ADDRESSING CYBER VULNERABILITIES THROUGH DETERRENCE

Nida Shahid* **& Ahmad Khan****

Abstract

The study analyses the possible responses to cyber-attacks through cyberspace deterrence. The inundated cyber-attacks have prompted major powers to establish cyber deterrence. However, in the absence of a model of punishment, as it is empirically found in the nuclear domain, the efficacy of cyber deterrence is limited. The model of punishment against cyber-attacks is based on the traditional nuclear deterrence model, which is either deterrence by denial or deterrence by punishment. Cyber deterrence may not be a replica of traditional deterrence and give similar response measures in a cyber-attack. The assured retaliation in cyber requires an explanation of response measures that do not cause collateral damage. The paper concludes that cyber aggressors escaped retaliation due to the lack of attribution and not being punished due to limited retaliatory measures.

Keywords*: Cyberspace, Deterrence, Networks, Doctrine, Communication, Credibility*

Introduction

The cyber domain has gained importance since the advent of computerized networks as the foundation for military and economic power.[1] As States' reliance on digital platforms increases, their

* Senior Research Fellow at Center International Strategic Studies, Islamabad. Email: nidaashahid3@gmail.com

** PhD in Strategic Studies, and spécialises in cyber security, space and nuclear technology. Email: ahmadsvi@gmail.com

1 There is voluminous literature on the importance of cyber domain in military and economic power of the state. e.g., John Naughton, "The Evolution of the Internet: from Military Experiment to General Purpose Technology," *Journal of Cyber Policy* 1, no.1 (2016): 5-28; Joseph Bussing, "The Degrees of Force Exercised in the Cyber Battle Space," *Connections* 12, no. 4 (2013): 1–14; Jeffrey L. Caton, "The Army Role In Achieving Deterrence In Cyberspace," *Strategic Studies Institute*, US Army War College, 2019, http://www.jstor.org/stable/resrep20084; also see Beth E. Lachman, et al,

national, military and economic securities remain at risk from cyber threats.[2] The States' and peoples' reliance on computer networks has grown more since the Covid-19 outbreak because of the worldwide lockdown.[3] The advent of the digital domain, the need and means to protect assets in the cyber world has gained traction.

One of the major issues within the cyber space is the lack of physical boundaries.[4] Clear physical and geographic boundaries, which demarcate the extent of land, sea and air domains, do not exist in cyberspace. Thus, the scope of securing the cyber space becomes a more daunting task.[5] In cyberspace, it is not enough to merely secure the computer networks. No matter how holistic, security is, it can be breached by a single well-planned cyber-attack exploiting an overlooked area.[6] There have been many examples in the past of such incidents where nefarious actors have successfully circumvented a state's cyber security to launch a successful attack. One such attack that targeted American intelligence agencies was the SolarWinds cyber-attack in December 2020.[7] With technological breakthroughs in cyberspace weaponry happening at lightning speed, states have started engaging in warfare by cyber means.[8]

"Information Technology Trends," In *Key Trends That Will Shape Army Installations of Tomorrow* (Santa Monica, CA: RAND Corporation, 2013), 171–206.

2 Julian Jang-Jaccard and Surya Nepal, "A Survey of Emerging Threats in Cyber Security," *Journal of Computer and System Sciences* 80, no. 5 (August 2014): 973-993.

3 Rahul De', Neena Pandey and Abhipsa Pal, "Impact of Digital Surge during Covid-19 Pandemic: A Viewpoint on Research and Practice," *International Journal of Information Management* 55, no.1 (December 2020), and also see Pew Research Centre's quantitative assessment of digital reliance during the pandemic, Colleen Mcclain, "The Internet and the Pandemic," *Pew Research Center,* September 1, 2021, https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/.

4 Kenneth J. Miller, "Understanding the Unique Challenges of the Cyber Domain," (Dissertation. Air University, Maxwell Air Force Base, Alabama, March 2010).

5 There is general understanding that cyberspace is created by man whereas land, sea and air are by nature. This concludes that cyberspace is easier to change and border less. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 77, no. 2 (2015): 8-15.

6 Dan Lohrmann, "Planning for a Nation-State Cyber Attack — Are You Ready?" *Government Technology* (blog), February 13, 2022, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/planning-for-a-nation-state-cyber-attack-are-you-ready.

