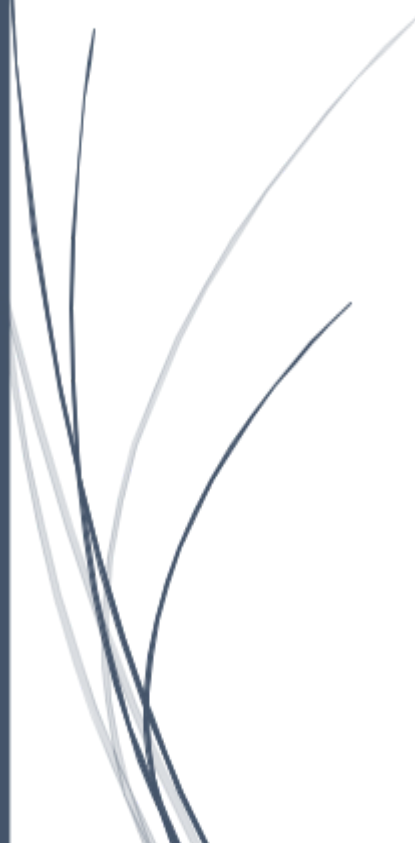


A dark blue vertical bar on the left side of the slide. A blue arrow points to the right from this bar, containing the date 1/31/2024.

1/31/2024

The need for the legal regulation of Economic warfare conducted by individual and state actors.

Economic Warfare: The Unregulated War

Several thin, curved, light blue lines that sweep upwards from the bottom left towards the center of the slide.

Christopher Farmer
The University of Worcester

Declaration

I hereby certify that this dissertation is the result of my own work except where otherwise indicated and due acknowledgement is given.

I also certify that this dissertation is 11000 words long excluding: the Bibliography, Footnotes, Acknowledgements, Abstract, Cases Cited, Legislation Cited and Nomenclature.

DATE OF SUBMISSION: 31/01/2024

SIGNED: Christopher I V Farmer

DATE: 31/01/2024

Title Page

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

Christopher I V Farmer

The University of Worcester

Dissertation submitted to the Faculty of Law at The University of Worcester for

the degree of Legum Magister LL.M

Autumn Term, 2022

Acknowledgements

I extend my deepest gratitude to Christopher Monaghan, whose scholarly mentorship and incisive critique have been the bedrock of this research endeavour. His unwavering commitment to academic excellence and meticulous guidance have profoundly shaped the analytical framework and intellectual rigor of this dissertation.

The generous financial patronage from the Farmer family has been instrumental in facilitating a comprehensive and meticulous exploration of the subject matter. Their support not only underscores the importance of this research but also reflects an unwavering belief in the academic value and potential impact of this work. Additionally, I extend my gratitude to the university's librarians, research assistants, and study participants, whose valuable insights and support, though brief, were instrumental to this project.

In the intricate tapestry of academic pursuit, the role of one's family cannot be overstated. To my wife and mother, I owe a profound debt of gratitude for their constant support and boundless patience. Finally, for the joy and inspiration derived from my daughter's presence, a beacon of light, providing both motivation and solace throughout this rigorous journey; there can be no words. This dissertation is not merely a reflection of my dedication but a testament to the collective wisdom, support, and faith of all the remarkable individuals who have contributed to its fruition.

Table of Contents

Declaration.....	1
Title Page.....	2
Abstract.....	7
Cases Cited.....	9
Legislation Cited.....	10
Dissertation Overview.....	11
Table 1:.....	11
Table 2:.....	11
1. Introduction.....	12
1. Objective.....	12
2. Defining the Legal Difference between Warfare and Economic Warfare.....	13
3. Definition and Characteristics of Warfare.....	14
1. PMSCs and Their Utilization.....	21
4. The individual and the state.....	25
2. The Case of Multinational Corporations and Conflict.....	28
1. Introduction.....	28
2. Case Studies.....	28
a. The Extractive Industry in the Democratic Republic of Congo (DRC).....	28
b. The Oil Industry in Nigeria.....	29
c. The Arms Trade in Yemen.....	29
3. The Need for Regulation.....	30
4. Conclusion.....	31
3. Economic Cyber-warfare: The twenty first century hidden war.....	32
1. Who is carrying out these attacks and why?.....	36

2.	Economic Cyber-Warfare urgency and Danger	40
3.	Conclusion	41
4.	Establishing precedent; internal legislation of note	43
1.	The Sanctions and Anti-Money Laundering Act 2018	43
2.	The Magnitsky Act	47
5.	Limitations of Current Policy: Reasons for Specific Legislation on Economic Warfare	52
1.	Introduction	52
2.	Limitations of Current Frameworks	54
	Scope and Jurisdictional Reach:	54
	The Nuances of Economic Warfare:	54
	Political and Diplomatic Implications:	55
	Enforcement and Jurisdictional Challenges:	55
3.	Conclusions and Recommendations	56
	UK-Specific Policy on Economic Warfare	56
	Targeting Indirect Perpetrators and Funding Sources	56
	Adaptability to Emerging Threats in Economic and Cyber Warfare	57
4.	Summative Remarks	57
6	Addressing Economic Warfare: Legal Strategies and Policies	58
1.	Introduction	58
	UK Economic Warfare Prevention and Response Act (UK-EWPRA)	59
1.	Preamble:	59
2.	Definitions For the purposes of this Act:	60
3.	Provisions	60
4.	Integration with International Law	62
5.	Implementation	62
6.	Further Recommendations	64
	Title:	64
	Purpose:	64

	Key Provisions:	64
1.	Mandatory Reporting:	64
2.	Reporting Time Frame:	64
3.	Details to be Reported:	64
4.	Centralized Cyber Incident Database:	65
5.	Confidentiality and Data Protection:	65
6.	Penalties and Compliance:	65
7.	Support and Resources:	65
8.	Public Awareness and Education:	65
9.	International Collaboration:	65
7.	Critical Review	66
8.	Conclusion	67
7.	Conclusion	68
1.	Reflective Analysis	68
2.	Final Remarks	70
	<i>Bibliography</i>	73
	<i>Books</i>	73
	<i>Articles</i>	75
	<i>Websites</i>	81
	<i>Journal</i>	83
	<i>Other Works</i>	85

Abstract / Executive Summary

This dissertation critically evaluates the evolving landscape of economic warfare, advocating for the development of a specialized international charter to regulate it. Recognizing economic warfare as an increasingly favored conflict mode utilized by both individual and state actors, this study examines the multifaceted legal, political, and ethical dimensions. It scrutinizes the efficacy of existing legal frameworks—such as the Sanctions and Anti-Money Laundering Act 2018 and the Sergei Magnitsky Act—underscoring their insufficiency in comprehensively addressing the modern spectrum of economic warfare tactics.

The research delves into the complexities of cyber-economic aggression, financial terrorism, and the strategic manipulation of economic tools, emphasizing the challenges posed by non-state actors and third-party proxies. To address these legislative voids, this study proposes a dynamic, adaptable legislative architecture: the UK Economic Warfare Prevention and Response Act (UK-EWPRA).

Designed within the UK context but potentially extendable globally, this proposed framework ensures extensive coverage of both direct and indirect economic warfare methods. Furthermore, the dissertation contends that continuous regulatory adaptation is imperative to keep pace with technological and strategic evolutions in algorithmic and cyber warfare.

Ultimately, this study presents a compelling case for legal innovation to bolster national and global economic integrity against escalating threats. It underscores the urgent necessity for robust, modern regulations to navigate the complex landscape of digital and economic conflict.

Cases Cited

UK

Campaign Against Arms Trade, R (On the Application Of) v Secretary of State for International Trade [2023] EWHC 1343

Campaign Against Arms Trade, R (On the Application Of) v The Secretary of State for International Trade [2019] EWCA Civ 1020

McKinnon v Government of the United States of America and another [2008] UKHL 59

US/Other

The Bermuda (1865) 70 US 514.

‘Resolution 53/18 (Syria) A/HRC/RES/53/18’ [2023] United Nations Human Rights Council

Prosecutor v Charles Ghankay Taylor SCSL-03-1-T

ICC, The Prosecutor v Ali Muhammad Ali Abd-Al-Rahman” Ali Kushayb” (2021) ICC-02/05-01/20 Lewis, P 11

R’ios Montt v Ministry of National Defense 2290-2007

Wiwa v. Royal Dutch Petroleum Company 226 F.3d 88 (2d Cir. 2000)

Legislation Cited

The Sanctions and Anti-Money Laundering Act 2018

Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law
Accountability Act 2012

Geneva Conventions Act 1957

Kellogg–Briand Pact 1928

Executive Order 13818 — Blocking the Property of Persons Involved in Serious
Human Rights Abuse or Corruption 2017

Hague Conventions of 1899 and 1907

Charter of the United Nations and Statute of the International Court of Justice 1945

Dissertation Overview

Table one shows the distinction between primary concepts of warfare that are widely accepted and the new concept we attempt to outline.

Table 1:

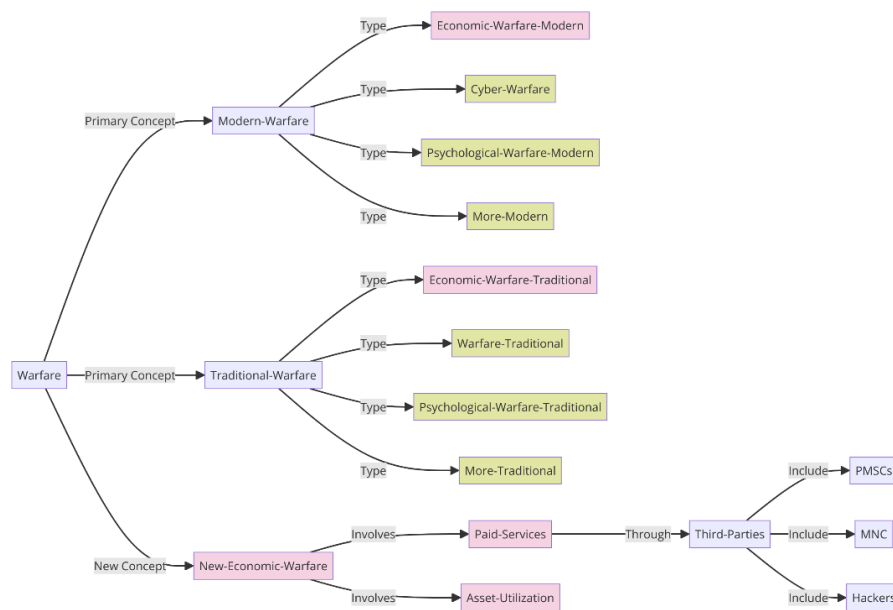
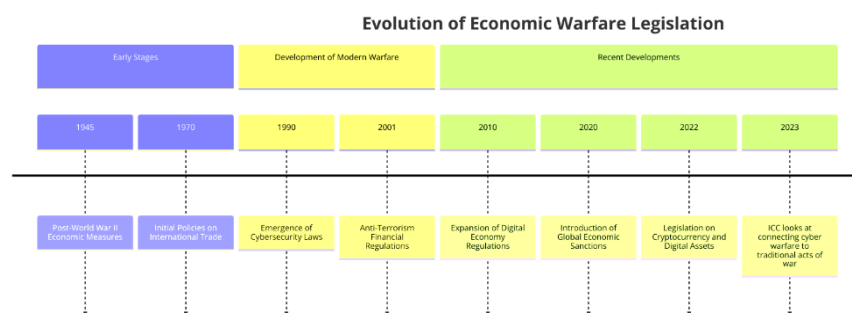


Table 2 shows an illustrative timeline for the evolution of legislation.

