation is considered a better course of action. In a situation where one country has hacked the electrical grid of another nation, it may be preferable to allow this to go unchallenged so that the injured State may act in kind. The problem here is that although this action may be rational when dealing with countries, and thus having direct legislation addressing it may seem unnecessary, when these acts can be committed by an individual or group it becomes much more difficult to balance one's losses.

5.2.4 Enforcement and Jurisdictional Challenges

The enforcement of sanctions and regulations outlined in SAMLA 2018 and the Magnitsky Act faces significant challenges. These include the difficulty in tracing illicit financial flows, the complexities of international cooperation in enforcement, and jurisdictional limitations. Non-state actors, who increasingly participate in economic warfare, often exploit these challenges, operating in the shadows of the global financial system. These entities are often for hire and without specific geographical allegiance.

5.2.5 Post-submission Legislation: Cyber Resilience Is Not Economic-warfare Response

The legislative field has moved since submission. As at 5 August 2026, the Cyber Security and Resilience (Network and Information Systems) Bill had completed its Commons stages, received its second reading in the House of Lords and was awaiting Lords committee stage; the current text was HL Bill 32, as brought from the Commons on 17 June 2026.[155] It would amend the Network and Information Systems Regulations 2018, extend the regime to additional essential and digital dependencies, including relevant managed service providers and data centres, strengthen regulatory powers and revise incident reporting. It is subsequent material and is not placed here as though available on 31 January 2024.

The Bill vindicates an important part of the submitted proposal. Its reporting model requires a light-touch initial notification within twenty-four hours and a fuller report within seventy-two hours. It is intended to capture ransomware, spyware and pre-positioning where likely significant impact exists even though disruption has not yet occurred, and to give the NCSC the incident information at the same time as the competent regulator.[156] That is substantially stronger than a rule which waits until an essential service has already failed, and it confirms the dissertation's contention that the State cannot assemble a national threat picture from voluntary disclosure made after commercial or physical harm is complete.

Yet the Bill does not displace the proposed Economic Warfare Prevention and Response Act. Its object is the security and resilience of systems used or relied upon for essential activities; it regulates the duties of entities and the competence of sectoral regulators. It does not create a general statutory classification of economic warfare, determine when corporate or private support becomes hostile

[154] Gordon (n 35).

[155] Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 32 (2026–27); UK Parliament, 'Cyber Security and Resilience (Network and Information Systems) Bill' https://bills.parliament.uk/bills/4035 accessed 5 August 2026.

[156] Department for Science, Innovation and Technology, 'Incident Reporting' (Cyber Security and Resilience (Network and Information Systems) Bill factsheet, updated 30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/incident-reporting accessed 5 August 2026.

participation, supply a common attribution process for proxy campaigns, or establish the response ladder proposed in Chapter 6. It is principally a resilience and reporting measure, not a code for identifying and answering the foreign State, financier, contractor or autonomous infrastructure behind the incident.

The difference is not semantic. A water operator which fails to report a compromise and a foreign service which paid for that compromise have committed different wrongs. The first may have breached a resilience duty; the second may have carried out or directed hostile action. A complete system requires both laws, with information capable of lawful transfer from the regulatory report to the attribution body and with safeguards preventing commercially sensitive reports from becoming public accusations before verification. The later Bill consequently narrows, but does not remove, the legislative gap diagnosed by this dissertation.

5.3 Conclusions and Recommendations

5.3.1 UK-specific Policy on Economic Warfare

Conclusion: The UK's vulnerability to economic warfare, originating from both state and non-state actors, is heightened by existing legislative loopholes. These gaps expose the UK to diverse threats, including sanctions evasion, financial terrorism, and cyber-attacks.

Recommendation: Formulate a comprehensive UK-centric policy on economic warfare. This policy should not only align with international laws, such as those set by the UN Security Council, but also include specific guidelines addressing the UK's unique economic and security needs. It should close existing legal gaps while being adaptable to evolving economic warfare tactics.

5.3.2 Targeting Indirect Perpetrators and Funding Sources

Conclusion: The current legal framework is inadequate in addressing the growing trend of indirect economic warfare methods, such as financing third parties or using proxies, which pose significant challenges in tracing and accountability.