7 Marcus Willett, "Lessons of the Solar Winds Hack," *Survival* 63, no. 2 (2021): 7-26.

8 Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-

Stuxnet and the Russian-Georgian cyber conflict and tactical cyber operations by the US against Islamic State (IS) in Afghanistan are examples of such cyber operations.[9] Thus, cyber warfare is being employed for desired effects at the strategic and tactical levels.[10]

Thus, states consider responses through deterrence strategy to protect the cyber space, which may deter nefarious actors from instigating such attacks.[11] The question, however, remains whether cyber deterrence is even possible.[12] As is the case in traditional deterrence models, the threat of punishment must be evident and credible so that there is no ambiguity regarding retaliation.[13] It must be etched in words as well as

---

Attacks And Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7, no.1 (November 2021): 8176-8186; and also RA Atrews, "Cyberwarfare: Threats, Security, Attacks, and Impact," *Journal of Information Warfare* 19, no. 4 (2020): 17–28.

9 For details on reported cyber incidents (2006-March 2021), "Significant Cyber Incidents Since 2006," *Center for Strategic and International Studies*, accessed May 15, 2022, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; and also Sico van der Meer, "State-level Responses to Massive Cyber-Attacks: a Policy Toolbox," *Clingendael Institute*, December 2018.

10 Answers to some key questions like the utility of military cyber capabilities in conflict situation are explored by Matthias Schulze, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations," in *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020*, G. Visky et al (eds.) (Tallinn 10132, Estonia: The NATO Cooperative Cyber Defence Centre of Excellence, 2020), 183-197.

11 For U.S cyber deterrence, *Cybersecurity: Deterrence Policy* (Washington DC: Congressional Research Service, January 18, 2022). Russian cyber deterrence is analysed by Erica Lonergan and Keren Yarhi-Milo, "Cyber Signaling And Nuclear Deterrence: Implications For The Ukraine Crisis," *War on the Rocks (blog),* April 21, 2022, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/; and Chinese cyber deterrence policy is explained by Ariel E. Levite et al., *China-U.S. Cyber-Nuclear C3 Stability* (Washington DC: CEIP, April 2021).

12 American understanding is that a limited US cyber deterrence strategy is possible with limited success with the help of effective cooperation with partner states. See Timothy M. McKenzie, *Is Cyber Deterrence Possible?* (Maxwell, AL: Air Force Research Institute, 2017). As far as SolarWinds attack is concerned, the U.S. did not retaliate despite knowing the origin of the attack. This reflects that deterrence in cyber space is limited to an extent that its communication part exists but employment or punishment is completely missing.

13 Robert Jervis, "Review of Deterrence Theory Revisited," by Alexander George and Richard Smoke, *World Politics* 31, no. 2 (1979): 289–324; Glenn H. Snyder, "Deterrence and Power," *The Journal of Conflict Resolution* 4, no. 2 (1960): 163–78; and also Todor Tagarev, "Theory and Current Practice of

actions. Any possible deterrence theory for cyberspace will constitute the same critical facets as the theories which came in the past.[14] The study aims to understand present theories and concepts related to deterrence strategies and subsequent actions in cyberspace. Conceptualizing and preparing actions and subsequent responses to a cyberattack are daunting since the basic foundations of cyber deterrence are unclear despite a dearth of traditional and nuclear deterrence theories. Finding a mix of passive and active deterrent actions is the key to building a retaliatory cyberspace strategy.

Finding an answer to the question of how cyber deterrence works is the study's primary objective. It focuses on the nature of cyber warfare and security, the emerging cyber threats, impacts of cyber-attacks as well as the challenges in cyberspace. Keeping these attributes in mind as well as looking at empirical evidence from recent cyber-attacks, the study attempts to ascertain the possibility and means of understanding cyber deterrence theory. The paper is divided into four sections: In the beginning, most recent cyber-attacks are exemplified to understand, how modernized cyber warfare is and what are its impacts? The second section explains cyber-space vulnerabilities and challenges. The third section addresses these vulnerabilities through cyber deterrence concerning the effectiveness of the model of punishment. The last section focuses on the ingredients required to establish cyber deterrence.

Understanding Cyber Attacks

The world has witnessed more cyber-attacks since the twenty-first century. As the states' and individual reliance and access to network systems increases, so does their ability as well as vulnerability in cyberspace. At least three international skirmishes have escalated to conflict levels initiated by cyber-attacks. These include the Israeli-Palestinian conflict of 2000,[15] the Russo-Estonian conflict of 2007,[16] and

---

Deterrence in International Security," *Connections* 18, no. 1/2 (2019): 5–10.

