Private Active Cyber Countermeasures

ABSTRACT

The persistent onslaught of cyber-attacks faced by private actors triggers a re-examination of the current response options to the threat. This Opinion analyses the current regime and suggests a road map to unlocking the potentials of private actors through duly regulated self-help active cyber countermeasures. While active cyber countermeasures in the low-to-medium risk spectrum could be harnessed by private actors, some limits and safeguards are necessary. This Opinion makes this case by exploring a broad array of questions we must consider when thinking about private active cyber countermeasures.

TABLE OF CONTENTS

EXECUTIVE SUMMARY[1]

Cyberspace has become the fifth warfare domain. Cyber-attacks incessantly fill the headlines, from the recent malware attack which suspended COVID-19 certification service in Ireland,[2] the hacking of World Health Organization's networks,[3] to WannaCry and EthernalBlue that crippled hospitals in the U.K. Significant efforts have been taken yet they are unable to contain the pernicious cyber onslaught. Private sectors are warned of the next seismic pandemic – the cyber pandemic.

This struggle points towards unlocking the potentials of private actors through duly regulated self-help countermeasures as a supplementary response option. This option would permit private actors to defend themselves through low-risk and high utility cyber countermeasures under some circumstances and conditional upon safeguards.

This Opinion does not endorse destructive hacking back. Active Countermeasures which involve infiltration and asserting control of the adversary's network should remain prohibited unless authorized.[4]

It is hoped that the proposed framework and recommendations in this Opinion would help National Cyber Security Centre's (NCSC) deliberation in taking forward this cyber strategy to the Cyber and Government Security Directorate, and in turn shaping the trajectory of the private cyber defence landscape.

---

[1] I wish to express thanks to my supervisor, Professor Frederick Mostert, for his unparalleled support and invaluable insight.

[2] Craig Hughes, 'Ireland Shuts Down Health IT System After Ransomware Attack'(*MailOnline*,2021) <https://www.dailymail.co.uk/news/article-9578763/Ireland-shuts-health-ransomware-attack.html>accessed 31 August 2021.

[3] Christopher Bing and others, 'Elite Hackers Target WHO As Coronavirus Cyberattacks Spike'(*Reuters*,2020)<https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN>accessed 31August 2021.

[4] Whilst there is no agreed definition, the term "Active Countermeasures" adopted in this Opinion denotes a continuum of cyber-measures, which fall between passive and offensive measures (*see Figure 1*), and undertaken external to a defender's network or its third-party servers against initial cyber-attacker. The term "defender" denotes victims of cyber-attacks who employ Active Countermeasures.

KEY FINDINGS AND OPINION

1. Measures that can produce effects within and outside of a defender's network are proposed as an additional category to the existing typology of Active Countermeasures.

2. Active Countermeasures can be further classified into synchronous, succeeding, anticipatory, and preventive.

3. Current response options are inadequate:
    (i) Passive defences are ineffective.
    (ii) Legal solutions are of questionable utility as domestic legislation is limited in scope in criminalizing certain unlawful cyber-related offences.
    (iii) Practical hurdles remain a challenging complication to a successful claim.

4. Active Countermeasures are prohibited in most jurisdictions. Some jurisdictions neither prohibit nor explicitly authorise Active Countermeasures while some are unable to control these practices.

5. Various aspects of Active Countermeasures are consistent with the traditional doctrines of self-defence under common law and international law, hot pursuit, nuisance, and private just war.

6. Primary distinctions between a kinetic attack and a cyber-attack are, among others, the lethality of attack, the imminence of threat, the weapons used, the severity of harm, the intention of attacker, and the ease of attribution.

7. There are complications to the implementation of Active Countermeasures, namely the risks of escalation, misattribution, and collateral harm to innocent intermediaries. These complications may be minimised over time as attributional technology improves.

8. Key benefits of Active Countermeasures include deterrence, efficiency, speed, preservation of Intellectual Property, and confidentiality.

9. The proposed framework for Active Countermeasures is outlined as follows:

Stage 1 *Ex-ante* Regulation and Intervention

1. Licensing Requirement

- Only licensed private actors can undertake Active Countermeasures
- Imposition of sliding scale of security requirements on licensees
- Periodical review of license requirements

2. Registration Requirement

- Mandatory registration with NCSC and professional body

3. Accreditation Requirement

- Mandatory completion of accredited programs and continuing professional development training
- NCSC to act as patron of accreditation
- NCSC to develop technical proficiency standards required of defenders and certify cybersecurity firms for engagement
- NCSC to publish a list of registered defenders

⇩

Stage 2 Cyber Incident Response

Defenders to engage cyber incident response teams to decide the feasibility of Active Countermeasures and estimate the extent of damage and collateral damage

⇩

Stage 3 Authorisation

- Defenders to submit Proportionality Review and Collateral Damage Estimate Report to the designated high-level entity ("Authorisation Body")

- Authorisation Body to review and authorise the employment of Active Countermeasures or propose other countermeasures

⇩

Stage 4 Launching of Active Countermeasures

- Defenders to adhere to Code of Conduct
- Defenders to permit authorised officers on-site to ensure proper execution of Active Countermeasures if required

⇩

Stage 5 Third-parties Complaint Mechanism

- Third-parties are entitled to lodge complaints
- Third-parties are permitted to bring legal claims

⇩

Stage 6 *Ex-Post* Regulation and Oversight

- Defenders to submit after-action report
- Authorisation Body to subject to oversight by parliamentary bodies and judicial review
- Transparent disclosure of information by Authorisation Body

10. Other issues examined are summarized as follows:

Issues	**Recommendations**
Which Active Countermeasures are permissible?	Permissible Active Countermeasures should be countermeasures which are: 1) proportionate to the cyber-attack;

	2)duly limited in employment duration; 3) necessary; 4)reversible or impose the least irreversible harm; and 5) categorically restricted. Defenders should satisfy negotiation and notification requirements, where necessary. *(See Part VIII (C))*
Which entities would be permitted to employ Active Countermeasures?	Defenders which are permitted to employ Active Countermeasures should be entities that satisfy licensing, registration, and accreditation requirements; and possess sufficient technical maturity. *(See Part VIII (A))*
What level of certainty is required for attribution prior to the employment of Active Countermeasures?	All counterstrikes should be subject to a high evidentiary standard of proof: "balance of probabilities" standard if the source of attack is within the U.K. and "beyond reasonable doubt" standard for cross-border cyber-attacks and claims against State or State-sponsored actors. Stricter requirements in terms of nature and amount of evidence are imposed if the source of attack appears to be originating from State and State-sponsored attackers. *(See Part VIII (B))*
Which entity may authorise Active Countermeasures?	Review and authorisation should be undertaken by a high-level governmental entity, who works jointly with, including but not limited to, Secret Intelligence Service (MI6), Security

	Service (MI5), Government Communications Headquarters (GCHQ), Centre for the Protection of National Infrastructure (CPNI), National Crime Agency and its National Cyber Crime Unit, City of London Cybercrime Unit, Ministry of Defence, Defence Science and Technology Laboratory (DSTL) and NCSC. *(See Part VIII (A))*
What oversight and regulation are imposed?	Authorisation Body should be subject to oversight by parliamentary bodies and judicial review. Authorisation Body should be required to disclose information on licensing approval and authorization on the employment of Active Countermeasures. If necessary, certain information would be redacted. *(See Part VIII (A))*

11. Several challenges are identified and a summary of the proposed solutions are outlined as follows:

Challenges	**Proposed Solutions** *(See Part VIII)*
Irresponsible market practices in developing, supplying, and obtaining Active Countermeasure tools	1. Imposition of licensing requirement on vendors 2. Export control regulation for suspicious sales abroad 3. Transparency requirements in licenses
Misattribution and Collateral Damage	1. Imposition of criminal liability 2. Imposition of civil penalties

	3. Imposition of non-criminal enforcement actions, such as administrative penalties, caution, suspension and termination of licenses, and naming and shaming the offenders. 4. Adherence to Code of Conduct 5.Prohibition on employment of Active Countermeasures for non-attributable cyber-attack 6.Imposition of high evidentiary standard of proof for attribution 7.Strict requirements on attributional evidence prior to deployment 8.Transparency requirement to disclose attributional evidence to allow cross-checking and verification 9. Authorisation Body to subject to judicial review 10. Funding support for research and development in attributional technology
Complications of Cross-border Cyber-Attacks	1. Establishment of international cyber arbitration forum 2. Establishment of international cyber court 3. International treaties and protocols 4. Political commitments with allies 5. Issuance of public statement to put other States on notice 6. Increased international cooperation 7. Increased participation in international forums

Lack of Incentives to share information, cooperate, and report cyber incidents	1. Explore the potential application of Privacy Enhancing Technologies 2. Explore new model of information sharing,
Costs and technological barriers	1. Permit collective countermeasures and allow injured entities to seek help from other affected entities 2. Proactive role by NCSC to promote strong passive defence practices 3. Imposition of mandatory baseline or enhanced passive defence requirements on critical infrastructure operators and important private actors 4. Incentivise the technology industry to produce quality code 5. Encourage and educate private and public sectors to leverage contracting power appropriately 6. Awareness campaigns on the value of software updates
Legality of Active Countermeasures	Consider passing of legislation to permit limited employment of Active Countermeasures

12. The near-term recommendations for NCSC would be to set up an internal task force and an interagency working group on Active Countermeasures. NCSC should facilitate an establishment of a specialized threat focus hub to be led by private industry. NCSC should publish reports and a beta version of Active Countermeasures framework to gather feedback before taking forward the proposal to the Cyber and Government Security Directorate.

Part II. Definitions

Active Countermeasures are often used interchangeably with "hacking back" or "active defense". Whilst hacking back is a common contention when discussing active defence, it is not synonymous with active defence.[5]

It should be noted that the term "active defense" carries a different connotation in the U.K. and the U.S. The American usage is related to the circumstance where a victim counterstrikes with an out-of-network operation. In the U.K., active defence refers to in-network defensive capacities which are more active in nature.[6]

Active defense is defined by the United States Department of Defence (DoD) as "**synchronized, real-time** capability to discover, detect, analyse, and mitigate threats and vulnerabilities" which "operates at networks speed by using sensors, software, and intelligence to detect and stop malicious activity **before** it can affect DoD networks and systems" (emphasis added).[7] This interpretation, I submit, is only usable partially, as active defence is not only employed before malicious activity can affect a defender's networks but also during and after the occurrence of hostile cyber-attacks. Further, most cyber-attacks are not detected synchronously. The median time of a cyber-attacker being present on a network before detection is 146 days.[8]

An alternative definition is provided by the SysAdmin, Audit, Network, and Security (SANS) Institute which defines "active cyber defense" as "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network".[9] This definition, in my view, is incomplete as private entities increasingly use third-party servers

---

[5] The George Washington University Center for Cyber & Homeland Security,'Into The Gray Zone The Private Sector And Active Defense Against Cyber Threats'(2016)<https://spfusa.org/research/gray-zone-private-sector-active-defense-cyber-threats/> accessed 31 August 2021. *See also* Figure 1.

[6] Ciaran Martin, 'A New Approach For Cyber Security In The UK'(*Ncsc.gov.uk*,2016) <https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk>; The Hackback Debate'(*Cyberblog*,2012)<https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/>accessed 31 August 2021.

[7] 'Department Of Defense Strategy For Operating In Cyberspace'(US Department of Defense,2011)<https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>accessed 31 August 2021.

[8] 'M-Trends 2016'(Mandiant Consulting, 2016)<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf> accessed 31 August 2021.

[9] Robert Lee, 'The Sliding Scale of Cyber Security', *SANS Analyst White Paper* (2015)10 <https://www.sans.org/white-papers/36240/> accessed 31 August 2021.

and cloud infrastructure beyond their networks to host information. Therefore, I submit that any interpretation of Active Countermeasures should take into consideration processing in cloud infrastructure and third-party servers engaged by the defender.

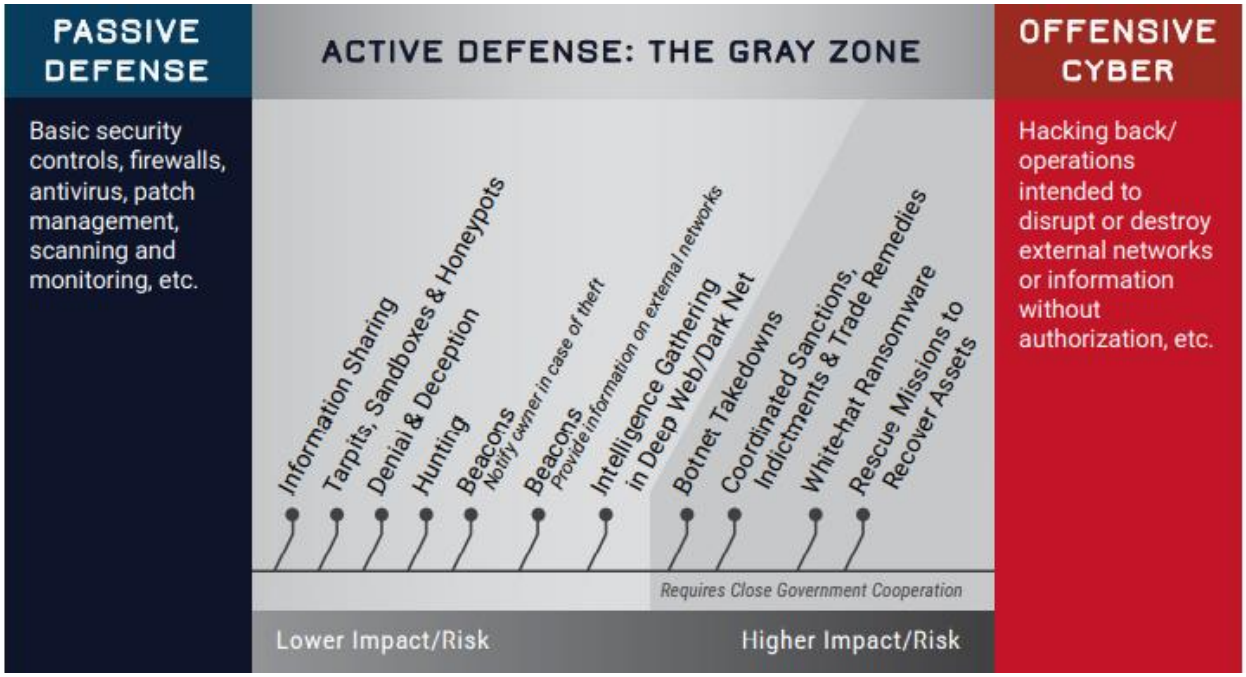


Figure 1 contains the main components of Active Countermeasures although there are differing opinions as to the constituents of the grey zone.[10]

Rosenzweig classified Active Countermeasures based on the effects they inflict on networks, namely "observation", "access", "disruption" and "destruction", and whether the countermeasures are internal or external to a defender's network.[11]

In my view, there is missing a third classification in Rosenzweig's typology, which is measures that can produce both the effects – internal and external to the defender's network. For instance, denial and deception measures which mix internal legitimate information with false data to

[10] *Supra* note 5 at 10. *See also* Appendix 1 and 2.
[11] Paul Rosenzweig, 'International Law And Private Actor Active Cyber Defensive Measures'(2014) 50 Stan. J. Int'L L.

confuse attackers. Further, it is unclear whether the external network effects in Rosenzweig's typology include effects on third-party networks which are not intermediaries or attackers.

The sampling of these interpretations suggests that there is no clear consensus on the definition of Active Countermeasures. In my view, the problem of definition is not merely one of wording. Both the conceptual and technical issues remain unsettled. Further, these definitions were shaped to suit the agendas of those drafting them and may not be very useful.

The term "hacking" is commonly interpreted as all forms of unauthorized access to one's computer, system, or network.[12] Just as diverse as the scope of hacking, Active Countermeasures can take many forms. In that spirit, I would like to suggest the following classification:

1. Synchronous Active Countermeasures

These are measures undertaken concurrently during a cyber intrusion. For example: using sandboxes or tarpits to slow attackers during the intrusion.

2. Succeeding Active Countermeasures

These are measures undertaken after cyber-attacks and when threats have disappeared. For example: gaining access into an attacker's network subsequent to the attack to delete or retrieve stolen data.

3. Anticipatory Active Countermeasures

These are measures undertaken when a threat is imminent or anticipated but before cyber-attacks. For example: accessing the system of a potential intruder to extract information before being attacked upon receipt of suspicious code.

4. Preventive Active Countermeasures

These are measures undertaken when there is no imminent or anticipated threat of cyber-attacks. For example: inserting a logic bomb within the software when it is being created.

[12]Computer Misuse Act 1990 (UK). *See also* Computer Fraud and Abuse Act (US), Cybercrime Act 2001 (Australia).

It should be noted that although it is possible to devise different labels according to the different activities concerned and the effects they may have, the categories may merge into one another in practice.

PART III. Current Response Options

This Part analyses the current lawful response options for a defender.

The first option is to undertake passive defence measures. For instance, a defender can deny network traffic or disable access to a system that is being attacked. Another option is to report the cyber-attack to law enforcement and seek to impose legal liabilities on the attackers and/or third parties who do not satisfy their responsibilities to guard against cyber-attacks.

1. Passive Defence

Passive defence is necessary for a resilient network but is no longer sufficient to address sophisticated cyber-attacks. Notably, the advanced persistent threat is characterized as "a new attack doctrine built to circumvent the existing endpoint defenses." [13] Only 6 percent of companies had detected cyber-attackers through passive defences.[14] To boot, 96 percent of networks monitored by FireEye with traditional defence measures were breached. [15] The recent figures further attest to this - 304 cases of significant attacks against critical sectors were recorded in Europe in 2020, more than double the 146 cases recorded in 2019. [16] This is despite that Europe fares the best regionally in terms of cyber capacity building and awareness as well as research and development according to the Global Cybersecurity Index 2020 and recorded more international agreements than other regions in the world.[17]

---

[13] Eric Chabrow, 'Tricked' RSA Worker Opened Backdoor To APT Attack' (*Bankinfosecurity.com*, 2011)<https://www.bankinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504>accessed 31 August 2021.

[14] *Supra* note 8 at 11.

[15] 'Maginot Revisited: More Real-World Results From Real-World Tests'(*FireEye*, 2015) <https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-maginot-revisited.html> accessed 31 August 2021.

[16] Nick Walsh, 'Serious Cyberattacks In Europe Doubled In The Past Year'(*CNN*, 2021) <https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html>accessed 31 August 2021.

[17] 'Global Cybersecurity Index 2020' (International Telecommunication Union, 2021) <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> accessed 31 August 2021.

2. Legal Solutions

(i) Claims against Cyber-attackers

In the U.K., Computer Misuse Act 1990 (CMA) criminalizes a broad variety of offences. It is an offence to cause a computer to perform any function with intent to secure unauthorized access to a program or data in any computer.[18] This includes employees' unauthorized access to employers' computers.[19] A person who intentionally or recklessly impairs the operation of a computer or data without authorization can be held liable under s. 3 of CMA.

Reading alongside Serious Crime Act 2015 (Explanatory Notes), s. 3 offences include circulating viruses, deleting files, and launching denial-of-service attacks (DoS). DoS is further prohibited under s. 36 of the Police and Justice Act 2006. Section 3ZA of CMA, Terrorism Acts 2000 and 2006, and common law offences, such as criminal damage, provide redresses for large-scale cyber-attack and cyber-terrorism.

Furthermore, it is an offence to make,[20] supply,[21] and obtain tools for computer misuse offences.[22] However, I submit that s. 3A of CMA is no longer fit for purpose. It merely criminalises creation, supply, and acquisition of such tools but excludes leased or rented tools. This is despite the fact that it is increasingly common for cyber-attackers to rent a botnet.[23]

I further submit that the term "unauthorized" should be revised to reflect development in technology. Pursuant to s. 17(8) of CMA, an act done in relation to a computer is unauthorized if the person doing the act is not himself "has responsibility for the computer and is entitled to determine whether the act may be done" and "does not have consent to the act". This concept of "unauthorised" assumes that all access could only take place within a computer owned or in the control of the defender. However, this no longer holds water. Access can take place in third-party servers or cloud infrastructure not owned by the defender.