Recommendation: Develop legal provisions that hold both direct and indirect perpetrators accountable, including financiers and facilitators. This inclusive approach should apply uniformly to individuals, groups, and states, ensuring comprehensive coverage under the law.

5.3.3 Adaptability to Emerging Threats in Economic and Cyber Warfare

Conclusion: The rapidly changing landscape of economic and cyber warfare, marked by the emergence of new tactics and technologies, demands a legal framework that can evolve accordingly.

Recommendation: Design an economic warfare policy that is broad in scope and inherently adaptable. Regular reviews and updates should be mandated to ensure the policy remains relevant and effective in a fast-changing environment, keeping pace with technological advancements and shifts in warfare tactics.

5.4 Summative Remarks

The current UK legislative framework's limitations in the context of economic warfare underscore the pressing need for specific, comprehensive, and flexible legal measures. These measures should be capable of addressing the complexities of contemporary economic conflicts.

Implementing a tailored, dynamic legal framework is crucial for the UK to effectively safeguard its economic integrity and national security. This framework should be robust yet adaptable, capable of countering the diverse and evolving threats of economic warfare.

6. Addressing Economic Warfare: Legal Strategies and Policies

6.1 Introduction

The definition of economic warfare must be broadened beyond both its traditional confines and the understanding developed since the American Civil War. The utilisation of personal assets has never before held such potential, or such potentially devastating ramifications. This presents unique challenges to the current international legal framework. As illustrated by Elon Musk's involvement in the Russia–Ukraine conflict,[157] individual actors with significant economic power and influence can have a profound impact upon international conflicts. With the rise of groups such as REvil and Anonymous Sudan, however, the disposable income required to represent a threat is diminishing. There is a notable absence of a comprehensive legal framework to regulate the actions of individuals,[158] groups or States partaking in this type of economic warfare, demarcated by its use of third parties, proxies and personal wealth. In line with the discussion in Chapter 1 concerning third-party financiers and proxies, the recommendations must extend beyond traditional direct perpetrators. The proposed legal provisions therefore encompass direct and indirect modes of economic aggression, aligning the remedy with the modern methods identified throughout the dissertation. This chapter proposes a foundational legal framework, capable of enactment by the United Kingdom, to regulate the use of economic means to obfuscate responsibility under international law. The cyber analysis in Chapter 3 demonstrates the United Kingdom's vulnerability in its digital economic infrastructure. The proposed policy answers the corresponding gaps in cybersecurity measures and protocols,[159] thereby fortifying the country's resilience against cyber-economic attack.

6.2 The UK Economic Warfare Prevention and Response Act

An Act to address the evolving nature of economic warfare, to fill legal gaps in current legislation, and to protect the United Kingdom's economic, infrastructural and security interests, domestically and abroad.

6.2.1 Purpose and Definitions

The proposed Act should apply to direct and indirect conduct intended, known or reasonably foreseen to coerce, disable or materially destabilise the United Kingdom, a protected person, an allied operation or protected critical functions by economic, financial, technological or cyber means. "Economic warfare" should include the financing, commissioning, facilitation or concealment of such conduct and the deliberate provision of indispensable infrastructure, but should exclude lawful competition, industrial action, journalism, academic research, good-faith security testing and political advocacy. A wide purpose without express exclusions would become the vague catch-all instrument which this dissertation rejects.

"Protected critical functions" should include energy, water, health, food, finance, communications, transport, electoral administration, emergency services, defence and those supply-chain services whose loss is capable of disabling them. "Controller" should include a person who supplies the objective, finance or essential infrastructure and possesses the practical power to prevent, suspend or materially

[157] Marina Hyde, 'And Then Elon Musk Said There'll Be No More War—Not via His Satellite' *The Guardian* (8 September 2023) https://www.theguardian.com/commentisfree/2023/sep/08/elon-musk-satellite-war-starlink-system-ukraine accessed 31 July 2026; Victoria Kim, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' *The New York Times* (8 September 2023) https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html accessed 31 July 2026.

[158] Lanovoy (n 41).