14 Cyber deterrence is different from nuclear deterrence however the punishment model may resemble the nuclear deterrence model. States' digital reliance and economic activities are dependent on the cyber domain therefore their survival may be ensured through establishing deterrence strategies in the cyber domain while having a punishment model to persuade the enemy not to commit any future course of aggression. Christopher Haley, "A Theory of Cyber Deterrence," *Georgetown Journal of International Affairs*, (February 06, 2013).

15 Patrick Allen and Chris Demchak, "The Palestinian-Israeli Cyberwar," *Military Review*, (March–April 2003).

16 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

the Russo-Georgian conflict of 2008.[17] The Ukraine war is also witnessing cyber-attacks by Russia and the US intelligence agencies have warned that Russia may launch cyber-attacks on the US and its western allies due to severing of diplomatic relations over the war.[18] The abovementioned incidents are not isolated events since cyber-attacks for political purposes, with or without governmental support, are becoming frequent.[19]

Not all cyber operations with malicious intent can be grouped as cyber-attack.[20] Merriam-Webster dictionary defines an attack as a violent act against something or someone. Translating that to the cyber space means that the state infrastructure, such as economic or military, is 'something' against which a cyber-act of violence has occurred. The Tallinn Manual on the International Law Applicable to Cyber Warfare describes a cyber operation, "whether offensive or defensive, as one which is expected to cause injury or death to persons or damage or destruction to objects."[21] Traditionally, experts have categorized a cyber-attack as (permanent) one which causes physical damage to property or injury to persons.[22] However, cyber operations categorized as disruptive, aggressive or causing temporary damage could also potentially rise to the level of a cyber-attack depending on their impact on intangible state infrastructures such as the economy.[23] The US SolarWinds attack of December 2020 is one of the most recent examples of a systemic cyberattack that exploited vulnerabilities in the network system of U.S' national agencies.[24]

---

17 Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 3–24.

18 David E. Sanger, "Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds," *The New York Times,* May 10, 2022, https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html

19 Ashley Lukehart, "2022 Cyber Attack Statistics, Data, and Trends," *Parachute*, January 4, 2022, https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/.

20 There is no single definition of cyber-attack. For that purpose see definitions prepared by IBM, Kaspersky, CISCO, and Microsoft etc.

21 "It identifies international law principles applicable to cyber warfare and enumerates ninety-five black-letter rules governing such conflicts. Topics addressed include sovereignty, state responsibility, the *jus ad bellum*, international humanitarian law, and the law of neutrality," Michael N Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn 10132, Estonia: The NATO Cooperative Cyber Defence Centre of Excellence, 2013).

22 Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7, no. (2021): 8176-8186.

23 McKenzie, "Is Cyber Deterrence Possible?" 4.

24 On SolarWinds finds President and Vice Chair of the Microsoft blog, Brad

US Solar Winds Attack

Solar Winds cyber hacking attack is one of the biggest cyber attacks that targeted US government agencies, including intelligence and nuclear administration agencies, labs and private companies.[25] The attack targeted ten major US agencies, including the National Nuclear Security Administration (NNSA), US Treasury, the Department of Homeland Security, the Department of Commerce and parts of the Pentagon.[26] The exact scale of the attack still remains unknown; however, more than eighteen thousand computers attached with over two hundred and forty networks being run by SolarWinds were attacked.[27] The SolarWinds breach highlights US cyber security vulnerabilities. The attack was carried out using "Trojanized" updates to SolarWinds' Orion IT monitoring and management software posted on the company's website. The Trojanized update run code created three backdoors (Sunburst, Sunspot and Teardrop) into the compromised networks that hackers exploited for credential theft. Cyber security companies, including Fire Eye, Microsoft and Crowd Strike, carried out an assessment of the Trojanized code and identified three different strains. [28]

Smith, " A Moment of Reckoning: the Need for a Strong and Global Cyber Security Response," *Microsoft* (blog), December 17, 2020; Microsoft identifies vulnerabilities in the networks in US intelligence agencies setup that led to the Solar Winds attack, "A Deep-Dive into the Solar Winds Serv-U SSH Vulnerability," *Microsoft,* September 2, 2021, https://www.microsoft.com/security/blog/2021/09/02/a-deep-dive-into-the-SolarWinds-serv-u-ssh-vulnerability/