---

[18] Computer Misuse Act 1990, s 1.
[19] *AG's Reference No. 2 of 1991*[1992]3 WLR 432.
[20] *Supra* note 18, s. 3A(1).
[21] *Ibid,* s. 3A (1) and (2).
[22] *Ibid,* s. 3A (3).
[23] Catalin Cimpanu,'You Can Now Rent A Mirai Botnet Of 400,000 Bots'(*BleepingComputer*,2016) <https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/>accessed 31 August 2021.

Where fraud is the essence of computer misuse offences, prosecutors can base charges under Fraud Act 2006 (FA). A case involving the use of a keyboard video mouse to hijack Barclay's Bank's systems is prosecuted under FA as opposed to CMA.[24] Phishing can potentially come under s. 6 and s. 7 of FA.

However, FA is only applicable to cyber-attacks that are conducted with the intent to defraud. Defenders may not have redress under FA for attacks that are conducted merely with intent to damage.

A person who unlawfully obtained personal data by means of a computer may be liable under s. 170 of the Data Protection Act 2018 (DPA). Nonetheless, DPA has its limitation as it will not be applicable to cases that do not involve personal data.

In respect of confidential information obtained and revealed by cyber-attackers, defenders can bring a claim under misuse of private information and breach of confidence.[25] Breach of contract may also extend to circumstances where an accused breached an implied duty of good faith in a commercial contract and accessed the defender's computer to download commercial information.[26]

On the face of it, these remedies may seem relevant but there are multiple obstacles in claiming damages. Where the defender's data has been stolen in cyber-attacks, it is a challenge to determine and quantify the damages until those exposed data is used against the defender. Another hurdle is that the defender would need to prove that a particular breach is sufficiently related to the damage, and not from other occasions of data breach.

---

[24]Lizzie Parry, 'Cyber Gang Led By Former Rave Promoter Dubbed The 'Acid House King' Are Facing Years Behind Bars For Plundering £1.25M'(*Mail Online*,2014)<https://www.dailymail.co.uk/news/article-2580383/Cyber-gang-led-former-rave-promoter-dubbed-Acid-House-King-facing-years-bars-plundering-1-25m.html>accessed 31 August 2021.

[25]*Ashton Investments Ltd v OJSC Russian Aluminium (Rusal)*[2006]EWHC 2545(Comm).

[26]*Bristol Groundschool Ltd v Intelligent Data Capture Ltd*[2014]EWHC 2145(Ch).

(ii) Claims against Third-parties

The main cause of DoS attacks is insecure software. [27] The current legal regimes provide for product liability claims where data breaches result from suboptimal code of software.

Product liability claims may be brought under the Consumer Protection Act 1987 (CPA), breach of contract, or negligence. However, I submit that there are significant hurdles for successful claims under these causes of action.

Firstly, CPA applies only to products and not services.[28] Courts' stance on whether software is considered as service or good varies. [29] Further, these claims may be defeated by the available defences. For instance, software and hardware producers may not be liable where "the defect did not exist in the product at the relevant time" [30] and where the product risks are not reasonably foreseeable during the product development. [31]

It is further submitted that elements of negligence are difficult to prove. To illustrate, even if a company has the obligation to protect its clients' data, the plaintiff must prove that the company's cybersecurity practices were so suboptimal that caused a breach of the duty of care. This may require a comparison of practices between different companies of similar operating environments to determine the level of "reasonable" cybersecurity practices.

Moreover, breach of contract claims often suffer from strict license agreements which disclaim or limit potential liabilities.

Additionally, there are significant hurdles to claim against intermediaries whose networks were used to launch cyber-attacks against the defenders. Firstly, requisite *mens rea* is often absent in

---

[27] Jennifer Chandler, 'Security In Cyberspace:Combatting Distributed Denial Of Service Attacks'(2003)1U Ottawa L & Tech Journal.
[28] Consumer Protection Act 1987, s 1(2).
[29] *See* for e.g., *Accentuate Ltd v Asigra Inc*[2009]EWHC 2655(QB)(software is intellectual property and hence is considered goods). *See also Computer Associates UK Ltd v The Software Incubator Ltd* [2018]EWCA Civ 518(supply of software in the form of a download is not sale of goods).
[30] *Supra* note 29, s 4(1)(d).
[31] *Ibid*, s 4(1)(e).

such claims. Secondly, there appears to be no case law in the U.K. and U.S. that shows that intermediaries owe a duty of care to victims of cyber-attack.

Further Analysis of Legal Solutions

As a practical matter, legal solutions are not very helpful to defenders.

Naturally, victims of cyber-attack could bring action against cyber-attackers. The civil and criminal liabilities mentioned above could all potentially be tied to the attackers. The prospects of success, however, may be uncertain due to attributional issues. It may be impossible to find and trace back to the responsible parties. In such cases, defenders may have no practical recourse against the attackers.

A second complication is when attackers are outside the country and hence beyond the effective reach of a domestic legal action. Therefore, even if the attribution hurdle can be overcome, it may still be impossible to bring a claim. Furthermore, civil suits are expensive and may attract adverse publicity.

Criminal liability may overcome some limitations of civil suits. For instance, law enforcement can exercise better investigatory ability besides its capability to seek extradition. Criminal conviction may have a better deterrence effect from judgment-proof scenario in a civil suit. In practice, however, law enforcement's track record is not encouraging.

The office for national statistics crime survey for England and Wales recorded 1764,000 cases of CMA offences, with 573,000 cases for s.1 CMA offences from April 2016 to March 2017.[32] However, the total cases for s.1, s.2, s.3, and s.3A CMA offences proceeded against are a mere 390

[32] 'Nature Of Fraud And Computer Misuse In England And Wales - Office For National Statistics' (*Ons.gov.uk*, 2019)<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#trends-in-computer-misuse>accessed 31 August 2021.

from 2007 to 2017.[33] Over this ten-year period, less than 1% of CMA offences result in conviction and sentencing.[34]

Additionally, criminal liability may not be a particularly effective tool against State actors or State-sponsored actors, especially foreign intelligence agents who engage in such activities as they are less likely to be arrested in custody. Further, studies had shown that legal deterrence only works with beginners and with young hackers under the age of twenty-five. [35]

[33]'FOI Releases For April 2017'(*GOV.UK*,2017)<https://www.gov.uk/government/publications/foi-releases-for-april-2017>accessed 31 August 2021.
[34]*Ibid.*
[35]Raoul Chiesa, Stefania Ducci and Silvio Ciappi, *Profiling Hackers : The Science Of Criminal Profiling As Applied To The World Of Hacking* (1st edn, CRC Press 2008) 74.

Part IV Legality of Active Countermeasures

United Kingdom

There are no specific laws prohibiting passive countermeasures undertaken internal to a defender's network, provided that they comply with data protection laws, CMA, and other relevant laws. Private actors are, however, prohibited from employing Active Countermeasures.

In 2018, the U.K. became the signatory of the Paris Call for Trust and Security Cyberspace ("Paris Call"). Principle 8 of the Paris Call is a general prevention on private hacking-back. UK's current stance does not run counter to the position taken in this Opinion, which is that offensive countermeasures, including hacking back, should be prohibited. Within these constraints, low-risk and properly circumscribed Active Countermeasures should be explored.

That said, the extent to which Paris Call will affect signatories' actions is arguable. In my view, it is but a representation of the need for cyber-diplomacy. Firstly, Paris Call is non-binding. Further, despite being a signatory, Microsoft undertook drastic measures in response to SolarWinds attack by quarantining malicious binaries that were used to install malware.[36] Additionally, the committee of Paris Call admitted that there is considerable ambiguity with the boundaries of "hacking-back" under Principle 8.[37] Influential State actors, such as the U.S, Iran, China, Russia, Israel, India, and Brazil are not signatories while other signatories express reservations with certain principles.[38]

United States

---

[36] Christopher Budd, 'Microsoft Unleashes 'Death Star' On Solarwinds Hackers In Extraordinary Response To Breach'(*GeekWire*, 2020)<https://www.geekwire.com/2020/microsoft-unleashes-death-star-solarwinds-hackers-extraordinary-response-breach/>accessed 31 August 2021.

[37] 'The Call And The 9 Principles — Paris Call'(*Pariscall.international*) <https://pariscall.international/en/principles>accessed 31 August 2021.

[38] 'Access Now To Join The Paris Call For Trust And Stability In Cyberspace'(*Access Now*, 2018) <https://www.accessnow.org/access-now-to-join-the-paris-call-for-trust-and-stability-in-cyberspace/>accessed 31 August 2021.

Provisions of Computer Fraud and Abuse Act (CFAA), particularly those that prohibit unauthorised access, typically prohibit Active Countermeasures. Legality of some Active Countermeasures which use less force than hacking back remains uncertain. Reversal of DoS attack to the origin server was held by Malinowski, the former head of New York Police Department's computer crime unit, as "action falling in grey zone".[39] Further, some scholars postulated that certain honeypot scenarios would not amount to unauthorised access although they may implicate other CFAA provisions.[40]

Additionally, Active Countermeasures may implicate state-level cybercrime legislation. As of August 2021, 50 U.S. states had adopted laws addressing unauthorised access; 26 states had adopted laws addressing distributed DoS attacks; 10 states had adopted laws addressing ransomware, and 22 states had adopted laws addressing spyware.[41] Nonetheless, the exact boundaries of these prohibited cybercrimes vary from state to state.

In my view, the *mens rea* requirement of the Washington Revised Code, is more stringent than many other states and CFAA. Mere intent would not suffice; "malicious" intent has to be proved for several offenses.[42]

Cybercrime legislation of some states is more specific and extensive than others. Connecticut, for instance, specifically provides for "destruction of computer equipment" and "misuse of computer information".[43] Florida Statutes provides for "offences against intellectual property".[44] In contrast to CMA, some States adopt affirmative defences. Texas Penal Code, for instance, provides defence for employees of "communication common carrier or electric utility" if their actions are necessary to protect their employers' property.[45]

---

[39] Deborah Radcliff, 'Can You Hack Back?' (*Edition.cnn.com*, 2000) <http://edition.cnn.com/2000/TECH/computing/06/01/hack.back.idg/>accessed 31 August 2021.
[40] 'Active Cyber Defense And Interpreting The Computer Fraud And Abuse Act' (*Lawfare*, 2018) <https://www.lawfareblog.com/active-cyber-defense-and-interpreting-computer-fraud-and-abuse-act> accessed 31 August 2021.
[41] *See* Appendix 3.
[42] *See* for e.g. RCW 9A.90.060; RCW9A.90.080
[43] Conn.Gen.Stat.Ann §§53a-251.
[44] Fla.Stat.§§815.04.
[45] Tex. Penal Code Ann.§§33.03.

Importantly, there are legislative proposals in the U.S. to legalise private Active Countermeasures. Georgia passed a bill in 2018 to permit Active Countermeasures although it was subsequently vetoed by the Georgia governor, citing national security implications.[46] In my view, the problem lies not with the right of private actors to defend themselves, but the excessively broad scope of the Georgia bill. It loosely endorsed hacking for "legitimate business activity", "violations of terms of service or user agreements" and "cybersecurity active defense". [47] These exemptions were unqualified and undefined in the bill and could easily be exploited for anti-competitive practices or malicious hacking under the guise of cybersecurity active defense.

Active Cyber Defense Certainty Act (ACDC) was re-introduced in the 116th Congress.[48] In June 2021, Study on Cyber-Attack Response Options Act was introduced in the Senate. This bill mandates the Secretary of Homeland Security to examine, among others, the potential consequences and benefits of private Active Countermeasures.[49]

In advocating for Active Countermeasures, Stewart Baker, the former official of the U.S. Department of Homeland Security, contended that a defender who retrieves stolen data from an attacker's computer may not violate CFAA even without authorization by virtue of the defender's ownership of stolen data on the attacker's computer.[50] Professor Kerr disagreed and asserted that CFAA's rationale is to protect the rights of computer owners, and not data owners, therefore authorization requirements cannot be circumvented.[51]

In my opinion, authorization requirement could be sidestepped on account of the defender's ownership of stolen data. However, Baker's argument is more fitting to CMA than CFAA. This is because the prohibition of unauthorized access in s. 1 of CMA is directed at "computer material" whereas the prohibition of unauthorized access in CFAA is aimed at "computer" as illustrated in

---

[46] Dillon Roseen, 'Georgia'S Governor Is About To Sign A Terrible Cybersecurity Bill'(*Slate Magazine*, 2018)<https://slate.com/technology/2018/04/georgias-governor-is-about-to-sign-a-terrible-cybersecurity-bill-into-law.html>accessed 31 August 2021.
[47] GA. S.B. 315 (2017).
[48] H.R. 3270,116th Congr. (2019). *See* Part VIII (2).
[49] S. 2292, 117th Congr. (2021).
[50] *Supra* note 5.
[51] *Ibid.*

§1030 (a)(1) – (7). Similar to CMA, the unauthorized access provision of most jurisdictions is data-centric, rather than computer-centric.

Other Jurisdictions

Majority of the countries have enacted cybercrime laws with similar provisions to CMA or CFAA, albeit with varying terms.[52]

My observation is that some jurisdictions, such as Bolivia and Guinea-Bissau, appear to neither prohibit nor explicitly authorise Active Countermeasures while some countries are unable to control or choose to actively ignore these practices.

Active Countermeasures are typically reserved for the States. For instance, South Korea expressly provides that the Minister of Science, ICT, and Future Planning shall perform "proper countermeasures against intrusion" and may order the Korea Internet and Security Agency to perform such a function.[53]

Some States allow internet service providers to undertake certain Active Countermeasures but with government oversight. For instance, France allows electronic communications operators to implement technical markers to detect security risks. [54] Technical markers are Active Countermeasures in the grey zone. Nonetheless, I submit that such markers are to be viewed as passive defences in this instance as they are allowed only on the internal networks of electronic communications operators.

[52] *See* Appendix 4.
[53] Act on Promotion of Information and Communications Network Utilisation and Information Protection, art. 48-2 (Korea)
[54] *Code des postes et des communications électroniques*, art.33-14 & 34-1 (France)

PART V LEGAL ANALOGIES

The purpose of this Part is to survey bodies of law and analogies that could conceivably support the legality of Active Countermeasures. Although these analogies have their limitations due to the distinctions in the physical world and cyberspace, they offer useful heuristics for thinking through the legal basis for Active Countermeasures.

1. Self Defence in Common Law

Active Countermeasures can draw support from self-defence as it is the most recognised right to ward off threats. Self-defence is available as a defence to a person in face of imminent bodily harm provided that (a) it is committed in defence of his own person, [55] and; (b) no more than reasonably necessary force is used or at least grossly disproportionate force is avoided. [56] A person is also justified in using force to avoid injury to his property.[57]

However, the distinctions between the physical world and cyberspace should not be overlooked. Self-defence in a physical world often involves an imminent threat whereas Active Countermeasures would most likely be undertaken after careful attribution, and in most cases, subsequent to the cyber-attacks when the danger is no longer imminent.

In my view, this does not necessarily preclude Active Countermeasures as a permissible act of self-defence. Defence of loss of control can traditionally be invoked provided that a victim can establish a reliant on the fear of serious future violence. [58] From the virtual perspective, if a network can be compromised in the first place, there is a threat that the networks could succumb to further cyber-attacks if left untreated. Self-defence against a future or persistent threat is

[55] *Moriarty v Brooks* [1834] EWHC Ech J79.
[56] *Cook v Beal* (1697) 1 LdRaym 176 (Drawing a sword and cutting off B's hand because A is struck by B is exerting disproportionate force).
[57] *Weaver v Bush* (1798) 8 Term Rep 78.
[58] Coroners and Justice Act 2009, s 54 & s 55.

acceptable, provided that reasonable force is used. Further, the interpretation of the imminence requirement should take into consideration the nature of cyber operations.

In a physical attack, people can ordinarily see and identify who the attacker is. In cyber-attacks, it may not be easy to identify which network belongs to the attacker and which belongs to the intermediary. Nonetheless, the law cannot expect a victim to absorb unjustified and serious harm although the harm is caused by or via an innocent party. In my view, such an expectation would compel the victim to subordinate his right to the interests of the malicious actors. The exception to the principle of no violence against innocent persons is recognised by Nozick, in which he wrote that one can use force in defense against a threat, even though "he is innocent and deserves no retribution".[59] Further, it is possible to draw support from case law. For instance, in *R v Hitchens,* it was held that self-defence can be used against an innocent person, provided that they pose an unjust threat.[60] Therefore, I submit that a cyber-attack victim may use force even against an intermediary. The caveats, however, are that: (i) it is necessary to use force; (ii) lesser force should be used; and (iii) the victim may be expected to absorb some of the harm.

Further, the weapons used in response to an attack in the physical world often involve nearby items picked up instinctively in the heat of the moment. However, in cyber-attacks, the tools used in counter-attacks are often carefully weighed and developed after investigation and attribution. This indicates that the level of harm that defenders seek to impose by means of cyber countermeasures could be adjusted to satisfy the proportionality requirement more easily compared to physical counter-attacks.

Another distinction is that the harm from cyber-attacks is less likely to involve fatality, except in the rare scenario of cyber-attacks on critical infrastructures, such as hospitals and air traffic systems. However, this distinction can be overcome as many Active Countermeasures are non-aggressive. Unlike physical fights, Active Countermeasures rarely inflict physical harm or fatality. Although the measure of what amounts to proportionate force should be assessed on a case-by-

[59] Robert Nozick, *Anarchy, State, And Utopia*(Ingram Publisher Service 1974)34.
[60] [2011]EWCA Crim 1626.

case basis and contingent upon the first assault, I submit that deleting the stolen copy in the attacker's system is proportional to the harm of an attacker hacking into the defender's system to steal the intellectual property.

Some commentators view Active Countermeasures as vigilantism.[61] In my view, vigilantism should be differentiated from self-defence. Vigilantism involves premeditation and voluntary engagement even when law enforcement is available [62] whereas self-defence is safeguarding oneself from existing threats, particularly when law enforcement is not within easy reach. Although there are regulations and legislation prohibiting unauthorised access to computers, law enforcement is not readily available as prosecution against cyber-attackers is extremely challenging and rarely be brought. Furthermore, vigilantism does not include acts undertaken by companies for commercial profit or acts undertaken by "responsible" citizens with State's support.[63] By contrast, any employment of Active Countermeasures is subject to approval by the government and undertaken by eligible practitioners.

That said, new principles may need to be developed. Concepts such as "grossly disproportionate force" and "reasonably necessary" clearly require a more definitive interpretation considering the unique characteristics of Active Countermeasures. This potentially opens the gates to different standards of reasonableness as the perspectives of prosecutors, judges, academicians, victims, and cybersecurity experts may vary substantially. To add, there is a plethora of different nature of cyber-attacks and cyber countermeasures tools. Synchronous Active Countermeasures further complicate the matter as it is difficult to ascertain the level of harm one would eventually suffer if the attacker is still launching the attack in the defender's network.

2. Self-defence in International Law

The right of self-defence is recognised under Article 51 of the United Nations Charter. [64] The Tallin Manual on the International Law Applicable to Cyber Operations 2013 (Tallin Manual) also

---

[61] Condé Nast, 'The Digital Vigilantes Who Hack Back'(*The New Yorker*, 2018) <https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back>accessed 31 August 2021.
[62]Les Johnston, 'What Is Vigilantism?'(1996)36The British Journal of Criminology.
[63] *Ibid.*
[64] (1945)1UNTS XVI.

sets out acceptable responses to cyber-attacks by drawing on the doctrine of self-defence. Specifically, Rule 9 states that "a State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures" while Rule 13 provides that "a State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence".[65]

From the language of the U.N. Charter, it is clear that an "armed attack" must have occurred to justify self-defence. "Armed attack" is not defined in the U.N. Charter. There are, however, three prevailing approaches to determine whether a cyber-attack constitutes an armed attack, namely the instrument-based,[66] target-based,[67] and effect-based approach.[68]

I submit that the effects-based approach should prevail. The International Court of Justice (ICJ) in the *Military and Paramilitary Activities in and against Nicaragua* case (Nicaragua case) ruled that self-defence is allowed only when the "armed attack" shows adequate "scale and effects" that "meet the threshold corresponding to the gravest forms of the use of force".[69] This "scale and effects" requirement, I submit, is in line with the "effects-based" doctrine, which is absent in the instrument-based and target-based approaches.