Table 2:



1. Introduction

1. Objective

This dissertation aims to establish the necessity of a comprehensive legal framework specifically addressing economic warfare. It advocates for amendment to international law or to inspire domestic legislation that could shape future internationally recognized laws and directives¹. The examination of British legislation, particularly The Sanctions and Anti-Money Laundering Act 2018 (SAMLA 2018)², sets legislating against emerging threats. Similarly, the Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012 (Magnitsky Act)³ from the US provides an example of how internal policy can be adopted internationally⁴.

This paper posits that recent developments in cyber warfare are instrumental in understanding the need for specific legislation against economic warfare. The United Nations Security Council’s decision to consider equating certain cyber warfare acts with traditional warfare acts is significant.⁵ It not only identifies who to prosecute and for which crimes but also sets a precedent for how to classify such crimes. The complexity of curtailing cyber warfare acts underscores the need for a similar focus

¹ Alan Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press 2007)

² The Sanctions and Anti-Money Laundering Act 2018

³ Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012

⁴ Martin Russell, ‘Global human rights sanctions’ (2021) Members' Research Service PE 698.791 <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698791/EPRS_BRI\(2021\)698791_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698791/EPRS_BRI(2021)698791_EN.pdf)> accessed 28 September 2023

⁵ Jens David Ohlin, Kevin Govern, and Claire Finkelstein, *Cyber War Law and Ethics for Virtual Conflicts* (Oxford University Press 2015)

on economic warfare. Without this, the continuation of indirect, third-party warfare, where primary instigators operate within legal ambiguities, is likely.⁶

This dissertation will examine elements currently not included or addressed in international charters, aiming to present a cogent argument for their analysis and enhancement. We will pay special attention to the actions and potential actions of both state and individual actors who conduct warfare within legally ambiguous context.

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 law⁷. While international law traditionally regulated physical conflicts by establishing rules to prevent unnecessary human suffering⁸, the advent of economic warfare has raised pertinent questions about the applicability and adequacy of existing laws⁹. This section aims to dissect the legal differences between traditional warfare and economic warfare, exploring how these distinctions vary based on the actor involved.

⁶ Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014)

⁷ Comptroller and Auditor General, 'Investigation: WannaCry cyber-attack and the NHS Report – Value for money' (2017) <<https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>> accessed 27 September 2023

⁸ Geneva Conventions Act 1957

⁹ Nils Ole Oermann, Hans-Jürgen Wolff, *Trade Wars: Past and Present* (Oxford University Press 2022)

The case of *Fraser, Trenholm & Co.* (1865) serves as a pivotal moment in the historical development of economic warfare. *Trenholm & Co.* a British bank, significantly influenced the intersection of warfare and economic warfare by engaging in the trade of Confederate cotton for British arms, effectively aiding the Confederacy's war efforts¹⁰. The bank's 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 an act of 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 distinctions¹¹. 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.

3. Definition and Characteristics of Warfare

Warfare, or traditional armed conflict, entails open hostilities between states or organized armed groups, involving the deployment of military forces and

¹⁰ *The Bermuda* (1865) 70 US 514

¹¹ Analysis and Research Team, 'The Business of War – Growing risks from Private Military Companies' (2023) <https://www.consilium.europa.eu/media/66700/private-military-companies-final-31-august.pdf> accessed 27 September 2023

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*¹², as established in customary international law¹³ and formalized in treaties like the Geneva Conventions¹⁴ and the Hague Conventions¹⁵. These principles are designed to uphold humanitarian standards and ensure the protection of both civilians and combatants¹⁶.

This legal framework, entrenched in both treaty and customary international law, is significantly shaped by the United Nations Charter¹⁷. It regulates state use of force, permitting military action primarily for self-defence¹⁸ or when authorized by the UN Security Council. The principles of *jus in bello*¹⁹, vital to international humanitarian law and detailed in the Geneva Conventions²⁰, govern the conduct of armed conflict. They stipulate key concepts such as distinction, proportionality, and precautionary measures, aiming to protect civilians and reduce human suffering.

¹² 'jus ad bellum and jus in bello' [2010] ICRC

¹³ Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (Cambridge University Press 2005)

¹⁴ Geneva Conventions Act 1957

¹⁵ Hague Conventions of 1899 and 1907

¹⁶ Kellogg–Briand Pact 1928; 'Resolution 53/18 (Syria) A/HRC/RES/53/18' [2023] United Nations Human Rights Council; RL Fruchterman Jr, 'Enforcement: The Difference Between the Laws of War and the Geneva Conventions' (2015) *Georgia Journal of International & Comparative Law*

¹⁷ Charter of the United Nations and Statute of the International Court of Justice 1945

¹⁸ Vladyslav Lanovoy, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 *EJIL* 455

¹⁹ Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, Cambridge University Press 2010)

²⁰ Geneva Conventions Act 1957

Violations of these principles can lead to international criminal liability and sanctions²¹.

In the context of UK law, these principles shape domestic policies concerning warfare. The Geneva Conventions Act of 1957²², amended in 1995, incorporate these international norms into British law, criminalizing grave breaches of the conventions. This act exemplifies the UK's commitment to adhering to international standards in warfare.²³ Moreover, the UK's Law of Armed Conflict²⁴, drawing from International Humanitarian Law (IHL)²⁵, customary international law, and relevant treaties, governs the UK's military engagements²⁶. This body of law emphasizes the importance of distinguishing combatants from non-combatants and ensures proportionality and precaution in military operations to minimize civilian harm.

The UK's rules of engagement (ROE)²⁷, 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,

²¹ 'Methods (and Means) of Warfare' (The Practical Guide to Humanitarian Law) <<https://guide-humanitarian-law.org/content/article/3/methods-and-means-of-warfare/>> accessed 25 March 2023

²² Geneva Conventions Act 1957

²³ Andrew Clapham and Paola Gaeta, *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press 2014)

²⁴ Dieter Fleck, *The Handbook of International Humanitarian Law* (3rd edn, Oxford University Press 2013); Iain McNair, *The Joint Service Manual Of The Law Of Armed Conflict* (Joint Service Publication 383, 2004 Edition) <<https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf>> accessed 25 November 2023

²⁵ 'Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949' (International Humanitarian Law Databases) <<https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949>> accessed 28 September 2023

²⁶ 'The Law Governing Armed Conflict' (Parliament) <<https://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/1224/122405.htm>> accessed 31 July 2023

²⁷ Ministry of Defence, 'A Soldier's Guide to the Law of Armed Conflict' (2001) <<https://assets.publishing.service.gov.uk/media/5a81f044ed915d74e6234ec0/2017-04714.pdf>> accessed 14 April 2023; Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press 2016)

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 characterized by complex hierarchies²⁸ 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 combat²⁹.

Operational tactics in warfare³⁰ have evolved to include the use of specialised units and methods, such as special forces, guerrilla tactics³¹, 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

²⁸ 'Army Leadership Doctrine' (Army) <<https://www.army.mod.uk/who-we-are/our-schools-and-colleges/centre-for-army-leadership/leadership-doctrine/>> accessed 26 November 2023; '5 Command Issues' (Parliament) <<https://publications.parliament.uk/pa/cm200304/cmselect/cmdfence/465/46508.htm>> accessed 2 December 2023

²⁹ Tilman Rodenhäuser, 'The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law' (2023) p543 <<https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3054&context=ils>> accessed 30 May 2023

³⁰ Benjamin Sutherland, *Modern Warfare, Intelligence and Deterrence: The Technologies That Are Transforming Them* (Routledge 2016)

³¹ Charles R. King, 'Revolutionary War, Guerilla Warfare, and International Law', (1972) 4Case W. Res. J. Int'l L.91 <<https://scholarlycommons.law.case.edu/jil/vol4/iss2/2>> accessed 30 September 2023

gather intelligence. Such tactics, while not involving direct physical violence, can have debilitating effects on a nation's security and economy.³² Psychological warfare, another key aspect, employs methods like propaganda and disinformation to influence public perception and morale. Additionally, economic warfare tactics, including sanctions, trade embargoes, and financial restrictions, aim to weaken an adversary's economy.³³ 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.³⁴ The legal framework governing economic warfare is less clearly defined than that of traditional warfare, leading to ongoing debates about its legality and legitimacy³⁵.

Economic warfare, characterized by its non-kinetic approach, hinges on economic leverage rather than physical force³⁶. Its legality is shaped by different principles than those governing traditional warfare, with concepts of sovereignty,

³² Jens David Ohlin, Kevin Govern, and Claire Finkelstein, *Cyber War Law and Ethics for Virtual Conflicts* (Oxford University Press 2015)

³³ 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 4 March 2023

³⁴ Mitch Rogers, 'From Freeze to Fire: How Economic Sanctions against Japan Led to the War in the Pacific' (2018) *The Thetean: A Student Journal for Scholarly Historical Writing*; Executive Order 8832 - Freezing Japanese and Chinese Assets in the United States 1941; Joy Gordon, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2012)

³⁵ TM Hagemeyer-Witzleb, *The International Law of Economic Warfare* (Springer, Cham 2021)

³⁶ Cheng H Teo, *The Acme of Skill. Nonkinetic Warfare* (techspace rep, Air Command and Staff College, Maxwell 2008)

non-intervention, and non-interference in internal affairs playing pivotal roles in legal assessments³⁷.

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 tactics³⁸. 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.³⁹ This funding could be used to support cyberattacks 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 mercenaries⁴⁰ 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 actor⁴¹.

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

³⁷ Tor Egil Førland, 'The History of Economic Warfare: International Law, Effectiveness, Strategies' (1993) *Journal of Peace Research* Vol. 30, No. 2, pp. 151-162

³⁸ Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014)

³⁹ Roscini, 38 17

⁴⁰ Vladyslav Lanovoy, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 *EJIL* 455

⁴¹ Tilman Rodenhäuser, 'The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law' (2023) p10 <<https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3054&context=ils>> accessed 30 May 2023

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.

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 statutes⁴². Addressing this growing challenge requires an expansion and adaptation of international legal frameworks to encompass and regulate these indirect, economically driven forms of warfare⁴³.

⁴² Graham Cronogue, 'Rebels, Negligent Support, And State Accountability: Holding States Accountable for The Human Rights Violations Of Non-State Actors' (Duke Journal Of Comparative & International Law, Vol 23:365 2013) <<https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1390&context=djcil>> accessed 25 July 2023

⁴³ Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, 'The Law of Cyber-Attack' (California Law Review, Inc. 2012) <https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf> accessed 16 September 2023

1. PMSCs and Their Utilization

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 law⁴⁴. This chapter explores the legal ambiguities surrounding the use of PMSCs and how states and non-state actors exploit these ambiguities.⁴⁵

The Geneva Conventions, comprising four treaties established between 1864 and 1949, set standards for humane conduct. Article 47 of Protocol I defines “mercenary” and prohibits their use in conflicts. Yet, this definition is narrow and excludes many private actors in warfare, posing challenges in enforcement and applicability.

The UN Mercenary Convention, adopted in 1989⁴⁶, aims to eradicate the use of mercenaries by prohibiting their recruitment, financing, training, and use in armed conflicts. However, due to limited ratification by major countries involved in PMSC use⁴⁷, effectiveness is limited⁴⁸.