[159] Green (n 97) ch 5.

alter the operation. “Indirect actor” should include a financier, broker, PMSC, cyber contractor, corporate vehicle or knowing infrastructure provider. Liability should require an expressly defined mental element proportionate to the consequence: intention or knowledge for the principal offence; recklessness only for tightly confined aggravated facilitation; and civil reporting liability where an organisation, without reasonable excuse, fails to perform a prescribed duty.

6.2.2 Direct, Indirect and Attributed Responsibility

The Act should apply to perpetrators and to those who commission, direct, finance or knowingly facilitate economic warfare. It should not declare a foreign State criminally liable in a domestic court contrary to rules of immunity; it should authorise evidence collection, individual or entity designation, civil restraint and a formal recommendation for inter-State measures. Corporate liability should attach where senior management authorised or connived in conduct, or where a failure to prevent offence is proved subject to reasonable-procedures defence. The statute should permit aggregation of mutually supporting acts where there is proof of common purpose, coordinated campaign or common controller, but should forbid aggregation by nationality alone.

Jurisdiction should extend to conduct in the United Kingdom, conduct by United Kingdom persons abroad, conduct against protected United Kingdom systems, and foreign conduct producing or intended to produce substantial and foreseeable effects in the United Kingdom. A sufficient nexus and the Attorney General’s consent should be required for prosecution of wholly foreign conduct. Evidence gathered abroad should be received subject to ordinary rules of fairness, disclosure, reliability and public-interest immunity; intelligence may initiate restraint but should not alone sustain final criminal conviction unless lawfully disclosed or replaced by admissible proof.

6.2.3 Mandatory Reporting and the Centralised Database

Every operator of protected critical functions, and every business meeting a proportionate statutory threshold, should report a material cyber incident to a designated national authority. An initial notice should be required as soon as practicable and, save where prevented by operational necessity, within twenty-four hours for a critical-function incident and seventy-two hours for other material incidents. The first notice should be short: affected function, time detected, present operational effect, suspected persistence and contact point. A fuller report should follow as evidence becomes available. The duty should not require a victim to delay containment whilst lawyers perfect a narrative.

The authority should maintain a centralised, access-controlled incident database capable of correlating infrastructure, malware, payments, indicators, targeted functions and jurisdictional routes. Identifiable personal, commercially sensitive and security-classified material should be separated, minimised and retained for stated periods. Reports made for collective defence should receive carefully drawn protection against public disclosure and collateral regulatory use, without granting immunity for deliberate misconduct or preventing the use of independently obtained evidence. An organisation which conceals an incident, destroys relevant material or knowingly files a false report should face proportionate civil penalties and, for deliberate obstruction, criminal liability.

Small and medium-sized enterprises should receive reporting templates, emergency technical support and a safe channel through which to seek assistance. Public education and sector exercises are not ornaments: a reporting obligation which regulated persons cannot understand will produce delay and defensive silence. The database should also support sanitised warnings to industry and structured information-sharing with foreign partners under agreements governing purpose, security, onward disclosure and redress.

6.2.4 Rapid Attribution and Decision Structure

Speed is a substantive part of defence. Upon a serious incident the proposed Economic Warfare Response Authority should convene a joint cell including the NCSC, National Crime Agency, intelligence agencies, police, defence representatives, HM Treasury, the Foreign, Commonwealth and Development Office and the affected regulator. The cell should produce a tiered assessment which separates: technical attribution; identification of natural and corporate actors; legal attribution to a State; confidence level; contrary evidence; present capability; and maximum reasonably credible and foreseeable harm.

Where delay would materially increase loss, the Prime Minister or a designated Secretary of State, acting through the National Security Council machinery, should be permitted to authorise urgent non-forcible protective measures upon recorded reasons. These may include compulsory preservation notices, emergency isolation of government systems, financial restraint, suspension of specified public contracts, blocking of malicious infrastructure where domestic law and territorial jurisdiction permit it, requests for foreign assistance and temporary directions to critical operators. The Attorney General should certify the asserted legal basis for measures extending beyond ordinary incident response. Operational reasons may be classified, but the decision, legal basis, confidence level and anticipated civilian effects must be recorded at the time rather than reconstructed afterwards.