Further, the ICJ indicated that the term "armed" does not necessarily imply the use of weapons. In the words of the ICJ, "'[t]he Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons".[70] This is out of line with the "instrument-based" approach. This ruling, I further submit, suggests that self-defence would also be possible against an attack conducted by means of cyber weapons.

My observation, however, is that although characterizing cyber-attacks as "armed attacks" under Article 51 is not impossible, cyber-attacks are rarely declared as such in practice. To illustrate,

---

[65] Michael Schmitt (ed.)*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)41.
[66] Daniel Silver, 'Computer Network Attack As A Use Of Force Under Article 2(4)', *Computer Network and International Law* (1st edn, 2014).
[67] Eric Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense' (2002)38 Stan. J. Int'L L.
[68] Michael Schmitt, 'Computer Network Attack And The Use of Force In International Law: Thoughts On A Normative Framework' (1999)37Columbia Journal of Transnational Law.
[69] 1986 I.C.J.14.
[70]*Ibid*.

many significant cyber-attacks, for instance, the attack on Ireland's National Health Service in May 2021; the 2007 cyber-attack on Estonia which affected its parliament, banks, and government ministries; Operation Olympic Games which impacted the Iranian nuclear facilities in 2006; and the Stuxnet attack on Iran in 2010 – none have been recognized officially as an "armed attack".

Another issue is whether self-defence under international law should be extended to include instances when an attack is not attributable to a State actor. Rule 33 of the Tallin Manual reads that "international law, by and large, does not regulate cyber operations conducted by non-State actors, such as private individuals or companies".[71] Some commentators even went as far as suggesting that international law does not have a role in private hack-back.[72]

It is my submission that this understanding is flawed. Firstly, State may be responsible for the conduct of private parties if it fails to undertake due diligence [73] and necessary measures to prevent harm to another state. [74] Secondly, international instruments, such as Paris Call, specifically mention private hack-back. Thirdly, the enforcement and development of international law are dependent on private actors. To illustrate, some treaties are the products of negotiations with the significant involvement of non-governmental organizations. Multilateral copyright convention negotiations are even being described as a "battle between private corporations", and "academics and NGO". [75]

The more strenuous problem, in my view, is the absence of a harmonized international instrument to clarify the matter. Private actors may risk infringement of foreign domestic legislation, even if Active Countermeasures are legal in the U.K. Developing international norms in this sphere would be necessary to address this concern.

3. Private Just War Doctrine

[71] *Supra* note 65, 41.
[72] *Supra* note 11,107.
[73] *Supra* note 65, 179.
[74] Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001, Rule 4.
[75] Pamela Samuelson, 'The US Digital Agenda at WIPO', (1997)37 Va. J. Int'l L. 369, 432-33

The right of private actors is omitted from the Tallinn Manual as discussed above. However, such right is articulated by the Father of International Law, Grotius, in *De Jure Praedae* where he asserted that every human being possesses the right to carry on private wars, including "cases in which they are waged in conjunction with allies or through the agency of subjects".[76]

In De Jure Belli ac Pacis, Grotius wrote that "[w]ar is made against those who cannot be restrained in a judicial way".[77] He included acts of punishment and self-defense as just causes for wars.[78] Drawing from this conception of *bellum iustum privatum* (private just war), one could justify private Active Countermeasures in self-defence or when law enforcement is incapable of providing sufficient protection.

Nevertheless, I submit that before a cyber counter-strike can come within the scope of this private just "war" doctrine, one must ask if a cyber-attack can be assimilated to war.

A more appropriate contemporary definition of war is arguably the version propounded by Pufendorf, namely "a state of men who are naturally inflicting or repelling injuries or are striving to extort by force what is due to them".[79]

In my view, certain cyber incidents may fall squarely within or outside the scope of "war". Although most cyber-attacks would involve a breach of a state's territorial integrity, some of the attacks are not conducted with the aim of "inflicting injuries" or extorting what is due to the attacker. Furthermore, the weapons and consequential harms inflicted are mostly short of the lethality typically inflicted by an act of war.

---

[76]Hugo Grotius, *Commentary On The Law Of Prize And Booty(De Jure Praedae)*(2012 edn,Martine Julia van Ittersum(ed), Liberty Fund 2012).
[77]Hugo Grotius, *The Rights of War and Peace*(*De Jure Belli ac Pacis*)(2005 edn, vol. 1, Book I, Jean Barbeyrac, Richard Tuck (ed),Liberty Fund 2005.
[78]*Ibid.*
[79]Murray Alder, *The Inherent Right Of Self-Defence In International Law*(Springer Science & Business Media 2012).

In view of the above, I submit that a cyber incident that inflicts serious damage to critical national infrastructure and significantly harms national security may rise to the level of "war". On the other hand, a cyber incident that merely causes inconvenience is short of an act of war, for instance, a DoS attack that temporarily blocks the network traffic. Nevertheless, drawing a clear line between cyber incidents which come within the threshold of a "war" and those below the threshold can be difficult, compounded by the differences between a kinetic war and cyber war.

It is my submission that even if a cyber-attack is short of an act of war, a private actor's right to self-defence is not negated. Still and all, an attack short of war means that a less lethal countermeasure should be employed in such instances. Furthermore, the special moral rules of a "war" that restrict the negative effects of war could still be applied with appropriate adjustments. These include principles such as proportionality and necessity as discussed in Part VIII(C) below.

4. Hot Pursuit

Another doctrine that can be advanced in support of Active Countermeasures is the doctrine of hot pursuit, a right affirmed by Grotius in *De Jure Praedae* [80]

I. Sea

Maritime hot pursuit may be undertaken when competent authorities of a coastal State have good reason to believe that a foreign ship has violated its laws.[81] This right is enshrined in the Geneva Convention on the High Seas 1958 (Article 23) and the U.N. Convention on the Law of the Sea 1982 (Article 111), both of which were ratified by the U.K.

[80] *Supra* note 76.
[81] United Nations Convention on the Law of the Sea, Art.111(1).

Maritime hot pursuit is justified for "effective administration of justice of the injured State".[82] I submit that this objective which justifies maritime hot pursuit will also support its application to cyber hot pursuit. If hot pursuit is granted as necessary to maintain the order of sea, it is equally as necessary for such right in cyberspace.

II. Land

Pursuit by land across borders has not been recognized as a right in customary international law. **83**

However, it should be noted that some States proceeded to conclude bilateral and multilateral agreements to allow for such right. For instance, Schengen Convention on Border Controls 1990 (Schengen II) provides that officers are allowed to continue pursuing individuals in the territory of another contracting party without prior authorization. [84]

Those individuals being pursued must be caught in committing offences under Art. 4 of Schengen II. Receiving stolen goods and burglary are among the offences. [85] In my opinion, stealing data via unauthorized access to computers is akin to these two offences. I further submit that intentional destruction of critical infrastructure through malware can be analogized to the listed offence of "willful damage through the use of explosives".[86]

III. Air

Pursuit by aircraft beyond domestic air space is not recognised as customary international law.[87] States are entitled to require civil aircraft flying above their territory to land.[88] However, the use of aircraft in maritime hot pursuit is permitted [89].

---

[82] Nicholas Poulantzas, *The Right of Hot Pursuit in International Law* (2nd edn, The Hague: Martinus Nijhoff, 2002)2.
[83] *Ibid,* 11–12.
[84] Schengen Convention on Border Controls 1990, Art. 41(1)
[85] *Ibid,* Art. 4(4) (a)
[86] *Ibid,* Art. 41(4)(a)
[87] Hugo Caminos, 'Hot Pursuit' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law*, para 3.
[88] Article 3BIS Convention on International Civil Aviation
[89] *Yearbook of the International Law Commission* (1951) Vol I, 285

IV. Cyberspace

Upon analysis, there are several complications if hot pursuit were to be applied in the cyber context.

Firstly, hot pursuit, whether by sea or land, is only exercisable by law enforcement or the government. In particular, hot pursuit may be exercised only by ships or aircraft identifiable as "government service and authorized to that effect".[90] The statutory hot pursuit power under s. 86 of the Policing and Crime Act 2017 is exercisable only by "law enforcement officer". Under s. 38 of the Modern Slavery Act 2015, it is exercised only by "English and Welsh constable". A strict application would appear to preclude cyber hot pursuit by private actors.

Secondly, hot pursuit must commence when a foreign ship is within waters of the pursuing state, and may only continue outside the territorial sea if the pursuit is uninterrupted.[91] Interpretation of boundaries for pursuit in cyberspace is challenging. In my opinion, it could be interpreted as the boundary of a defender's own network or the territorial boundary of a jurisdiction. If we take the former interpretation, it may be complicated by the fact that not all cyber countermeasures are network-focused. For example, the law enforcement hacking tactic which was held to be lawful in *United States v. Henderson* involves overcoming the security of an encrypted device to gain access to data-at-rest.[92] Further, the boundaries of computer networks are often difficult to delineate. If we take the latter interpretation, the fact that cyber-attacks traverse multiple jurisdictions poses further challenges. Moreover, international consensus is difficult to achieve as States often attempt to construct borders around their internet infrastructure. There may also be varying interpretations of "uninterrupted pursuit" in cyberspace.

Maritime hot pursuit requires that pursuit be ceased as soon as a foreign ship enters the territorial sea of its own State or a third State".[93] Further, there is a requirement that the pursuit

[90] *Supra* note 81, Art.111(5).
[91] *Ibid,* Art.111(1).
[92] *United States of America v. Bryan Gilbert Henderson*, US Court of Appeals 9th Circuit No. 17-10230 (2018).
[93] *Supra* note 81, Art.111(3).

is a "hot" one.[94] Succeeding Active Countermeasures would certainly fail this rule as it is carried out after the cyber-attack.

Nonetheless, some Active Countermeasures scenarios may still fit the bill. I submit that tracking stolen data across servers and freezing the data before it reaches the attacker's network could be considered a legitimate application of hot pursuit in cyberspace.

Importantly, all of the requirements for maritime hot pursuit as stipulated in the UN Convention on the Law of the Sea are cumulative.[95] It is doubtful that Active Countermeasures could satisfy all the requirements if a strict interpretation is adopted.

That said, many States have begun to recognize the evolving threats. In fact, they sought to adjust the stringent requirements. For instance, a bilateral agreement was signed between France and Australia, authorizing hot pursuit beyond their territorial sea.[96] I submit that similar flexibility can be accorded to cyber hot pursuit.

In my view, hot pursuit is not precluded in all its rigour. As discussed above, hot pursuit is permitted until it touches the jurisdiction of another State. I submit that at the very least it is still applicable to cyber-attacks that occurred within a jurisdiction.

5. Nuisance

Another possible analogy is the doctrine of nuisance. "Nuisance" is incapable of exact definition.[97] Any interference with the use or enjoyment of a property that causes damage in relation to the ownership right can be a nuisance.

There are at least two scenarios in which the analogy is applicable. Firstly, cyber incidents which do not directly affect a property, but cause interference which prejudices the use of the property, are akin to a nuisance. Secondly, a person who creates nuisance can be liable even if he does not

[94] *Ibid,* Art.111(1).
[95] *Ibid*, Art. 111.
[96][2005] ATS 6.
[97]*Bamford v Turnley*[1862] EWHC Exch J63.

have the occupation of the property from which the nuisance proceeds.[98] This is relevant to the scenario where an attacker launches a DoS attack through zombie computers.

A victim has the right to abate nuisance, provided that (a) there is no breach of peace; (b) no more than the offending portion is removed;(c) no unnecessary damage is done; (d) where there are alternative ways to abate nuisance, the less mischievous is followed; and (e) notice is given when possible or necessary.[99] Applying this logic to the cyber context, if there is an intrusion to a defender's network, reasonable force could be used to abate such nuisance.

However, the doctrine of nuisance cannot be applied unreservedly to Active Countermeasures. Mere damages would not make an act a nuisance.[100] Only substantial interference would constitute a nuisance. It is thus submitted that cyber-attacks that cause minor interference may not rise to the level of nuisance.

Further, cyber incidents such as those which involve stolen data may not fit the bill as they do not interfere with the use or enjoyment of the defender's property. The defender still retains the data ownership. Additionally, the right to abate nuisance cannot be claimed if damages cannot be proved in cyber-attacks.

In my opinion, cyber-attacks that constitute physical intrusion or dispossession of networks more closely resemble a trespass than nuisance. The concepts of nuisance and trespass are, however, mutually exclusive.

[98] *Hubbard v Pitt* [1975] EWCA Civ J0513-1, at 19 per Orr LJ.
[99] Halsbury's Laws (5th edn, 2018) vol 78, para. 221.
[100] *See* for e.g., *Harrison v Good* (1871) LR11Eq 338(establishment of a school near a residence does not amount to nuisance); *Bamford v Turnley* (1862) 3B&S66 at 83 (discomfort caused by neighbour smoking his weeds does not constitute nuisance).

PART VI BENEFITS OF ACTIVE COUNTERMEASURES

This Part analyses the benefits of permitting Active Countermeasures.

1) Deterrence

Proponents assert that Active Countermeasures discourage attackers and would-be attackers through imposing costs, denying benefits, or encouraging restraint. [101]

In my view, a more pertinent question is whether Active Countermeasure is "adequate" to achieve the desired deterrence effect. The motivations of cyber-attackers are varied and vast. Increased costs and efforts might dissuade some of them, but it is likely to have a lesser impact on those who are motivated by personal satisfaction. Similarly, this deterrence argument is rendered unpersuasive against cyber-attackers with ideological and political motivations as they are not conveniently deterrable.

However, I would argue that the value of deterrence goes deeper than this. Even though it may not ward off all the malicious actors, deterring some of them still serves the larger public good. Harbouring some doubts on the exact efficacy of deterrence does not nullify this value.

2) Protection of Intellectual Property

Going one step further, Mostert aptly observed that Active Countermeasures could be used to hit counterfeiting at its source by preventing access to information necessary to create counterfeits, and to recover stolen knowhow.[102]

Examples of Active Countermeasures which are suited for this purpose would include deception tactics, such as DNS from Hell and Tripwire, [103] which lead attackers to false information;

---

[101] *Supra* note 9.

[102] Frederick Mostert, 'Digital Tools Of Intellectual Property Enforcement: Their Intended And Unintended Norm Setting Consequences', *Research Handbook on Intellectual Property and Digital Technologies* (1st edn, 2020). *See also* Frederick Mostert and Lianna Chan, 'Hacked Off: Protecting Intellectual Property Online' (2014) Intellectual Property Magazine 33.

[103] John Strand, *Offensive Countermeasures The Art of Active Defense* (2nd ed,2017)26.

watermarkers that track stolen information; beacon which reports IP addresses of attackers when files are stolen.

In fact, it was reported that Sony enlisted the help of Amazon Web Services to launch a counter-DoS attack to disrupt downloads of its stolen files.[104]

3) Efficiency and speed

Law enforcement, from investigation, prosecution to conviction is slow and frequently constrained by resources and jurisdictional issues.

Synchronous or anticipatory Active Countermeasure would allow an immediate response, preventing further harm when judicial remedy responds too slow, which is unproductive for cyber-attacks that proliferate at speed.

A case in point: In Operation Aurora, Google's immediate retaliation to a cyber-attack successfully avoided further theft and alteration of source codes. The counterattack also enabled Google to alert law enforcement that more than thirty other companies had been affected.[105]

4) Confidentiality

Private entities may be more inclined to undertake Active Countermeasures than resort to lawsuits as the latter attract publicity and may render their vulnerabilities openly. This might

[104] Dawn Chmielewski and Arik Hesseldahl,'Sony Pictures Tries To Disrupt Downloads Of Its Stolen Files'(2014)<https://recode.net/2014/12/10/sony-pictures-tries-to-disrupt-downloads-of-its-stolen-files>accessed31 August 2021.
[105] *Supra* note 61.

adversely affect their stock price[106]and/or reputation.[107] Further, these vulnerabilities may be used by competitors to their advantage. [108]

To illustrate, SolarWinds Orion's stock tumbled by 32% after the revelations of a devastating Supernova cyber-attack. [109]

[106]Katherine Campbell,'The Economic Cost Of Publicly Announced Information Security Breaches: Empirical Evidence From The Stock Market'[2013]J. Comput Secur.

[107] Nicole Perlroth, 'Some Victims Of Online Hacking Edge Into The Light'(*Nytimes.com*, 2013) <https://www.nytimes.com/2013/02/21/technology/hacking-victims-edge-into-light.html?ref=todayspaper> accessed 31 August 2021.

[108] '2004 CSI/FBI Computer Crime And Security Survey' (Computer Security Institute, 2004) <http://dls.virginia.gov/commission/pdf/2004%20CSIFBI%20Computer%20Crime%20and%20Security%20Survey.pdf>accessed 31 August 2021.

[109]Tomi Kilgore, 'Solarwinds Releases Updates In Response To SUPERNOVA Hack' (*MarketWatch*, 2020) <https://www.marketwatch.com/story/solarwinds-releases-updates-to-in-response-supernova-hack-2020-12-24>accessed 31 August 2021.

PART VII RISKS OF ACTIVE COUNTERMEASURES

This part analyses the risks and downsides of Active Cyber Countermeasures. Many of these risks are aggravated by attributes of the information environment itself.

1) Escalation

Commentators propounded that Active Countermeasures may serve as a vehicle for more attacks. [110] The identity of an attacker, especially when it is a State, State-condoned, or State-sponsored actor, complicates the matter. For example, engaging in a counter-attack against a foreign target may be misunderstood as a hostile action from a State. This could transform a cyber-attack into a genuine international crisis.

Looking through the historical lens, it is worth noting that there is yet to have serious escalation issues or cyberwar, despite the fact that cyber-attacks have been recurring for decades. That said, many safeguards have been proposed in this Opinion to mitigate against this risk. [111] To name one, the government would retain full authority for cyber-attacks involving State actors.

Another issue is that cybersecurity experts hired by private actors may have no interest in bringing the cyber-attack to an end and may even prolong it for higher rewards. I submit that this can be addressed by incorporating performance clauses into the contracts. This would provide cybersecurity experts with a clear incentive to complete the tasks they have been contracted for.

2) Misattribution and Collateral Damage

Admittedly, misattributing a cyber-attack could risk collateral damage to innocent parties. Often, hackers route their signals via many compromised third-party networks. To illustrate, DoS attack against the U.S. in 2009 was launched from an estimated 20,000-166,000 networks in at

[110] Josephine Wolff, 'When Companies Get Hacked, Should They Be Allowed To Hack Back?' (*Atlantic*, 2017) <https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/> accessed 1 September 2021.
[111] *See* Part VIII.

least six countries. [112] SolarWinds attack further demonstrates the complex attribution issue, with the U.S. appearing to be blaming Russia[113] while others believe it involved China. [114]

Nonetheless, the misattribution argument is probable but not insurmountable.

I submit that, firstly, if these compromised networks are left untreated, this will cause more rampant cyber-attacks. Many third-party networks are compromised because they do not have adequate passive defense safeguards and thus they are thought to assume some responsibility. Further, counterstriking against compromised networks does not inflict any "real" harm. Above all, these networks are already compromised.

There is a strong possibility of accurate attribution if appropriate technology is utilized. The U.S. government had successfully attributed cyber-attacks not only to the particular hacker units, but also the identity of the hackers within those units.[115] Besides, scholars and technologists are optimistic about the prospect of advancing technology which will ultimately solve some of the existing attribution issues. [116]

Moreover, many safeguards have been proposed in this Opinion to address this risk. In particular, counterstrike would be subject to a high standard of proof and would only be permitted if

---

[112]Elinor Mills, 'Botnet Worm In DOS Attacks Could Wipe Data Out On Infected Pcs'(*CNET*, 2009) <https://www.cnet.com/tech/services-and-software/botnet-worm-in-dos-attacks-could-wipe-data-out-on-infected-pcs/>accessed 31 August 2021.

[113]Lucas Ropek, 'U.S. Government Officially Blames Russia For Solarwinds Hack'(*Gizmodo*, 2021) <https://gizmodo.com/u-s-government-officially-blames-russia-for-solarwinds-1845996001>accessed 31 August 2021.