⁴⁴ Lou Pingeot, *Dangerous Partnership* (Global Policy Forum and Rosa Luxemburg Foundation 2012)

⁴⁵ Amy E Eckert, *Outsourcing War: The Just War Tradition in the Age of Military Privatization* (Georgetown University Press 2016)

⁴⁶ ‘International Convention against the Recruitment, Use, Financing and Training of Mercenaries’ (United Nations)
<<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-against-recruitment-use-financing-and>> accessed 3 May 2023

⁴⁷ International Convention Against the Recruitment, Use, Financing and Training of Mercenaries, Chapter XVIII Penal Matters (adopted 4 December 1989, entered into force 20 October 2001) 2163 UNTS 75 UN List of those that ratified, note: (Britain, United States, Russia, France, China, India and Japan have not yet ratified.)
<https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-6&chapter=18&clang=en> accessed 17 December 2023

⁴⁸ ‘UN Expert Meeting Recommends Clearer Definition Of Mercenaries And Calls For Increased Accountability Of Private Security Companies’ (United Nations, 22 May 2002)
<<https://www.ohchr.org/en/press-releases/2009/10/un-expert-meeting-recommends-clearer-definition-mercenaries-and-calls>> accessed 30 July 2023

The Geneva Conventions and the United Nations Mercenary Convention, address the use of mercenaries in armed conflicts but provide a narrow definition that does not encompass all private actors. PMSCs, offering a range of services from logistical support to armed combat, often fall outside this definition. Additionally, international humanitarian law primarily applies to states and organized armed groups, leaving PMSCs in a regulatory vacuum despite efforts made internally by some states to regulate them⁴⁹.

Circumventing International Obligations: States may use PMSCs to bypass their international law obligations⁵⁰. For instance, a state might hire a PMSC for operations it cannot undertake directly, such as targeting civilians. This outsourcing allows states to evade direct responsibility for violations of international humanitarian law⁵¹.

Plausible Deniability: Employing PMSCs provides states with plausible deniability for actions that may violate international law. If a PMSC commits human

⁴⁹ Foreign & Commonwealth Office, 'Promoting high standards in the UK PMSC industry' (Gov.UK, 21 June 2011) <<https://www.gov.uk/government/news/promoting-high-standards-in-the-uk-pmsc-industry>> accessed 15 November 2023; Iain Overton, Elisa Benevilli, Laura Bruun, 'Britain is the world centre for private military contractors – and it's almost impossible to find out what they're up to' (Open Democracy, 20 December 2018) <<https://www.opendemocracy.net/en/opendemocracyuk/britain-is-world-centre-for-private-military-contractors/>> accessed 27 October 2023; Foreign & Commonwealth Office, 'Promoting high standards in the UK PMSC industry' (Gov.UK, 21 June 2011) <<https://www.gov.uk/government/news/promoting-high-standards-in-the-uk-pmsc-industry>> accessed 15 November 2023

⁵⁰ Dr Wojciech Palka, 'The Awakening of Private Military Companies' (Warsaw Institute, 20 August 2020) <https://warsawinstitute.org/wp-content/uploads/2020/08/RS_08-2020_EN.pdf>, accessed 2 July 2023; Amy E Eckert, *Outsourcing War: The Just War Tradition in the Age of Military Privatization* (Georgetown University Press 2016)

⁵¹ Mucahid Durmaz and Murtala Abdullahi, 'White hands': The rise of private armies in African conflicts' (Al Jazeera, 28 April 2022) <<https://www.aljazeera.com/features/2022/4/28/white-hands-the-rise-of-private-militaries-in-african-conflict>> accessed 2 December 2023

rights abuses, the hiring state can claim no direct involvement, as PMSCs are private entities.

Avoiding Legal Accountability: The ambiguous legal status of PMSCs and their employees complicates efforts to hold them accountable. Their classification as combatants or civilians under international humanitarian law is unclear, as is the jurisdiction for prosecuting crimes committed during armed conflicts⁵².

In conclusion, the rise of PMSCs in warfare highlights the need to address the ambiguity in their legal status. The lack of regulatory framework allows actors to circumvent international law, maintain plausible deniability, and avoid legal accountability.⁵³ Addressing these issues requires re-evaluation and development of comprehensive legal frameworks that recognize the evolving nature of modern warfare and the role of private actors.

⁵² Coalition Provisional Authority Order No 17 of 2004 (Revised) 2004

⁵³ Thomas Jäger, Gerhard Kümmel (eds), *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects* (Springer 2008); Amy E Eckert, *Outsourcing War: The Just War Tradition in the Age of Military Privatization* (Georgetown University Press 2016)

4. The individual and the state

When contrasting the actions of states with those of individuals or nonstate actors, significant differences emerge. States hold specific rights and obligations, and 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 constraints⁵⁴. 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 Convention⁵⁵ 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. While a state's use of chemical weapons is a clear violation of international law, an individual might only receive repercussions under domestic law, lacking direct mechanisms for international accountability⁵⁶. Moreover, non-state entities, including guerrilla groups and terrorist organizations, may employ tactics that are strictly prohibited for states. Such actions, while equally destructive, often fall outside the purview of

⁵⁴ Article 51 of the Charter of the United Nations <https://www.nato.int/cps/en/natolive/official_texts/16937.htm> Accessed 19 September 2023

⁵⁵ 'Chemical Weapons Convention' (Organisation for the Prohibition of Chemical Weapons) <<https://www.opcw.org/chemical-weapons-convention>> accessed 11 June 2023

⁵⁶ 'Russia's Poisoning Of Sergei And Yulia Skripal' (Early Day Motions, 14 March 2018) <<https://edm.parliament.uk/early-day-motion/51540/russias-poisoning-of-sergei-and-yulia-skripal>> accessed 17 December 2023

existing international law, leading to enforcement challenges and accountability issues.

It is not to say that there are no international laws that deal directly with individuals, but these laws are often difficult to enforce. Individual citizens perpetrating war crimes, such as violence against civilians or unlawful use of force, can be criminally accountable under international criminal law,⁵⁷ as evidenced by prosecutions at the International Criminal Court (ICC) and other tribunals⁵⁸. The ICC has the authority to prosecute individuals for grave breaches of international humanitarian law,⁵⁹ irrespective of their official status or nationality⁶⁰. States are obligated under the principle of complementarity to investigate and prosecute such crimes domestically if they have jurisdiction.

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 conflict⁶¹. State support for foreign rebel groups can breach international non-intervention principles and infringe on state sovereignty; individual participation, rarely attracting 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.

⁵⁷ Prosecutor v Charles Ghankay Taylor SCSL-03-1-T

⁵⁸ ICC, The Prosecutor v Ali Muhammad Ali Abd-Al-Rahman” Ali Kushayb” (2021) ICC-02/05-01/20 Lewis, P 11

⁵⁹ About The Court <<https://www.icc-cpi.int/about/the-court>> Accessed 16 September 2023

⁶⁰ R’ios Montt v Ministry of National Defense 2290-2007

⁶¹ Vaughan Lowe, Antonios Tzanakopoulos, *Economic Warfare* (MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, Rüdiger Wolfrum, ed., Oxford University Press, 2012)

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 actors⁶².

2. The Case of Multinational Corporations and Conflict

1. Introduction

Economic warfare has traditionally been associated with the actions of states. However, the increasing globalization 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

⁶² 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 9 December 2023

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. Case Studies

a. The Extractive Industry in the Democratic Republic of Congo (DRC)

The DRC is rich in natural resources, including minerals such as coltan, gold, and diamonds. However, the extractive industry has been marred by accusations of human rights abuses and indirect support of armed groups. MNCs operating in the DRC have been accused of indirectly fuelling conflicts by sourcing minerals from mines controlled by armed groups, or by paying protection money to these groups. For example, a 2002 report by the United Nations accused several MNCs of indirectly supporting armed groups in the DRC by sourcing minerals from areas controlled by these groups⁶³. Although many of the accused companies denied the allegations, the case highlighted challenges regulating the supply chain of conflict minerals.

b. The Oil Industry in Nigeria

The oil industry in Nigeria has been associated with various human rights abuses, including forced evictions, environmental degradation, and violence against local communities. MNCs operating in the Niger Delta have been accused of indirectly fuelling conflicts by providing financial support to armed groups or security forces involved in human rights abuses. For example, Shell has faced multiple lawsuits alleging that it was complicit in human rights abuses committed by Nigerian security

⁶³ 'Report on Exploitation of Resources of Democratic Republic of Congo is Challenged in Security Council' (United Nations, 5 November 2002) <<https://press.un.org/en/2002/sc7561.doc.htm>> accessed 14 November 2023

forces in the 1990s⁶⁴. Although Shell denied the allegations⁶⁵, the case highlighted the need for greater oversight and regulation of MNCs operating in conflict-affected regions.

c. The Arms Trade in Yemen

The conflict in Yemen has been exacerbated by the involvement of various external actors, including MNCs involved in the arms trade. Several Western countries and their MNCs have been accused of indirectly fuelling the conflict by selling arms to parties involved in the conflict, despite evidence of human rights abuses. For example, in 2019, the Campaign Against Arms Trade (CAAT) won a legal challenge against the UK government, arguing that the sale of arms to Saudi Arabia for use in Yemen was unlawful due to the risk of human rights abuses⁶⁶. Although the UK successfully appealed the decision on June 6th 2023⁶⁷, the case highlighted the need for greater regulation of the arms trade and its role in fuelling conflict.

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

⁶⁴ *Wiwa v. Royal Dutch Petroleum Company* 226 F.3d 88 (2d Cir. 2000)

⁶⁵ Chris Kahn, 'Shell settles human rights suit for \$15.5M' (Business & Human Rights Resource Centre, 8 June 2009) <
<https://www.business-humanrights.org/en/latest-news/shell-settles-human-rights-suit-for-155m/>>
 accessed 18 June 2023

⁶⁶ *Campaign Against Arms Trade, R (On the Application Of) v The Secretary of State for International Trade* [2019] EWCA Civ 1020

⁶⁷ *Campaign Against Arms Trade, R (On the Application Of) v Secretary of State for International Trade* [2023] EWHC 1343

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.

4. Conclusion

Economic warfare is not limited to the actions of states. MNCs often operate in conflict-affected regions, where they may indirectly fuel conflicts through business with armed groups or governments involved in human rights abuses. There is a need for a comprehensive legal framework that regulates the actions of MNCs in conflict-affected regions and ensures accountability for those that indirectly support

human rights abuses. Implementing such a framework is crucial for promoting peace, security, and respect for human rights in a globalized world.

3. Economic Cyber-warfare: The twenty first century hidden war

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”⁶⁸. Hackers are individuals or groups whose job (or hobbies) are to find these vulnerabilities and exploit them. Motivation can stem from the glory or thrill of the challenge, to help create a more secure cyberspace, and for 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 and methodology used to conduct these attacks differ greatly, making it 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,

⁶⁸ Alexander Keewatin Dewdney, ‘Computer Recreations: Of Worms, Viruses and Core War’, (1989) Scientific American PL 110

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, they would still be unsure if said 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 in the field struggle to keep up to date with these exploits, it is no surprise that legislation and regulations sanctioning these attacks are slow to come into fruition⁶⁹; those written are done so by individuals or organizations with little to no knowledge of these systems or the implications of their legislation⁷⁰. As mentioned in previous chapters, these could allow for legislative loopholes that organizations or individuals will pursue to avoid the scope of the law. Although there are standards that help define and protect assets from cyber-attacks, for example, ISO27K⁷¹ which are written from a technical mindset and often lack legal expertise furthering. Such technical standards often lack legal expertise, furthering complexity. Furthermore, basic protocols, ideally common practice, such as updating operating systems (OS)⁷² are often ignored to the detriment of stakeholders. This is not to say

⁶⁹ Lucas Kello, 'Cyber legalism: why it fails and what to do about it' (2021) <<https://ora.ox.ac.uk/objects/uuid:00c3488c-6eb4-4f2c-b1bc-143e91f6389b/files/rgh93gz99z>> accessed 23 October 2023

⁷⁰ Ashley Belanger, 'Judge in US v. Google trial didn't know if Firefox is a browser or search engine', (Ars Technica, 12 September 2023) <<https://arstechnica.com/tech-policy/2023/09/judge-in-us-v-google-trial-didnt-know-if-firefox-is-a-browser-or-search-engine/>> accessed 20 November 2023

⁷¹ International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27000:2022, Information technology — Security techniques — Information security management systems — Overview and vocabulary (5th ed, 2022) <https://webstore.iec.ch/preview/info_isoiec27000%7Bed5.0%7Den.pdf> accessed 23 October 2023

⁷² Mary-Ann Russon, 'NHS: Millions of medical devices in UK hospitals are completely unprotected against hackers', (The Standard, 23 June 2023)

that governing bodies have not made a move to create legislation and to punish actors who commit these crimes. As the Ukraine-Russia conflict intensified, Russia turned to cyber-warfare to inflict damage on the Ukraine military and citizens⁷³. As these attacks were not traditional, despite critical infrastructure (hospitals, banks and power grids) being targeted, the Geneva convention was unbroken. The International Criminal Court (ICC) has now received a Rome Statute, Article 15⁷⁴, communication from Lindsay Freeman⁷⁵, UC Berkeley's Human Rights Center, to prosecute these crimes⁷⁶. a counterpart to the Geneva Convention for cyber-warfare has not yet been written⁷⁷.

