Conceptualizing an International Framework for Active Private Cyber Defence[1]

Arindrajit Basu[2] *and Elonnai Hickok*[3]

I. Introduction and Scope

The ubiquity of Information Communication Technologies ('ICTs') in the modern day has increased the dependence of individuals, governments and institutions on cyberspace for the discharge of economic, social and political functions. At the same time, the vulnerabilities in information infrastructure have led to its misuse for malicious cyber activity across traditional territorial borders, culminating in economic, national security or political damage - proving it to be a space that is difficult to regulate and govern. This has challenged prevailing conceptions of municipal law, which seeks to govern its own territorial boundaries, and international law, which has been driven by the understanding that sovereign states have been successful in organizing

---

[1] A previous version of this paper was presented at a conference organised by The Hague Program for Cyber Norms, Leiden University in 2018. Subsequently, parts of this paper were used for submissions the Global Commission on the Stability of Cyberspace (GCSC) in 2019 by the Centre for Internet & Society. The full text of CIS's intervention can be found here. <https://cis-india.org/internet-governance/files/gcsc-response>.

[2] Research Manager, Centre for Internet & Society, India.

[3] Chief Operating Officer, Centre for Internet & Society, India.

domestic society and structuring external affairs.[4] Malicious cyber activity by rogue states and actors, regardless of jurisdiction, calls into question the very ability of a state to protect its sovereign interests including those of its citizens and industry. Recent attacks on the private sector coupled with the inability of governments to comprehensively respond has propelled discourse on the extent to which private sector organisations should be involved in this space. This includes the existence and limits of the right and corresponding responsibility that private sector organisations have to protect themselves, their customers, and a nation in cyberspace.[5]

Deployment of cyber defence by the private sector in cyberspace has largely involved passive deflection measures, such as building up robust cyber defence networks and incorporating greater resilience into their organizational cybersecurity strategy.[6] The private sector has traditionally provided similar products and services to governments as well. The increasing complexity and frequency of attacks has led to a deteriorating state of cybersecurity at organization and national levels.[7] Foiling an offensive operation that is already underway becomes particularly difficult if the target network has already been penetrated before detection of the attack.[8] Governments have started responding to this challenge by developing and deploying offensive cyber operations and active cyber defence.[9] Yet, state enabled Active Cyber

---

4 Hendrik Spruyt, *The Sovereign State and its Competitors: An Analysis of Systems Change* (Princeton University Press 1994).

5 Jan E. Messerschmidt, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' (2013) 52(1) Columbia Journal of Transnational Law <http://jtl.columbia.edu/wp-content/uploads/sites/4/2014/05/MesserschmidtNoteHackback.pdf> accessed November 2, 2018; Carnegie Live,, 'The Private Sector and Active Cyber Defence and Closing Remarks'(*YouTube* April 18 2017) <https://www.youtube.com/watch?v=TYW237udDx0> accessed November 2 2018.>.; Beatrice Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law' (2017) 126(5) Yale Law Journal <https://www.yalelawjournal.org/note/duties-owed-low-intensity-cyber-attacks-and-liability-for-transboundary-torts-in-international-law> accessed November 2, 2018.

6 Robert Anderson, Brian Lum, and Bhavjit Walha, Offense vs. Defence (December 11, 2005) <https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/OffenseVsDefence.pdf>.

7 Lotte Schou-Zibell & Nigel Phair, 'Cyber-Insecurity: The Dark Side of Digital Financial Services' (*Newsroom*, 1 August 2018) <https://newsroom.unsw.edu.au/news/science-tech/cyber-insecurity-dark-side-digital-financial-services>.

8 Anderson, Lum, and Walha (n 6).

9 GIP Digital Watch Observatory for Internet Governance and Digital Policy, *UN GGE and OEWG* <https://dig.watch/processes/ungge> accessed November 2, 2018. (Indeed, a map created by the Diplo Foundation identifies 23 countries with state enabled offensive cyber capabilities and 8 countries indicating a move to adopting such measures)

Defence[10] ('ACD') only addresses this challenge from the perspective of individual states.[11]

Indeed, this challenge has propelled private actors to increasingly look beyond government-driven security mechanisms and resort to aggressive measures to protect themselves, either by developing their own cyber capabilities or by hiring third party cyber security companies. At the same time, governments are increasingly looking to the private sector to not only provide security products but also to actively utilize their resources in addressing threats to national cyber space. This paradigm has led to discussions that expand ACD measures to the private sector as a means to further enhance national cyber security and enable companies to protect their own infrastructure. For the purposes of this paper, Active Private Cyber Defence ('APCD') refers to any active defence measure taken by the private sector.

It is interesting to note that these private sector mechanisms are emerging despite existing legislation outlawing use of active defence by individuals and non-state entities. Thus, a key window exists for policy-makers in the possibility of establishing a framework for existing APCD practices that would enable optimal utilisation of private sector capabilities for securing cyberspace at an organizational and national level. This must happen in consonance with circumscribing their operations within the boundaries of the rule of law, both in terms of domestic legislation and international law.

Conceptualizing such a framework is in many ways shaped by national, international, and geo-political dynamics and challenged by the evolving nature of technology. This paper seeks to unpack the complexities that underscore each of these challenges and identify avenues towards resolving some of them.

The paper is divided into four sections. The first section reviews the spectrum of active private defence and demarcates the various kinds of offensive and defensive capabilities that would fit along various rungs in this spectrum. It also maps existing policy initiatives enabling APCD from key jurisdictions. The second section outlines relevant standards of international law and analyzes the extent to which they might help circumscribe the legal

---

[10] For the purposes of this paper, Active Cyber Defence ('ACD') refers to any cyber operation that has an impact in the adversary's network and extends beyond mere passive resilience.

[11] Nelson, Steven, and Marina Hutchinson, 'Active Cyber Defence' or Vigilantism?' *Washington Examiner* (February 8, 2018) <https://www.washingtonexaminer.com/active-cyber-defence-or-vigilantism> accessed November 2, 2018. As noted by Rep. Tom Graves when explaining the proposed APCD Bill in the US, "The status quo is unacceptable, and people are yearning for a solution. Even just minor steps like we're trying to provide here".

limits of APCD and resolve any geopolitical tensions that might arise. The final section projects the potential ramifications of APCD and articulates the drivers that could determine how a robust norm on active cyber defence might shape responsible behaviour in cyberspace by both state and non-state actors alike. The paper concludes with a set of points and questions with the aim of articulating a baseline from which municipal legislators and global policy-makers can take this debate forward.

This paper restricts itself to evaluating the response to low-intensity cyber-attacks: attacks that are below the threshold of 'use of force' i.e., those cyber-attacks that cause physical damage to life or property akin to a traditional kinetic (non-cyber) attack. We have limited the scope for two reasons. First, most of the cyber-attacks presently faced by the private sector do not amount to the 'use of force' as laid out in Article 2(4) of the United Nations Charter. A Hackmageddon report suggests that in 2016 and 2017 only 3.4% and 4.3% of cyber-attacks were conducted with the underlying motivation of causing physical damage akin to the use of force.[12] The attacks are also largely aimed at accomplishing thefts of intellectual property, distributed denial of service attacks and ransomware Second, the perceived monopoly states have over the right to 'use of force' has specific connotations from a global governance and international law perspective. This question deserves to be treated separately from low-intensity attacks and is therefore left for another paper.

II. Mapping the Landscape of Active Private Cyber DefencE

A. Identifying the spectrum

Operations undertaken for the purpose of cyber defence differ greatly from one operation to another. Therefore, these operations must be distinguished from one another and classified based on impact, intention of the attacker and reversibility of the attack.

As a starting point ,'active' and 'passive cyber defence' should be separated when discussing cyber defensive operations.[13] Activities whose impact

[12] Passeri, Paolo, '2017 Cyber Attacks Statistics' (*Hackmageddon*, 30 September 2018) <https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/> accessed November 2, 2018.