[114] Lucas Ropek, 'The Solarwinds Hack Just Keeps Getting More Wild'(*Gizmodo*, 2021) <https://gizmodo.com/the-solarwinds-hack-just-keeps-getting-wilder-1846193313>accessed 31 August 2021.

[115] CBS News, 'Most China-Based Hacking Done By Select Few' (2011) <https://www.cbsnews.com/news/most-china-based-hacking-done-by-select-few/>accessed 31 August 2021.

[116]Eva-Nour Repussard, 'There Is No Attribution Problem, Only A Diplomatic One' (*E-International Relations*, 2020) <https://www.e-ir.info/2020/03/22/there-is-no-attribution-problem-only-a-diplomatic-one/>accessed 31August 2021.

attribution can be proven.[117] The imposition of liabilities, either through legal remedies or insurance, is further suggested to internalize the costs of collateral damage.[118]

[117] *See* Part VIII.
[118] *Ibid.*

PART VIII RECOMMENDATIONS

This Part contains my recommendations to facilitate feasible and safe employment of Active Countermeasures as a supplementary measure to address the evolving cyber threats.

The recommendations are organised into four sections:

(A) Proposed Framework;
(B) Legislative Intervention;
(C) Principles for Permissible Active Countermeasures; and
(D) Barriers and Potential Solutions.

(A) Proposed Framework

Stage 1 *Ex-ante* Regulation and Intervention

1. Licensing Requirement

It is proposed that licensing requirement should be imposed to ensure that **only eligible players can employ Active Countermeasures**.

Different categories of licenses could be devised for such purposes. For instance, the licenses for Active Countermeasures which involve controls circumvention would have stricter requirements compared with the licenses for Active Countermeasures which only involve monitoring and intelligence gathering.

However, if this proposed measure were to be effective, policymakers should be mindful of the resources disparity among private actors as different sectors may have different levels of technology maturity, operating environment, and risk profile. Therefore, I would suggest **developing a sliding scale of security responsibilities** that the licensees would have to meet. For instance, licensees in sectors with a higher risk profile would have more onerous security commitments. The license requirements may include, for instance, a duty to report cyber incidents, audit obligation, and professional insurance subscription.

Requirements imposed on the licensees should be periodically reviewed in consultation with private stakeholders and cybersecurity experts.

I would further suggest the following non-exhaustive considerations before granting licenses for Active Countermeasures:

a. past conduct of licensee or its personnel which indicate a lack of fitness in performing Active Countermeasures;
b. internal policies of licensee on employment of Active Countermeasures, including third-party complaint mechanisms, and monitoring, investigation, and disciplinary procedures;
c. technical maturity, expertise, and capacity of the licensee;
d. possession of requisite qualifications and accreditation; and
e. lawful development, acquisition, and use of Active Countermeasures tools.

2. Registration Requirement

Defenders wishing to employ Active Countermeasures should register with the designated professional body and/or NCSC.

NCSC should **maintain a list of registered and licensed defenders.** This list could be published, if necessary, to serve as deterrence for would-be attackers.

3. Accreditation Requirement

In-house cybersecurity specialists and external contractors would be required to complete accredited programs and fulfill **mandatory continuing professional development** requirements.

I suggest that NCSC could act as a patron of the relevant cybersecurity accreditation and training. In this role, NCSC would:

a. **develop training and accredited programs**;
b. **develop standards for technical proficiency required of Active Countermeasures practitioners** (Technical Proficiency Standards); and
c. **certify cybersecurity firms and professionals for engagement by defenders** in line with the Technical Proficiency Standards.

Stage 2 Cyber Incident Response

When private actors are hit by cyber-attacks, they should first engage their **in-house specialists or incident response entities to advise** them on:

a. the suitability of employing Active Countermeasures;
b. which Active Countermeasures to be employed, and the impact and reversibility of such countermeasures;
c. estimation of damage caused by the cyber-attack;
d. estimation of damage to the intended target and collateral damage to third-party if Active Countermeasures were to be employed;
e. whether there is another recourse. This could include identifying whether any available passive defence measures could stop the attack, for instance, finding a decryption key to ransomware.

These incident response entities may include NCSC, cybersecurity firms, cyber-insurance providers, forensic investigators, threat intelligence analysts, legal firms, and negotiation firms.

Stage 3 Authorisation

Due to the potential risks, the **review of countermeasures and the decision to conduct counter-attack should be taken by a high-level governmental entity** ("Authorisation Body"). The Authorisation Body should collaborate with, among others, NCSC; major intelligence agencies, such as Secret Intelligence Service (MI6), and Security Service (MI5); Government Communications Headquarters (GCHQ); Centre for the Protection of National Infrastructure (CPNI); National Crime Agency; and City of London Cybercrime Unit; Ministry of Defence.

NCSC's current role as the cyber incident response contact could facilitate the role of the Authorisation Body.

If private actors decide to employ Active Countermeasures, they must prepare and submit a Proportionality Review and Collateral Damage Estimate Report ("Report") to the Authorisation Body.

The Authorization Body will then review whether to permit the employment of Active Countermeasures proposed in the Report, or suggest other countermeasures.

As time is of the essence for cyber incidents, I suggest that **different levels of review mechanisms could be devised, depending on the complexity of an attack and the nature of cyber threat,** for instance:

a) simplified review when defenders or authorised officers of the Authorisation Body assess the risk of damage as low, or that the countermeasures are of low impact;

b) standard review; and

c) enhanced review which involves an expedited process. This is applicable when the defender is a critical infrastructure operator or when there is a risk of serious damage to national security.

Stage 4 Employment of Active Countermeasures

As stated above, defenders would become registered members of a professional body. The professional body, in consultation with NCSC and other stakeholders, should **formulate a Code of Conduct** for responsible employment of Active Countermeasures.[119]

Defenders would undertake to adhere to the Code of Conduct. Additionally, defenders are obligated to comply with the directions given by the Authorisation Body and the license requirements. Any omission or breach would attract sanctions, penalties, and/or legal liabilities.[120]

Defenders would be required to permit authorised officers on-site to oversee and ensure proper execution of Active Countermeasures.

Stage 5 Third-parties Complaint Mechanism

[119] *See* Appendix 6.
[120] *See* Part VIII(B).

Third-parties or affected intermediaries are entitled to lodge a complaint through third-party or whistleblower complaint mechanisms if they have concerns about the conduct of defenders. Clear and easily accessible information on such mechanisms should be provided.

Additionally, **third parties or affected intermediaries should be permitted to bring legal claims against defenders**.[121]

Stage 6 *Ex-Post* Regulation and Oversight

I propose the following *ex-post* mechanisms:

(a) **Defenders would be required to submit after-action report**;
(b) **Authorisation Body may be required to disclose after-action reports and related investigation reports, and information relating to approval of Active Countermeasures**. If necessary, certain information would be redacted to protect commercial confidentiality and national security;
(c) **Authorisation Body would be subject to oversight by parliamentary bodies and judicial review**; and
(d) **Authorisation Body/relevant licensing agency may be required to disclose information relating to licenses approval.**

Near-term Recommendations

I would suggest that NCSC should first consider establishing an **internal task force**. A core function of the task force would be to consider policy proposals for Active Countermeasures.

NCSC should additionally establish and lead an **interagency working group** on Active Countermeasures. This working group would consist of representatives from private and public sectors, including governmental bodies, law enforcement, industry associations, and international organisations. The core functions of the working group would be to seek input from private and public stakeholders, identify challenges, and devise solutions.

[121] *See* Part VIII.

NCSC should facilitate the establishment of a **specialized threat focus hub** on Active Countermeasures. This threat focus hub would be led by private industry. The primary objective of the hub is to engage private stakeholders and industries to share and devise strategies for the employment of Active Countermeasures. Representatives from NCSC should participate in activities organised by the hub to collect and exchange information.

NCSC should **publish reports on Active Countermeasures and a beta version of the adoption framework to gather feedback** before taking forward the proposal to the Cyber and Government Security Directorate.

(B) Legislative Intervention

1. Affirmative Defence

CMA does not provide for any defences to s. 1, 2, 3, 3A, and 3ZA offences. I suggest that a qualifying defence can be introduced for qualified Active Countermeasures.

In this regard, the proposed ACDC Act could serve as a useful guide. ACDC provides defence for those who utilise "attributional technology" and permissible "active cyber defense measures" upon certain conditions.[122]

"Active cyber defense" measure is defined as measure undertaken by, or at the defender's direction, consisting of unauthorized access to the attacker's computer to gather information.[123] Defender is defined as victim of persistent unauthorised computer intrusion.[124]

The term "persistent" is included to possibly steer clear of floodgates in litigation if ACDC is open for invocation by defender who experiences only insignificant intrusion. However, more clarity is required for its interpretation.

Chesney suggests a series of intrusions by the same actor, or dwell-time, or both, as viable interpretations for "persistent". [125] Lin asked whether intrusions need to be similar to qualify as "persistent".[126]

I concur with Chesney. I would, however, add that one must be careful to **not equate "fleeting" with "insignificant"**. There are continuous intrusions that may not be hostile. Likewise, there may be short-lived yet extremely aggressive intrusion that can result in significant losses. For instance, a one-off intrusion into the healthcare system which causes medical devices to malfunction is brief but could cause significant harm.

---

[122] *Supra* note 48, s. 4.
[123] *Ibid.*
[124] *Ibid.*
[125] Robert Chesney, 'Legislative Hackback: Notes On The Active Cyber Defense Certainty Act Discussion Draft' (*Lawfare*, 2017) <https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft> accessed 31 August 2021.
[126] Herb Lin, 'More On The Active Defense Certainty Act' (*Lawfare*, 2017) <https://www.lawfareblog.com/more-active-defense-certainty-act>accessed 31 August 2021.

A better way, I suggest is to **clarify the term with indicators** of, including but not limited to, the degree and extent of the harm (whether or not the harm is anticipated), and the duration and frequency of the attack within a specified period. I would also suggest that such an approach should take account of the harm threshold in collective action by defenders.[127]

ACDC will not protect defender who intentionally destroys information not belonging to defenders on others' computer. [128] It is unclear whether this includes circumstances in which a defender encrypts the data on the attacker's computer, [129] or information replicated from systems of other victims.[130]

I would further add that **this section is unclear whether or not it also includes the circumstance where a defender mistakenly deletes or destroys certain data**, thinking that it is his or her data but which turns out to be erroneous.

ACDC will not protect defender who "recklessly causes physical injury or financial loss" to another person.[131] My view is that apart from physical injury and financial loss, other forms of non-financial losses, such as **reputational and emotional harm, should also be considered**. This is because private information obtained through unauthorized access is often released intentionally to cause negative reputational and emotional effects on the victims.

Similarly, ACDC will not protect defender who creates a threat to public health or safety.[132] The interpretation of "threat, public health, and public safety" is vague and the precise degree of risk should be clarified.[133]

A better way to define these terms, I submit, is to **include foreseeability of such threat**, and secondly to **include particular *mens rea* requirement**, such as recklessness, negligence, or with intent.

---

[127] *See* Part VIII(D)(5).
[128] *Supra* note 48, s.4(3)(B)(ii)(I).
[129] *Supra* note 125.
[130] *Supra* note 126.
[131] *Supra* note 48, s.4(3)(B)(ii)(II).
[132] *Ibid,* s.4(3)(B)(ii)(III).
[133] *Supra* note 125.

Additionally, ACDC will not protect defender who intentionally exceeds the level required to perform reconnaissance on an intermediary for attribution of the origin of intrusion or defender who intentionally results in intrusive or remote access into an intermediary's computer.[134]

I submit that this is potentially problematic as the **defender may not aware whether a particular network is a mere "intermediary" or belongs to an attacker**. I thus suggest that the **defence of mistaken belief** could be introduced in this respect.[135]

S. 5 of ACDC contains a **notification requirement** to the FBI National Cyber Investigative Joint Task Force prior to employment of Active Countermeasures.[136] I agree that the notification requirement should be a prerequisite. Nevertheless, I would suggest **a stricter regime, which requires specific approval**, rather than mere acknowledgment receipt.

If a similar path to that of ACDC were to be followed, I would suggest including a sunset clause, similar to that of s. 9 of ACDC.

2. Criminal Liability

One potential solution to mitigate against the risks of collateral damage is to permit affected third parties to claim against defenders.

In constructing the criminal liability for misconduct by defenders, I propose the following non-exhaustive considerations:

a) whether to criminalise attempts;
b) whether to impose accessorial liabilities;
c) defences to misconduct;
d) severity of harm and seriousness of misconduct; and
e) *mens rea* requirements.

[134] *Supra* note 48, s.4(3)(B)(ii)(IV) and (V).
[135] *See* for e.g., *DPP v Morgan*[1976]A.C.182 (mistake has to be "honest");*R v Tolson* (1889)23QBD 168(mistake must be both "honest" and "reasonably held").
[136] *Supra* note 48, s. 5 (m).

Determining the scope of offences is challenging, therefore consultation from the Attorney General's Office, Ministry of Justice, cybersecurity industry, academia, and the relevant stakeholders should be carried out.

3. Civil Liability

CMA does not currently have a parallel scheme of civil penalties.

I submit that the **introduction of civil penalties in the CMA** for the purposes of Active Countermeasures is desirable for two reasons. First, it is foreseeable that defenders may lack the requisite intent for prosecution. Secondly, there may be countervailing public interests against prosecution, such as the employment of unlawful but not unethical countermeasures.

There have been precedents for such parallel scheme. One example is the Investigatory Powers Act 2016 (s.7 and Schedule 1) which provides for the imposition of Monetary Penalty Notice in unlawful interceptions. Additionally, similar amendment was made to the Data Protection Act 1998 (s 55A-55E).

NCSC currently does not possess any regulatory function but Investigatory Powers Commissioner may be a potential regulator for the imposition of civil penalties in such cases.

4. Non-criminal Penalties

I suggest that other enforcement actions should be made available as an alternative to prosecution and for cases that are of lesser severity. In my opinion, the following options should be considered:

a) suspension and termination of licenses for defenders;
b) administrative penalties;
c) administrative caution; and
d) naming and shaming the offenders.

Procedural Concerns

From the procedural perspective, judiciary with sufficient technical knowledge is desirable. To that end, my recommendation is to develop a manual on Active Countermeasures to educate judges.

Besides that, both the prosecutorial and sentencing guidelines should be revised if Active Countermeasures were to be permitted.

(C) Principles for Permissible Active Countermeasures

In deciding which Active Countermeasures should be permissible, I propose the following principles, drawing from the several bodies of laws surveyed in Part V, including self-defence, private just war, hot pursuit, and nuisance.

I also draw support from the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001 ("Article").

1. Proportionality [137]

Active Countermeasures employed must be proportionate to the attack and respect fundamental human rights.[138]

The interpretation of "proportionality" may vary from case to case. In determining the proportionality, I suggest consideration of the following non-exhaustive factors:

(a) severity of damage (anticipated and actual);

(b)nature of damage (physical, mental, and/or financial harm);

(c) any recourse to damage suffered;

(d) potential impact of countermeasures; and

(e) possible intent of the attacker.

As proposed above, policymakers should mandate defenders to conduct proportionality review and collateral damage estimate before employing Active Countermeasures. An accurate estimation of the extent of attack and the impact of countermeasures may be difficult but such estimation should be based on an objectively reasonable standard.

2. Notification Requirement

[137]Articles on Responsibility of States for Internationally Wrongful Acts 2001, Art. 51.
[138] *Ibid,* Art. 50(1).

The Article requires that all countermeasures be preceded by notice and an offer of negotiation unless it is urgent cases of necessity.[139]

I depart from the Article on this issue. In the cyber setting, notification requirement may defeat the need for speed and secrecy for Active Countermeasures. In some cases, this might even prompt the attackers to take hostile action sooner than anticipated.

In my view, notification requirement should be considered on a case-by-case basis and should be dispensed with when necessary. Similarly, the negotiation requirement may not be effective in certain circumstances, particularly when it involves State-sponsored actors.

I would thus suggest that in cases where intermediaries can be identified, the defender should notify the affected intermediaries and seek their cooperation before the employment of Active Countermeasures, unless it is time-sensitive in which intermediaries would be informed after the response.

In cases where the defender is unable to determine which network belongs to the intermediaries, they would be notified after the response.

In cases where there is no notification, Active Countermeasures should be limited to a smaller, less critical, and more knowable parts of the attacker's or intermediary's network or system. This also applies in circumstances where intermediaries have been identified but refuse to cooperate, or there is difficulty in estimating the collateral damage.

3. Limited Time and Duration

The Article stipulates that countermeasures may not be taken if the "wrongful act has ceased" and dispute settlement procedures are pending.[140]

I agree that any Active Countermeasures should cease if a dispute resolution is underway. However, certain succeeding Active Countermeasures can be undertaken even if the attack has ceased, provided that the aim is to mitigate harm, and not for retribution. For instance, Active

[139] *Ibid,* Art 52(1).
[140] *Ibid*, Art 52.3.

Countermeasures which seek to retrieve and delete files stolen on the attacker's system may be allowed in certain circumstances, even if the attack has ceased.

Furthermore, the duration for employment of Active Countermeasures should be limited appropriately. A defender should cease controlling the attacker's or intermediary's network after Active Countermeasures are no longer required, or once the attacker has complied with settlement terms. The duration can be duly increased for persistent cyber-attacks.

4. Necessity

Active Countermeasure practitioners should be required to not use Active Countermeasures except in self-defence or to prevent a particularly serious crime involving grave threats to life and property.

5. Reversibility

Defenders should consider reversible countermeasures. For instance, a DoS attack is reversible as it causes a temporary traffic denial and the operation could resume when the countermeasure ceases. However, this reversibility requirement should not be absolute and should be reviewed on a case-by-case basis. If there is a choice between several feasible countermeasures with similar efficacy, countermeasures that are reversible, or that will incur the least irreversible harm should prevail.

The harm threshold for employment decisions by the Authorisation Body should be reduced appropriately for Active Countermeasures with lower risk and reversible effect.

6. Categorical restrictions

Certain excessively dangerous and irreversible Active Countermeasures should be banned outright.

It is stated in the Tallin Manual that anticipatory or pre-emptive countermeasures are prohibited.[141] I derail from this rule and submit that the prevalence and speed of cyber incidents justify anticipatory countermeasures. However, these countermeasures should only be allowed in cases of imminent cyber-attack which will cause serious harm, for instance, damages to critical national infrastructure which could harm lives. This is parallel to the right of self-defence where pre-emptive attack is considered lawful provided that it is reasonably necessary. [142]

In my view, synchronous Active Countermeasure could be undertaken during the cyber-attack provided that misattribution risk is low.

However, I would submit that preventive Active Countermeasure which is employed when no imminent threat is detected should be impermissible or only permitted in exceptional circumstances.

7. Attributable

Any malicious cyber-attack should be attributable to a high degree of accuracy before the employment of Active Countermeasures. Attribution should be made based on convincing and reliable evidence and information.

Active Countermeasures should not be deployed or authorised in non-attributable cyber-attacks. The standard of proof and requirements for such attribution are discussed in Part VIII(D)(2) below.

[141] *Supra* note 65, 118.
[142] *See* for e.g., *R v Deana* [1909] 2 Cr App R 75 (CA); *Beckford v The Queen* [1988] AC 130, 144 (PC).

(D) Barriers to Permitting Qualified Active Countermeasures and Proposed Solutions

1. Irresponsible market practices in developing, supplying and obtaining Active Countermeasures tools

It is reasonable to assume that defenders are either going to develop Active Countermeasures tools in-house, utilise pre-existing public vulnerabilities, or acquire the tools from a third party.

Investing in these tools from a third party can incentivise the development of a vulnerability market. It is not difficult to envision that vendors would sell these tools for profit to entities that utilize them in wrongful acts. In fact, vendors often offer these tools to controversial customers, including countries with atrocious civil rights records such as Ethiopia and Sudan.[143]

However, it may be difficult to ascertain the ultimate user of these tools and the purposes for which these tools are used. Additionally, an outright ban is not desirable.

The optimal framework, I suggest, would be to permit such sales only with sufficient *ex-ante* assessment and *ex-post* supervision.

One approach, in my view, is by imposing licensing requirement. Vendors, who wish to sell these tools, whether domestically or abroad, would have to be licensed. These license requirements should be categorical, for instance, it should exclude less intrusive hacking tools.