Due to the lack of regulations, the ease of these crimes, and their potential devastation, the demand for cyber-crime is growing. Distributed Denial of Service (DDoS) is one of the most common cyber-crime services offered and can be bought for as little as \$50⁷⁸. More notorious vulnerabilities, which can have a massive impact, can be sold for millions⁷⁹. Additionally, it's becoming common place for

<<https://www.standard.co.uk/news/tech/cybersecurity-nhs-trust-hospitals-ransomware-hackers-b1089347.html>> accessed 30 Sept 2023

⁷³ Marcus Willett, 'The Cyber Dimension of the Russia-Ukraine War' (2022) Survival, PL 7

⁷⁴ Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 <<https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf>> accessed 23 April 2023

⁷⁵ Yola Verbruggen, 'Cybercrimes under consideration by the ICC' (International Bar Association, 13 October 2023) <<https://www.ibanet.org/cybercrimes-under-consideration-by-the-ICC>> accessed 25 November 2023

⁷⁶ Lindsay Freeman, 'Russian Cyberattacks Need an International Criminal Court Response' (CEPA, 19 July 2022) <<https://cepa.org/article/russian-cyberattacks-need-an-international-criminal-court-response/>> accessed 19 November 2023

⁷⁷ Andy Greenberg, 'The International Criminal Court Will Now Prosecute Cyberwar Crimes' (Wired, 7 September 2023) <<https://www.wired.com/story/icc-cyberwar-crimes/>> accessed 5 October 2023

⁷⁸ A. Zand, G. Modelo-Howard, A. Tongaonkar, S. J. Lee, C. Kruegel and G. Vigna, 'Demystifying DDoS as a Service', (2017) Vol 55 IEEE Communications Magazine, PL 14

⁷⁹ 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/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNv%20bS8&guce_referrer_sig=AQAAAM91tzRG983XWY5dkxlkKJ5wa99kAcVoZf6Z%20hrKxsNqIIW_TjvzHwfDBN>

individuals, organizations, states, and governing bodies to solicit and employ cyber-mercenaries⁸⁰. Cyber-warfare also includes the insertion of vulnerabilities into products before they are sent to retail. China has been known to pay or politically pressure companies to introduce back-doors or other vulnerabilities into technologies before selling them to the western world (notably the USA)⁸¹. As a result, a new form of economic cyber-warfare is emerging⁸² where countries compete to produce the most advance technologies while sanctioning their opponents⁸³. Countries can hinder their adversaries economically while reducing cyber-vulnerabilities and at the same time keeping development of these newer technologies in-house.

1. Who is carrying out these attacks and why?

The most notorious cyber-warfare incidents have a clear link to traditional warfare⁸⁴. The 2007/8 Russian-Georgian and Russian-Estonian conflicts, where a simultaneous ground assault and cyber-attack were launched against Georgia and Estonia, caused major communication disruptions and confusion⁸⁵. No one knows who conducted these attacks. Although, the Commissar of Nashi, a pro-Kremlin group, took accountability for some of them, they fall outside the jurisdiction of

E15B0OHxC1412zIyfvXAEeNuvdwaN2f9aeXMSgy%20u7e1XT_Dc3OHPYp6E2rDegf8nbaYvPC-%20WEfvJCLwF8z7VCCzp8nZPYwetXKZbn2sbTHoTcV4Qz5X4> accessed 30 September 2023

⁸⁰ Martin C. Libicki, David Senty and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (1st Ed., Rand Corporation 2014); Jonathan Mayer, 'Government Hacking' (2017) Yale Law Journal PL 570

⁸¹ Jeffrey Schwartz, 'Zero-Days in Edge Devices Become China's Cyber Warfare Tactic of Choice' (Dark Reading, 12 November 2023) <<https://www.darkreading.com/vulnerabilities-threats/zero-days-in-edge-devices-become-china-s-cyber-warfare-tactic-of-choice>> accessed 20 November 2023

⁸² James A Green, *Cyber Warfare*, (2015 Routledge) Chapter 5

⁸³ Sabrina Korreck Exploring Prospects for Digital Europe in the Age of the US-China Technology Race [2021] Observer Research Foundation

⁸⁴ James A Green, *Cyber Warfare*, (2015 Routledge) Chapter 5

⁸⁵ Gochua, Alik, Thornike Zedelashvili, and Gela Giorgadze, 'Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats' (2022) Ukrainian Policymaker, Volume 10, 27-36 <<https://doi.org/10.29202/up/10/4>> accessed 27 November 2023

Interpol⁸⁶. Titan Rain was a series of cyber-attacks between 2003 and 2006 against US installations. Likely originating from China, many studies suggest that these were a series of 'trial' attacks designed to hinder the US and test their growing cyber-warfare divisions⁸⁷.

Many mercenary groups have added cyber-attacks to their repertoire, and it is often difficult to link them to their state sponsors. In the Russian-Georgian conflict, the Russian Business Network (RBN) was suspected not only of the attacks but of reserving state sponsorship⁸⁸. The suspicion arose from the timing of "trial" DDoS attacks that occurred weeks prior to the conflict⁸⁹.

Additionally, groups such as Anonymous can act to rebel 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 they declared war on the Islamic State (IS), vowing to avenge atrocities and dismantle their online presence⁹⁰. Leveraging its decentralized, yet formidable network to orchestrate a

⁸⁶ Natali Olovson, *Hacking for the State? The Use of Private Persons in Cyber Attacks and State Responsibility* (Swedish Defence University 2020 [English])

⁸⁷ Richard Stiennon, *Cyber Warfare* (1st Ed, Routledge 2015) 26

⁸⁸ Andrzej Kozłowski, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan' (Vol 3 International Scientific Forum 2013) PL 236

⁸⁹ Cooper Quintin, 'Tracking the Worlds Dumbest Cyber Mercenaries' (DEF CON 31, 11 August 2023) <<https://www.youtube.com/watch?v=zccAvgC4UxU>> accessed 16 September 2023

⁹⁰ '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 30 September 2023; 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 30 September 2023; Agence France-Presse, 'Anonymous Hackers Declare War on Islamic State After Paris Attacks' (Gadgets 360, 17 November 2015) <<https://www.gadgets360.com/internet/news/anonymous-declares-war-on-islamic-state-following-after-paris-attacks-766044>> accessed 30 September 2023

series of cyberattacks, their actions included; suspending thousands of IS-related Twitter accounts, conducting DDoS attacks on websites, leaking information about IS members, and launching public awareness campaigns. Such operations, aimed at combating terrorism, were underpinned by a deeply relatable moral stance. Their actions resonated with public sentiment and built upon the good faith they gained after the Charlie Hebdo attacks where they targeted extremists' online platforms⁹¹.

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 conducting organized DDoS attacks against major financial institutions like the IMF, the World Bank and the Federal Reserve⁹². More recently, in 2023, collaborations between groups like KillNet, REvil, and Anonymous Sudan targeted the US and European banking systems⁹³, as well as major financial institutions in the UAE, including First Abu Dhabi Bank, RAKBANK, and Mashreq Bank⁹⁴. These attacks, driven by geopolitical motives, disrupted services and posed risks to sensitive financial data.

⁹¹ 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 10 November 2023

⁹² 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 25 September 2023

⁹³ SpiderLabs Researcher, 'KillNet, Anonymous Sudan, and REvil Unveil Plans for Attacks on US and European Banking Systems' (Trust Wave, 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 30 November 2023

⁹⁴ 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 30 Nov 2023

Sophisticated botnets, like Mirai variants, caused temporary disruptions and raised serious cybersecurity concerns⁹⁵.

The capriciousness of individual, and group, actors illustrating potentially disrupting, unilateral, action taken 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 leveraging economic power to influence the Russian-Ukraine war⁹⁶, For instance.

Similarly, Examples of leveraging individual cyber power include Gary “Solo” McKinnon and Jonathan James. McKinnon conducted several attacks against the US Military and NASA between 2001 and 2002⁹⁷, causing outages of over 2000 military computers and estimated damages of \$700,000. Likewise, in 1999, James, a teenager, hacked NASA and The Pentagon “for fun”⁹⁸. His attacks compromised highly classified software, used to control the International Space Station (ISS); valued at \$1.7million. Legal challenges differed greatly with James sentenced to house arrest; being the first juvenile to be arrested for cybercrime and an American citizen and McKinnon facing extradition under the UK-US extradition treaty. The extradition sparked significant legal discussion, including appeals to the House of Lords and the European Court of Human Rights. The UK Home Secretary

⁹⁵ Karl Greenberg, ‘Anonymous Sudan’s Attack of European Investment Bank: Money, Politics and PR’ (Tech Republic, 26 June 2023) <<https://www.techrepublic.com/article/anonymous-sudan-attacks-european-investment-bank/>> accessed 12 December 2023

⁹⁶ Christopher Miller, Mark Scott, and Bryan Bender, 'UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground' (Politico, 6 September 2022) <<https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039>> accessed 20 March 2023

⁹⁷ Paul Arnell & Alan Reid, ‘Hackers beware: the cautionary story of Gary McKinnon’ (2009), Information & Communications Technology Law, PL 1

⁹⁸ Kevin Poulsen, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* (1st edn, Crown Publishers 2011)

eventually halting the extradition, citing McKinnon's Asperger's syndrome and depression; balancing his human rights with the treaty's legal obligations.⁹⁹

Finally, big businesses; motivated for their own growth or hindering their competition. Large copyright holders, such as Universal and Sony, have been known to hire groups to conduct DDoS attacks on individuals or groups who they suspect of distributing their products¹⁰⁰. Additionally, there is evidence of these organisations conducting attacks on their competitors to steal sensitive information or to hinder their competition. This has been seen in the US where Internet Service Providers (ISPs) will try to hinder and slow down their competitors services to gain market advantage¹⁰¹.

2. 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 dollars in Bitcoin to resolve the incident¹⁰².