[13] Paul Rosenzweig, Steven P Bucci, and David Inserra, *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defence* (*The Heritage Foundation*, 5 May 2017) <https://www.heritage.org/sites/default/files/2017-05/BG3188.pdf>.

is only felt within the defendant's network may be termed passive cyber defence. These include measures like basic security controls, antivirus and patch management.[14]To qualify as active cyber defence, the operation must, at least partially impact external networks – networks which belong either to adversaries or are proxy networks utilised by adversaries.[15] Several scholars have attempted to classify both offensive and defensive cyber operations on a spectrum. Paul Rosenzweig has drafted a comprehensive spectrum of ACD measures based on the effects the measures could have on information infrastructure—including observation, access, disruption, and destruction.[16] The Centre for Homeland Security at George Washington University (CHSGWU) have created a spectrum of active cyber defence tactics, ranging from offensive to defensive, based on the intent of the actor implementing them.[17] For example, the use of tarp its, sandboxes and honey pots which are technical tools that prevent the hacker from entering a network's perimeter are on the defensive end of the spectrum.[18] On the other hand, the use of botnets or hackbacks[19] to infiltrate the adversary's networks and recover stolen information would fall within the offensive end of the ACD spectrum. Table 1 shows examples of measures at various rungs of the Active Cyber Defence Spectrum.

TABLE 1: SPECTRUM OF ACTIVE CYBER DEFENCE MEASURES

PASSIVE DEFENCE MEASURES (BUILDING RESILIENCE IN DEFENDANT'S NETWORK)	Basic security controls, firewalls, anti-virus, scanning and monitoring, security controls
ACTIVE CYBER DEFENCE (LOW IMPACT/LOW RISK)	Information sharing, tar pits, sandboxes, honeypots, Intelligence Gathering in dark web

[14] Active Defence Task Force, *Into the Gray Zone: The Private Sector and Active Defence Against Cyber Threats* (Centre for Homeland Security, George Washington University, October 2016) <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenceReportFINAL.pdf>

[15] Wyatt Hoffman, Ariel Levite, 'Rethinking Corporate Activity Cyber Defence' (*Lawfare*, 17 July 2017) <https://www.lawfareblog.com/rethinking-corporate-active-cyber-defence>.

[16] Paul Rosenzweig, 'International Law and Private Actor Active Cyber Defensive Measures' (2014) 50(1) Stanford Journal of International Law 2.

[17] Active Defence Task Force (n 14).

[18] Joseph Menn, 'Hacked Companies Fight Back with Controversial Steps' *Reuters* (17 June 2012) <http://www.reuters.com/article/2012/06/17/us-media-techsummit-cyber-strikeback-idUSBRE85G07S20120617>.

[19] Hackbacks are the most offensive ACD measure and refers to operations intended to destroy the networks of adversaries without any form of authorization. See Farzaneh Badil, 'Legalizing Hackbacks' (*Internet Governance*, 4 May 2017) <https://www.internetgovernance.org/2017/05/04/legalizing-hackbacks/> accessed 02 November 2018.

ACTIVE CYBER DEFENCE (HIGH IMPACT/HIGH RISK)	Botnet take downs, 'hot pursuit' to recover assets
ACTIVE CYBER DEFENCE ('HACKBACK')	Operations intended to disrupt or destroy external networks without authorization

(*Source: Adapted from Into the Gray Zone)*

B. Configuring models of state-private actor relationships in the APCD context

Historically, governments used to engage with the private sector in two ways. First was by co-opting their capabilities within the framework of a national cyber-security ecosystem, and the second was by putting in place a law that prohibited individual entities from infiltrating external networks, thereby effectively banning APCD. While these two configurations remain the official status quo, APCD is increasingly being considered, as States are beginning to view the role of the private sector in the cybersecurity ecosystem differently.

In understanding the developments around ACD and APCD, their complexities, and finding a way forward, it is important to place APCD in the larger context of the relationship between governments and the private sector. Maurer has articulated three major models for government engagement with private actors in cyberspace.[20] The first model is *delegation* - where the government exercises clear oversight over their actions through screening and selection of actors, exercise of punitive sanction and a clear demarcation of potential effects. The second model is *orchestration*, where the government passively supports the private actor but does not establish clear oversight mechanisms.[21] Finally, *sanctioning* entails that the state does not acknowledge the actions taken by the private actors operating from their territory and effectively turns a blind eye.[22] We attempt to extend these models to the configurations we observed when mapping developments in the APCD space. We have also added two additional configurations that reflect the trends we observed in our research. Articulating these configurations and mapping the state of private-public partnerships is crucial for identifying the different kinds of challenges and opportunities within each configuration,

[20] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press 2017) 29.
[21] ibid.
[22] ibid.

As a note, policy or use-cases in a country may fall within multiple configurations. For example, some countries sanction an underground market that allows for APCD despite having a law that bans it.[23] In the context of APCD, a private sector company may work with multiple governments, multiple companies, and across multiple jurisdictions - which poses an additional complexity which we address in Part IV of this paper.

C. "PRE"-APCD Configurations

Often private-public partnerships in cyber defence are confused with those engaging in active cyber defence. Further, private-public partnerships that are 'pre-APCD' configurations often start to engage in active cyber defence at some point. Thus, our mapping takes into account private-public partnerships that do not necessarily engage in active cyber defence.

i. Configuration 1: Co-optation

This configuration covers scenarios where private sector actors, security researchers and commercial cyber-security researchers work with law enforcement authorities, military, and other nodal agencies responsible for cyber security as part of a multi-stakeholder unit. Decisions are taken by the unit as a whole rather than by individual actors.

Various models of co-optation have been deployed by countries across the globe. The first model is a permanent unit that synchronizes the planning of cyberspace operations in collaboration with various stakeholders. The United States Cyber Command is an example of this.[24]It is one of the ten unified commands that come under the aegis of the United States Department of Defence.[25] Israel's cyber strategy also involves an ecosystem approach which includes both passive and active defence and offensive capabilities across military domains.[26] Singapore's Cyber Security Agency, which was set up in 2015 under the Prime Minister's Office (PMO) was set up to protect critical information infrastructure and " coordinate efforts across

---

[23] *See* example of cyber defence contractors in U.S. below.

[24] US Cyber Command, 'Achieve and Maintain Cyberspace Superiority' (*Cybercom.mil*, April 2018) <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf?ver=2018-06-14-152556-010> accessed 2 November 2018.

[25] US Cyber Command, 'Mission and Vision'(*Cybercom.mil*) <https://www.cybercom.mil/About/Mission-and-Vision/> accessed 2 November 2018.

[26] Michael Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy' (S. Rajaratnam School of International Studies, January 2015) <https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf> accessed 2 November 2018.

government, industry, academia, businesses and the people sector, as well as internationally."[27]

Other instances of co-optation are voluntary cyber response units that deploy civilians working in the private sector on a voluntary basis. The Cyber Defence Unit[28] of the Estonian Defence League[29] is a case in point. The league was set up as a voluntary unit in 1918 and was re-established when Estonia broke away from the Soviet Union.[30] The voluntary nature of the force allows private actors to aid governmental authorities - Estonian State Information System Authority, who are responsible for coordinating the group's efforts.[31]

The cyber unit has two main functions.[32] The first is improving capacity across society, through regular trainings and cyber security exercises. The second is working as a cohesive unit when called upon to respond to specific cyber emergencies.[33]

The United States has taken some steps towards emulating the Estonian model. Lawmakers have put forward a bill that would create special units in the National Guard to respond to cyber-attacks.[34] The National Cyber Guard Civil Support Teams will work to co-ordinate state, federal and local level resources and assist the private sector with response and recovery.[35]

---

[27] Cyber Security Agency of Singapore, 'Singapore's Cybersecurity Strategy' (2016) <https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf> accessed 2 November 2018.

[28] Kaitseliit, 'Estonian Defence League's Cyber Unit' <http://www.kaitseliit.ee/en/cyber-unit> accessed 2 November 2018. "EDL CU objectives:
- development of cooperation among qualified volunteer IT specialists
- raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training
- creation of a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation
- education and training in information security
- participation in international cyber security training events"

[29] Monica M. Ruiz, 'Is Estonia's Approach to Cyber Defence Feasible in the United States?'(*War on the Rocks*, 9 January 2018) <https://warontherocks.com/2018/01/estonias-approach-cyber-defence-feasible-united-states/> accessed 2 November 2018.

[30] ibid.

[31] ibid.

[32] Kaitseliit (n 28).