The second approach is through export control regulation for suspicious sales abroad. Wassenaar Arrangement is one export control framework we could model on. However, I would submit that the restrictions on export control should not be excessively broad to include products that are typically used for legitimate security and vulnerability research.

It should be noted that there may be enforcement challenges as it would be difficult to establish whether there has been any breach with the licensing terms when the activity and tools which are licensed are offered to overseas buyers. I submit that this could be addressed by incorporating transparency requirements in the license, which require vendors to disclose information related to such sales. Periodical compliance reports should be mandated, and

[143] Janus Rose,'Here Are All The Sketchy Government Agencies Buying Hacking Team's Spy Tech'(*Motherboard.vice.com*)<https://motherboard.vice.com/en_us/article/nzeg5x/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech>accessed 31 August 2021.

adequate resources should be allocated to the designated licensing agency for constant monitoring.

2. Misattribution and Collateral Damage to Third Parties

Another barrier is the potential risks of collateral harm to innocent third parties.

Firstly, I would suggest imposing a high evidentiary standard of proof for attribution before defenders could employ Active Countermeasures. Policymakers should consider imposing different standards of proof based on the nature of the threat. For instance, any attribution by defenders should satisfy the "balance of probabilities" standard if the source of an attack is within the U.K. while the "beyond reasonable doubt" standard is required for cross-border claims and claims against State or State-sponsored actors.

Stricter requirements should also be imposed in terms of nature and amount of evidence to be provided by defenders if the source of attack appears to be originating from State, State-sponsored, and State-condoned attackers. The Authorisation Body should decide whether the government should take the matter into its own hands when the cyber incident involves State or State-sponsored actors or affects the community as a whole.

Additionally, policymakers should impose a transparency requirement that requires defenders to disclose their attributional evidence to allow for cross-checking and verification by other parties. A case in point is the publication of an investigation report by Crowdstrike on the hacking of the Democratic National Committee networks attack which was subsequently verified by the Senate Intelligence Committee. [144]

Moreover, there should be *ex-post* mechanisms that subject the Authorisation Body to judicial review. The Authorisation Body should be required to explain the basis for its decision to approve Active Countermeasures applications by defenders.

[144] 'Our Work With The DNC: Setting The Record Straight'(*crowdstrike.com*,2020) <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>accessed 31 August 2021.

Although time-consuming, these measures promote cautious and credible attribution and reduce risks of collateral damage to third parties.

To further encourage the development of better attributional technology, the government should consider funding research and development in this sphere. Direct financial support could be provided for research to be undertaken by universities, governmental bodies, non-governmental bodies, and some private firms.

3. Complications of Cross-border Cyber-Attacks

Undeniably, responding to a cross-border cyber-attack would raise many transnational issues.

(i) International Cyber Arbitration

In the event of disputes with international elements, one way to hold foreign cyber-attackers liable without unconscionably imperilizing State sovereignty is through international arbitration.

The establishment of a specialized arbitral system for cross-border cyber disputes is desirable in this respect. This would open another avenue for affected defenders and States to recover damages from attackers.

I submit that the Court of Arbitration for Sport (CAS) could serve as a useful precedent. Analogous to the CAS, cyber arbitration could adopt the Convention on the Recognition and Enforcement of Foreign Arbitral Award (New York Convention). As of August 2021, 168 nations had ratified the New York Convention.[145] This worldwide enforceability of arbitral awards would allow redress against attackers who reside in other jurisdictions. Confidentiality of procedure and skilled panel of arbitrators are other added advantages. As for the cyber arbitration forum, International Telecommunication Union (ITU) may be a viable option.

(ii) International Cyber Court or Tribunal

Many commentators advocated for the establishment of an international cyber court. I concur that this would be one feasible solution to adjudicate on jurisdictional issues encountered in a cross-border cyber-attack.

---

[145] 'Contracting States'(*Newyorkconvention.org*)
<https://www.newyorkconvention.org/countries>accessed 31 August 2021.

Presently, the International Criminal Court (ICC) does not have jurisdiction over cybercrimes. [146] Although it is possible to broaden the jurisdiction of the ICC to include serious cyber offenses, this would be a time-assuming and arduous process in practice. An international cyber court would be a viable alternative. In fact, a Draft United Nations Treaty on an International Criminal Court for Cyberspace had been published by a former judge in support of such establishment. [147]

(iii) International Treaties and Agreements

Inconsistent interpretation of common cybercrime terms hinders effective communication and partnership. As a starting point, common cybercrime taxonomy should be explored.

International agreements and treaties would serve as an ideal forum within which to harmonise the taxonomy and approach for Active Countermeasures. New protocols on cybersecurity and cyber-attacks could be developed for inclusion in the Budapest Convention given the traction that it has garnered.[148] For instance, the Draft Second Protocol to Budapest Convention ("Draft Protocol") is a major step towards removing some of the barriers in prosecuting cross-border cyber-attacks as it provides for expedited disclosure when an emergency arises.

However, in practice, treaty-making on a multilateral basis is time-consuming. The first meeting of the drafting group was in 2017 but the Draft Protocol was only approved on 28 May 2021.[149] Further, there is often little consensus on the subjects of cyber-attacks among the participating countries.[150]

I suggest that, in such cases, agreements relating to cyber issues could first be formulated as political commitments with like-minded allies. To take one example, many duties in international environmental law have been drawn up as principles, instead of binding legal terms. [151] Furthermore, political commitments offer the benefit of inclusion of private

---

[146] UN General Assembly, *Rome Statute of the International Criminal Court* (17 July 1998)
[147] Stein Schjolberg, 'A Cyberspace Treaty' (*Cybercrimelaw.net*, 2010) <https://www.cybercrimelaw.net/Papers_on_Cybercrime.html> accessed 31 August 2021.
[148] See Appendix 4 for adoption rate of Budapest Convention and other international instruments.
[149] 'Protocol Negotiations'(*Council of Europe*) <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>accessed 31 August 2021.
[150]Antonia Chayes, 'Rethinking Warfare: The Ambiguity Of Cyber Attacks' (2015) 6 Harvard National Security Journal.
[151]*Ibid.*

stakeholders such as Internet Service Providers whereas an international treaty could only involve States and international organisations.[152]

(iv) Issuance of Public Statement

Given the unsettled law in this sphere, the government should publicly articulate its interpretation and policy of Active Countermeasures and put other States on notice, if the government decides to legalise Active Countermeasures.

For instance, the government could publicly state its taxonomy of Active Countermeasures, which countermeasures are permissible and which are banned, and any prerequisite for the undertaking of countermeasures.

This could offer several advantages. A first is to act as deterrence to would-be attackers. Secondly, it could lessen misunderstandings between States which in turn reduces the chances of escalation if Active Countermeasures are undertaken. Thirdly, this could contribute to the formation of *opinio juris* and customary international law on Active Countermeasures as many issues remain unsettled as a matter of international law.

As cyber-attacks often involve victims spanning multiple jurisdictions, the government should also consider negotiation with other like-minded States to cooperate on a joint undertaking of collective countermeasures.

(v) Increased International Cooperation

Additionally, the government should participate more actively in international forums such as The North Atlantic Treaty Organisation (NATO), United Nations General Assembly, and Open-Ended Working Group. This would help to develop consensus on Active Countermeasures.

In addition to its existing partners, NCSC should fully explore cooperation with domestic, international, and regional policing bodies, for instance, the International Criminal Police Organisation (INTERPOL), particularly through its Global Cybercrime Expert Group (IGCEG),

[152] *Ibid.*

ASEAN Chiefs of National Police (ASEANAPOL), The Police Community of the Americas (AMERIPOL), and the US Department of Homeland Security.

4. Lack of Incentives to share information, cooperate and report cyber incidents

There are numerous examples of cooperation between law enforcement, non-governmental organisations, and private sectors, such as the No More Ransom![153] led by the Europol, and the Global Cyber Alliance led by the City of London Police Commissioner.[154] Yet, many of these initiatives are inadequately utilized. Private actors tend to be reluctant to report cyber incidents and share information with the public sector due to commercial and privacy concerns.

I propose that the government should consider exploring the potential application of Privacy Enhancing Technologies (PETs) in cybersecurity information sharing and investigation. Examples of PETs, namely secure multiparty computing, federated learning, and homomorphic encryption, have been recently utilized in financial services[155] and healthcare.[156] PETs provide data owners full control and protect data confidentiality, while still making it possible for data evaluation by the recipient. This could potentially alleviate data protection and privacy challenges, domestically and internationally, that have restricted the participation of private actors.

5. Costs and technological barriers

[153]'No More Ransom: How 4 Millions Victims Of Ransomware Have Fought Back Against Hackers' (*Europol*, 2020)<https://www.europol.europa.eu/newsroom/news/no-more-ransom-how-4-millions-victims-of-ransomware-have-fought-back-against-hackers> accessed 31 August 2021.

[154] 'Cyber Attacks Increase As People Work From Home'(*Cityoflondon.police.uk*, 2020) <https://www.cityoflondon.police.uk/news/city-of-london/news/2020/template4/press-releases/cyber-attacks-increase-as-people-work-from-home/>accessed 31 August 2021.

[155]Sujata Dasgupta, 'EXPLAINER: The PET Revolution - How Preserving Data Privacy In Intelligence Sharing Is A Game Changer In The Global Fincrime Sector'(*AML Intelligence*, 2021)<https://www.amlintelligence.com/2021/01/insight-the-pet-revolution-preserving-data-privacy-to-change-the-game-in-fincrime-intelligence-sharing/>accessed 31 August 2021.

[156]James Scheibner and others, 'Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, And Ethical Synthesis' (2021) 23 Journal of Medical Internet Research.

Some private actors may have legitimate needs but lack expertise and resources to employ Active Countermeasures. This may intensify the digital divide.

One possible approach to minimise resource disparities is to permit an injured private entity to request help from other affected private entities who suffer from the interconnected cyber-attacks to support each other's response plan, provided that the countermeasures are proportionate to the attack. This could take the form of information sharing, attribution support, and/or collective counter-attack against the attacker. However, such collective action should be subject to a stricter review by the Authorisation Body.

Furthermore, passive defences are important in helping under-resourced private actors to maintain resilient networks against future attacks. The U.K. government's proposed legislation to impose cyber-security baseline requirements for smart products is laudable.[157] I suggest that similar baseline passive defence or enhanced security requirements should be extended to certain critical infrastructure operators and important private actors.

Another effective way, in my view, is to incentive the technology industry to produce quality code. Different incentive schemes, such as tax relief schemes, could be developed for different sectors, from software producers to Internet Service Providers, to incentivize them to improve cybersecurity products and services.

NCSC should also encourage and educate private and public sectors to leverage contracting power appropriately to create a pro-defence impact. This could include, for instance, educating defenders on the importance of requesting certain cybersecurity steps in place before executing contracts with security firms to employ Active Countermeasures.

Moreover, NCSC should consider including awareness campaigns on the value of software updates to its existing engagement and training programs. This could improve awareness of the risks of supply-chain cyber-attacks.

---

[157] 'Government Response To The Call For Views On Consumer Connected Product Cyber Security Legislation'(*GOV.UK*, 2021)<https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation> accessed 31 August 2021.

PART VIII CONCLUSION AND NEXT STEPS

The path forward is to consider low-risk and high utility Active Countermeasures as a supplementary response option to cyber-threats. Offensive countermeasures that pose detrimental risks to human welfare, notably hacking back, should be prohibited. Various aspects of Active Countermeasures are clearly consistent with the traditional doctrines of self-defence, hot pursuit, nuisance, and private just war; and require no special justification. These countermeasures are justified in many contexts, specifically when law enforcement is incapable of offering adequate protection or in defending critical sectors against serious cyber-threats.

Potential complications, particularly misattribution and collateral damage can be mitigated through the proposed safeguards and framework in the forms of regulation, liability, and incentives. Efforts in fostering public-private collaboration, cyber-diplomacy, and developing international norms are instrumental for responsible employment of Active Countermeasures. It may be that some of the contemplated complications are less problematic than anticipated in practice.

All in all, it would not only be feasible but advisable to experiment with a pilot project of Active Countermeasures within a sunset period. Several low-risk but high-utility countermeasures could be considered as a starting point.

Based on the analysis in this Opinion, I recommend the following action points to be considered by NCSC.

Near-term Recommendations

NCSC should consider:

1 establishing an internal taskforce

2 establishing an interagency working group

3 facilitating the establishment of a specialized threat focus hub

4 publishing report and a beta version of adoption framework on Active Countermeasures to gather feedback

5 coordinating public-private cooperation, domestically and internationally, in developing an implementation plan for Active Countermeasures

6 funding Active Countermeasures related research and development

7 taking forward the proposed policy to the Cyber and Government Security Directorate

8. conducting research on mandatory security requirements on critical infrastructure operators and significant private actors

9. including awareness campaigns on the value of software updates to its engagement programs

Medium and Long-term Recommendations

NCSC should consider:

1. supporting the passing of legislation for qualified Active Countermeasures

If Active Countermeasures are legalised, NCSC should consider:

1. encouraging the development of code of conduct and best practices

2. developing accredited programs in consultation with private actors

3. developing Technical Proficiency Standards required of defenders

4. supporting capacity building for judiciary and revision of prosecution and sentencing guidelines for the employment of Active Countermeasures

5. supporting the introduction of legal liabilities and non-criminal penalties for unlawful employment of Active Countermeasures

6. supporting the imposition of licensing, registration, and accreditation requirements concerning Active Countermeasures

7. supporting the regulation of making, supplying, and obtaining Active Countermeasures tools

8. supporting the establishment of a specialized system for international cyber arbitration and International Cyber Court

9. supporting and promoting proper and transparent governance and oversight mechanisms for the employment of Active Countermeasures

Appendix 1

Note: White-hat ransomware is ranked below coordinated sanctions, indictments, and trade remedies in terms of its level of impact/risk when compared to Figure 1.
Source:Paul Rosenzweig, Steven Bucci and David Inserra, 'Next Steps For U.S. Cybersecurity In The Trump Administration: Active Cyber Defense' (2017) <https://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense>

Appendix 2 Definition of Active Cyber Defense Measures

Source: The George Washington University Center for Cyber & Homeland Security, 'Into The Gray Zone The Private Sector And Active Defense Against Cyber Threats' (2016) <https://spfusa.org/research/gray-zone-private-sector-active-defense-cyber-threats/>

Appendix 3

STATE-LEVEL CYBERCRIME LAWS

Laws addressing Hacking, Unauthorised Access, Computer Trespass, Viruses and Malware

No.	Name of State	Title of Legislation and Relevant Provisions
1.	Alabama	Alabama Code §§ 13A-8-112
2.	Alaska	Alaska Statutes § 11.46.740
3.	Arizona	Arizona Revised Statutes §§ 13-2316,13-2316.01,13-2316.02
4.	Arkansas	Arkansas Code §§ 5-41-101 et seq.
5.	California	California Penal Code § 502
6.	Colorado	ColoradoRevised Statutes §§ 18-5.5-101 to -102
7.	Connecticut	Connecticut General Statutes §§ 53a-250 to 53a-261, 53-451
8.	Delaware	Delaware Code title 11 §§ 931 to 941
9.	Florida	Florida Statutes §§ 815.01 to 815.07, 668.801to .805
10.	Georgia	Georgia Code §§ 16-9-90 to 16-9-94, 16-9-150 to 16-9-157
11.	Hawaii	Hawaii Revised Statutes §§ 708-890 to 708-895.7
12.	Idaho	Idaho Code §§ 18-2201 et seq.
13.	Illinois	Illinois Compiled Statutes Chapter 720 §§ 5/17-50 to -55
14.	Indiana	Indiana Code §§ 35-43-1-8, 35-43-2-3
15.	Iowa	Iowa Code §§ 716.6B, 702.1A, 702.14, 714.1(8)
16.	Kansas	Kansas Statutes § 21-5839
17.	Kentucky	Kentucky Revised Statutes §§ 34.840, 434.845, 434.850, 434.851, 434.853, 434.855, 434.860
18.	Louisiana	Louisiana Revised Statutes §§ 14:73.1 to 14:73.8
19.	Maine	Maine Revised Statutes title 17-A, §§ 431 to 435

20.	Maryland	Maryland Code Criminal Law § 7-302
21.	Massachusetts	Massachusetts General Laws chapter 266 § 33A, chapter 266 § 120F
22.	Michigan	Michigan Compiled Laws §§ 752.791 et seq.
23.	Minnesota	Minnesota Statutes §§ 609.87 to 609.893
24.	Mississippi	Mississippi Code §§ 97-45-1 et seq.
25.	Missouri	Missouri Revised Statutes §§ 537.525, 569.095, 569.097, 569.099
26.	Montana	Montana Code Annotated §§ 45-2-101, 45-6-310, 45-6-311
27.	Nebraska	Nebraska Revised Statutes §§ 28-1341 to 28-1348
28.	Nevada	Nevada Revised Statutes §§ 205.473 to 205.513
29.	New Hampshire	New Hampshire Revised Statutes §§ 38:16, 638:17, 638:18, 638:19
30.	New Jersey	New Jersey Revised Statutes §§ 2A:38A-1 to -3, 2C:20-2, 2C:20-23 to 34
31.	New Mexico	New Mexico Statutes §§ 30-45-1 to 30-45-7
32.	New York	New York Penal Law §§ 156.00 to .50
33.	North Carolina	North Carolina General Statutes §§ 14-453 to 14-458
34.	North Dakota	North Dakota Century Code § 12.1-06.1-08
35.	Ohio	Ohio Revised Code §§ 909.01(E-G), 2909.04(B), 2909.07(A)(6), 2913.01 to 2913.04
36.	Oklahoma	Oklahoma Statutes title 21, §§ 1951 to 1959
37.	Oregon	Oregon Revised Statutes § 164.377
38.	Pennsylvania	Pennsylvania Consolidated Statutes title 18 §§ 7601 et seq.
39.	Rhode Island	Rhode Island General Laws §§ 11-52-1 to 11-52-8

40.	South Carolina	South Carolina Code §§ 16-16-10 to 16-16-40
41.	South Dakota	South Dakota Cod. Laws §§ 43-43B-1 et seq.
42.	Tennessee	Tennessee Code §§ 9-14-601, 602, 604, 605
43.	Texas	Texas Penal Code § 33.01
44.	Utah	Utah Code §§ 76-6-701 et seq.
45.	Vermont	Vermont Statutes Annotated title 13, §§ 4101 et seq.
46.	Virginia	Virginia Code §§ 18.2-152.1 to -152.15,19.2-249.2
47.	Washington	Washington Revised Code §§ 9A.90.010 et seq.
48.	West Virginia	West Virginia Code §§ 61-3C-3 to 61-3C-21
49.	Wisconsin	Wisconsin Statutes § 943.70
50.	Wyoming	Wyoming Statutes §§ 6-3-501 et seq., 40-25-101

Laws addressing Denial of Service Attacks

No.	Name of State	Title of Legislation and Relevant Provisions
1.	Alabama	Alabama Code § 13A-8-112(5)
2.	Arizona	Arizona Revised Statutes § 13-2316(4)
3.	Arkansas	Arkansas Code § 5-41-203(a)
4.	California	California Penal Code § 502
5.	Connecticut	Connecticut General Statutes § 53a-251
6.	Delaware	Delaware Code title 11, § 934
7.	Florida	Florida Statutes § 815.06(2)(b)
8.	Georgia	Georgia Code § 16-9-93(b)(2)
9.	Indiana	Indiana Code § 35-43-1-8
10.	Louisiana	Louisiana Revised Statutes Annotated § 14:73-4
11.	Mississippi	Mississippi Code § 97-45-5
12.	Missouri	Missouri Revised Statutes § 569.099
13.	Nevada	Nevada Revised Statutes § 205.477
14.	New Hampshire	New Hampshire Revised Statutes Annotated § 638:17
15.	North Carolina	North Carolina General Statutes § 14-456, 14-456.1
16.	Ohio	Ohio Revised Code § 2909.01
17.	Oklahoma	Oklahoma Statutes title 21 § 1953
18.	Pennsylvania	Pennsylvania Consolidated Statutes § 7612
19.	South Carolina	South Carolina Code § 16-16-10(3)
20.	Tennessee	Tennessee Code § 39-14-601