This paper focuses on the economic costs. However, these attacks could cause reactor meltdowns, and at a respectively low cost were such a group to be hired by

⁹⁹ McKinnon v Government of the United States of America and another [2008] UKHL 59

¹⁰⁰ Jonathan A. Ophardt, 'Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow's Battlefield' (2010) Duke L. & Tech. Rev PL 9

¹⁰¹ Jonathan 92 37

¹⁰² Lawrence Abrams, 'JBS paid \$11 million to REvil ransomware, \$22.5M first demanded' (Bleeping Computer, 10 June 2021) <<https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/>> accessed 13 December 2023; Arielle Waldman, 'JBS USA paid \$11M ransom to REvil hackers' (Tech Target, 10 June 2021) <<https://www.techtarget.com/searchsecurity/news/252502288/JBS-USA-paid-11-million-ransom-to-REvil-hackers>> accessed 13 December 2023; Associated Press, 'Meat Company JBS Confirms it Paid \$11M Ransom in Cyberattack' (Security Week, 10 June 2021) <<https://www.securityweek.com/meat-company-jbs-confirms-it-paid-11m-ransom-cyberattack/>> accessed 13 December 2023

another actor¹⁰³. Comparable cyber-attacks have been made on major infrastructure with China being known to target US power plants, causing outages¹⁰⁴. Had a coordinated attack been made on all New York power plants, the US economy would have been devastated. Just one known group in China, the “Red Hacker Alliance”, has over 80,000 active Chinese hackers with only one hacker required to cause significant harm. Such hacking programs have been described, by the FBI, as being more prolific than that of all other governments in the world combined¹⁰⁵.

3. Conclusion

An intricate network of actors – state-sponsored groups, cyber-mercenaries, ideologically motivated collectives, individual hackers, and even corporate entities – have 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.

¹⁰³ 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 15 December 2023; James A Green, *Cyber Warfare*, (2015 Routledge) Chapter 5

¹⁰⁴ Craif Huber, ‘Chinese hackers targeted Texas power grid, Hawaii water utility, other critical infrastructure’ (Spectrum News, 12 December 2023) <<https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2023/12/11/report--chinese-hackers-targeted-texas-power-grid--hawaii-water-utility--other-critical-infrastructure->>> accessed 15 December 2023

¹⁰⁵ Sean Lyngaas, ‘Chinese hacking group targeting US agencies and companies has surged its activity, analysis finds’ (CNN, 2 October 2022) <<https://edition.cnn.com/2022/10/02/politics/china-hacking-espionage-us-agencies/index.html>> accessed 24 September 2023

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.

Transitioning to the next chapter, it becomes crucial to analyse 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

1. The Sanctions and Anti-Money Laundering Act 2018

The Sanctions and Anti-Money Laundering Act 2018 (SAML 2018)¹⁰⁶, a cornerstone of the UK's legal strategy against economic warfare, represents a critical shift in the international legal landscape, particularly in the post-Brexit era. This Act reflects the UK's necessity to establish an autonomous sanctioning regime, a response to the limitations of existing international frameworks in addressing the complexities of contemporary economic threats¹⁰⁷. With increased penalties for breaches of financial sanctions, potentially leading to criminal offenses punishable by up to ten years of imprisonment, the seriousness with which the UK government views violations is evident¹⁰⁸. Nevertheless, this escalation in punitive measures adds to the severity and potential contentiousness of the Act.

Central to SAML 2018, detailed in Sections 1(1)–1(2), is the broad empowerment of the Secretary of State and the Treasury, indicative of a strategic shift towards more autonomous national security policies. This empowerment, while administrative, underscores the UK's commitment to addressing multifaceted economic threats, encompassing financial destabilisations, trade disruptions, and cyber threats articulated in Section 1(5)(a)–(f). Reflecting the evolving

¹⁰⁶ The Sanctions and Anti-Money Laundering Act 2018

¹⁰⁷ Neil Whiley, 'A Review Of The Uk Autonomous Sanctions Regime' (UK Finance, 23 September 2021) <<https://www.ukfinance.org.uk/news-and-insight/blogs/review-uk-autonomous-sanctions-regime>> accessed 17 October 2023

¹⁰⁸ 'OFSI Enforcement And Monetary Penalties For Breaches Of Financial Sanctions' (Office of Financial Sanctions Implementation, HM Treasury, December 2023) <https://assets.publishing.service.gov.uk/media/65844e9a23b70a000d234ded/Monetary_Penalty_and_Enforcement_Guidance_December_2023.pdf> accessed 4 December 2023

methodologies of economic aggression and necessitating agile and encompassing legal mechanisms.

SAMLA 2018 introduces description-based sanctions in Sections 1(2) and 9. This aspect addresses the challenges posed by the shadowy realm of economic warfare, where actors navigate legal ambiguities. The Act's focus on financial sanctions under Section 3 address the operational capabilities of entities engaged in economic warfare. Further, the Act has been used to respond to international events or actions, such as the poisoning of Sergei and Yulia Skripal in Salisbury¹⁰⁹, which led to sanctions against Russian individuals and entities.

SAMLA 2018's expansion of financial sanctions reporting requirements under Section 15 in the 2017 amendments, place a significant onus on financial institutions and professionals. Extending beyond the financial sector to include auditors, lawyers, and tax advisers, creating ambiguities regarding the extent of these obligations. This is a strategic acknowledgment of the role such entities play in facilitating and preventing economic warfare. However, the expansion of these reporting obligations, while strategic in enhancing vigilance, introduces burdensome requirements organizations, increasing compliance costs¹¹⁰.

Despite these strengths, SAMLA 2018 is not without its limitations. The Act's broad discretionary powers have raised concerns about potential overreach and a lack of oversight with the House of Lords referring to it as a "constitutional car

¹⁰⁹ 'Russia's Poisoning Of Sergei And Yulia Skripal' (Early Day Motions, 14 March 2018) <<https://edm.parliament.uk/early-day-motion/51540/russias-poisoning-of-sergei-and-yulia-skripal>> accessed 17 December 2023

¹¹⁰ Dominic Bright, 'UK Autonomous Sanctions System: Substantial Increase in the Costs of Compliance?' (Lamb Chambers, 11 March 2020) <<https://www.lambchambers.co.uk/jus-cogens/uk-autonomous-sanctions-system-substantial-increase-in-the-costs-of-compliance/>> accessed 29 November 2023

crash”. 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; provisional extraterritorial reach potentially being perceived as a violation of sovereignty, leading to diplomatic tensions. SAMLA 2018’s effectiveness in countering non-state actors, specifically, terrorist groups or transnational criminal organizations, can also be limited due to their decentralized networks. Human rights concerns arise from the imposition of sanctions that can inadvertently disrupt civilian populations and hinder humanitarian efforts. Additionally, the Act risks further infringement on human rights with the inclusion of description-based sanctions, while innovative, introduces complexities in compliance and enforcement, potentially affecting a broader spectrum of individuals and entities than intended. Moreover, asset freezes and travel bans might affect family members of sanctioned individuals who are not themselves involved in the sanctioned activities. Sophisticated actors may also employ methods to evade sanctions, presenting a need for constant updates to sanction mechanisms and strategies.

In conclusion, SAMLA 2018 marks a pivotal step in confronting economic warfare, yet its broad discretionary scope and potential for human rights implications and potential enforcement issues reveal a pressing need for more refined legislation. Some critics argue that the Act lacks clarity in defining the criteria for imposing sanctions. This ambiguity may cause businesses and individuals to inadvertently

violate sanctions, with difficulty in understanding requirements for lifting sanctions exacerbating this. One fear is this could lead to arbitrary or politically motivated decisions, and concerns have been raised about the lack of checks and balances in the process of designating sanctions targets. These concerns highlight the necessity for a targeted legal act that unambiguously delineates the parameters of economic warfare and clearly defines the role of third-party actors. This act should not be a vague, catch-all instrument prone to indiscriminate application by the government. Instead, it must be a precise, comprehensible statute, serving both as a deterrent against economic aggression and as a remedy for the deficiencies in current international law. Such legislation would not only reinforce the global legal framework against economic threats but also ensure a balance between national security imperatives and the preservation of civil liberties, setting a new standard for international legal responses in this evolving domain¹¹¹.

¹¹¹ ‘The Sanctions and Anti-money Laundering Act 2018: New Challenges in Sanctions Compliance?’ (Sherman & Sterling, 4 June 2018) <<https://www.shearman.com/perspectives/2018/06/sanctions-and-anti-money-laundering-act>> accessed 29 June 2023

2. The Magnitsky Act

In the realm of international law and diplomacy, the Magnitsky Act stands as a critical legislative response to acts of economic warfare¹¹². The Magnitsky Act, Formally the Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012¹¹³, herein The Magnitsky Act, is a legislative response to economic warfare and related transgressions. Sergei Magnitsky was a Russian lawyer who exposed massive tax fraud and faced fatal consequences in custody¹¹⁴. The Act was initially enacted in the United States in 2012¹¹⁵ and subsequently adopted by various other countries¹¹⁶.

A comparative analysis with other similar legislation, such as the UK’s Global Human Rights Sanctions Regulations 2020 or the European Union’s human rights sanctions regime, reveals the Magnitsky Act’s unique position in the international legal landscape. While these legislation’s share a common goal of targeting human rights violators and corrupt officials, the Magnitsky Act stands out with a specific focus on individuals and entities involved in gross human rights violations, corruption, and acts of economic warfare¹¹⁷. Provisions such as asset freezes and

¹¹² Executive Order 13818 — Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption 2017

¹¹³ S1039 - Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012

¹¹⁴ N Newson, ‘Magnitsky sanctions’ [2021] House of Lords Library

¹¹⁵ Public Law 112 - 208 - Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012

¹¹⁶ M A & Collins-Chase E J Weber, ‘The Global Magnitsky Human Rights Accountability Act’ [2020] IN FOCUS, Congressional Research Service

¹¹⁷ Treasury Sanctions Russians Connected to Gross Human Rights Violations and Corrupt Leader of Belarus, ‘Press Release, U.S. Department of the Treasury’ [March 15, 2022]; Foreign Commonwealth Office and The Rt Hon Rishi Sunak MP, ‘UK announces first sanctions under new global human rights regime’ (Gov.UK, 6 July 2020) <<https://www.gov.uk/government/news/uk-announces-first-sanctions-under-new-global-human-rights-regime>> accessed 14 December 2023

travel bans¹¹⁸ are implemented with a distinct emphasis on individual accountability and extraterritorial reach¹¹⁹.

The Magnitsky Act has been instrumental in freezing assets and barring entry to human rights violators while presenting a strong message against economic aggression and human rights abuses on a global scale. However, the Act faces criticisms concerning the identification of sanctionable targets, diplomatic repercussions, and risk of abuse as a political expedient.

Furthermore, the Magnitsky Act influences international relations, especially between sanctioning countries and the states of sanctioned individuals, is noteworthy. It has, at times, strained diplomatic relations, as targeted countries may view the sanctions as an infringement of their sovereignty or an unjust interference in their internal affairs.¹²⁰ This aspect underscores the delicate balance between enforcing international legal norms and maintaining diplomatic relations in the global arena.

Like SAMLA, The Magnitsky act proposes consequences for human rights violations and reinforces the international community's commitment to protect fundamental freedoms and individual rights. Requiring continuous monitoring and adaptation of sanction enforcement mechanisms to counter evasion tactics, such as complex financial structures and proxy entities¹²¹.

¹¹⁸ Magnitsky legislation; Foreign Commonwealth Office & The Rt Hon Dominic Raab MP, 'Global Human Rights Sanctions regime: Foreign Secretary's statement to Parliament' (House of Commons, 6 July 2020) <<https://www.gov.uk/government/speeches/statement-on-the-global-human-rights-sanctions-regime>> accessed 22 June 2023

¹¹⁹ The Global Magnitsky Human Rights Accountability Act

¹²⁰ Joy Gordon, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2012)

¹²¹ 'The Magnitsky Act At Five Years: Assessing Accomplishments and Challenges' (Commission On Security And Cooperation In Europe, 14 December 2017) <<https://www.csce.gov/wp-content/uploads/2018/03/MagnitskyAt5.pdf>> accessed 14 December 2023

In terms of economic warfare, the Act serves as a vital tool by addressing the financial underpinnings of such illicit activities. Economic warfare tactics, which include covert financial manipulations and cyberattacks, pose complex challenges to global security and stability¹²². By targeting the financial resources of those orchestrating economic aggression, the Magnitsky Act disrupts their ability to conduct hostile actions¹²³.