[33] CCDCOE, 'Locked Shields 2017'(21 April 2017) <https://ccdcoe.org/locked-shields-2017.html> accessed 2 November 2018. Former Estonian President Thomas Hendrik Ilves stated "we have lots of talented people who work in the private sector and we offered them the possibility of working once a week for a more patriotic cause."

[34] Cimpanu, Catalin, 'New US Bill Wants to Create National Guard Cyber Units' (*Bleeping Computer*, 22 May 2018) <https://www.bleepingcomputer.com/news/government/new-us-bill-wants-to-create-national-guard-cyber-units/> accessed 2 November 2018.

[35] Ruiz (n 29).

Like the Estonian model, individuals on the cyber force will be civilians with full-time jobs in the private sector who will work with the government when called upon.[36]

ii. Configuration 2: Banning

Country has a law banning ACD measures by private companies or individuals. These laws are largely worded in the form of a prohibition against infiltrating external computer networks due to the risks posed by allowing a private sector to undertake government functions, and accessing security devices and the challenges with fostering accountability in this regard. For example, the Computer Fraud and Abuse Act ('CFAA') in the United States criminalizes 'unauthorized access' to a computer and 'unauthorized transmission of malware' and damage of computer networks.[37]

D. Configurations Where APCD is Enabled

i. Configuration 3: Delegation

In this configuration, *a country enables, through law, the private sector to undertake specific ACD actions to achieve specific and defined goals*.

This configuration comes in various forms through which clear and specific responsibilities are assigned to a private sector actor within the strict confines of relevant law and policy. Singapore has recognized the role of the private sector in protecting national security for the protection of national information infrastructure, including by taking pre-emptive strikes against perceived cyber threats[38] on critical infrastructure.[39] After being subject to an inordinate number of breaches, Singapore amended its Computer Misuse Act (amended to the Computer Misuse and Cybersecurity Act - CMCA) to reflect this recognition.[40] The 2014 Amendment is a clear example of delegation as it creates a middle ground where it does not fully legalize APCD but enables state-sanctioned APCD for the protection of critical

---

[36] ibid.

[37] 18 USC § 1030.

[38] Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis' (2015) 52(4) *American Business Law Journal* 721.

[39] Phneah, Ellyne, 'S'pore Beefs up Cybersecurity Law to Allow Preemptive Measures' *ZDNet* (14 January 2013) <http://www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/>.

[40] ibid.

information infrastructure after the issuing of certificates to 'specified persons.'[41] Singapore's approach to engagement with the private sector offers a hybrid as a model of co-optation through the Cyber Security Agency that "coordinates nationwide efforts coordinate efforts across government, industry, academia, businesses and the people sector, as well as internationally"[42] combined with government-delegated Active Defence Measures by the private sector when needed.

In the USA, Representatives Tom Graves (U.S. Representative, Georgia - Republican), Kyrsten Sinema (U.S. Representative, Arizona – Democrat), have attempted to follow suit by introducing a bill, titled the Active Cyber Defence Certainty Act (ACDC), as per this configuration.[43] The new draft legislation provides an exception to liability under the Computer Fraud and Abuse Act ('CFAA'). This bill would allow victims to enter the networks of their adversaries for evidence gathering purposes to identify the attacker and gather evidence to prove who the attacker was.[44] It has been improved after taking into account certain legitimate concerns.[45]

ii. Configuration 4: Orchestration

A government may recognize or underscore the importance of APCD but not regulate it. Unlike in delegation, where permitted capabilities are clearly defined and framed, in this configuration a whole range of capabilities may

---

[41] Computer Misuse and Cybersecurity Act (Cap 50A, 2013 Rev Ed), s 15(A)(1); Cybersecurity Act (Amendment Bill) 2018, cl 23.

[42] Cyber Security Agency of Singapore (n 27).

[43] Active Cyber Defence Certainty Act 2017 (USA).

[44] Chris Cook, 'Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defence Certainty Act' (*Just Security*, 20 November 2017) <https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defence-certainty-act/> accessed 2 November 2018.

[45] Tom Graves, Rep. Tom Graves Formally Introduces Active Cyber Defence Bill <https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398840> accessed 2 November 2018.

"Key changes to the bill that were made to address the concerns include.

- A voluntary review process that individuals and companies can utilize before using active-defence techniques;
  - This provision allows defenders to benefit from review of their proposed active-defence measures by the FBI Joint Taskforce, which will assist defenders in conforming to federal law and improving the technical operation of the measure;
  - The authority to conduct these reviews would exist under a two-year pilot program, and could be amended or renewed at a later date.
- Requires notification to the government for the use of active-cyber defence measures that go beyond beaconing;
- Clarification that the bill does not interfere with a person's right to seek damages;
- Requires an annual report on the federal government's progress in deterring cybercrime.

The updated legislation also makes other minor and technical change"

be possible. *We have observed that such a configuration is often enabled through a range of mechanisms including commitments to cooperation in national cyber security frameworks and strategies, MOU's and contracts framing public private partnerships in the framing of strengthening national security.*

For example, recently some governmental policy stances have worked towards serving as enablers of APCD in the context of it strengthening national security. For example, in its National Cyber Security Strategy 2016–2021, the UK government has claimed that it "will draw on its capabilities and those of industry to develop and apply active cyber defence measures to significantly enhance the levels of cybersecurity across UK networks."[46] However, the UK government is yet to state clearly the role and freedoms given to private sector corporations in discharging this role.

Loosely worded policy documents that encourage the private sector to engage in 'proactive' cyber-security measures without charting out guidelines detailing how these measures are to be implemented or the limits on their use could also be considered *orchestration*. For example, India's 2013 Cyber Security Policy states "To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, **proactive security posture** assessment and forensically enabled information infrastructure."[47]

Another example of orchestration might be governments working with cybersecurity companies without a clearly defined policy framework underscoring this co-operation. There are multiple instances of companies dismantling botnets with various degrees of collaboration with law enforcement officials. One such example is INTERPOL's collaboration with numerous cyber security companies to dismantle the Simda botnet that had infected 190 countries.[48]

---

[46] UK Government, National Cyber Security Strategy 2016–2021.

[47] Parliament of India, National Cyber Security Policy, 2013 (2013) <http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013(1).pdf> accessed 2 November 2018. This policy is set to be updated in 2020. The National Cybersecurity Co-ordinator has already sought responses to consultation from various stakeholders and is in the process of drafting a public version of this strategy. It is likely that this will serve as a complete overhaul of the 2013 cybersecurity policy.

[48] O'Brian and Dick, 'Simda Botnet Hit by Interpol Takedown'(*Symantec Security Response*, 13 April 2015) <https://www.symantec.com/connect/blogs/simda-botnet-hit-interpol-takedown> accessed 2 November 2018.

The orchestration configuration may be confused with the co-optation configuration in certain instances as both involve the government working with private actors. However, a key difference in this configuration is that the actors work with the government and are enabled through a variety of mechanisms but stop short of becoming a part of the government-as is the case with the co-optation configuration.

iii. Configuration 5: Sanctioning

Security companies developing these capabilities and using the same in contexts where governments explicitly prohibit such actions or in the absence of such legal frameworks. In such a relationship, *a company deploys ACD to secure its own organization or another private sector organization despite this relationship being illegal*. Though large companies like Google and Microsoft have the capability to carry out APCD and have done so in one-off instances in the past,[49] many companies rely on third party security companies to bring in these capabilities. Globally, the security market has been expanding. Private cyber security companies are increasingly resorting to taking active cyber defence measures include large defence-contractors such as Lockheed Martin in the US, BAE Systems in the UK and Airbus in Europe.[50]

These contractors have largely developed their own cyber security solutions and services,[51] although some have also hired commercial cyber security firms to bolster their capabilities. Lockheed Martin, for example, has developed its own portfolio and hired its first cybersecurity contractor, Industrial Defender[52] which added to Lockheed portfolio of intelligence-driven security solutions.[53] Start-ups such as Crowd Strike and CloudFare have attracted

---

[49] Matt Buchanan, 'Google Hacked the Chinese Hackers Right Back' (*Gizmodo*, 18 June 2013) <https://gizmodo.com/5449037/google-hacked-the-chinese-hackers-right-back> accessed 2 November 2018.