21.	Texas	Texas Penal Code § 33.022
22.	Utah	Utah Code § 76-6-703(10)
23.	Virginia	Virginia Code § 18.2-152.4
24.	Washington	Washington Revised Code § 9A.90.060
25.	West Virginia	West Virginia Code § 61-3C-8
26.	Wyoming	Wyoming Statutes § 6-3-504

Laws addressing Ransomware and Computer Extortion

No.	Name of State	Title of Legislation and Relevant Provisions
1.	California	California Penal Code § 523
2.	Connecticut	ConnecticutGeneral Statutes § 53a-262
3.	Indiana	2021 Indiana House Bill 1169
4.	Louisiana	Louisiana Revised Statutes §§ 51:2111 to 51:2116
5.	Maryland	2021 Maryland House Bill 425 / 2021 Senate Bill 623
6.	Michigan	Michigan Penal Code §§ 750.409b, Section 777.16t
7.	Oklahoma	2021 Oklahoma House Bill 1759
8.	Texas	Texas Penal Code § 33.02 and 2021 Texas House Bill 3390
9.	West Virginia	West Virginia Code §§ 61-3C-3 to 61-3C-4
10.	Wyoming	Wyoming Statutes §§ 6-3-506, 6-3-507

Laws addressing Phishing

No.	Name of State	Title of Legislation and Relevant Provisions
1.	Alabama	Alabama Code §13A-8-114
2.	Arizona	Arizona Code §§ 4-111-102, 4-111-103
3.	Arkansas	Arkansas Revised Statutes §§ 18-541 to-544
4.	California	California Business and Professions Code §§ 22948 to 22948.3
5.	Connecticut	Connecticut General Statutes § 53-454
6.	Florida	Florida Statutes §§ 668.701-.705
7.	Georgia	Georgia Code § 16-9-109.1
8.	Illinois	Illinois Compiled Statutes 740 §§ 7/1 - 7/15
9.	Kentucky	Kentucky Revised Statutes 434.697
10.	Louisiana	Louisiana Rev. Stat. §§ 51:2021 et seq.
11.	Michigan	Michigan Compiled Laws § 445.67a
12.	Minnesota	Minnesota Statutes § 609.527, Subd. 5a
13.	Montana	Montana Code Annotated §§ 30-14-1712, 33-19-410
14.	New Mexico	New Mexico Statutes § 30-16-24.1
15.	New York	New York General Business Law § 390-b
16.	Oklahoma	Oklahoma Statutes title 15, §§ 776.8 - 776.12
17.	Oregon	Oregon Revised Statutes § 646.A.808
18.	Rhode Island	Rhode Island General Laws §§ 11-52.1-1 to -5
19.	Tennessee	Tennessee Code §§ 47-18-5201 to 47-18-5205
20.	Texas	Texas Business and Commerce Code §§ 325.001 - .006
21.	Utah	Utah Code §§ 13-40-201 to -204, -401
22.	Virginia	Virginia Code Annotated § 18.2-152.5:1
23.	Washington	Washington Revised Code §§ 19.190.080 -090 -100

Laws addressing Spyware

No.	Name of State	Title of Legislation and Relevant Provisions
1.	Alaska	Alaska Statutes §§ 45.45.792 et seq., 45.50.471(51)
2.	Arizona	Arizona Revised Statutes §§ 18.501 et seq.
3.	Arkansas	Arkansas Code §§ 4-111-101 to -105, § 19-6-301, § 19-6-804
4.	California	CaliforniaBusiness and Proffessions Code§§ 22947-22947.6
5.	Georgia	Georgia Code §§ 16-9-152 et seq.
6.	Hawaii	Hawaii Revised Statutes § 708.890, 708.891, 708.891.5, 708.891.6
7.	Illinois	Illinois Compiled Statutes §§ 720:5/17-52, Illinois Compiled Statutes §§ 720:5/12-7.5(3)(a-4), Illinois Compiled Statutes 5/12-7.5(2)(2.2)
8.	Indiana	Indiana Code §§ 24-4.8-1 et seq.
9.	Iowa	Iowa Code §§ 715.1 to 715.8
10.	Louisiana	Louisiana Revised Statutes §§ 51:2006 to 51:2014
11.	Nevada	Nevada Revised Statutes § 205.4737
12.	New Hampshire	New Hampshire Revised Statutes §§ 359-H:1 to 359-H:6
13.	New York	New York Penal Law § 156.00
14.	Pennsylvania	Pennsylvania Statutes §§ 73:2330.1 et seq.
15.	Rhode Island	Rhode Island General Laws §§ 11-52.2-2, -3, -4, -5, -6, -7
16.	Texas	Texas Business and Commerce Code §§ 324.001 to 324.102
17.	Utah	Utah Code §§ 13-40-301 to -303, 13-40-402
18.	Virginia	Virginia Code § 18.2-152.4
19.	Washington	Washington Revised Code §§ 19.270.101 to 19.270.900
20.	Wyoming	Wyoming Statutes § 6-3-506
21.	Guam	Guam Code Annotated title 9 §§ 46.601 to .602
22.	Puerto Rico	Laws of Puerto Rico Annotated title 10 §§ 2181 et seq

Source: The above statutes are compiled from the National Conference of State Legislature Report on Computer Crime Statutes<https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>

Appendix 4

Status of Primary Cybercrime Legislation Worldwide

Country	Any Primary Cyber-crime Legislation currently in Force?	Any Draft primary Cyber-crime Law?	Name of Primary Cybercrime Legislation	Name of Draft Primary cybercrime law	Other comments	Treaties and International Agreements on Cyber Crime				
						Arab Convention on Combating Technology Offences	Convention on Cybercrime (Budapest Convention)	Agreement on Cooperation of the Member States of the Commonwealth of Independent States (CIS) in the fight against crimes in the field of information technology	The Shanghai Cooperation Agreement	United Nations Convention Against Transnational Organized Crime (Palermo Convention
Afghanistan	Yes	Yes	Cyber Crime Code	Draft Info-Communications Technology Law		No	No	No	No	Yes
Albania	Yes		Law No. 7895 from 27.01.1995, Criminal Code of Albania Law No. 7905 from 21.03.199			No	Yes	No	No	Yes

			5, Criminal Procedure Code of Albania Law No. 9918 from 19.05.2008, "On electronic communications" Law No. 9887 from 10.03.2008, "On protection of personal data" Law No. 9880 from 25.02.2008, "On electronic signatures" Law No. 02/2017 on							

			Cybersecurity							
Algeria	Yes		Loi n° 09-04 du 14 Chaâbane 1430 (Law No. 09-04 of Chaâbane 1430 corresponding to 5 August 2009 Containing Specific Rules on the Prevention and Fight against Information Technologies and Communications Crimes)			Yes	No	No	No	Yes
Andorra	Yes		Criminal Code			No	Yes	No	No	Yes
Angola	No	Yes		Draft Law to Combat Crime in the Field	Yet to have specific cybercri	No	No	No	No	Yes

				of ICT and Services for the Information Society (2011) Preliminary Draft Penal Code [e.g., Article 399 (Computer Damage)]	me legislation but Law no. 7/17 - Lei de Protecçã o das Redes e Sistemas Informáticos (Law for the Protection of Networks and Systems Computers) provides for protection of critical infrastructures, network and computer systems.					
Antigua and Barbuda	Yes		Computer Misuse Act, 2006			No	No	No	No	Yes

			Electronic Crimes Act, 2013							
Argentina	Yes		Codigo Penal de la Nacion Argentina (Penal Code) and amended by Ley 26.388 de Ley de Delitos Inform *á*ticos (Law no 26.388)			No	No	No	No	Yes
Armenia	Yes		Criminal Code			No	Yes	Yes	No	Yes
Australia	Yes		Criminal Code Act No. 12 of 1995 as amended by Cybercrime Legislation Amendment Act 2012, No. 120			No	Yes	No	No	Yes

			Cybercrime Act 2001							
Austria	Yes		Criminal Code			No	Yes	No	No	Yes
Azerbaijan	Yes		Criminal Code			No	Yes	Yes	No	Yes
Bahamas	Yes		Computer Misuse Act 2003			No	No	No	No	Yes
Bahrain	Yes		Law No. 60 of 2014 regarding IT Crimes			Yes	No	No	No	Yes
Bangladesh	Yes		Digital Security Laws Act No.46/2018 Information and Communication Technology Act 2006 Penal Code 1860			No	No	No	No	Yes

Barbados	Yes		Computer Misuse Act 2005			No	No	No	No	Yes
Belarus	Yes		Law N.455-Z (Law Of The Republic Of Belarus "On Information, Informatization and Protection of information") Criminal Code			No	No	Yes	No	Yes
Belgium	Yes		Law on computer crime (Loi relative à la criminalitéinformatique) Penal Code			No	Yes	No	No	Yes
Belize	Yes		Cybercrime Act 2020			No	No	No	No	Yes

Benin	Yes		Loi n° 2017-20 portant code du numérique enRépublique du Bénin (Digital Code)			No	No	No	No	Yes
Bhutan	Yes		Information, Communications, and Media Act of Bhutan 2018 (BCIMA)		BCIMA focuses on cybersecurity than primary cybercrime.	No	No	No	No	No
Bolivia	No – see comments		Criminal Code		There is no specific legislation for primary cybercrime. Bolivia Criminal Code only provides for (i) the offence of	No	No	No	No	Yes

					manipulating the processing or transfer of data to illicit benefit in detriment of an individual or a third party (Art 363(1)); and (ii) accessing, using modifying, removing or disabling data stored on a computer or on any informatics support causing harm to the informati					

					on owner (Art. 363(2))					
Bosnia and Herzegovina	Yes		Criminal Code			No	Yes	No	No	Yes
Botswana	Yes		Cybercrime and Computer Related Crimes Act			No	No	No	No	Yes
Brazil	Yes		Criminal Code			No	No	No	No	Yes
Brunei Darussalam	Yes		Computer Misuse Act 2007			No	No	No	No	Yes
Bulgaria	Yes		Criminal Code			No	Yes	No	No	Yes
Burkina Faso	Yes		Criminal Code			No	No	No	No	Yes
Burundi	Yes		Code PénalRevisé 2009 (Penal Code 2009)			No	No	No	No	Yes
Cabo Verde	Yes		Lei n°8/IX/2017 (Law n°8/IX/2017)			No	Yes	No	No	Yes

Cambodia	Yes	Yes	Criminal Code	Draft Cybercrime Law Criminal Code (Articles 317 to 320, Articles 427 to 432)		No	No	No	No	Yes
Cameroon	Yes		Law No. 12 of 2010 on Cybersecurity and Cybercrime (also known as "Law No. 12 of 2010 Relating to Cybersecurity and Cybercriminality")			No	No	No	No	Yes
Canada	Yes		Criminal Code			No	Yes	No	No	Yes
Central African Republic	No				Yet to have specific cybercrime legislation. Penal Code	No	No	No	No	Yes

					provides for fraud with electronic data (Art. 164) and child pornography (Art. 11)					
Chad	Yes		Loi n° 009/PR/2015 portant sur la cybersécurisation et la luttecontre la cybercriminalité (Law No. 009/PR/2015 on Cybersecurity and the Fight against Cybercrime)			No	No	No	No	Yes
Chile	Yes		Law on Automated Data			No	Yes	No	No	Yes

			Processing Crimes (also known as "Law No. 19,223 of 1993 on Categories of Computer-Related Offenses")							
China	Yes		Criminal Law of the People's Republic of China Chapter VI -Crimes of Obstructing the Administration of Public Order (中华人民共和国刑法) Cybersecurity Law (中华人民共和国网络安全法) National Security Law (中华			No	No	No	Yes	Yes

			人民共和国国家安全法) Counter-Terrorism Law (中华人民共和国反恐怖主义法)							
Colombia	Yes		Penal Code (as amended by Law No. 1273 of 2009 (Protection of Information and Data)			No	Yes	No	No	Yes
Comoros	No					No	No	No	No	Yes
Congo	No	Yes		Draft Law on the Fight Against Cybercrime		No	No	No	No	Yes
Costa Rica	Yes		Penal Code Código Penal Law (Penal Code)			No	Yes	No	No	Yes

Côte d'Ivoire	Yes		Loi N° 2013-451 relative à la luttecontre la cybercriminalité (Act No. 2013-451 on the fight against cybercrime)			No	No	No	No	Yes
Croatia	Yes		Criminal Code			No	Yes	No	No	Yes
Cuba	Yes		Codigo penal Resolution No 127/2007 on Safety Regulations for Information Technology			No	No	No	No	Yes
Cyprus	Yes		Law Ratifying the Cybercrime Convention of 2001 (No.			No	Yes	No	No	Yes

			22(III)/2004							
Czech Republic	Yes		Act on Cyber Security and Change of Related Acts No. 181/2014 Coll. Criminal Code No. 40/2009			No	Yes	No	No	Yes
Democratic People's Republic of Korea	Yes		Criminal Law			No	No	No	No	Yes
Democratic Republic of the Congo	No	Yes		Draft Law on the Fight against Cybercrime		No	No	No	No	Yes
Denmark	Yes		Law n. 1567 on Network and Information Security And			No	Yes	No	No	Yes

			Penal Code							
Djibouti	Yes		Penal Code			No	No	No	No	Yes
Dominica	No	Yes		Computer and Computer Related Crimes Bill 2005 Electronic Crime Bill		No	No	No	No	Yes
Dominican Republic	Yes		Law No. 53 of 2007 on High Technology Crimes			No	Yes	No	No	Yes
Ecuador	Yes		Organic Comprehensive Criminal Code (Law No. 180 of 2014)			No	No	No	No	Yes
Egypt	Yes		Anti-Cyber and Information Technology Crimes Law (Law No. 175/2018)			Yes	No	No	No	Yes

			Penal Code Telecommunication Regulation Law (Law No. 10 of 2003)							
El Salvador	Yes		Ley Especial Contra los DelitosInformáticos y Conexos (Special Law against Cybercrime and Related Offenses)			No	No	No	No	Yes
Equatorial Guinea	No					No	No	No	No	Yes
Eritrea	Yes		Penal Code			No	No	No	No	Yes
Estonia	Yes		Penal Code			No	Yes	No	No	Yes
Eswatini	No	Yes		Computer Crime and		No	No	No	No	Yes

				Cybercrime Bill 2013						
Ethiopia	Yes	Yes	Criminal Code (Proclamation No.414/2004)	Draft Cybercrime Law (2016) [called "(Draft) Computer Crime Proclamation No…/2016"]		No	No	No	No	Yes
Fiji	Yes		Crimes Decree 2009 (Decree No. 44 of 2009)			No	No	No	No	Yes
Finland	Yes		Criminal Code			No	Yes	No	No	Yes
France	Yes		Criminal Code Law No.2004-575 of 21 June 2004 regarding Confidence in the Digital Economy			No	Yes	No	No	Yes
Gabon	No	Yes		Draft Law on		No	No	No	No	Yes

				Cybercrime						
Gambia	Yes		Information and Communications Act 2009			No	No	No	No	Yes
Georgia	Yes		Criminal Code			No	Yes	No	No	Yes
Germany	Yes		Criminal Code			No	Yes	No	No	Yes
Ghana	Yes		Electronic Transactions Act (Act No. 772 of 2008) Criminal Code (Act 29 of 1960) (also known as "Criminal Offences Act")			No	Yes	No	No	Yes
Greece	Yes		Greek Criminal Code			No	Yes	No	No	Yes
Grenada	Yes		Electronic Crimes Act of 2013 Electronic Transactio			No	No	No	No	Yes

			ns Act 2008							
Guatemala	Yes		Penal Code			No	No	No	No	Yes
Guinea-Bissau	No				Law n° 5/2010 of May 2010 contain provisions concerning telecommunications sectors and internet governance (At. 105) but has no specific cybercrime provisions. Penal Code contains only general provisions concerning forgery	No	No	No	No	Yes

					and fraudulent activities.					
Guyana	Yes		Cybercrime Act 2018			No	No	No	No	Yes
Haiti	No					No	No	No	No	Yes
Honduras	Yes		Criminal Code			No	No	No	No	Yes
Hungary	Yes		Criminal Code			No	Yes	No	No	Yes
Iceland	Yes		General Penal Code			No	Yes	No	No	Yes
India	Yes		Information Technology Act 2000			No	No	No	No	Yes
Indonesia	Yes		Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions			No	No	No	No	Yes
Iran (Islamic Republic of)	Yes		Computer CrimeAct 2010			No	No	No	No	Yes
Iraq	No	Yes (but		Draft Informatic		Yes	No	No	No	Yes

		was revoked in 2013)		s Crimes Law 2010						
Ireland	Yes		Criminal Justice (Theft and Fraud Offences) Act 2001 Criminal Damages Act 1991			No	No	No	No	Yes
Israel	Yes		Computer Law of 1995			No	No	No	No	Yes
Italy	Yes		Criminal Code (amended by Law No. 547 of 23 December 1993Amendment of the Provisions of the Penal Code & the Code of Criminal Procedure in Relation to			No	No	No	No	Yes

			Computer Criminality)							
Jamaica	Yes		Cybercrime Act 2010			No	No	No	No	Yes
Japan	Yes		Act on Prohibition of Unauthorized Computer Access Penal Code			No	No	No	No	Yes
Jordan	Yes		Information Systems Crime Law of 2010			Yes	No	No	No	Yes
Kazakhstan	Yes		Criminal Code			No	No	Yes	Yes	Yes
Kenya	Yes		- Information and Communications Act 2009			No	No	No	No	Yes
Kiribati	Yes		Telecommunications Act2004 Computer Misuse and Cybercrim			No	No	No	No	Yes

			es Act 2018							
Kuwait	Yes		Law No. 63 of 2015 on combating cyber crimes			Yes	No	No	No	Yes
Kyrgyzstan	Yes		Criminal Code			No	No	Yes	Yes	Yes
Lao People's Republic	Yes		Law no 61/NA on Prevention and Combating Cybercrime			No	No	No	No	Yes
Latvia	Yes		Criminal Code			No	Yes	No	No	Yes
Lebanon	Yes		Law no 81/2018 related to Electronic Transactions and Personal Data			No	No	No	No	Yes
Lesotho	Yes	Yes	Penal Code Act 2010	Draft Computer Crime and Cybercrime Bill 2013		No	No	No	No	Yes
Liberia	No				Penal Code contains	No	No	No	No	Yes

					no provisions relating cybercrime. Telecommunications Act 2007 lays out the institutional framework for telecommunications sector.					
Libya	No	Yes		Draft Cybercrime Law Draft Cyber-IPR Law Draft e-Commerce Law Draft e-Transactions Law Draft Data Protection Law		Yes	No	No	No	Yes
Liechtenstein	Yes		Criminal Code			No	Yes	No	No	Yes

Lithuania	Yes		Criminal Code			No	Yes	No	No	Yes
Luxembourg	Yes		Penal Code			No	Yes	No	No	Yes
Macedonia (the former Yugoslav Republic of)	Yes		Criminal Code							
Madagascar	Yes		Act 2014-006 on the fight against cybercrime			No	No	No	No	Yes
Malawi	Yes		Electronic Transactions and Cyber Security Act 2016 (No. 33 of 2016) Communications Act 2016 (No. 34 of 2016)			No	No	No	No	Yes
Malaysia	Yes		Computer Crimes Act 1997			No	No	No	No	Yes

			Communications and Multimedia Act 1998							
Maldives	No					No	No	No	No	Yes
Mali	Yes		Penal Code			No	No	No	No	Yes
Malta	Yes		Criminal Code			No	Yes	No	No	Yes
Marshall Islands	No	Yes		Cybercrime Bill	Criminal Code 2011 does not contain provisions for cybercrime although it contains definition of illegal interception.	No	No	No	No	Yes
Mauritania	No	Yes		Draft Bill on Cybercrime		Yes	No	No	No	Yes
Mauritius	Yes		Computer Misuse and Cybercrime Act 2003			No	Yes	No	No	Yes

Mexico	Yes		Federal Criminal Code			No	No	No	No	Yes
Micronesia(Federated States of)	No	Yes		Draft Cybercrime Law		No	No	No	No	Yes
Moldova	Yes		Criminal Code			No	Yes	Yes	Yes	No
Monaco	Yes		Penal Code Loi n° 1.383 du 2 août 2011 sur l'Economie Numérique (Law on Digital Economy 2011) Loi n° 435 du 8 novembre 2016 relative à la luttecontre la criminalitétechnologique (Law n °			No	Yes	No	No	Yes