The effectiveness of the Magnitsky Act in countering economic warfare, however, depends on international cooperation and coordination. Economic warfare often involves activities that span multiple jurisdictions, making the transnational enforcement of sanctions a complex endeavour. The Act's success in deterring economic aggression¹²⁴ is thus, significantly influenced by the willingness of other states to recognize and enforce the imposed sanctions¹²⁵.

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

¹²² The Rt Hon Rishi Sunak MP, 'Responding to a more contested and volatile world' (Parliament, 13 March 2023) <https://assets.publishing.service.gov.uk/media/641d72f45155a2000c6ad5d5/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf> accessed 14 December 2023

¹²³ Evasion Efforts Targeting Key Sectors, Treasury Expands Military Supplies, and Intensifies Sanctions Against Russia, 'Press Release, U.S. Department of the Treasury' [February 24, 2023]

¹²⁴ F A Vrieze, 'The Magnitsky Sanctions and the politics of individual accountability' [2020] WFD

¹²⁵ Promoting Accountability for Human Rights Abuse with Our Partners, 'Press Statement, Antony J. Blinken, Secretary of State' [March 22, 2021]

fair and transparent application of sanctions, and mitigating potential diplomatic frictions that may arise from their implementation.

In conclusion, while the Magnitsky Act represents a significant stride in countering economic warfare and human rights violations, its efficacy 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 specific case scenarios. 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 corruption¹²⁶, 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 effective and holistic legal response in the international arena.

¹²⁶ Treasury Targets Individuals Involved in the Sergei Magnitsky Case and Other Gross Violations of Human Rights in Russia, 'Press Release, U.S. Department of the Treasury' [December 20, 2017]

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

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)¹²⁷ and the Sergei Magnitsky Rule of Law Accountability Act of 2012 (Magnitsky Act)¹²⁸ 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 these limitations as a rationale for the development of specific legislation on economic warfare, drawing from the analyses in the previous responses and the contextual background provided so far.

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 2020¹²⁹, which are the UK's adaption of the Magnitsky-style sanctions, target individuals involved in human rights abuses but do not specifically address the

¹²⁷ The Sanctions and Anti-Money Laundering Act 2018

¹²⁸ Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act 2012

¹²⁹ The Global Human Rights Sanctions Regulations 2020

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, emphasizing the need for a dynamic and inclusive legal policy.

The Global Human Rights Sanctions Regulations 2020 demonstrates the UK's commitment to addressing human rights violations globally and mark a commitment to adopting what is a large part of the Magnitsky Act. However, these regulations primarily focus on individual human rights abusers and corrupt officials, falling short in addressing the multifaceted tactics of economic warfare. This gap underscores the need for a broader approach that encompasses the various dimensions of economic conflict. Focusing then, on the examination of SAMLA 2018 and the Sergei Magnitsky Act, within the context of modern economic warfare, highlights three key limitations. First, the jurisdictional reach of these acts is confined and does not extend to the complexities of global economic aggression, often perpetrated by a mix of state and non-state actors. Second, while these legislations address direct financial crimes and human rights abuses, they fall short in confronting indirect tactics, such as cyber-attacks on financial systems and currency manipulation. Third, the enforcement mechanisms under these acts are inadequate in dealing with the anonymity and agility of actors engaged in economic warfare, especially in the digital realm.

2. Limitations of Current Frameworks

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, primarily addressing 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.

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.

Political and Diplomatic Implications:

The use of economic warfare tools, such as sanctions, can have significant political and diplomatic repercussions.¹³⁰ While intended to exert pressure on target

¹³⁰ Joy Gordon, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2012)

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 more preferential to allow this to go unchallenged so you can 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 ones losses.

Enforcement and Jurisdictional Challenges:

The enforcement of sanctions and regulations outlined in SAMLA 2018 and the Magnitsky Act face 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.

3. Conclusions and Recommendations

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.

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.

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.

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

1. Introduction

Economic warfare must be broadened to not only encompass its traditional definition, or its more modern understanding since the American Civil War. The utilisation of personal assets has never before had such potential, or potentially devastating ramifications. This presents unique challenges to the current international legal framework. As illustrated by the case of Elon Musk's involvement in the Ukraine-Russia conflict¹³¹, individual actors with significant economic power and influence can have a profound impact on international conflicts. However, with the rise of groups like REvil and Anonymous Sudan the amount of disposable income required to represent a threat is diminishing. There is a notable absence of a comprehensive legal framework to regulate the actions of individual actors¹³², 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 discussions in Chapter 5 regarding the indirect methods of economic warfare, such as the use of third-party financiers and proxies (Page 52), our recommendations extend beyond traditional direct perpetrators. We propose inclusive legal provisions that encapsulate both

¹³¹ Marina Hyde, 'And then Elon Musk said there'll be no more war – not via his satellite. Aren't we lucky to have the world in his hands?' (The Guardian, 8 September 2023) <<https://www.theguardian.com/commentisfree/2023/sep/08/elon-musk-satellite-war-starlink-system-ukraine>> accessed 23 December 2023; Victoria Kim, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' (New York Times, 8 September 2023) <<https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html>> accessed 28 November 2023

¹³² Vladyslav Lanovoy, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 EJIL 455

direct and indirect modes of economic aggression, ensuring a comprehensive approach that aligns with our earlier analysis of modern economic warfare tactics. This chapter proposes a foundational legal framework to regulate the use of economic means in obfuscating international law, one which could be enacted by the UK government. As highlighted in our analysis of cyber-warfare in Chapter 5, the UK faces significant vulnerabilities in its digital economic infrastructure. To address this, the recommendation to develop a specific UK policy on economic warfare (Page 54) is directly informed by our findings on the escalating threats in the digital domain. This policy will specifically target the gaps identified in the cybersecurity measures and protocols currently in place¹³³, thereby fortifying the UK's resilience against cyber-economic attacks.

UK Economic Warfare Prevention and Response Act (UK-EWPRA)

An Act to address the evolving nature of economic warfare, to fill the legal gaps in current legislation, and to ensure the protection of the United Kingdom's economic interests, both domestically and globally.

1. Preamble:

Recognizing the complex and evolving landscape of economic warfare, which includes threats from state and non-state actors, cyber-attacks on critical infrastructure, currency manipulation, and the use of third-party proxies, the UK-EWPRA is established to fortify the United Kingdom's economic defence mechanisms and to ensure a robust response to such threats. It acknowledges that in certain situations such threats can be tantamount to acts of war.

¹³³ James A Green, *Cyber Warfare*, (2015 Routledge) Chapter 5

2. Definitions For the purposes of this Act:

- "Economic warfare" is defined broadly to include direct and indirect actions, such as sanctions evasion, financial terrorism, cyber-attacks on economic infrastructure, currency manipulation, and the facilitation or financing of such activities by third parties or proxies.
- "UK interests" are defined as economic, financial, and infrastructural assets and interests that are critical to the United Kingdom's national security and economic stability.

3. Provisions**A. Addressing Direct and Indirect Economic Warfare:**

- The Act shall apply not only to direct perpetrators of economic warfare but also to those who finance or facilitate such actions, thereby holding accountable individuals, groups, and states engaged in or supporting economic warfare.
- Individual actors should be prohibited from engaging in economic actions that lead to outcomes which constitute war crimes, or acts or war, both directly or indirectly¹³⁴. For example, all actors should be wary of providing financial support to parties involved in armed conflict, as where such parties contribute to violations of international humanitarian law, said actors could be found complicit and in violation of the act.

¹³⁴War Crimes', (United Nations)
<<https://www.un.org/en/genocideprevention/war-crimes.shtml>> accessed 29 November 2023

- Non state actors should be prohibited from using economic means or personal assets to involve themselves in conflict scenarios without state consent.

B. Jurisdictional Reach and Enforcement:

- The UK-EWPRA will encompass actions undertaken by both state and non-state actors, within and beyond the UK's borders, that are deemed harmful to the nation's economic interests. Enforcement of this Act will be the responsibility of a dedicated task force within the Treasury, empowered to collaborate with international bodies for global compliance, and to impose sanctions and legal actions against violators.
- Enforcement mechanisms shall be strengthened to deal with the anonymity and agility of actors engaged in economic warfare, particularly in the digital realm. This includes the ability to trace illicit financial flows and to cooperate internationally in enforcement efforts.
- Enforcement mechanisms will vary dependent on the severity of the threat with both pre-emptive measures and the use of military force being permissible in situations where such action could deter substantive loss of life.

C. Adaptability and Review:

- The Act shall be dynamic, allowing for adaptability and responsiveness to emerging threats in economic and cyber warfare. Regular reviews and amendments shall be integral to the Act,

ensuring that it keeps pace with technological advancements and changes in warfare tactics.

4. Integration with International Law

The Act shall integrate with existing international laws and agreements, such as those posed by the UN Security Council, while also providing specific guidelines and mechanisms tailored to the UK's unique economic and security context. This policy has been formulated with careful consideration of existing international laws and UK legal standards.

5. Implementation

A. National Implementation:

- Relevant national authorities shall be tasked with monitoring compliance and enforcing the provisions of the Act.

B. International Collaboration:

- The UK shall engage in global efforts to establish comprehensive legal frameworks against economic warfare and advocate for the adoption of similar frameworks internationally.¹³⁵

The UK government can implement the proposed legal framework by incorporating aspects of it into national legislation. This can be achieved through the enactment of a new statute or the amendment of existing legislation. The UK government should also establish a national authority responsible for monitoring compliance, with publicising and enforcing the legal obligations of violating actors

¹³⁵ Alan Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press 2007)

and to recommend further actions when judicial or parliamentary oversight is necessary. This authority should have the power to impose administrative sanctions, such as fines and revocation of licenses, and to refer cases to judicial authorities for prosecution. Additionally, the UK government should actively engage in international efforts to establish a comprehensive legal framework for individual actors in economic warfare.¹³⁶ This may include participating in negotiations at the United Nations or other international forums and advocating for the adoption of the proposed legal framework at the international level.¹³⁷

6. Further Recommendations

I would recommend a policy that would require all businesses to report hacking activities. This hypothetical policy would aim to create a more secure and resilient cyber environment by ensuring that all businesses contribute to a collective understanding of the cyber threat landscape and aid in the national response to cyber incidents.

Illustrative Sample Policy:

Title: National Cybersecurity Incident Reporting Act

Purpose: To establish a mandatory reporting framework for all businesses operating within the country to ensure timely and efficient reporting of cybersecurity incidents. This would enable better tracking, analysis, and response to such incidents at a national level.

¹³⁶ Vladyslav Lanovoy, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 EJIL 455

¹³⁷ Alan Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press 2007)

Key Provisions:

1. **Mandatory Reporting:** All businesses, regardless of size or sector, must report cybersecurity incidents, such as data breaches, hacking attempts, ransomware attacks, and other forms of cyber intrusion, to a designated national cybersecurity agency.
2. **Reporting Time Frame:** Incidents must be reported within a specified timeframe from the moment the organization becomes aware of the incident. For example, within 72 hours of detection.
3. **Details to be Reported:** The report must include details of the incident, such as the nature and extent of the breach, type of data compromised, number of individuals affected (if applicable), and steps taken by the business to respond to and mitigate the incident.
4. **Centralized Cyber Incident Database:** Establishment of a national database to collect and analyze data on reported incidents. This database would be used to identify trends, issue alerts, and provide guidance on best practices for cybersecurity.
5. **Confidentiality and Data Protection:** Measures to ensure the confidentiality of sensitive information reported and compliance with data protection laws.