[50] Maurer (n 20); Peggy Hollinger, "Defence Groups Take Aim at Cyber Security" *Financial Times*, Mar 28, 2016 <https://www.ft.com/content/45aedb82-e676-11e5-bc31-138df2ae9ee6> (The record of their use for commercial security purposes remains sketchy at best and their largest customer base remains the government).

[51] 'About Us' (*Airbus CyberSecurity*) <https://airbus-cyber-security.com/about./> accessed 2 November 2018; 'Cyber Security Services' (*BAE Systems | Cyber Security & Intelligence*) <https://www.baesystems.com/en/cybersecurity/capability/cyber-security-services> accessed 2 November 2018.

[52] Loren Thompson, 'Lockheed Martin Moves To Dominate Cyber of Electric Grid & Energy Complex' (*Forbes*, 14 March 2014) <http://www.forbes.com/sites/lorenthompson/2014/03/14/lockheed-martin-moves-todominate-cyber-defence-of-electric-grid-energy-complex/>.

[53] ibid.

significant investment from corporations to engage in ACD.[54] Smaller cybersecurity companies like ManTech[55] in the US or NICE in Israel are also engaging in these measures.[56] It has been found that a cluster of companies have formed a cyber security-military industrial complex that work in the development and deployment of cyber weapons if the government is unable or unwilling to do so.[57] An under-cover market in the Netherlands has enabled the hiring of cyber security companies, including those located in foreign territory to attack the networks of potential adversaries.[58] This market operates largely without any oversight and potentially can replace the government as the final guarantor of financial security, as per one Dutch expert.[59]

The damage caused by Operation Aurora through 2009[60] signalled that passive cyber defence mechanisms may not be sufficient to ward off Advanced Persistent Threats ('APTs').[61] Operation Aurora is the name given to a series of cyberattacks from China which targeted U.S. private sector companies back in 2010.[62] This included a phishing company which compromised the networks of several large American companies including Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google and several others, in a gambit to steal trade secrets.[63] Cyber security companies CrowdStrike,[64] FireEye,[65]

---

[54] The Economist, 'Firewalls and Firefights' (August 10, 2013) <https://www.economist.com/business/2013/08/10/firewalls-and-firefights> accessed 2 November 2018.

[55] Securing the Future (*ManTech*) <https://www.mantech.com/> accessed 2 November 2018.

[56] Maurer (n 20), 18.

[57] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014) 119–120.

[58] Dennis Broeders, 'Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance' (Netherlands Defence Academy, 2015).

[59] ibid.

[60] Operation Aurora (Sophos Security Topics) <https://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx> accessed 2 November 2018. ("Operation Aurora is a targeted malware attack against at least 30 major companies—including Google and Adobe—which exploited a zero-day flaw in Internet Explorer. The exploit allowed malware to load onto users' computers. Once loaded, the malware could take control of the computer to steal corporate intellectual property").

[61] Kim Zetter, 'Google Hack Attack was Ultra Sophisticated, New Details Show' *WIRED* (14 January 2010) <http://www.wired.com/2010/01/operation-aurora/>.

[62] Council on Foreign Relations, *Operation Aurora* (January 2010) <https://www.cfr.org/interactive/cyber-operations/operation-aurora>.

[63] ibid.

[64] 'Cybersecurity Solutions' (*CrowdStrike*) <https://www.crowdstrike.com/solutions/> accessed 2 November 2018.

[65] 'Cyber Security Experts & Solution Providers' (*FireEye*) <https://www.fireeye.com/> accessed 2 November 2018.

Hexis,[66] and MITRE[67] have attempted to develop the Active Cyber Defence (ACD) industry by developing a range of solutions and articulating justifications for its legalization.[68]

A burgeoning industry of cybersecurity companies are providing honeypots and more aggressive ACD services.[69] These ACD services are part of a rapidly expanding cybersecurity industry that might reach 248.26 billion by 2023, in which ACD services occupy a fair share.[70] 36 per cent of respondents (private companies) to a survey conducted at the Black Hat Security conference claimed to have indulged in active cyber defence.[71] Due to fears of prosecution, many companies outsource their ACD measures to companies at home or abroad.[72] Some cybersecurity companies also reportedly set up entire divisions abroad so that they can engage in ACD measures that are at present, illegal in the United States.[73]

It is important to note that much of the cybersecurity market is concentrated in the United States, Israel, United Kingdom and Western Europe[74] with North America holding the largest market share by continent.[75] This is crucial to note as the market for ACD might be similarly skewed in favour

---

[66] 'Hexis Cyber Solutions' <https://www.immixgroup.com/hexis/> accessed 2 November 2018.

[67] 'Resiliency' (*The MITRE Corporation*, 27 January 2014) <https://www.mitre.org/capabilities/cybersecurity/resiliency>

[68] Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis' (2014) 52(4) American Business Law Journal 721.

[69] Whatt Hoffman & Ariel E. Levite, '*Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?*' (Carnegie Endowment for International Peace, 2017) <https://carnegieendowment.org/files/Cyber_Defence_INT_final_full.pdf>.

[70] 'Cybersecurity Market Worth $248.26 Billion by 2023' (Markets and Markets) <https://www.marketsandmarkets.com/PressReleases/cyber-security.asp> accessed 2 November 2018.

[71] 'Firewalls and Firefights' *The Economist* (10 August 2013) <https://www.economist.com/business/2013/08/10/firewalls-and-firefights> accessed 2 November 2018.

[72] Hoffman & Levite (n 69).

[73] Michael Riley and Jordan Robertson, 'FBI Probes if Banks Hacked Back as Firms Mull Offensives' *Bloomberg* (30 December 2014)<http://www.bloomberg.com/news/articles/2014-12-30/fbiprobes-if-banks-hacked-back-as-firms-mull-offensives> accessed 2 November 2018.

[74] 'Cybersecurity 500 List, 2018 Edition,' *Cybercrime Magazine* (22 May 2018) <https://cybersecurityventures.com/cybersecurity-500-list/>; Hadar and Tomer, 'How Did Israel Become a Leader in Cybersecurity?' *Automotive News* <http://www.autonews.com/article/20181001/SHIFT/181009995/israeli-intelligence-cybersecurity> accessed 2 November 2018 (There are over 400 cybersecurity companies active in Israel).

[75] Research and Markets,'Cybersecurity Market - Global Forecast to 2023: Innovation Spotlight on Splunk, Cyberbit, Carbon Black & Balbix' *PR Newswire* (28 September 2018) <https://www.prnewswire.com/news-releases/cybersecurity-market---global-forecast-to-2023-innovation-spotlight-on-splunk-cyberbit-carbon-black--balbix-300720906.html> accessed 2 November 2018.

of economically and militarily powerful countries, if enabled globally. The geo-political spill-off from this distribution is a major challenge for conceptualizing APCD at the global level and will be discussed in Part IV.

TABLE 2: MODELS DENOTING APCD CONFIGURATIONS

	MODEL	APCD CONFIGURATION	RELATIONSHIP BETWEEN AND PRIVATE ACTOR	EXAMPLES
ENABLES APCD	**DELEGATION**	Private actors engaging in ACD under 'effective control' of the government after delegation by a clearly defined legal/policy instrument	'Effective control'; every decision must be approved by the government	Singapore
	ORCHESTRATION	Government not being clear about the legality of APCD	Government gives tacit approval without explicitly invoking APCD in law or policy instruments	India, UK, INTERPOL
	SANCTIONING	Private actors operating under the radar despite ACD being illegal	Government does not recognize existence of the private actors operating under the radar	Markets in USA, Israel, UK and Western Europe

"PRE"-APCD	**CO-OPTATION**	Private sector actors work with the government in the form of a multi-stakeholder unit	Collective decisions are taken by the unit as a whole	USA Cyber Command, Estonian Cyber National Guard
	BANNING	Law explicitly banning ACD measures by the private sector	Despite the existence of a law, private sector actors often operate under the radar, which means that this model co-exists with 'sanctioning'	Albania, Antigua & Barbados, Kenya, Fiji, Japan, USA, Ghana, Austria[76]

III. The Role of International Law

The normative framework of international law often acts as a tool for resolving conflict and creating governance frameworks for actions where policy vacuums exist. Successful cyber security measures depend on cooperation between different stakeholders. The transboundary nature of the internet, the broad scope of cyber security itself, and the range of actors impacted by the same - means that the level of international cooperation influences the level of national cyber security as it enables information sharing, development of best practice, and *increases the interoperability and compatibility of cyber defence*.[77] Grounding APCD in international law can help in ensuring the compatibility and interoperability of APCD across national borders and in improving the level of trust that nations repose in the modus operandi of such measures.[78] Furthermore, as demonstrated by the section above, the use of APCD as is currently being carried out, is complex and raises important

[76] See Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis' (2015) 52(4) American Business Law Journal 721 et al for more detailed sampling

[77] Secretariat of the Security Committee, Finland, 'Finland's Cyber Security Strategy: Background Dossier' (2013) <https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf>.