			435 of 8 November 2016 on the fight against technological crime)							
Mongolia	Yes		Criminal Code			No	No	No	No	Yes
Montenegro	Yes		Criminal Code			No	Yes	No	No	Yes
Morocco	Yes		Penal Code			Yes	Yes	No	No	Yes
Mozambique	Yes		Penal Code			No	No	No	No	Yes
Myanmar	No				Electronic Transactions Law 2004 contains only provisions of illegal interception and data interference but no specific provisions for cybercrime.	No	No	No	No	Yes

Namibia	No	Yes		Cybercrime Bill 2013 Electronic Transactions Act of 2019 (yet to implement)	Electronic Transactions Act 4 of 2019 contains provisions for electronic transactions, internet service provider liability, cryptography providers, e-government services, and online marketing.	No	No	No	No	Yes
Nauru	No					No	No	No	No	Yes
Nepal	Yes	Yes	Electronic Transaction Act 2008Chapter 9Offense relating to Computer	Information and Technology Bill		No	No	No	No	Yes

Netherlands	Yes		Criminal Code			No	Yes	No	No	Yes
New Zealand	Yes		Crimes Act 1961			No	No	No	No	Yes
Nigaragua	Yes		Penal Code			No	No	No	No	Yes
Niger	Yes		Penal Code			No	No	No	No	Yes
Nigeria	Yes		Cybercrimes Act2015			No	No	No	No	Yes
Norway	Yes		Penal Code			No	Yes	No	No	Yes
Oman (Sultanate of)	Yes		Royal Decree No. 12 of 2011 Issuing the Cyber Crime Law			Yes	No	No	No	Yes
Pakistan	Yes	Yes	- Prevention of Electronic Crime Act 2016 Electronic Transactions Act 2002			No	No	No	No	Yes
Palau	Yes		Penal Code Title 17 Palau National			No	No	No	No	Yes

			Code Chapter 31							
Panama	Yes		Penal Code			No	Yes	No	No	Yes
Papua New Guinea	Yes		Cybercrime Code Act 2016			No	No	No	No	No
Paraguay	Yes		Criminal Code Law No. 1160/98 Law No. 4439/11			No	Yes	No	No	Yes
Peru	Yes		Law No. 30096 of 2013 (Computer Crimes Act) Law 30171 of 2014 [Law amending the Law No. 30096 of 2013 (Computer Crimes Act)]			No	Yes	No	No	Yes
Philippines	Yes		Cybercrime			No	Yes	No	No	Yes

			Prevention Act of 2012(Republic Act No. 10175 of 2012)							
Poland	Yes		Penal Code			No	Yes	No	No	Yes
Portugal	Yes		Law No. 109/2009, of September 15 (Cybercrime Law			No	Yes	No	No	Yes
Qatar	Yes		Cybercrime Prevention Law (Law No. 14 of 2014)			Yes	No	No	No	Yes
Republic of Korea	Yes		Criminal Act Information and Communication Network Act Information and Communications			No	No	No	No	Yes

			Infrastructure Protection Act							
Romania	Yes		Law on Certain Steps for Assuring Transparency in Performing High Official Positions, Public and Business Positions, for Prevention and Sanctioning the Corruption (Law No. 161/2003) Title III Preventing and Fighting Cyber Crime			No	Yes	No	No	Yes
Russian Federation	Yes		Criminal Code			No	No	Yes	Yes	Yes
Rwanda	Yes		Law on Prevention and			No	No	No	No	Yes

			Punishment of Cyber Crimes 2018							
Saint Kitts and Nevis	Yes		Electronic Crimes Act 2009			No	No	No	No	Yes
Saint Lucia	Yes	Yes	Criminal Code Act 9 of 2004	Electronic Crimes Bill 2009		No	No	No	No	No
Saint Vincent and the Grenadines	Yes		Criminal Code Electronic Transactions Act, 2007, Part X. Information Systems and Computer Related Crimes			No	No	No	No	Yes
Samoa	Yes		Crimes Act (No 10. of 2013)			No	No	No	No	Yes
San Marino	Yes		Penal Code			No	Yes	No	No	Yes
Sao Tome and Principe	Yes		Penal Code			No	No	No	No	Yes

			Cybercrime Law 2017							
Saudi Arabia	Yes		Anti-Cyber Crime Law 1428/2007			Yes	No	No	No	Yes
Senegal	Yes		Penal Code			No	Yes	No	No	Yes
Serbia	Yes		Criminal Code			No	Yes	No	No	Yes
Seychelles	Yes		Computer Misuse Act			No	No	No	No	Yes
Sierra Leone	No					No	No	No	No	Yes
Singapore	Yes		Computer Misuse Act (Cap. 50A) Cybersecurity Act No. 9/2018			No	No	No	No	Yes
Slovakia	Yes		Act No. 300/2005 Criminal Code			No	No	No	No	Yes
Slovenia	Yes		Penal Code			No	No	No	No	Yes
Solomon Islands	No					No	No	No	No	No
Somalia	No					No	No	No	No	No
South Africa	Yes	Yes	Electronic Communications and Transactio	Cybercrimes Bill 2015		No	No	No	No	Yes

			ns Act2002							
South Sudan	Yes		Penal Code Act 2008			No	No	No	No	No
Spain	Yes		Criminal Code			No	Yes	No	No	Yes
Sri Lanka	Yes		Computer Crime Act (No. 24 of 2007)			No	Yes	No	No	Yes
Sudan	Yes		The Informatic Offences (Combating) Act 2007			Yes	No	No	No	Yes
Suriname	No				Criminal Code 2015 provides for all the offences listed in Budapest Convention.	No	No	No	No	Yes
Sweden	Yes		Penal Code			No	No	No	No	Yes
Switzerland	Yes		Penal Code			No	Yes	No	No	Yes
Syrian Arab Republic	No					Yes	No	No	No	Yes
Tajikistan	Yes		Criminal Code			No	No	Yes	Yes	Yes

Tanzania	Yes		Cybercrimes Act 2015			No	No	No	No	No
Thailand	Yes		Computer Crime Act 2007			No	No	No	No	Yes
Timor-Leste	Yes		Penal Code			No	No	No	No	Yes
Togo	Yes		Law on Cybersecurity and the Fight against Cybercrime 2018			No	No	No	No	Yes
Tonga	Yes		Computer Crimes Act 2003			No	Yes	No	No	Yes
Trinidad and Tobago	Yes	Yes	Computer Misuse Act 2000	Cybercrime Bill 2017		No	No	No	No	Yes
Tunisia	Yes	Yes	Penal Law	Cybercrime Bill 2015		Yes	No	No	No	Yes
Turkey	Yes		Criminal Code Law No. 5651 on Regulation of Internet Publications and Combating Crimes			No	Yes	No	No	Yes

			Committed through such Publications 2007							
Turkmenistan	Yes		Criminal Code			No	No	No	No	Yes
Tuvalu		Yes		Draft Cybercrime Law		No	No	No	No	No
Uganda	Yes		Criminal Code			No	No	No	No	Yes
Ukraine	Yes		Criminal Code			No	Yes	Yes	Yes	Yes
United Arab Emirates	Yes		Criminal Code			Yes	No	No	No	Yes
United Kingdom of Great Britain and Northern Ireland	Yes		Computer Misuse Act 1990 Regulations of Investigatory Powers Act2000		Other relevant statutes include Forgery and Counterfeiting Act 1981 and Fraud Act 2006. Criminal Attempts Act 1981criminalises attempts; while	No	Yes	No	No	Yes

					aiding and abetting are dealt under Accessories and Abettors Act 1861, s. 8 (for indictable offences) and the Magistrates' Courts Act 1980, s. 44(1) (for summary offences).					
United States of America	Yes		United States Code Title 18 Part I Chapter 47 §1030 (Computer Fraud and Abuse Act)		Other relevant statutes include 18 United States Code, Chapter 47- Crimes and Criminal Procedur	No	Yes	No	No	Yes

					e, § 1028 -1029; Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications; Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access; and §3121, General prohibition on pen register and trap					

					and trace device use.					
Uruguay	Yes		Penal Code			No	No	No	No	Yes
Uzbekistan	Yes		Criminal Code			No	No	Yes	Yes	Yes
Vanuatu	No	Yes		Draft Bill for Cybercrime Act		No	No	No	No	Yes
Vatican City	No	No Data			The **basic laws of Vatican City**: 1. Law No. CXXXI of 22 February 2011 on the Rights of Citizenship and Sojourn 2. Law No. LXXI of 1 October 12008 on the Source of Laws 3. Law No. IV of	No	No	No	No	No

					7 June 1929 on Administrative Organization 4. Law No. V of 7June 1929 on Economic, Commercial and Professional Organization 5. Law No. VI of 7 June 1929 on Public Security 6. Fundamental Law of Vatican City State 2001 and the relevant **amending laws**i.e.Amendme					

					nto the Criminal Code and the Code of Criminal Procedure 2013 as well as Supplementary Norms on Criminal Law Matters 2013do not provide for cybercrime. The **primary IP laws** 1. Law No. CXXXII of 19 March 2011 on Copyright and Related Rights 2. Code of Canon Law					

					Also do not contain provisions on cybercrime. Vatican Secretary of State, however, expressed grave concerns for cybercrime in his message to the 27th Session of the UN Commission on Crime Prevention and Criminal Justice.[158]					
Venezuela (Bolivarian Republic of)	Yes		Special Law on Information Crimes 2001			No	No	No	No	Yes

[158]https://press.vatican.va/content/salastampa/en/bollettino/pubblico/2018/05/15/180515a.html

Vietnam	Yes		Criminal Code 2015 Law on Cybersecurity			No	No	No	No	Yes
Yemen	No	Yes		Draft Law on Combating Electronic Crime		Yes	No	No	No	Yes
Zambia	Yes	Yes	Computer Misuse and Crimes Act 2004 Electronic Communication and Transactions Act 2009	Draft Law for Combating Electronic Crimes		No	No	No	No	Yes
Zimbabwe	Yes	Yes	Criminal Law (Codification and Reform) Act	Cybersecurity and Data Protection Bill 2019 (gazetted in March2020)		No	No	No	No	Yes
*State of Palestine	Yes		**Gaza** :British		**Legislative**	No	No	No	No	No

			Mandate Penal Code Ordinance No. 74 of 1936 (as amended by Law No. 3 of 2009) **West Bank:**Law by Decree No. 15 of 2017 Regarding Electronic Transactions Law by Decree No. 10 of 2018 on Cybercrime (as amended by amended by Law by Decree No. 28 of 2020)		**Council of Gaza** issued Law No. 3 of 2009 amending the British Mandate Penal Code Ordinance No. 74 of 1936 to provide for criminalisation of piracy,cyber-publishing, and cyber-spying. **President of the Palestinian National Authority** issued Law by Decree No. 15 of 2017					

					Regarding Electronic Transactions to provide for offences relating to electronic signature. Law by Decree No. 16 of 2017 was enacted in 2017 to provide for cybercrime but was revoked after wide criticsm for its violations of basic human rights, particula					

					rly freedom of opinion and expressi on. Law by Decree No. 10 of 2018 on Cybercri me was subseque ntly issued and amended by Law by Decree No. 28 of 2020, which remains the primary law for cybercri mes in the West Bank.					

Note:

Primary cybercrime legislation/draft law in this list refers to legislation/draft legislation that contains provisions on cyber-dependent crime (such as unauthorized access to a computer system.)

Law as of 31 August 2021

27 out of 195 countries listed above do not have primary cybercrime legislation in force.

13 out of these 27 countries have issued draft cybercrime legislation.

114 out of 195 countries listed above subscribe to only 1 or does not subscribe to any of the 5 international agreements on cybercrime listed above.

Appendix 5

Principles of Active Countermeasures

The proposed principles below attempt to balance the right of self-defence of private actors and the potential risks of Active Countermeasures, and should be considered in the adoption and implementation of Active Countermeasures:

1. **Proportionality**: Countermeasures must be proportionate to the attack and respect fundamental human rights. The following factors should be considered in measuring proportionality:
    a. severity of the damage;
    b. nature of the damage (physical, mental, financial, tangible or intangible harm); and
    c. whether there is any recourse to the harm suffered.
    d. potential outcome of the countermeasures; and
    e. possible intent of the attacker.

2. **Time and Duration:** Countermeasures must cease if dispute resolution is underway and when countermeasures are no longer needed. Duration and scope of countermeasures must be limited appropriately.

3. **Notification Requirement:** Affected intermediaries who have been identified should be notified unless it is time-sensitive. In cases where there is no notification, countermeasures must be limited to smaller, less critical, and more knowable parts of the opposing network or system.

4. **Necessity**: Active Cyber Countermeasures should not be permissible except in self-defence and to prevent the perpetration of serious crime which could cause grave harm to life and property.

5. **Reversibility:** If there is a choice between several feasible countermeasures with similar efficacy, countermeasure which is reversible or that will incur the least irreversible harm is preferred.

6. **Categorical restrictions:** Certain excessively dangerous and irreversible Active Countermeasures should be banned outright. Anticipatory countermeasures should only be allowed in cases of imminent cyber-attack which are likely to cause serious harm. Synchronous countermeasures could be taken during the attack provided that misattribution risk is low. Preventive countermeasures which are employed when no imminent threat is detected should be impermissible or permissible in exceptional circumstances.

7. **Attributable:** Any malicious cyber-attack should be attributable to a high degree of accuracy before any Active Countermeasures can be undertaken. Attribution should be made based on convincing and reliable evidence and information.

Appendix 6

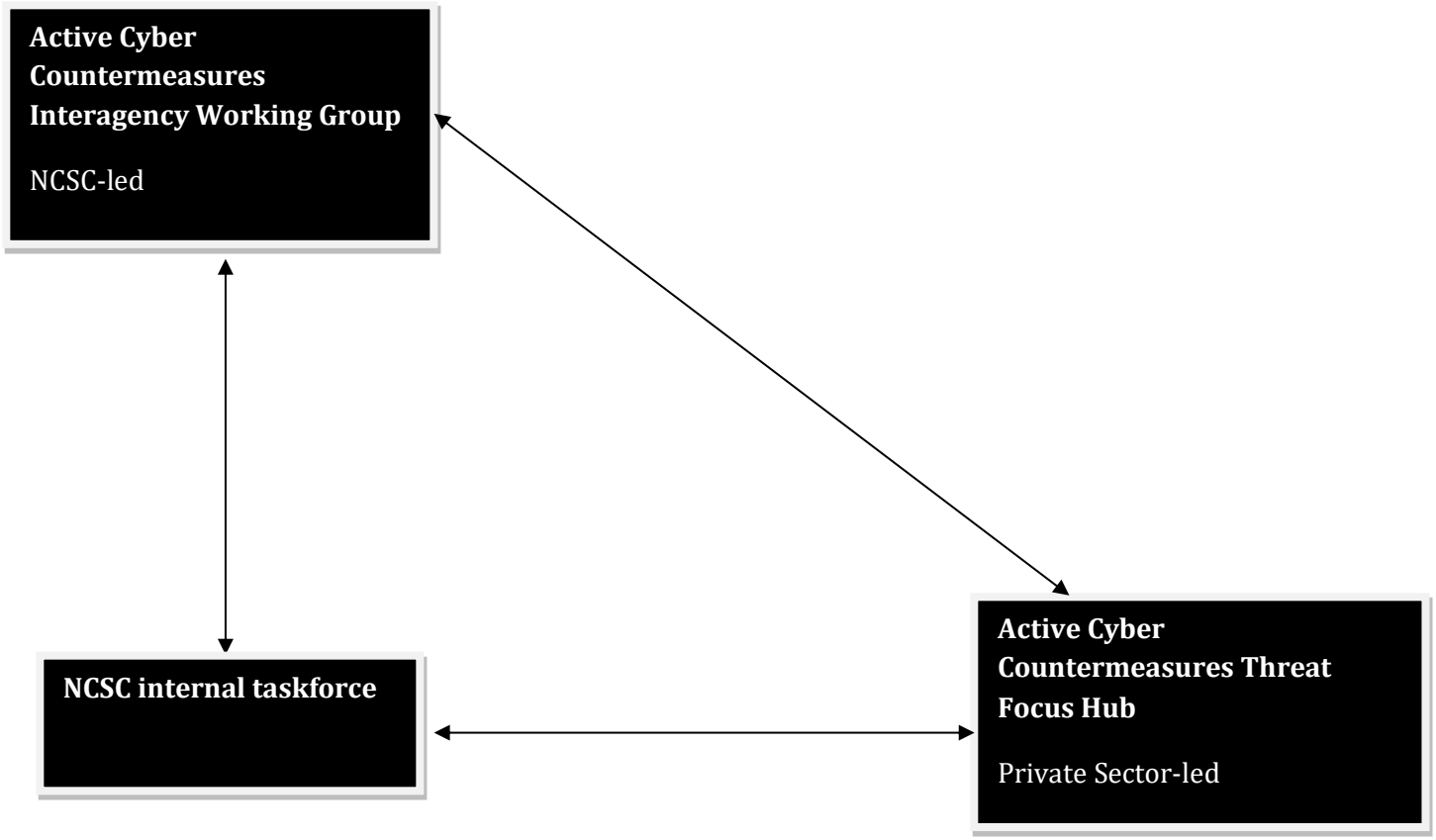
Code of Conduct for Active Cyber Countermeasures Practitioners

Active Cyber Countermeasures Practitioners agree and undertake to:

1. operate in accordance with the principles contained in this Code.
2. comply and require their personnel to comply with applicable national and international law and requirements imposed upon them.
3. respect fundamental rights and liberties of persons or entities they come into contact with, including the right against unlawful interference with privacy and deprivation of property.
4. not support, engage in, service, or contract with any government, entity, or person in a manner that would be contrary to the principles contained in this Code, applicable national and international law, or would pose a threat to national or international security.
5. require their personnel to not support, engage in, or seek to benefit from any conduct which is contrary to the principles contained in this Code, applicable national and international law, or would pose a threat to national or international security.
6. take all reasonable steps to deploy Active Countermeasures responsibly and make sure the deployment is proportionate to the attack and does not exceed what is strictly necessary.
7. develop, supply, or obtain Active Countermeasures tools in compliant with applicable national and international law and regulations.
8. report, and will require their personnel to report any known or reasonable suspicion of the commission of any unlawful deployment of Active Countermeasures, acquisition or supply of illegal Active Cyber Countermeasures tools or incompliance with this Code to the competent authorities in the country where the conduct took place.
9. support and establish a culture that encourages the ethical deployment of Active Cyber Countermeasures and adhere to the principles in this Code, which include providing appropriate training to its personnel.