6. **Penalties and Compliance:** Penalties for non-compliance, such as fines or other legal consequences. Regular audits and compliance checks might be conducted to ensure adherence to the reporting requirements.
7. **Support and Resources:** Provision of resources and support for businesses, particularly small and medium-sized enterprises, to help them understand their reporting obligations and improve their cybersecurity measures.
8. **Public Awareness and Education:** Initiatives to raise public awareness about cybersecurity threats and promote a culture of cybersecurity across all sectors of the economy.
9. **International Collaboration:** Mechanisms for sharing relevant information with international cybersecurity groups and organizations to combat global cyber threats.

7. 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 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 minimize unintended impacts on global economic interactions.

8. 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

1. Reflective Analysis

The proposed policies and legislation 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 policies and legislation 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 categorizing actions as economic warfare, especially in a rapidly evolving global landscape where economic aggression can be subtle and indirect.

The emphasis on the role of PMSCs in Chapter 6, while crucial, might overlook the complex legal status and diverse PMSCs modes of these entities¹³⁸. 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 PMSCs¹³⁹, balancing the

¹³⁸ Benjamin Sutherland, *Modern Warfare, Intelligence and Deterrence: The Technologies That Are Transforming Them* (Routledge 2016)

¹³⁹ Thomas Jäger, Gerhard Kümmel (eds), *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects* (Springer 2008)

need for accountability and the practical aspects of their operations in diverse conflict scenarios.

The discussion around the SAMLA 2018¹⁴⁰ 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 policies and legislation changes are a step in the right direction towards addressing modern economic warfare, they must contend

¹⁴⁰ The Sanctions and Anti-Money Laundering Act 2018

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.

2. Final Remarks

The rapid increase in individual wealth and technological advancements in recent years has democratized 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 developed North countries. For example, a wealthy individual or private entity could strategically invest in, or divest from, certain sectors of a developed country's economy to destabilize 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 organizations, 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.

Globalization: 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 destabilize 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 democratization 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 destabilize 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

Books

Boyle A, Chinkin C, *The Making of International Law* (Oxford University Press 2007)

Clapham A, Gaeta P, *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press 2014)

Contributions to Collections

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

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

Evans SW, *Essays: On the Action for Money Had and Received, on the Law of Insurances, and on the Law of Bills of Exchange and Promissory Notes* (Liverpool, Merrit & Wright 1802)

Fleck D, *The Handbook of International Humanitarian Law* (3rd edn, Oxford University Press 2013)

Gordon J, *Invisible War: The United States and the Iraq Sanctions* (Harvard University Press 2012)

Green J A, *Cyber Warfare*, (2015 Routledge) Chapter 5

Hagemeyer-Witzleb T M, *The International Law of Economic Warfare* (Springer, Cham 2021)

Henckaerts J, Doswald-Beck L, *Customary International Humanitarian Law* (Cambridge University Press 2005)

Jäger T, Kümmel G (eds), *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects* (Springer 2008)

Libicki M C, Senty D, Pollak J, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (1st Ed., Rand Corporation 2014)

Lowe V, Tzanakopoulos A, *Economic Warfare* (MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, Rüdiger Wolfrum, ed., Oxford University Press, 2012)

McNaill I, *The Joint Service Manual Of The Law Of Armed Conflict* (Joint Service Publication 383, 2004 Edition)
<<https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf>> accessed 25 November 2023

Nolan D, Hongkong Fir Shipping Co v Kawasaki Kisen Kaisha Ltd, The Hongkong Fir (1961) in C Mitchell and P Mitchell (eds), *Landmark Cases in the Law of Contract* (Hart 2008)

Oermann N O, Wolff H, *Trade Wars: Past and Present* (Oxford University Press 2022)

Ohlin J D, Govern K, and Finkelstein C, *Cyber War Law and Ethics for Virtual Conflicts* (Oxford University Press 2015)

Olovson N, *Hacking for the State? The Use of Private Persons in Cyber Attacks and State Responsibility* (Swedish Defence University 2020 [English])

Pingeot L, *Dangerous Partnership* (Global Policy Forum and Rosa Luxemburg Foundation 2012)

Poulsen K, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* (1st edn, Crown Publishers 2011)

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

Simons G, 'Imposing Economic Sanctions: Legal Remedy Or Genocidal Tool?' in (Pluto Press 1999).

Solis G D, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press 2016)

Stevens R, 'Is There a Law of Unjust Enrichment?' in S Degeling and J Edelman (eds), *Unjust Enrichment and Commercial Law* (Thomson 2008).

Stevens R, *Torts and Rights* (OUP 2007)

Stiennon R, *Cyber Warfare* (1st Ed, Routledge 2015) 26

Sutherland B, *Modern Warfare, Intelligence and Deterrence: The Technologies That Are Transforming Them* (Routledge 2016)

Teo C T, *The Acme of Skill. Nonkinetic Warfare* (techspace rep, Air Command and Staff College, Maxwell 2008)

Articles

— 'Discharge of Contract by Breach' (1981) 97 LQR 541.

'Geneva Conventions' British Red Cross.

'jus ad bellum and jus in bello' [2010] ICRC.

'Treasury Sanctions Russians Connected to Gross Human Rights Violations and Corrupt Leader of Belarus', (Press Release, U.S. Department of the Treasury) [March 15, 2022]

Abrams L, 'JBS paid \$11 million to REvil ransomware, \$22.5M first demanded' (Bleeping Computer, 10 June 2021)

<<https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/>> accessed 13 December 2023

Agence France-Presse, ‘Anonymous Hackers Declare War on Islamic State After Paris Attacks’ (Gadgets 360, 17 November 2015)

<<https://www.gadgets360.com/internet/news/anonymous-declares-war-on-islamic-state-following-after-paris-attacks-766044>> accessed 30 September 2023

Associated Press, ‘Meat Company JBS Confirms it Paid \$11M Ransom in Cyberattack’ (Security Week, 10 June 2021)

<<https://www.securityweek.com/meat-company-jbs-confirms-it-paid-11m-ransom-cyberattack/>> accessed 13 December 2023

Belanger A, ‘Judge in US v. Google trial didn’t know if Firefox is a browser or search engine’, (Ars Technica, 12 September 2023)

<<https://arstechnica.com/tech-policy/2023/09/judge-in-us-v-google-trial-didnt-know-if-firefox-is-a-browser-or-search-engine/>> accessed 20 November 2023

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 9 December 2023

Durmaz M, Abdullahi M, ‘“White hands”: The rise of private armies in African conflicts’ (Al Jazeera, 28 April 2022)

<<https://www.aljazeera.com/features/2022/4/28/white-hands-the-rise-of-private-militaries-in-african-conflict>> accessed 2 December 2023

Evasion Efforts Targeting Key Sectors, Treasury Expands Military Supplies, and Intensifies Sanctions Against Russia, 'Press Release, U.S. Department of the Treasury' [February 24, 2023]

F A Vrieze, 'The Magnitsky Sanctions and the politics of individual accountability' [2020] WFD

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/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNv%20bS8&guce_referrer_sig=AQAAAM91tzRG983XWY5dkxlkJ5wa99kAcVoZf6Z%20hrKxsNqIIW_TjvzHwfDBNE15B0OHxC1412zIyfvXAEeNuvdwaN2f9aeXMSgy%20u7e1XT_Dc3OHPYp6E2rDegf8nbaYvPC-%20WEfvJCLwF8z7VCCzp8nZPYwetXKZbn2sbTHoTcV4Qz5X4> accessed 30 September 2023

Freeman L, 'Russian Cyberattacks Need an International Criminal Court Response' (CEPA, 19 July 2022)
 <<https://cepa.org/article/russian-cyberattacks-need-an-international-criminal-court-response/>> accessed 19 November 2023

Greenberg A, 'The International Criminal Court Will Now Prosecute Cyberwar Crimes' (Wired, 7 September 2023)
 <<https://www.wired.com/story/icc-cyberwar-crimes/>> accessed 5 October 2023

Greenberg K, 'Anonymous Sudan's Attack of European Investment Bank: Money, Politics and PR' (Tech Republic, 26 June 2023)
 <<https://www.techrepublic.com/article/anonymous-sudan-attacks-european-investment-bank/>> accessed 12 December 2023

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 10 November 2023

Huber C, 'Chinese hackers targeted Texas power grid, Hawaii water utility, other critical infrastructure' (Spectrum News, 12 December 2023)
 <<https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2023/12/11/report--chinese-hackers-targeted-texas-power-grid--hawaii-water-utility--other-critical-infrastructure->> accessed 15 December 2023

Human Rights Abuse with Our Partners PA for, 'Press Statement, Antony J. Blinken, Secretary of State' [March 22, 2021].

Hyde M, 'And then Elon Musk said there'll be no more war – not via his satellite. Aren't we lucky to have the world in his hands?' (The Guardian, 8 September 2023)
 <<https://www.theguardian.com/commentisfree/2023/sep/08/elon-musk-satellite-war-starlink-system-ukraine>> accessed 23 December 2023

Isaac A, 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 15 December 2023

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 30 November 2023

Kim V, 'Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack' (New York Times, 8 September 2023)
<<https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html>> accessed 28 November 2023

Lyngaas S, 'Chinese hacking group targeting US agencies and companies has surged its activity, analysis finds' (CNN, 2 October 2022)
<<https://edition.cnn.com/2022/10/02/politics/china-hacking-espionage-us-agencies/index.html>> accessed 24 September 2023

M A & Collins-Chase E J Weber, 'The Global Magnitsky Human Rights Accountability Act' [2020] IN FOCUS, Congressional Research Service
Magnitsky legislation;

Miller C, Scott M, Bender B, 'UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground' (Politico, 6 September 2022)
<<https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039>> accessed 20 March 2023

N Newson, 'Magnitsky sanctions' [2021] House of Lords Library

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 4 March 2023

Reynolds F, 'Warranty, Condition and Fundamental Term' (1963) 79 LQR 534.

Russon A, 'NHS: Millions of medical devices in UK hospitals are completely unprotected against hackers', (The Standard, 23 June 2023)

<<https://www.standard.co.uk/news/tech/cybersecurity-nhs-trust-hospitals-ransomwar-e-hackers-b1089347.html>> accessed 30 Sept 2023

Schwartz J, 'Zero-Days in Edge Devices Become China's Cyber Warfare Tactic of Choice' (Dark Reading, 13 November 2023)

<<https://www.darkreading.com/vulnerabilities-threats/zero-days-in-edge-devices-become-china-s-cyber-warfare-tactic-of-choice>> accessed 20 November 2023

Sergei Magnitsky Case TTII in the and Human Rights in Russia OGV of, 'Press Release, U.S. Department of the Treasury' [December 20, 2017].

Sexton J, 'Transatlantic financiers and the Civil War' [2008] American Nineteenth Century History.

SpiderLabs Researcher, 'KillNet, Anonymous Sudan, and REvil Unveil Plans for Attacks on US and European Banking Systems' (Trust Wave, 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 30 November 2023

Targeting Key Sectors EE, Military Supplies TE, and Russia ISA, 'Press Release, U.S. Department of the Treasury' [February 24, 2023].