Urgency does not require paralysis by prior parliamentary debate; neither does it require unreviewable power. A designated judicial commissioner should review intrusive domestic measures within seventy-two hours. Ministers should notify an appropriate parliamentary committee as soon as security permits and ordinarily within seven days, with a classified annex where necessary. Continuing measures should lapse unless renewed upon current evidence. The Investigatory Powers Commissioner, courts and Parliament already demonstrate that rapid executive action and serious ex post scrutiny are not opposites.

6.2.5 Response Ladder and the Use of Force

The Act should authorise a response ladder: assistance and hardening; evidence preservation and criminal process; retorsion; targeted financial and travel measures; coordinated diplomatic and economic restrictions; lawful countermeasures; and, at the outer threshold, a recommendation to use force. Each rung must have its own legal gateway. The statute may supply domestic authority and decision procedure, but it cannot amend the United Nations Charter, turn a crime into an armed attack or make internationally unlawful force lawful.

Non-forcible countermeasures should be directed towards inducing compliance, be proportionate to the injury and, so far as circumstances permit, follow a demand for cessation and notice. They must not affect the prohibition of force, fundamental human rights or applicable humanitarian obligations.[160] A cyber measure operating in another State's territory therefore requires a distinct analysis of sovereignty, intervention, necessity, consent and countermeasures; the Act should not hide those questions beneath the word "pre-emptive".

Military force should remain available for consideration where a cyber or economically facilitated operation constitutes an actual or imminent armed attack and force is necessary and proportionate in self-defence, or where the Security Council authorises it. The decision should examine attribution, immediacy, continuing capability, feasible non-forcible alternatives, anticipated civilian harm and the consequences of striking dual-use infrastructure. The measure of the initiating operation should include its maximum reasonably credible and foreseeable harm. Thus an interrupted attempt to disable an NHS data and treatment network, water-control system or winter energy grid may be graver than the

[160] International Law Commission (n 53) arts 49–54, especially art 50(1)(a).

immediate outage reveals; successful mitigation should not reward the aggressor by legally erasing the deaths which the operation was capable, intended and close to producing.

Deterrence is relevant to the choice between measures which are otherwise lawful, necessary and proportionate. It is not, alone, a Charter basis for punitive force after danger has passed. Where an identified individual, PMSC unit or autonomous system operates from a discrete location and broad sanctions would burden a population without influencing the actor, direct action against the responsible capability may be strategically preferable. Yet a person does not lose human rights or become an "object of war" by violating a social contract. In armed conflict the lawful target is a combatant, a member of an organised armed group with a continuous combat function, a civilian for such time as directly participating in hostilities, or an object making an effective contribution to military action whose neutralisation offers a definite military advantage.[161] Outside armed conflict, lethal force remains governed by the more restrictive law-enforcement and human-rights framework except where the law of self-defence between States is engaged and IHL becomes applicable. A server room is not targetable because it contains an offender; a specific node may become a military objective only upon the facts and subject to distinction, proportionality in attack and feasible precautions.

6.2.6 Adaptability, Review and International Collaboration

The Act should require annual technical schedules capable of amendment, but Parliament must retain the elements which define liability, coercive power and the force decision. An independent reviewer should report yearly upon use, false positives, unequal sectoral burdens, designation challenges, civilian effects and technological evasion. A fuller statutory review should occur every three years. Sunset clauses should apply to exceptional emergency powers, not to the reporting and assistance architecture upon which accumulated knowledge depends.

The United Kingdom should negotiate reciprocal arrangements for preservation requests, rapid technical assistance, secure federated search and evidential handover. International collaboration must not become indiscriminate transfer. Each arrangement should specify permitted purpose, authentication, data minimisation, audit, onward disclosure and the procedure by which erroneous indicators are corrected. The object is to prevent a financier, contractor or autonomous system from defeating responsibility merely by dividing its operation amongst several States, whilst preserving the very legality which the proposed statute exists to defend.

6.2.7 Illustrative Reporting Policy

The original proposal for a National Cybersecurity Incident Reporting Act is incorporated within the wider UK-EWPRA. Its key provisions remain: mandatory reporting; defined twenty-four- and seventy-two-hour time frames; staged details; a centralised cyber-incident database; confidentiality and data protection; proportionate penalties; support and resources; public awareness and education; and international collaboration. The refinement is institutional rather than ideological. Reporting becomes the evidential foundation of attribution and rapid defence, not a detached compliance exercise.