Appendix 7

Proposed Operational Framework for Public-private Cooperation



BIBLIOGRAPHY

Cases

AG's Reference No. 2 of 1991 [1992] 3 WLR 432

Arqiva Ltd &Ors v Everything Everywhere Ltd &Ors [2011] EWHC 1411 (TCC)

Ashton Investments Ltd v OJSC Russian Aluminium (Rusal)[2006] EWHC 2545 (Comm)

Bamford v Turnley[1862] EWHC Exch J63

Brown Jordan International, Inc. v Carmicle, 846 F. 3d 1167, 1173-74 (11th Cir. 2017)

Bristol Groundschool Ltd v Intelligent Data Capture Ltd [2014] EWHC 2145 (Ch)

Cook v Beal [1697] 1 LdRaym 176

DPP v Morgan[1976] A.C. 182

Hubbard v Pitt[1975] EWCA Civ J0513-1

Moriarty v Brooks [1834] EWHC Ech J79

Nicaragua v. United States of America 1986 I.C.J. 14

Palmer v R [1971] 1 All ER 1077

R v Tolson (1889) 23 QBD 168

Weaver v Bush [1798] 8 Term Rep 78

United States of America v. Bryan Gilbert Henderson, No. 17-10230 (9th Cir. 2018)

United States v. Czubinski, 106 F.3d 1069, 1078-79 (1st Cir. 1997)

Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC. 774 F. 3d 1065, 1073 (6th Cir. 2014)

Bills and Statutes

United States

Georgia Code

18 U.S. Code § 1028

18 U.S. Code § 1029

18 U.S. Code § 1030

18 U.S. Code § 1343

H.R. 3270 - Active Cyber Defense Certainty Act 2019

S. 2292 - Study on Cyber-Attack Response Options Act

United Kingdom

Computer Misuse Act 1990

Consumer Protection Act 1987

Coroners and Justice Act 2009

Data Protection Act 2018

Fraud Act 2006

Investigatory Powers Act 2016

Modern Slavery Act 2015

Police and Justice Act 2006

Policing and Crime Act 2017

Serious Crime Act 2015 (Explanatory Notes)

Terrorism Acts 2000

Terrorism Acts 2006

Australia

Cybercrime Act 2001

Agreement with the Government of the French Republic on Cooperation in the Maritime Areas Adjacent to the French Southern and Antarctic Territorities, Heard Island and the McDonald Islands[2005] ATS 6

Canada

Criminal Code

South Korea

Act on Promotion of Information and Communications Network Utilisation and Information Protection

Singapore

Computer Misuse Act (Cap. 50A)

Cybersecurity Act No. 9/2018

United Nations and Other International Instruments

Article 3BIS Convention on International Civil Aviation

Articles on Responsibility of States for Internationally Wrongful Acts 2001

Charter of the United Nations 1945

Convention on the Law of the Sea 1982

Convention on the Recognition and Enforcement of Foreign Arbitral Award 1958

Geneva Convention on the High Seas 1958

Schengen Convention on Border Controls 1990

Yearbook of the International Law Commission

Journals, Books, Websites, News and Reports

'Access Now To Join The Paris Call For Trust And Stability In Cyberspace - Access Now' (*Access Now*, 2018) <https://www.accessnow.org/access-now-to-join-the-paris-call-for-trust-and-stability-in-cyberspace/>

'Active Cyber Defense And Interpreting The Computer Fraud And Abuse Act' (*Lawfare*, 2018) <https://www.lawfareblog.com/active-cyber-defense-and-interpreting-computer-fraud-and-abuse-act>

'AFJOC - African Joint Operation Against Cybercrime' (*Interpol.int*) <https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime>
Alder M, *The Inherent Right Of Self-Defence In International Law* (Springer Science & Business Media 2012)

'Annual Review 2020' (National Cyber Security Centre 2020) <https://www.ncsc.gov.uk/annual-review/2020/docs/ncsc_2020-annual-review_s.pdf> accessed 17 August 2021

Bill, A. and Smolanoff, J., 2017. Hacking Back Against Cyberterrorists: Could You? Should You?.*Defense Against Terrorism Review*, [online] 9. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096555>

Bing C, Satter R, and Stubbs J, 'Exclusive: Elite Hackers Target WHO As Coronavirus Cyberattacks Spike' (*Reuters*, 2020) <https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN>

Budd C, 'Microsoft Unleashes 'Death Star' On Solarwinds Hackers In Extraordinary Response To Breach' (*GeekWire*, 2020) <https://www.geekwire.com/2020/microsoft-unleashes-death-star-solarwinds-hackers-extraordinary-response-breach/>

'2004 CSI/FBI Computer Crime And Security Survey' (Computer Security Institute 2004) <http://dls.virginia.gov/commission/pdf/2004%20CSI-FBI%20Computer%20Crime%20and%20Security%20Survey.pdf>

Campbell K and others, 'The Economic Cost Of Publicly Announced Information Security Breaches: Empirical Evidence From The Stock Market' [2003] Journal of Computer Security <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.7735&rep=rep1&type=pdf>

CBS News, 'Most China-Based Hacking Done By Select Few' (2011) <https://www.cbsnews.com/news/most-china-based-hacking-done-by-select-few/>

Chandler J,'Security In Cyberspace:Combatting Distributed Denial Of Service Attacks' (2003) 1U Ottawa L & Tech Journal.

Chayes A, 'Rethinking Warfare: The Ambiguity Of Cyber Attacks' (2015) 6 Harvard National Security Journal <https://heinonline.org/HOL/LandingPage?handle=hein.journals/harvardnsj6&div=12&id=&page=>

Chesney R, 'Legislative Hackback: Notes On The Active Cyber Defense Certainty Act Discussion Draft' (*Lawfare*, 2017) <https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft>

Chesney R, 'Hackback Is Back: Assessing The Active Cyber Defense Certainty Act' (*Lawfare*, 2019) <https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act>

Chiesa R, Ducci S, and Ciappi S, *Profiling Hackers : The Science Of Criminal Profiling As Applied To The World Of Hacking* (1st edn, CRC Press 2008)

Cimpanu C, 'You Can Now Rent A Mirai Botnet Of 400,000 Bots' (*BleepingComputer*, 2016) <https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/>

Cole E, *Advanced Persistent Threat* (Syngress 2013)

'Contacting States » New York Convention' (*Newyorkconvention.org*) <https://www.newyorkconvention.org/countries>

Cox J, 'The US Military Just Publicly Dumped Russian Government Malware Online' (*Vice.com*) <https://www.vice.com/en/article/8xpa7k/us-military-cybercom-publicly-dumped-russian-government-malware-fancy-bear-apt28>

Custers, B. and Pool, R., 2017. The Police Hack Back: Legitimacy, Necessity and Privacy Implications of the Next Step in Fighting Cybercrime. *Criminal Law and Criminal Justice*, [online] 25, pp.123-144. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047223>

'Cyber Attacks Increase As People Work From Home' (*Cityoflondon.police.uk*, 2020) <https://www.cityoflondon.police.uk/news/city-of-london/news/2020/template4/press-releases/cyber-attacks-increase-as-people-work-from-home/>

'Cyber.Dhs.Gov - Binding Operational Directive 20-01' (*Cyber.dhs.gov*, 2020) <https://cyber.dhs.gov/bod/20-01/>

'Cyberlaw 101: A Primer On US Laws Related To Honeypot Deployments | SANS Institute' (*Sans.org*, 2007) <https://www.sans.org/white-papers/1746/>

Dasgupta S, 'EXPLAINER: The PET Revolution - How Preserving Data Privacy In Intelligence Sharing Is A Game Changer In The Global Fincrime Sector - AML Intelligence' (*AML Intelligence*, 2021) <https://www.amlintelligence.com/2021/01/insight-the-pet-revolution-preserving-data-privacy-to-change-the-game-in-fincrime-intelligence-sharing/>

'Ddos Attacks With Zombie Computers – 'North Korea's Powerful Hacker Army'? - The H Security: News And Features' (*H-online.com*, 2009) <http://www.h-online.com/security/news/item/DDoS-attacks-with-zombie-computers-North-Korea-s-powerful-hacker-army-742435.html>

Department of Defense, 'Strategy For Operating In Cyberspace' (2011) <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>

Edwards L, 'Dawn Of The Death Of Distributed Denial Of Service: How To Kill Zombies' (2006) 24 Cardozo Arts & Entertainment Law Journal <https://eprints.soton.ac.uk/42068/>

'Final Report Of The Defense Science Board (DSB) Task Force On Cyber Deterrence' (Department of Defense Defense Science Board 2017) <https://www.armed-services.senate.gov/download/dsb-cd-report-2017-02-27-17_v18_final-cleared-security-review>

'FOI Releases For April 2017' (*GOV.UK*, 2017) <https://www.gov.uk/government/publications/foi-releases-for-april-2017>

Fox News, 'Pentagon Official: North Korea Behind Week Of Cyber Attacks' (2009) <http://www.foxnews.com/story/2009/07/09/pentagon-official-north-korea-behindweek- cyber-attacks/.>

'GLACY+' (*Interpol.int*) <https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Glacy>

'Global Cybersecurity Index 2020' (International Telecommunication Union 2021) <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

Gonsalves A, 'Nearly Two-Dozen Bugs Easily Found In Critical Infrastructure Software' (*CSO Online*, 2012) <https://www.csoonline.com/article/2132583/nearly-two-dozen-bugs-easily-found-in-critical-infrastructure-software.html>

'Government Response To The Call For Views On Consumer Connected Product Cyber Security Legislation' (*GOV.UK*, 2021) <https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation>

Green J, 'Fluctuating Evidentiary Standards For Self-Defence In The International Court Of Justice' (2009) 58 The International and Comparative Law Quarterly <http://Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice>

Grimmelmann J, *Internet Law: Cases And Problems* (11th edn, Semaphore Press 2021)

Grotius H, *Commentary On The Law Of Prize And Booty* (1st edn, Liberty Fund 2012)

'Hackerone' (*HackerOne*) <https://hackerone.com/ncsc_uk?type=team>

Halsbury's Laws (5th edn, 2018)

Haupt, C., Balkin, J., Schmitt, M., Turner, R., Kohlmann, E., Bijou, R., Haupt, C. and Balkin, J., 2013. *Cyberspace and International Law: The Penumbral Mist of Uncertainty*. [online] Harvardlawreview.org. Available at: <https://harvardlawreview.org/2013/04/cyberspace-and-international-law-the-penumbral-mist-of-uncertainty/>

Hughes C, 'Ireland Shuts Down Health IT System After Ransomware Attack' (*Mail Online*, 2021) <https://www.dailymail.co.uk/news/article-9578763/Ireland-shuts-health-ransomware-attack.html>

Jeremy R, and Ariel R, 'Navigating Conflicts In Cyberspace: Legal Lessons From The History Of War At Sea' (2013) 14 <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiHpI-R4pryAhXTTMAKHYZ2BYMQFnoECAcQAw&url=https%3A%2F%2Fchicagounbound.uchicago.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D1402%26context%3Dcjil&usg=AOvVaw1CBZbhHNgs3_0U4GXLdynP>

Johnson D, 'New Federal Contracting Rule Cuts Off Kaspersky -- FCW' (*FCW*, 2018) <https://fcw.com/articles/2018/06/15/kaspersky-rule-contractors.aspx>

Johnston L, 'What Is Vigilantism?' (1996) 36 The British Journal of Criminology <https://academic.oup.com/bjc/article-abstract/36/2/220/563555?redirectedFrom=PDF>

'Joint Cybercrime Action Taskforce (J-CAT)' (*Europol*) <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>

Karnow C, 'Launch On Warning: Aggressive Defense Of Computer Systems' (2021) 7 Yale Journal of Law & Technology <https://digitalcommons.law.yale.edu/yjolt/vol7/iss1/4/>

Katyal N, 'Community Self-Help' (2005) 1 The Journal of Law, Economics & Policy <https://scholarship.law.georgetown.edu/facpub/533/>

Kerr O, 'Virtual Crime, Virtual Deterrence: A Skeptical View Of Self-Help, Architecture, And Civil Liability' (2005) 1 Journal of Law, Economics, and Policy <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=605964>

Kesan J, and Haynes C, 'Mitigative Counterstriking: Self-Defense And Deterrence In Cyberspace' [2012] Harvard Journal of Law and Technology <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1805163>

Kesan J, and Mullins C, 'Thinking Through Active Defense In Cyberspace' [2010] Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1691207>

Kilgore T, 'Solarwinds Releases Updates In Response To SUPERNOVA Hack' (*MarketWatch*, 2020) <https://www.marketwatch.com/story/solarwinds-releases-updates-to-in-response-supernova-hack-2020-12-24>

Lambert P, 'The Basics of Using a Proxy Server for Privacy and Security' (*Techrepublic, 2012*), <http://www.techrepublic.com/blog/it-security/the-basics-of-using-a-proxy-server-for-privacy-and-security/>

Lee R, "The Sliding Scale of Cyber Security," *SANS Analyst White Paper, SANS Institute InfoSec Reading Room* (2015), <https://www.sans.org/readingroom/whitepapers/analyst/sliding-scale-cyber-security-36240>

Lin H, 'More On The Active Defense Certainty Act' (*Lawfare*, 2017) <https://www.lawfareblog.com/more-active-defense-certainty-act>

Lipton J, 'Mixed Metaphors in Cyberspace: Property in Information and Information Systems' (2003) Loyola University Chicago Law Journal 235 <https://lawecommons.luc.edu/luclj/vol35/iss1/9/ >

'Maginot Revisited: More Real-World Results From Real-World Tests | Fireeye' (*FireEye*, 2015) <https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-maginot-revisited.html>

Martin C, 'A New Approach For Cyber Security In The UK' (*Ncsc.gov.uk*, 2016) <https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk>

Maurer, T. and Hinck, G., 2020. Cloud Security: A Primer for Policymakers. [online] Available at: <https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597>

Messerschmidt J, 'Hacback: Permitting Retaliatory Hacking By Non-State Actors As Proportionate Countermeasures To Transboundary Cyberharm' (2021) 52 Columbia Journal of Transnational Law <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309518>

Mills E, 'Botnet Worm In DOS Attacks Could Wipe Data Out On Infected Pcs' (*CNET*, 2009) <https://www.cnet.com/tech/services-and-software/botnet-worm-in-dos-attacks-could-wipe-data-out-on-infected-pcs/>

Mitnick D, 'Access Now To Join The Paris Call For Trust And Stability In Cyberspace - Access Now' (*Access Now*, 2018) <https://www.accessnow.org/access-now-to-join-the-paris-call-for-trust-and-stability-in-cyberspace/>

Mostert F, 'Digital Tools Of Intellectual Property Enforcement: Their Intended And Unintended Norm Setting Consequences', *Research Handbook on Intellectual Property and Digital Technologies* (1st edn, 2020)

Mostert F, and Chan L, 'Hacked Off: Protecting Intellectual Property Online' (*Intellectual Property Magazine*, 30 April 2014)

'M-Trends 2016' (Mandiant Consulting 2016) <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf>

Nast C, 'Google Hack Attack Was Ultra Sophisticated, New Details Show' (*Wired*, 2010) <https://www.wired.com/2010/01/operation-aurora/>

Nast C, 'The Digital Vigilantes Who Hack Back' (*The New Yorker*, 2018) <https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back>

'Nature Of Fraud And Computer Misuse In England And Wales - Office For National Statistics' (*Ons.gov.uk*, 2019) <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#trends-in-computer-misuse>

'No More Ransom: How 4 Millions Victims Of Ransomware Have Fought Back Against Hackers' (*Europol*, 2020) <https://www.europol.europa.eu/newsroom/news/no-more-ransom-how-4-millions-victims-of-ransomware-have-fought-back-against-hackers>

Nozick R, *Anarchy, State, And Utopia* (Ingram Publisher Service 1974)

'NVD - Vulnerabilities' (*Nvd.nist.gov*) <https://nvd.nist.gov/vuln>

'List Of Cybersecurity Associations And Organizations' (*Cybercrime Magazine*) <https://cybersecurityventures.com/cybersecurity-associations/>

'Our Sharing Model - Cyber Threat Alliance' (*Cyber Threat Alliance*) <https://cyberthreatalliance.org/our-sharing-model/>

'Our Work With The DNC: Setting The Record Straight' (*crowdstrike.com*, 2020) <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> accessed 23 August 2021

'Paris Call For Trust And Security In Cyberspace — Paris Call' (*Pariscall.international*) <https://pariscall.international/en/>

Parry L, 'Cyber Gang Led By Former Rave Promoter Dubbed The 'Acid House King' Are Facing Years Behind Bars For Plundering £1.25M' (*Mail Online*, 2014) <https://www.dailymail.co.uk/news/article-2580383/Cyber-gang-led-former-rave-promoter-dubbed-Acid-House-King-facing-years-bars-plundering-1-25m.html>

Paul Rosenzweig, Steven Bucci and David Inserra, 'Next Steps For U.S. Cybersecurity In The Trump Administration: Active Cyber Defense' (2017) <https://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense>

Perlroth N, 'Some Victims Of Online Hacking Edge Into The Light (Published 2013)' (*Nytimes.com*, 2013) <https://www.nytimes.com/2013/02/21/technology/hacking-victims-edge-into-light.html?ref=todayspaper>

Pfefferkorn R (Stanford Law School The Center for Internet and Society 2018) <http://cyberlaw.stanford.edu/publications/security-risks-government-hacking>

'Policy And Disclosure: 2021 Edition' (*Googleprojectzero.blogspot.com*, 2021) <https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html>

'Protocol Negotiations' (*Council of Europe*) <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>

Rose J, 'Here Are All The Sketchy Government Agencies Buying Hacking Team's Spy Tech' (*Motherboard.vice.com*) <https://motherboard.vice.com/en_us/article/nzeg5x/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech>

Rosenzweig P, 'International Law And Private Actor Active Cyber Defensive Measures' [2013] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2270673>

Repussard E, 'There Is No Attribution Problem, Only A Diplomatic One' (*E-International Relations*, 2020) <https://www.e-ir.info/2020/03/22/there-is-no-attribution-problem-only-a-diplomatic-one/>

Ropek L, 'The Solarwinds Hack Just Keeps Getting More Wild' (*Gizmodo*, 2021) <https://gizmodo.com/the-solarwinds-hack-just-keeps-getting-wilder-1846193313>

Roseen D, 'Georgia'S Governor Is About To Sign A Terrible Cybersecurity Bill (Update: Or Not!)' (*Slate Magazine*, 2018) <https://slate.com/technology/2018/04/georgias-governor-is-about-to-sign-a-terrible-cybersecurity-bill-into-law.html>

'Russia Planned Cyber-Attack On Tokyo Olympics, Says UK' (*the Guardian*, 2021) <https://www.theguardian.com/world/2020/oct/19/russia-planned-cyber-attack-on-tokyo-olympics-says-uk>

'Russian Cyber-Criminal Sentenced To 27 Years In Prison For Hacking And Credit Card Fraud Scheme' (*Justice.gov*, 2017) <https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme>

Scheibner J and others, 'Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, And Ethical Synthesis' (2021) 23 Journal of Medical Internet Research <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7952236/>

Schjolberg S, 'A Cyberspace Treaty' (*Cybercrimelaw.net*, 2010) <https://www.cybercrimelaw.net/Papers_on_Cybercrime.html>

Scroxton A, 'NHS Weathers Cyber Crime Storm During Pandemic, Says NCSC' (*ComputerWeekly.com*, 2020) <https://www.computerweekly.com/news/252491487/NHS-weathers-cyber-crime-storm-during-pandemic-says-NCSC>

Schmitt M (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press 2017)

'Secure By Design' (*GOV.UK*, 2019) <https://www.gov.uk/government/collections/secure-by-design>

Shamsi J and others, 'Attribution In Cyberspace: Techniques And Legalimplications' [2016] Security and Communication Network Special Issue Paper <https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1485>

Smith B, 'Hacking, Poaching, And Counterattacking: Digital Counterstrikes And The Contours Of Self-Help' (2005) 1 The Journal of Law, Economics and P <https://jlep.net/home/issues/volume-1/>

Sorcher S, 'Influencers: Companies Should Not Be Allowed To Hack Back' (*The Christian Science Monitor*, 2015) <https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0401/Influencers-Companies-should-not-be-allowed-to-hack-back>

'The Call And The 9 Principles — Paris Call' (*Pariscall.international*) <https://pariscall.international/en/principles>

The George Washington University Center for Cyber & Homeland Security, 'Into The Gray Zone The Private Sector And Active Defense Against Cyber Threats' (2016) <https://spfusa.org/research/gray-zone-private-sector-active-defense-cyber-threats/>

'The Hackback Debate' (*Cyberblog*, 2012) <https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/>

'Tokyo Games Organizers Hit By Data Breach And Info Leak' (*The Japan Times*, 2021) <https://www.japantimes.co.jp/news/2021/06/04/national/tokyo-olympics-data-breach/>

'Department Of Defense Strategy For Operating In Cyberspace' (US Department of Defense 2011) <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>

'Virustotal' (*Virustotal.com*) <https://www.virustotal.com/gui/>

Walsh N, 'Serious Cyberattacks In Europe Doubled In The Past Year' (*CNN*, 2021) <https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html>

'War In The Fifth Domain' (*The Economist*, 2010) <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>

Williams M, 'U.K., Not North Korea, Source Of DDOS Attacks, Researcher Says' (*Computerworld*, 2009) <https://www.computerworld.com/article/2526790/u-k---not-north-korea--source-of-ddos-attacks--researcher-says.html>

Wolff J, 'When Companies Get Hacked, Should They Be Allowed To Hack Back?' (*Atlantic*, 2017) <https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/> accessed 1 September 2021