[78] Martha Finnemore and Duncan Hollis, 'Constructing Norms for Global Cybersecurity'(2016) 110(3) American Journal of International Law 425, 427; Lawrence

questions about legality and jurisdiction. Furthermore, the understanding of how international law applies to APCD measures is an extension of the issues being negotiated in the UN Group of Governmental Experts (UN-GGE) and other international forums- particularly on the right to self-defence and international law of state responsibility and countermeasures. International law is by no means a panacea and would not substitute the domestic governance frameworks and discursive practices that would determine the framing of domestic policy. However, by devising model universal best practices, it could nudge nations into devising and implementing effective policy on this front. To get there, however, a doctrinal application and interpretation of the existing standards of international law to existing scenarios must be the starting point.

There exists a body of legal scholarship that has sought to evaluate the doctrinal validity of APCD capabilities as enabled by a state. For example, Messerschmidt makes three analytical assertions that demonstrate how APCD measures can comply with existing standards of international law, if it is at the receiving end of cyber-attacks. Towards understanding how international law may apply to APCD we examine Messerschmidt's three assertions and attempt to call out various legal complexities that arise with each.

A. Violation of International obligations

Is there a violation of an international obligation by the state from whose territory an attack emanates from?

The customary international law on the responsibility of states for the commission of internationally wrongful acts, which have been codified in the Articles on State Responsibility,[79] recognize that a state can be held responsible in International Law if two elements are fulfilled:

1. the act or omission that leads to the breach of an international obligation and
2. attribution of that act or omission to the state in question.[80]

On the first point, it is clear that active cyber defence measures that intrude into external computer systems could be internationally wrongful

Lessig, 'The Regulation of Social Meaning'(1995) 62 University of Chicago Law Review 943.

[79] Adopted by UNGA in 2005

[80] International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its 53rd session, A/56/10, August 2001, UN GAOR, 56th Sess Supp No 10, UN Doc A/56/10(SUPP) (2001), art 4(1) ("Articles on State Responsibility").

acts. First, they may violate the prohibition on the use of force in Article 2(4) of the UN Charter. The Tallinn Manual- sponsored by NATO and authored by an International Group of Experts (IGE) proposes eight criteria to determine when a cyber operation amounts to a use of force: severity, immediacy, directness, invasiveness, measurability, military character and presumptive legality.[81] ACD measures on the active end of the spectrum such as hack backs or botnet attacks could in certain cases be counted as a use of force based on this criterion. Second, these could violate the norm against norm-intervention, which is a part of customary international law, by violating the territorial sovereignty of another nation in cyber space.[82] Finally, active cyber defence measures might also be considered cybercrimes as per the framework of The Budapest Convention. The Budapest Convention, entered into force in 2004, is the only binding international instrument in this regard and has thus far has sixty four signatories including Australia, Canada, US, Japan, and most European Union States (but notably not India.)[83] It requires state parties to adopt legislation or other measures to criminalize the international commission of certain offenses. These include: illegal access to computer systems, illegal interception of data, data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud.[84] Active cyber defence measures used on external systems will amount to the aforementioned offenses under The Budapest Convention as they are likely to damage infrastructure in another state party's jurisdiction than other purely investigative measures.[85] While the Budapest Convention has not been

---

[81] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2017) "(a) Severity: How many people were killed? How large an area was attacked? How much damage was done within this area? (b) Immediacy: How soon were the effects of the cyber operation felt? How quickly did its effects abate? (c) Directness: Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects? (d) Invasiveness: Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country? (e) Measurability: How can the effects of the action be quantified? Are the effects of the action distinct from the results of parallel or competing actions? How certain is the calculation of the effects? (f) Military character: Did the military conduct the cyber operation? Were the armed forces the target of the cyber operation? (g) State involvement: Is the State directly or indirectly involved in the act in question? But for the acting State's sake, would the action have occurred? (h) Presumptive legality: Has this category of action been generally characterized as a use of force, or characterized as one that is not? Are the means qualitatively similar to others presumed legitimate under international law?"

[82] Thomas Payne, 'Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations' (2016) 20(2) Lewis & Clark Review 699.

[83] Chart of Signatures and Ratifications of Treaty 185, Council of Europe <http://perma.cc/57D7-XPBF>

[84] Convention on Cybercrime 2001 ('Budapest Convention').

[85] Alexandra Van Dine, 'When is Cyber Ddefence a Crime? Evaluating Active Cyber Ddefence Measures under the Budapest Convention' (2020) 20(2) Chicago Journal of International Law 562.

universally accepted, it has been ratified by a number of states engaging in active cyber defence measures and therefore it is clear that they need to adopt legislation that constrains the same.

A plain reading of the articles would indicate that acts of private persons or groups are not attributable to the state, unless the non-state actor operating under the 'effective control' of the state.[86] However, the Commentary published along with the articles by the International Law Commission declares that a state may be held responsible for the acts of private parties if they failed to take necessary measures to prevent the wrongful acts.[87]

The obligation to take 'necessary preventive measures' indicates a due diligence obligation to prevent the use of its territory for the commission of wrongful acts.[88] Messerschmidt approaches this question through the customary international law on the prevention of significant transboundary harm, which results in 'liability' rather than state responsibility.[89] The key difference between liability and responsibility lies in the fact that the act which caused significant transboundary harm need not be an internationally wrongful act.[90] A state is liable if any activity from its territory causes significant transboundary harm, even if the state did not exercise 'effective control' over the private party. In such scenarios, even if a state is not responsible in international law, they could potentially be held liable. Messerchmidt traces the evolution of this obligation in international law from its origin in the *Trail Smelter* arbitration[91] through its recognition by the International Court

---

[86] State responsibility is imputed if imputes state responsibility "if the conduct of a non-state actor is "acting under the instructions of or under the direction and control of the state carrying out the said conduct." This test, known as the 'effective control' test was laid down by the International Court of Justice in Nicaragua and imported by the ILC into Article 8. The test essentially requires a state to "exercise such a degree of control in all fields, as to justify the non-state actors on its behalf". It implies that the state must have directed each allegedly wrongful act in order to attract international responsibility. This test has been criticized by several scholars as being too high a threshold and therefore limiting greatly the scope of state responsibility.

[87] "For example, at page 39,, "a receiving State is not responsible, as such, for the acts of private individuals in seizing an embassy, but it will be responsible if it fails to take all necessary steps to protect the embassy from seizure, or to regain control over it."

[88] Timo Koivurova, 'Due Dilligence' in Max Planck Encyclopedia of Public International Law (2013) <https://www.arcticcentre.org/loader.aspx?id=78182718-d0c9-4833-97b3-b69299e2f127> accessed 2 November 2018.

[89] Messerschmidt (n 5).

[90] See M.B. Akehurst, 'International Liability for Injurious Consequences Arising out of Acts not Prohibited by International Law' (1985) 16 NYIL 3; A.E. Boyle, 'State Responsibility and International Liability for Injurious Consequences of Acts not Prohibited by International Law: A Necessary Distinction?' (1990) 39 International and Comparative Law Quarterly 1.