6.3 Critical Review

The proposed UK Economic Warfare Prevention and Response Act (UK-EWPRA), as discussed, raises several critical considerations for international trade and economic activity. Its broad definition of economic warfare, including both direct and indirect actions (Chapter 6, UK-EWPRA Provisions), presents a robust framework against a range of economic threats. However, this expansive scope may

[161] Protocol I (n 17) arts 48, 51(3), 52(2) and 57; ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (2009) https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc-002-0990.pdf accessed 5 August 2026.

inadvertently affect legitimate global economic engagements, increasing regulatory compliance for businesses and possibly slowing down international transactions due to enhanced scrutiny. This is particularly pertinent given the Act's commitment to address the challenges posed by state and non-state actors (Chapter 6, UK-EWPRA Introduction).

Furthermore, the Act's extensive jurisdictional reach could lead to potential diplomatic tensions, as its provisions might intersect with the economic interests of other nations (Chapter 6, Jurisdictional Reach and Enforcement). The dynamic nature of the Act, while essential for adapting to evolving threats, introduces an element of uncertainty in international economic relations, impacting trade stability and investment planning (Chapter 6, Adaptability and Review).

Despite these challenges, the strategic importance of UK-EWPRA in safeguarding national economic security is undeniable. The Act's comprehensive approach to economic warfare, especially in the contemporary context of cyber threats and global financial manipulations, is a crucial step in protecting the UK's economic interests. It represents a necessary response to the multifaceted nature of modern economic aggression, as highlighted throughout the text.

However, the implications of UK-EWPRA on international trade and economic relations underscore the need for a balanced approach. While the benefits of a robust legal framework against economic warfare are significant, the potential costs to international trade dynamics cannot be overlooked. This necessitates deeper analysis and debate, particularly in the context of ensuring that the Act aligns with international legal standards and facilitates, rather than impedes, legitimate international economic activities. Therefore, while acknowledging the benefits of the proposed Act, it is essential to engage in further comprehensive discussions to refine its provisions and minimise unintended impacts on global economic interactions.

6.4 Conclusion

In this chapter, we have advocated for the UK Economic Warfare Prevention and Response Act (UK-EWPRA) as a necessary legal framework to address the complexities of contemporary economic warfare, including cyber threats. This Act, with its broad coverage of both direct and indirect economic aggressions, is vital for protecting the UK's economic interests. However, its implementation must be carefully balanced against the potential impact on international economic activities. Ongoing refinement and adaptation of the Act are essential to ensure that it remains effective and aligned with the evolving global economic and security landscape. The goal is to maintain a strong defence against economic threats while supporting healthy international trade and cooperation.

7. Conclusion

7.1 Reflective Analysis

The proposed policies and legislative changes in the text aim to address the complexities of modern economic warfare, particularly highlighting the roles of various actors like states, non-state actors (including hackers), private military and security companies (PMSCs), and multinational corporations (MNCs). However, these policy and legislative changes, while forward-looking, encounter several potential weaknesses and objections.

Firstly, the text acknowledges the blurring lines between traditional warfare and economic warfare, advocating for comprehensive legal frameworks to address these evolving threats. However, a potential weakness lies in the broad definitions and scope of what constitutes economic warfare. The proposed policies might face challenges in accurately identifying and categorising actions as economic warfare, especially in a rapidly evolving global landscape where economic aggression can be subtle and indirect.

The emphasis upon the role of PMSCs in Chapter 6, while crucial, might overlook the complex legal status and diverse modes of operation of these entities.[162] The existing international legal framework, including the Geneva Conventions and the UN Mercenary Convention, provides a somewhat narrow definition of mercenaries, which may not fully encompass the modern operations of PMSCs. The proposed policies need to ensure that they can effectively regulate PMSCs,[163] balancing the need for accountability and the practical aspects of their operations in diverse conflict scenarios.