Waldman A, 'JBS USA paid \$11M ransom to REvil hackers' (Tech Target, 10 June 2021)

<<https://www.techtarget.com/searchsecurity/news/252502288/JBS-USA-paid-11-million-ransom-to-REvil-hackers>> accessed 13 December 2023

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 30 September 2023

Websites

‘5 Command Issues’ (Parliament)

<<https://publications.parliament.uk/pa/cm200304/cmselect/cmdfence/465/46508.htm>> accessed 2 December 2023

‘Army Leadership Doctrine’ (Army)

<<https://www.army.mod.uk/who-we-are/our-schools-and-colleges/centre-for-army-leadership/leadership-doctrine/>> accessed 26 November 2023

‘Chemical Weapons Convention’ (Organisation for the Prohibition of Chemical Weapons) <<https://www.opcw.org/chemical-weapons-convention>> accessed 11 June 2023

‘Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949’ (International Humanitarian Law Databases) <<https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949>> accessed 28 September 2023

‘International Convention against the Recruitment, Use, Financing and Training of Mercenaries’ (United Nations) <<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-against-recruitment-use-financing-and>> accessed 3 May 2023

‘Methods (and Means) of Warfare’ (The Practical Guide to Humanitarian Law) <<https://guide-humanitarian-law.org/content/article/3/methods-and-means-of-warfare/>> accessed 25 March 2023

‘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 25 September 2023

‘Report on Exploitation of Resources of Democratic Republic of Congo is Challenged in Security Council’ (United Nations, 5 November 2002)
 <<https://press.un.org/en/2002/sc7561.doc.htm>> accessed 14 November 2023

‘The Law Governing Armed Conflict’ (Parliament)
 <<https://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/1224/122405.htm>> accessed 31 July 2023)

‘The Sanctions and Anti-money Laundering Act 2018: New Challenges in Sanctions Compliance?’ (Sherman & Sterling, 4 June 2018)
 <<https://www.shearman.com/perspectives/2018/06/sanctions-and-anti-money-laundering-act>> accessed 29 June 2023

‘UN Expert Meeting Recommends Clearer Definition Of Mercenaries And Calls For Increased Accountability Of Private Security Companies’ (United Nations, 22 May 2002)
 <<https://www.ohchr.org/en/press-releases/2009/10/un-expert-meeting-recommends-clearer-definition-mercenaries-and-calls>> accessed 30 July 2023

‘War Crimes’, (United Nations)
 <<https://www.un.org/en/genocideprevention/war-crimes.shtml>> accessed 29 November 2023

About The Court <<https://www.icc-cpi.int/about/the-court>> Accessed 16 September 2023

Article 51 of the Charter of the United Nations

<https://www.nato.int/cps/en/natolive/official_texts/16937.htm> accessed 19 September 2023

Foreign & Commonwealth Office, 'Promoting high standards in the UK PMSC industry' (Gov.UK, 21 June 2011)

<<https://www.gov.uk/government/news/promoting-high-standards-in-the-uk-pmsc-industry>> accessed 15 November 2023

Kahn C, 'Shell settles human rights suit for \$15.5M' (Business & Human Rights Resource Centre, 8 June 2009) <
<https://www.business-humanrights.org/en/latest-news/shell-settles-human-rights-suit-for-155m/>> accessed 18 June 2023

Neil Whiley, 'A Review Of The Uk Autonomous Sanctions Regime' (UK Finance, 23 September 2021)

<<https://www.ukfinance.org.uk/news-and-insight/blogs/review-uk-autonomous-sanctions-regime>> accessed 17 October 2023

Yola Verbruggen, 'Cybercrimes under consideration by the ICC' (International Bar Association, 13 October 2023) <
<https://www.ibanet.org/cybercrimes-under-consideration-by-the-ICC>> accessed 25 November 2023

Journal

Arnell P, Reid A, 'Hackers beware: the cautionary story of Gary McKinnon' (2009), *Information & Communications Technology Law*, PL 1

Cleland B, *'The Confederate States of America and the British Empire: Neutral Territory and Civil Wars'* [2016] *Journal of Military and Strategic Studies*

Dewdney A K, 'Computer Recreations: Of Worms, Viruses and Core War', (1989) *Scientific American* PL 110

Forland TE, *'Economic Warfare' and 'Strategic Goods': A Conceptual Framework for Analyzing COCOM'* [1991] *Journal of Peace Research*

Førland TE, 'The History of Economic Warfare: International Law, Effectiveness, Strategies' (1993) *Journal of Peace Research* Vol. 30, No. 2, pp. 151-162

Fruchterman R L Jr, 'Enforcement: The Difference Between the Laws of War and the Geneva Conventions' (2015) *Georgia Journal of International & Comparative Law*

Gochua A, Zedelashvili T, Giorgadze G, 'Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats' (2022) *Ukrainian Policymaker*, Volume 10, 27-36 <<https://doi.org/10.29202/up/10/4>> accessed 27 November 2023

King C R, 'Revolutionary War, Guerilla Warfare, and International Law', (1972) 4 *Case W. Res. J. Int'l L.* 91 <<https://scholarlycommons.law.case.edu/jil/vol4/iss2/2>> accessed 30 September 2023

Kozlowski A, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan' (Vol 3 *International Scientific Forum* 2013) PL 236

Lanovoy V, 'The Use of Force by Non-State Actors and the Limits of Attribution of Conduct' (2017) 28 *EJIL* 455

Lucas Kello, 'Cyber legalism: why it fails and what to do about it' (2021) <
<https://ora.ox.ac.uk/objects/uuid:00c3488c-6eb4-4f2c-b1bc-143e91f6389b/files/rgh93gz99z>> accessed 23 October 2023

Mayer J, 'Government Hacking' (2017) Yale Law Journal PL 570

Opeskin B, 'Damages for Breach of Contract Terminated under Express Terms' (1990) 106 LQR 293

Ophardt J A, 'Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow's Battlefield' (2010) Duke L. & Tech. Rev PL 9

Rogers M, 'From Freeze to Fire: How Economic Sanctions against Japan Led to the War in the Pacific' (2018) The Thetean: A Student Journal for Scholarly Historical Writing

Willett M, 'The Cyber Dimension of the Russia–Ukraine War' (2022) Survival, PL 7

Zand A, Modelo-Howard G, Tongaonkar A, Lee S J, Kruegel C, Vigna G, 'Demystifying DDoS as a Service', (2017) Vol 55 IEEE Communications Magazine, PL 14

Other Works

'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 30 September 2023

‘OFSI Enforcement And Monetary Penalties For Breaches Of Financial Sanctions’ (Office of Financial Sanctions Implementation, HM Treasury, December 2023)

<https://assets.publishing.service.gov.uk/media/65844e9a23b70a000d234ded/Monetary_Penalty_and_Enforcement_Guidance_December_2023.pdf> accessed 4 December 2023

‘Russia's Poisoning Of Sergei And Yulia Skripal’ (Early Day Motions, 14 March 2018)

<<https://edm.parliament.uk/early-day-motion/51540/russias-poisoning-of-sergei-and-yulia-skripal>> accessed 17 December 2023

‘The Magnitsky Act At Five Years: Assessing Accomplishments and Challenges’ (Commission On Security And Cooperation In Europe, 14 December 2017) <<https://www.csce.gov/wp-content/uploads/2018/03/MagnitskyAt5.pdf>> accessed 14 December 2023

Analysis and Research Team, ‘The Business of War – Growing risks from Private Military Companies’ (2023) <<https://www.consilium.europa.eu/media/66700/private-military-companies-final-31-august.pdf>> accessed 27 September 2023

Article 51 of the Charter of the United Nations (https://www.nato.int/cps/en/natolive/official_texts/16937.htm).

Baloch T, ‘Unjust Enrichment in the Contractual Context’ (DPhil thesis, 2008).

Coalition Provisional Authority Order No 17 of 2004 (Revised) 2004

Comptroller and Auditor General, ‘Investigation: WannaCry cyber-attack and the NHS Report – Value for money’ (2017)

<<https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>> accessed 27 September 2023

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

<<https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1390&context=djcil>> accessed 25 July 2023

Dominic Bright, ‘UK Autonomous Sanctions System: Substantial Increase in the Costs of Compliance?’ (Lamb Chambers, 11 March 2020)

<<https://www.lambchambers.co.uk/jus-cogens/uk-autonomous-sanctions-system-substantial-increase-in-the-costs-of-compliance/>> accessed 29 November 2023

Duarte d’Almeida L, ‘Defences and Defeaters’ (DPhil thesis, 2011).

Executive Order 8832 - Freezing Japanese and Chinese Assets in the United States 1941

Foreign Commonwealth Office & The Rt Hon Dominic Raab MP, ‘Global Human Rights Sanctions regime: Foreign Secretary’s statement to Parliament’ (House of Commons, 6 July 2020) <

<https://www.gov.uk/government/speeches/statement-on-the-global-human-rights-sanctions-regime>> accessed 22 June 2023

Foreign Commonwealth Office and The Rt Hon Rishi Sunak MP, ‘UK announces first sanctions under new global human rights regime’ (Gov.UK, 6 July 2020) <
<https://www.gov.uk/government/news/uk-announces-first-sanctions-under-new-global-human-rights-regime>> accessed 14 December 2023

Hathaway O A, Crooto R, Levitz P, Nix H, Nowlan A, Perdue W, Spiegel J, 'The Law of Cyber-Attack' (California Law Review, Inc. 2012)
<https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf> accessed 16 September 2023

International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27000:2022, Information technology — Security techniques — Information security management systems — Overview and vocabulary (5th ed, 2022) <https://webstore.iec.ch/preview/info_isoiec27000%7Bed5.0%7Den.pdf> accessed 23 October 2023

Ministry of Defence, 'A Soldier's Guide to the Law of Armed Conflict' (2001)
<<https://assets.publishing.service.gov.uk/media/5a81f044ed915d74e6234ec0/2017-04714.pdf>> accessed 14 April 2023

Overton I, Benevilli E, Bruun L, 'Britain is the world centre for private military contractors – and it's almost impossible to find out what they're up to' (Open Democracy, 20 December 2018)
<<https://www.opendemocracy.net/en/opendemocracyuk/britain-is-world-centre-for-private-military-contractors/>> accessed 27 October 2023

Palka Dr W, 'The Awakening of Private Military Companies' (Warsaw Institute, 20 August 2020)
<https://warsawinstitute.org/wp-content/uploads/2020/08/RS_08-2020_EN.pdf>, accessed 2 July 2023

Promoting Accountability for Human Rights Abuse with Our Partners, 'Press Statement, Antony J. Blinken, Secretary of State' [March 22, 2021]

Quintin C, 'Tracking the Worlds Dumbest Cyber Mercenaries' (DEF CON 31, 11 August 2023) <<https://www.youtube.com/watch?v=zccAvgC4UxU>> accessed 16 September 2023

Rodenhäuser T, 'The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law' (2023) p10, p543
<<https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3054&context=ils>> accessed 30 May 2023

Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3
<<https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf>> accessed 23 April 2023

Russell M, 'Global human rights sanctions' (2021) Members' Research Service PE 698.791
<[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698791/EPRS_BRI\(2021\)698791_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698791/EPRS_BRI(2021)698791_EN.pdf)> accessed 28 September 2023

Sabrina Korreck Exploring Prospects for Digital Europe in the Age of the US-China Technology Race [2021] Observer Research Foundation

The Rt Hon Rishi Sunak MP, 'Responding to a more contested and volatile world' (Parliament, 13 March 2023) <
https://assets.publishing.service.gov.uk/media/641d72f45155a2000c6ad5d5/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf> accessed 14 December 2023

Treasury Targets Individuals Involved in the Sergei Magnitsky Case and Other Gross Violations of Human Rights in Russia, 'Press Release, U.S. Department of the Treasury' [December 20, 2017]