[91] Trail Smelter (*United States v Canada*), 3 RIAA 1905, 1924-33 (1938).

of Justice in the *Corfu Channel Case*[92] to its codification in the Draft Articles produced by the International Law Commission in 2001.[93]

Even though some commentators have argued that *Trail Smelter* arbitration advocated for a strict liability standard,[94] the ILC Draft Articles have laid down a due diligence obligation.[95] The Commentary articulates that a due diligence obligation requires reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures in a timely fashion to address them."[96]

The International Court of Justice has stated that due diligence is an obligation of conduct and not of result.[97] The due diligence standard should be evaluated on a two-pronged test - of knowledge and capacity.[98] The knowledge prong entails assessment of whether the state possessed the knowledge of a specific cyber-attack or whether it ought to have known about the operation given the means at its disposal ('Constructive Knowledge')[99]. The capacity prong entails that the state makes full use of its institutional, resource and territorial capacity to detect cyber threats and prosecute them, if need be. [100]

The due diligence principle has also been flagged off by Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Rule 7) which " requires a state to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of and produce serious adverse consequences for other states."[101] The commentary does not lay down any guidelines on the duty of host states to prevent potential attacks, the duties of states through which the attack is routed and how the 'constructive knowledge' test applies to cyber operations.[102] At the same time, the

---

[92] Corfu Channel (*United Kingdom v Albania*), 1949 ICJ 4, 22 (April 9).

[93] The Draft Articles are yet to be adopted by the General Assembly but are widely recognised as an authoritative codification of the customary international law on the subject.

[94] Trail Smelter (*United States v Canada*), 3 RIAA 1905, 1924-33 (1938).

[95] Commentary to Draft art 71.

[96] ibid.

[97] J.G. Lammers, *Pollution of International Watercourses: A Search for Substantive Rules and Principles* (Martinus Nijhoff Publishers, 1984) 524.

[98] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia & Montenegro) [2007] ICJ 2 (Feb. 26) [430].

[99] Kimberley N. Trapp, 'State Responsibility for International Terrorism: Problems and Prospects' (2011) 23(1) European Journal of International Law 67.

[100] ibid.

[101] Schmitt (n 81).

[102] (1) Clearly defined cyber security policy and/or legislation, (2) Use of government funds to create nodal agencies responsible for cybersecurity, (3) Continuous communication if any hazardous cyber activities are detected, (4) Response to any requests for evidence by international bodies.

Manual is clear that there is no duty to monitor cyber activities originating from their territory owing to surveillance concerns.[103]

It is clear that international law imposes an obligation of due diligence when there is actual or constructive knowledge and capacity to prevent transboundary harm. However, jurisprudence and scholarship on the practical ramifications came out before the proliferation of cyber-attacks and the unique challenges states face with regard to detecting and attributing cyber-attacks. Existing scholarship fails to apply doctrinal theory to cyberspace, which renders it difficult for host states and the rest of the international community to determine whether due diligence obligations in cyberspace are being fulfilled.[104] This in turn complicates the assessment of legal active countermeasures that can be undertaken by the private sector.

B. ACD under International Law

Do active cyber defence mechanisms qualify as legal counter-measures under international law?

The right to take counter-measures against internationally wrongful acts has been understood by experts as an essential feature of a decentralized global political set-up that lacked a global law enforcement authority.[105] It is key to note that counter-measures are only available against internationally wrongful acts committed by other states and not available against states that are liable for prevention of acts that are not internationally wrongful and merely caused significant transboundary harm.

The customary international law doctrine of counter-measures has been codified by the International Law Commission in Articles 49-54 of the Articles on State Responsibility.[106] Article 49 sets out three important conditions which restrain the use of counter-measures:

1. Counter-measures are only available in response to and attributable to a state.

---

[103] Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice'(2018) 112(4) American Journal of International Law 583.

[104] ibid.

[105] Oona Hathaway and Scott J. Shapiro, 'Outcasting: Enforcement in Domestic and International Law' (2011)121 Yale Law Journal 252, 300-320; Louis Henkin, *How Nations Behave: Law and Foreign Policy* (2nd edn, 1979) 24.

[106] Draft articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, arts 4-6, Vol II, *Yearbook of the International Law Commission*, 2001. <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>.

2. Their aim is a restoration of legality between the two states, rather than the imposition of punitive sanction. For that reason, they are usually temporary or provisional.

3. As far as possible, counter-measures chosen should be reversible. Paragraph 1 of Article 50 further states that countermeasures should not change, in any way:

    a. The obligation set out in Article 2(4) to refrain from the use of force;

    b. Obligations relating to the protection of fundamental human rights. They must also not violate peremptory norms of International Law known as jus cogens.

    c. Further, they must be proportionate to the injury suffered both in terms of the gravity and the rights infringed.

    d. The Commentary mentions that every countermeasure must have a clearly defined purpose that is designed to ensure that the wrongful act ceases and not extend to purposes of retribution.

Ideally, states are also expected to notify the state engaging in the wrongful act before taking counter-measures, although in urgent cases this may not be feasible.[107] In his articulation of the UK's position on the application of International Law in cyberspace, the UK Attorney-General has stated prior notification may not be a legal obligation in the case of cyber counter-measures due to the need for a rapid response in many cases and the sensitive nature of cyber capabilities involved.[108] The Attorney-General's argument may be valid if there are instances of repeated cyber-attacks being directed at one state from the territory of another. For example, a one-off notice[109] may be sufficient to justify future counter-measures in the case of China repeatedly transgressing its obligation to prevent transboundary

[107] However, the injured State may take "such urgent counter-measures as are necessary to preserve its rights" even before any notification of the intention to do so.

[108] Office of Attorney General, 'Cyber and International law in the 21st Century' (Government of UK, 23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed July 13, 2018 [hereinafter Wright speech].

[109] Press Release, U.S. Department of State, 'Statement on Google Operations in China' (U.S. Department of State, 12 January 2010) <http://www.state.gov/secretary/rm/2010/01/135105.html> ("We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. [Secretary of State Clinton] will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear."

harm from its territory against U.S. firms. The Tallinn Manual suggests that if notification of the intent to take a countermeasure would defeat the objective of taking the counter-measure, then notice need not be provided.[110] The majority of experts who drafted the Manual claimed that prior negotiations with the erring state was not a requirement before taking countermeasures.[111] The Tallinn Manual thus fails to provide any guidance on the parameters that states might use to decide whether to provide notice or engage in negotiations.[112]

This position may not be tenable as it vitiates the purpose of counter-measures, which is to bring about a cessation of the wrongful act and restore status quo. *Without notification to, and communication with, the host state, one-off counter-measures might result in continued escalation, particularly when private sector actors are involved*. Apart from the Tallinn Manual, no document has clearly resolved this tension. While it is true that prior notification might jeopardize the success of certain active cyber defence measures, at the bare minimum states need to develop confidence building mechanisms and other frameworks of co-operation that prevent the escalation that the Articles on State Responsibility were designed to protect against.

C. Private sector and ACD

Can the private sector engage in countermeasures?

The Articles on State Responsibility (‘**ASR**’) clearly articulates that only states can engage in legal countermeasures. Messerschmidt attempts to get around this legal hurdle by invoking reciprocity.[113] His claim rests on the premise that the internationally wrongful act is the breach of an obligation to prevent transboundary harm by a private actor. Therefore, it is justified for the victim state to enable the private sector to engage in counter-measures.

This argument is unfeasible. Neither the ASR nor other principles of customary law of international responsibility recognize that reciprocity is an exception to the rule that only states can engage in counter-measures. The right vests solely with states because they are better equipped than non-state actors to detect an internationally wrongful act, attribute it to a state and determine the responses that would be most appropriate for bringing about a cessation of the act.

---

[110] Schmitt (n 80), 120.
[111] ibid.
[112] Efrony & Shany (n 103).
[113] Messerschmid (n 5), 279.

Private actors can take legal counter-measures only if its relationship with the state is such that it is acting on behalf of the state. Drawing from the categorisation in the Articles on State Responsibility, Maurer lays down a workable typology of proxy-state relationships in conjunction with the international law perimeters laid down in the Law on State Responsibility.[114] Within this framework, three kinds of relationships between the state and non-state groups demarcated in the Articles on State Responsibility can come within the ambit of delegation or active-state sponsorship, which would entail that the state is held responsible for the commission of any wrongful act. This includes:

1. Non-state actor exercising **governmental authority** (**Arts 4-6**),
2. Non-state actor acting under the **direction or control of a state** satisfying the **'effective control' criteria** (**Art. 8**) which means that the state is in control of the specific operation through planning, direction and support. As per the ICJ, the satisfaction of the effective control requires the state to "exercise such a degree of control in all fields, as to justify the non-state actors on its behalf"[115] and direct every act undertaken by the private actor.
3. **Overall control**, which means that the state exerts general control and influence in terms of planning and supervising of the group in general but not in the execution or direction of the specific operation.[116]

The Articles on State Responsibility attribute the acts of non-state actors to the state in the first two models i.e. when they are effectively acting on behalf of the state and taking direct instructions for each act. Therefore, providing individual companies the discretion to engage in counter-measures without direct state authorisation, supervision, and accountability would not be in compliance with International Law.