The discussion around the SAMLA 2018[164] and the Magnitsky Act in addressing economic warfare also raises concerns. These Acts, while significant, may not fully capture the complexities of economic warfare, particularly in terms of jurisdictional reach and enforcement. Economic warfare often involves transnational activities, and unilateral sanctions or legal actions might not be sufficient or effective in a global context. Additionally, the Acts' focus on financial crimes and human rights abuses might not encompass other forms of economic aggression, such as cyber-attacks on financial systems or currency manipulation.

Furthermore, the text's call for specific legislation on economic warfare, particularly cyber-economic warfare, is commendable. However, it must be acknowledged that creating and enforcing such legislation poses significant challenges. The dynamic and borderless nature of cyberspace, combined with the rapid pace of technological advancements, makes it difficult to develop legislation that remains relevant and enforceable.

The proposal for a UK-centric policy on economic warfare also raises questions about international coordination and compatibility. Economic warfare is a global issue, and a UK-specific policy might need to be aligned with international laws and frameworks to be effective. This requires extensive international collaboration, which can be complex and time-consuming.

In conclusion, while the proposed policy and legislative changes are a step in the right direction towards addressing modern economic warfare, they must contend with challenges related to broad definitions, legal ambiguities, jurisdictional complexities, and the need for international cooperation. The effectiveness of these policies will depend on their ability to adapt to the evolving nature of economic warfare and to integrate with existing international legal frameworks.

[162] Sutherland (n 31).

[163] Jäger and Kümmel (n 55).

[164] Sanctions and Anti-Money Laundering Act 2018.

7.2 Final Remarks

The rapid increase in individual wealth and technological advancements in recent years has democratised the means of economic warfare, making the developed North more vulnerable to these practices. While historically, economic warfare was predominantly waged by States, the rise of ultra-wealthy individuals, multinational corporations, and non-state actors equipped with advanced technology has expanded the range of actors capable of engaging in economic-warfare tactics.

Wealth Concentration: The concentration of wealth in the hands of ultra-wealthy individuals and private entities means that they now possess financial power that, in some cases, rivals that of nation-States. These actors can leverage their wealth to influence global markets, manipulate currencies, fund adversarial groups, or engage in economic sabotage, all of which can have significant implications for the economies of countries in the developed North. For example, a wealthy individual or private entity could strategically invest in, or divest from, certain sectors of a developed country's economy to destabilise its financial markets.

Technological Advancements: Advancements in technology have enabled new forms of economic warfare that can be waged by a broader range of actors. For example, cyber-attacks on critical infrastructure, financial systems, or key industries can be carried out by non-state actors, such as hacktivist groups or criminal organisations, with potentially devastating consequences for the economies of the developed North. Similarly, the rise of cryptocurrencies and other digital assets provides new tools for economic manipulation that can be exploited by a wider range of actors.

Globalisation: The interconnectedness of the global economy means that actions taken by actors in one part of the world can have ripple effects across the globe. For example, a wealthy individual or private entity in a developing country could engage in economic-warfare tactics that destabilise the global supply chain, affecting the economies of the developed North. Similarly, the proliferation of digital platforms and social media has made it easier for disinformation campaigns, another form of economic warfare, to be waged by non-state actors from anywhere in the world.

Legal Grey Areas: The existing legal and regulatory frameworks are ill-equipped to deal with the challenges posed by the democratisation of economic warfare. Many of the tactics employed by non-state actors fall into legal grey areas, making it difficult to hold them accountable for their actions. For example, while there are international conventions that specifically regulate the actions of States in times of conflict, there is no comprehensive equivalent framework that regulates the actions of State and non-state actors engaged in economic warfare.

In conclusion, the increase in individual wealth and technological advancements has created a situation where the developed North is at greater risk of economic-warfare practices from a broader range of actors. The democratisation of economic warfare means that not only States but also ultra-wealthy individuals, private entities, and non-state actors equipped with advanced technology can engage in economic-warfare tactics that destabilise the economies of the developed North.

It is crucial for the developed North to be aware of these emerging threats and to develop strategies and regulatory frameworks to mitigate their impact.