D. Analysis vis-à-vis APCD configurations

The present international legal framework clearly renders configurations of sanctioning and orchestration illegal simply because private actors are the key decision-makers in those configurations. In the case of orchestration,

---

[114] Maurer (n 20), 126.

[115] Nicaragua v. United States of America, 1986 I.C.J 14 at 62-64, 65..

[116] *Prosecutor v Tadić*, Case No. IT-94-1-T, Appeal Judgment, ¶ 120 (July 15, 1999) (As per existing international law, proving that a state has overall control over is not sufficient to hold the state responsible for an internationally wrongful act. The overall control test was evolved in a different legal context by the International Criminal Tribunal for Yugoslavia for the purpose of determining whether an international armed conflict existed and is yet to be accepted by any tribunal for the purposes of invoking state responsibility).

loosely worded policies like the Indian Cyber Security Strategy prevent the state from exercising effective control over each cyber operation.[117] When turning a blind eye, the state effectively gives a free reign to private actors, thereby violating their due diligence obligations to prevent cyber harm.

A strictly defined model of delegation may be legal if the following criteria are met. First, the state retains 'effective control' over the private actor such that its actions are attributable to the state. Second, there must be a framework for communication and confidence-building in lieu of notification as per the Articles on State Responsibility. The Singapore Cyber Security Act is an example of a well-drafted law that enables the government to retain effective control over the private actor. As per the Bill, the Minister needs to satisfy himself of the need for engaging a private actor to use ACD and also issue a certificate that specifies the measures that the actor can take. [118]

While the doctrinal analysis of international law is important, we are still left with important and unresolved questions-not least because international law is unclear and ill-equipped in its present form to deal with the frequency, pace and stealth of cyber conflict. We therefore must consider the geo-political and practical ramifications that might help fill some of the grey zones in international legal theory and help identify parameters that can make this theory relevant in the present factual scenario.

IV. Projecting Consequences

The developments and legal hurdles mapped out in the preceding sections present a key set of benefits and risks before policy-makers. In this section, we put forward a set of potential consequences of developing APCD globally and the regulatory challenges involved. First, we map out the benefits and risks at a high-level before evaluating how they apply at the level of each configuration.

High-level challenges

The first set of challenges arises from the political dynamics of governing a phenomenon as unique as cyberspace.[119] First, the dynamic and possibly

[117] While this strategy is likely to be updated in 2020, as of now there is no clarity on offensive cyber operations and India's cyber doctrine, including in relation to active cyber defence

[118] Parliament of Singapore, 'Cybersecurity Bill' <https://www.parliament.gov.sg/docs/default-source/default-document-library/cybersecurity-bill-2-2018.pdf> accessed 2 November 2018.

[119] Lucas Kello, *The Virtual Weapon and International Order*, (Yale University Press 2017) 82. He identifies three orders of cyber-revolution. Third-order revolution or systemic

quasi-anarchic nature of cyberspace and the diffusion of power to individual actors means that regulation and attribution capabilities driven by the government will always be playing catch-up with technological advancements spearheaded by the private sector. As the private sector is driving technological innovation, the state-centric model of security is under threat. Second, the incentive structure and strategic intent of various states behind launching operations in cyberspace differs, based on their current geopolitical ambitions. This has an impact on the relationship each state wishes to forge with private actors operating in cyberspace. The United States and China, for example, choose to hold their cyber proxies 'on a tight leash'[120], whereas Iran - reminiscent of the tactics used during and since the Iranian revolution[121]- grants them far more autonomy in their actions.[122] The democratic nature of the state enabling APCD also raises questions about the legitimacy of these measures in the eyes of the international community. Third, there is still no consensus among states on how the standards of international law apply to operations in cyberspace, which makes evolving a universally accepted set of standards difficult to gauge. While it is true that certain acts might be legal at a national level but still have negative geo-political consequences, a determination of legality lends a level of universal certainty to global policy and serves as the edifice for the demarcation of norms of responsible behaviour. Fourth, if the state enables the private sector to engage in increasingly aggressive action in cyberspace, a key challenge is ensuring that they remain accountable to the government and the government is able to enforce punishment for any collateral damage.

Proponents of APCD see the evolution of this practice as a necessity. The greater digitisation of key infrastructure means an increase in vulnerabilities that can be exploited by attackers, which has caused security experts to recognise a diminishing value to ramping up cyber defence mechanisms.[123] A hacker will be able to exploit a zero-day vulnerability at some point,

---

disruption results in drastic changes within the confines of the existing state structure. The drastic changes happen in both the material ingredients of power which are, in this case, defined by (1) A change in the physical architecture that defines power at the international level and (2) A change in the norms and rules which govern interactions between states. He then identifies second-order cyber revolution, which is brought about when a state or a group of states reject the shared purpose of the existing units, (systems revision) which may be exemplified by North Korea's weaponization of cyberspace.

120 Maurer (n 20), 71–80.

121 Daniel L. Byman, 'Proxy Power: Understanding Iran's Use of Terrorism' (*Brookings*, 26 July 2006) <https://www.brookings.edu/opinions/proxy-power-understanding-irans-use-of-terrorism/>.

122 Maurer (n 20), 81-93.

123 Michael V. Hayden, 'The Future of Things "Cyber" (2011) 5(1) Strategic Studies Quarterly 3, 5.

regardless of how robust the defence mechanisms are.[124] Proponents from the private sector argue that traditional remedies involve lengthy prosecution times and jurisdictional challenges, that are ineffective in responding to and deterring viruses and worms that move at extraordinary speed.[125] Further, law-enforcement authorities arguably lack adequate capacity to comprehend and respond to attacks infiltrating national information infrastructure or that of private actors. By responding aggressively to attackers, APCD has the potential to deter future attacks by increasing the cost to attackers in mounting a cyber-attack.

The detractors argue that it is unlikely that APCD will enable the swift recovery of data or prevent its further dissemination. First, it is estimated that the time lag between the occurrence of a breach and its detection is roughly 100 days.[126] Second, attribution is difficult for most private sector entities who lack the data, intelligence and knowledge of the adversary, which could result in them taking action on the wrong machines or attackers.[127] While this is also possible in the case of government action, historically the government has had diplomatic, intelligence and confidence building tools at its disposal-something that international relations scholars have found lacking with private actors.[128]This could lead to escalation, both in terms of continued offensive cyber operations by the attacker and counter-measures taken by victims, with the potential of bringing more actors into the equation when incorrect machines or actors are targeted through APCD measures.

Challenges within each configuration

These escalatory outcomes are far more likely in sanctioning or orchestration models where private actors act alone or with parts of the government machinery without co-ordination either between themselves or with various units of the government. Hence, geopolitical realities affirm the doctrinal logic behind banning these configurations-something that was discussed in the previous section.

---

[124] ibid 7.

[125] Messerschmidt (n 5). For example, the devastating Sapphire/Slammer worm doubled in size every eight and a half seconds.

[126] Roi Perez, 'FireEye Says Criminals Now as Sophisticated as Nation States' *Cybersecurity News, Reviews and Opinion* (16 March 2017) <https://www.scmagazineuk.com/fireeye-says-criminals-sophisticated-nation-states/article/1475041> accessed November 2, 2018.

[127] Andrea Limbagao, 'The 'Hacking Back' Bill Isn't the Answer to Cyberattacks' (*War on the Rocks*, 31 October 2017) <https://warontherocks.com/2017/10/the-hacking-back-bill-isnt-the-solution-to-cyberattacks/> Accessed November 2, 2018.

[128] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press 2015).

The advantages of co-option which lie in pooling resources at various levels of government-including the military, the Computer Emergency Response Team (CERT) teams, law enforcement and intelligence agencies are absent in a model that relies on the government failing to clearly lay the boundaries of private action. Further, there is a need for a clearly defined national policy framework that restricts APCD coupled with implementation of the policy such that an illegal underground market does not get sanctioned and legitimized. Lacunae in these two core requirements could further geo-political instability as other states and private actors would be unsure of the range of responses they can expect in the form of offensive cyber action. As was seen with the uncertainty that prevailed during the arms race during the Cold War between USA and USSR[129], uncertainty in the cyber context might cause all parties to ramp up both their offensive and defensive capabilities.

TABLE 3: BENEFITS AND RISKS OF APCD

	Benefits	**Risks**
Accuracy and expediency	Avoids legal fetters such as jurisdictional issues, lengthy prosecutions and lack of capacity	Time and accuracy constraints in attribution of the cyber-attack coupled with lack of intelligence
Impact	Swift response to attack vectors, thereby mitigating impact and increased chances of recovery of data	Collateral damage if the response penetrates third-party networks
Geo-political consequences	Deterring future attacks by raising the immediate cost to the attacker	Potential for escalation of conflict due to continued retaliation by private actors

(Source: Adapted from Hoffman and Levite)

A clearly established framework of delegation, on the other hand, ensures that governments play a key role in demarcating the limits of private action and holding companies to account for the same, while also utilising the private sector to craft a credible perception of national cyber resilience. This could enable the private sector to play a defined and understood role in the protection of information infrastructure from both existing and future

[129] Thomas C. Schelling, *The Strategy of Conflict* (Whitefish, MT: Literary Licensing 2011).

threats at an organizational, sectoral, and national level. Though a delegation framework can easily be applied at a national level, the complicated nature of the private sector and private sector security market raises geopolitical and jurisdictional concerns that national frameworks are not necessarily equipped to resolve.

However, delegation may not rectify all deficiencies that arise when a core governmental function is delegated to a private actor. One major challenge is holding the private actor accountable. The accountability problem is explained by the problem of divergent interests, that Singer has explained in the context of Private Military Security Companies ('PMSCs'). The state might have an interest in stability due to fear of retaliation and responsibility in International Law.[130] However, the non-state actor carrying out the operation will not bear the brunt of retaliatory responses or be held responsible or liable under international law. They would solely be driven by the mandate issued by the government (and the profits resulting from it), which is to carry out the measure successfully unless the government imposes accountability obligations on the private actor. To do so however would require the government to monitor the actions of the private actor, which would require further deployment of private resources. One potential way of doing this efficiently would be combining delegation with co-optation, where the private actor does not act alone but in cohesion with an ecosystem of both state and non-state actors working on cyber-security.

Further, the adoption of APCD measures need to be considered in terms of geopolitical realities also. First, cyberspace is intricately interconnected and crosses jurisdictional boundaries. Therefore, a situation where different countries adopt different models of APCD could result in continued cyber-attacks against countries that restrict the autonomy given to private sector actors. This is the scenario in status quo. Second, cyber security companies might work for multiple governments, which would lead to a conflict of interest. Further, the legal and policy implications of a company headquartered in one country using APCD in another country after being authorized by the second government are unclear. Third, delegation and co-opting can be accomplished effectively only if the government of a country is sufficiently more powerful than the private sector operating in that country. This is not necessarily the case in many countries in the developing world. We are also seeing this trend in relation to large tech-corporations in the developing world- where there is a high level of dependency on technology

[130] P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (updated ed., Ithaca: Cornell University Press 2008) 151–152.

companies from the US or China. Even in states that are able to exercise regulatory authority more effectively, technology companies can influence a number of decisions through excessive lobbying. Finally, the cyber security market is skewed in favour of countries in the developing world as they have a larger talent pool and financial resources. This could lead to a scenario where APCD mechanisms is being deployed more frequently by the developed world, even though the developing world has the same legal and policy enablers-thereby putting the Global South at a disadvantage.

Cyber defence analysts have often pointed out the perils of being complacent regarding the potential of regulating cyberspace solely through international law or norms. The geo-political risks, as documented above, remain prevalent and need to be grappled with and complacency in silver bullet solutions are undoubtedly misguided-particularly given that there is no certainty in the rules of international law that shape this space. However, the well-established tenets of international law offer a starting point to identify behaviour that could receive international sanction and facilitate continuous discourse and engagement between both states and non-state actors over a period of time.[131]

V. Looking Ahead

TOWARDS A CYBER STABILITY NORM HARNESSING ACTIVE PRIVATE CYBER DEFENCE AND AREAS FOR FURTHER RESEARCH.

Norm evolution can happen through three potential vectors. Existing research has shown that the development of standards by global bodies such as the International Standards Organization, spurred on through commercially driven norm-entrepreneurship by insurance companies led to the proliferation of universal standards[132] for the regulation of conduct by maritime security companies.[133] Standards enable the harmonised transmission of information across different contexts and help determine the roles of various actors. Applying this to private sector entities working on private defence allows for greater stability and predictability. The second vector is

[131] Monica Hakimi, 'The Work of International Law' (2017) 58(1) Harvard International Law Journal 1.

[132] Wyatt Hoffman & Ariel E. Levite, 'Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?', <https://carnegieendowment.org/files/Cyber_Defence_INT_final_full.pdf 4>.

[133] Marc-Antoine & Carreira Da Cruz, 'Regulating Private Maritime Security Companies by Standards: Causes and Legal Consequences' (2017) 3 Maritime Safety and Security Law Journal <http://www.marsafelawjournal.org/wp-content/uploads/2017/12/MarSafeLaw_Carreira-Da-Cruz_Issue-3.pdf>.

increasingly empowered private sector organisations themselves engaging in norm entrepreneurship. Microsoft's Digital Geneva Convention, Siemen's Charter of Trust and the recently published tech accords are cases in point.[134] Realising the entanglement of economic dimension of cyberspace which relies on consumer trust to thrive, private actors have sought to develop norms that would ferment clearer standards of cyber security. While they seek to engage in active defence mechanisms, they should keep in mind the benefits of having predictability and certainty in the international normative framework driven by deference to structures of International Law.

We made a number of unique contributions to existing scholarship. The first section of this paper mapped the existing scenarios and put forward five configurations that illustrated the relationship between the government and the private sector. The first two-banning and co-optation do not envisage autonomy given to the private sector actor and therefore cannot be classified as APCD. The remaining three envisage varying degrees of autonomy. We observed that law and policy across nations conformed to a model that compelled restraint, such as banning but was disconnected from reality. The second section examined the enabling provisions of international law and highlighted the gaps in this field, particularly in terms of applying settled debates in traditional international law to the cyber domain. Multilateral efforts at the United Nations and across jurisdictions need to identify and plug this gap The final section looked at the five models from the perspective of geo-political risk and concluded that having a strong government through delegation or co-optation was less likely to result in escalation than mechanisms that delegated more decision-making power to the private sector.

This predictability will have an overall positive effect on the global cyber ecosystem. Deterrence is furthered on the basis of 3Cs - capability, credibility and communication.[135] Roping in private sector capabilities by optimizing the use of APCD and communicating this both through international channels but also through robust municipal legislation may work to further each of the 3Cs. The international legal standards outlined in Part III are not obsolete but need to be made relevant by ensuring that legislation implementing these standards are workable for today's pragmatic challenges. Further

---

[134] Chris Bing, 'Hoping to Fill a Global Void, Private Companies Push for 'Cyber Norms' (*Cyberscoop*, 22 February 2018) <https://www.cyberscoop.com/siemens-cybersecurity-charter-of-trust-airbus-dxp-cyber-norms/>. Jessica Woodall, *Cyber Norms and the Australian Private Sector* (*International Cyber Policy Centre*) <https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ICPC-Private-sector-cyber-norms.pdf?EDM_hjeuRpko0j54MPGHjm234TPXAio1>.

[135] Jesse C. Johnson, Brett Ashley Leeds & Ahra Wu, 'Capability, Credibility, and Extended General Deterrence' (2015) 41(2) International Interactions 309.

research on possible regulatory models, insurance schemes and particularly, how the developing world fits into this scheme are important for determining its future.

However, for now, 'reining in' through clearly enforced delegation and co-optation, rather than banishing or letting loose these private sector companies has the potential to improve cyber security standards across the globe. The state must still retain its position as the final arbiter and guarantor of peace and security, while recognizing that the advances of modern society dictate that it cannot walk this path alone.