Bibliography

—— ‘Anonymous Hackers Declare War on Islamic State’ *Sky News* (16 November 2015) https://news.sky.com/story/anonymous-hackers-declare-war-on-islamic-state-10339388 accessed 31 July 2026

—— ‘OpSacred 2017: Financial Institutions to Face Anonymous-Driven DDoS Attacks’ (Data Foundry, 12 June 2017) https://www.datafoundry.com/blog/opsacred-ddos-attacks-anonymous-2017 accessed 31 July 2026

—— ‘The Pirate Bay Files Charges against Media Companies’ *TorrentFreak* (24 September 2007) https://torrentfreak.com/the-pirate-bay-files-charges-against-media-companies-070924/ accessed 31 July 2026

Boyle A and Chinkin C, *The Making of International Law* (OUP 2007)

Bruetsch N, ‘Market for Force: The Emerging Role of Private Military and Security Companies in Non-Traditional Fields’ (The Security Distillery, 10 April 2021) https://thesecuritydistillery.org/all-articles/market-for-force-the-emerging-role-of-private-military-and-security-companies-in-non-traditional-fields accessed 31 July 2026

Cerone J, ‘Wiwa v Shell: The $15.5 Million Settlement’ (2009) 13(14) *ASIL Insights* https://asil.org/insights/volume-13-issue-14/ accessed 31 July 2026

Clapham A and Gaeta P (eds), *The Oxford Handbook of International Law in Armed Conflict* (OUP 2014)

Cronogue G, ‘Rebels, Negligent Support, and State Accountability: Holding States Accountable for the Human Rights Violations of Non-State Actors’ (2013) 23 *Duke Journal of Comparative & International Law* 365

De Vrieze F, *The Magnitsky Sanctions and the Politics of Individual Accountability* (Westminster Foundation for Democracy 2020)

Dewdney AK, ‘Computer Recreations: Of Worms, Viruses and Core War’ (1989) 260(3) *Scientific American* 110

Dinstein Y, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, CUP 2010)

Eckert AE, *Outsourcing War: The Just War Tradition in the Age of Military Privatization* (Cornell University Press 2016)

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

Franceschi-Bicchierai L, ‘Russian Zero-Day Seller Offers $20m for Hacking Android and iPhones’ *TechCrunch* (27 September 2023) https://techcrunch.com/2023/09/27/russian-zero-day-seller-offers-20m-for-hacking-android-and-iphones/ accessed 31 July 2026

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

Green JA (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015)

Greenberg K, ‘Anonymous Sudan’s Attack on European Investment Bank: Money, Politics and PR’ *TechRepublic* (26 June 2023) https://www.techrepublic.com/article/anonymous-sudan-attacks-european-investment-bank/ accessed 31 July 2026

Guchua A, Zedelashvili T and Giorgadze G, ‘Geopolitics of the Russia–Ukraine War and Russian Cyber Attacks on Ukraine–Georgia and Expected Threats’ (2022) 10 *Ukrainian Policymaker* 27

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

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

Hern A, ‘Anonymous Claims Victory over Jihadi Twitter Accounts in #OpIsis’ *The Guardian* (10 February 2015) https://www.theguardian.com/technology/2015/feb/10/anonymous-claims-victory-over-jihadi-twitter-accounts-in-opisis accessed 31 July 2026

Hyde M, 'And Then Elon Musk Said There'll Be No More War—Not via His Satellite' *The Guardian* (8 September 2023) https://www.theguardian.com/commentisfree/2023/sep/08/elon-musk-satellite-war-starlink-system-ukraine accessed 31 July 2026

Isaac A and Lawson A, 'Sellafield Nuclear Site Hacked by Groups Linked to Russia and China' *The Guardian* (4 December 2023) https://www.theguardian.com/business/2023/dec/04/sellafield-nuclear-site-hacked-groups-russia-china accessed 31 July 2026

Jäger T and Kümmel G (eds), *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects* (VS Verlag 2007)

Kello L, 'Cyber Legalism: Why It Fails and What to Do about It' (2021) 7(1) *Journal of Cybersecurity* tyab014

Khaitan A, 'Anonymous Sudan Attacks UAE Banks: Cybersecurity Breach Raises Concerns' *The Cyber Express* (12 May 2023) https://thecyberexpress.com/uae-banks-cyber-attack-by-anonymous-sudan/ accessed 31 July 2026

Kim V, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' *The New York Times* (8 September 2023) https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html accessed 31 July 2026

King CR, 'Revolutionary War, Guerrilla Warfare, and International Law' (1972) 4 *Case Western Reserve Journal of International Law* 91

Kozłowski A, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan' (2014) 3 *European Scientific Journal* (special edn) 237

Lanovoy V, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 *European Journal of International Law* 563

Libicki MC, Senty D and Pollak J, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (RAND Corporation 2014) https://www.rand.org/pubs/research_reports/RR430.html accessed 5 August 2026

Louderback J, 'Inside the Attack that Crippled Revision3' (Revision3, 29 May 2008)

Lowe V and Tzanakopoulos A, 'Economic Warfare' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2012)

Mayer J, 'Government Hacking' (2018) 127 *Yale Law Journal* 570

Miller C, Scott M and Bender B, 'How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare' *Politico* (9 June 2022) https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039 accessed 31 July 2026

Nutt D, 'Economic Sanctions Evolved into Tool of Modern War' *Cornell Chronicle* (11 January 2022) https://news.cornell.edu/stories/2022/01/economic-sanctions-evolved-tool-modern-war accessed 31 July 2026

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

Ohlin JD, Govern K and Finkelstein C (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015)

Olovson N, *Hacking for the State? The Use of Private Persons in Cyber Attacks and State Responsibility* (Master's thesis, Swedish Defence University 2020) https://www.diva-portal.org/smash/record.jsf?pid=diva2:1577790 accessed 31 July 2026

Pałka W, *The Awakening of Private Military Companies* (Warsaw Institute 2020)

Pingeot L, *Dangerous Partnership: Private Military and Security Companies and the UN* (Global Policy Forum and Rosa Luxemburg Stiftung 2012) https://www.globalpolicy.org/en/publication/dangerous-partnership accessed 5 August 2026

Poulsen K, 'Former Teen Hacker's Suicide Linked to TJX Probe' *Wired* (9 July 2009) https://www.wired.com/2009/07/hacker-3/ accessed 31 July 2026

Rodenhäuser T, 'The Legal Boundaries of (Digital) Information or Psychological Operations under International Humanitarian Law' (2023) 100 *International Law Studies* 536

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

Russell M, *Global Human Rights Sanctions* (European Parliamentary Research Service, PE 698.791, 2021) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698791/EPRS_BRI(2021)698791_EN.pdf accessed 31 July 2026

Russon M-A, 'NHS: Millions of Medical Devices in UK Hospitals Are Completely Unprotected against Hackers' *Evening Standard* (23 June 2023) https://www.standard.co.uk/tech/nhs-medical-devices-cyber-attack-hackers-b1089559.html accessed 31 July 2026

Singel R, 'MediaDefender Emails Reveal Secret Government Project' *Wired* (18 September 2007) https://www.wired.com/2007/09/mediadefender-emails-reveal-secret-government-project/ accessed 31 July 2026

—— 'MediaDefender DDoS Attack Took Down Revision3' *Wired* (29 May 2008) https://www.wired.com/2008/05/mediadefender-d/ accessed 31 July 2026

Solis GD, *The Law of Armed Conflict: International Humanitarian Law in War* (2nd edn, CUP 2016)

Sutherland B (ed), *Modern Warfare, Intelligence and Deterrence: The Technologies that Are Transforming Them* (Profile Books 2011)

Teo CH, *The Acme of Skill: Nonkinetic Warfare* (Wright Flyer Paper No 30, Air University Press 2008)

Trustwave SpiderLabs, 'KillNet, Anonymous Sudan, and REvil Unveil Plans for Attacks on US and European Banking Systems' (15 June 2023) https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/killnet-anonymous-sudan-and-revil-unveil-plans-for-attacks-on-us-and-european-banking-systems/ accessed 31 July 2026

Zand A and others, 'Demystifying DDoS as a Service' (2017) 55(7) *IEEE Communications Magazine* 14

Zorabedian J, 'Anonymous Declares War on Islamic State after Paris Attacks' (Sophos News, 16 November 2015) https://news.sophos.com/en-us/2015/11/16/anonymous-declares-war-on-islamic-state-after-paris-attacks/ accessed 31 July 2026