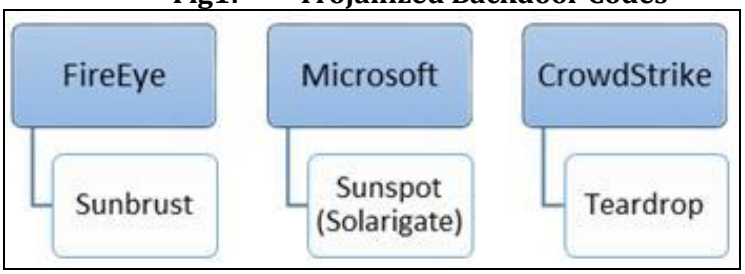
25 David E. Sanger, Nicole Perlroth and Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies were Hit," *New York Times*, September 9, 2021, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

26 "Explained: A Massive Cyberattack in the US, using a Novel Set of Tools," *Indian Express*, December 29, 2020, https://indianexpress.com/article/explained/us-solarwinds-hack-cybersecurity-fireeye-russia-7110550/

27 Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of The Solar Winds Hack," *NPR*, April 16, 2021.

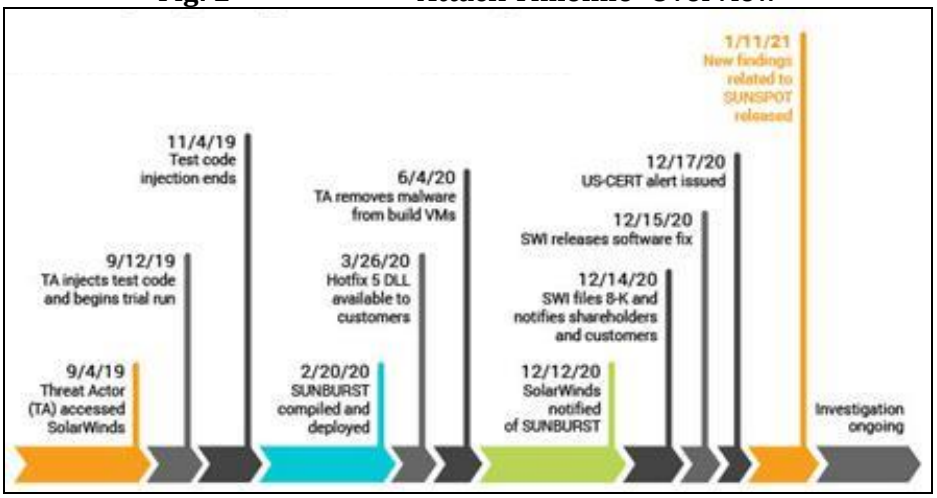
28 Highly Evasive Attacker Leverages Solar Winds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, *Fire Eye*, December 13,2020, https://www.fireeye.com/blog/threat-research/2020/12/

Fig1: Trojanized Backdoor Codes



It was assessed that the cyber-attack remained dormant for weeks before being detected. A timeline of events mapped by SolarWinds shows that the attack began in September 2019.

Fig: 2 Attack Timeline- Overview



All Events, Dates and Times Approx. and Subject to Change, Pending Completed Investigation.

The Solar Winds attack highlighted the US cyber-security vulnerabilities as well as problems associated with attribution in the cyber space. If a developed country like the US remains vulnerable to such cyber-attacks despite its advanced Cyber Security Directive, there is reason to assume that countries with nascent cyber-security programs remain even more vulnerable. The Trump administration blamed Russian involvement in the attack.[29] American officials have blamed the Russian military hacking group "Cozy Bear" for the breach. FireEye, Microsoft and Crowd-Strike have assessed that Sunburst and Sunspot source codes resemble Kazuar. It is a malware strain linked to the Turla group, which is alleged to

[29] US Secretary of State Mike Pompeo has blamed Russia for what is being described as the worst-ever cyber espionage attack on the US government. See, "US Cyber-Attack: Russia 'Clearly' behind Solar Winds Operation, says Pompeo," *BBC News*, December 19, 2020.

be Russia's most sophisticated State-sponsored cyber espionage outfit. Researchers at Kaspersky and Symantec have identified similarities between Sunburst and Kazuar source codes. However, Russian intelligence agencies denied the involvement.[30] The attack left more diplomatic bitterness in US-Russia relations.

The Solar Winds cyber-attack suggests limited US cyber deterrence responses. The US was preparing to retaliate against Russia. However, no specific details were shared. The White House press secretary Jen Psaki stated that the government will carry out "a mix of actions seen and unseen."[31] President Biden announced more sanctions on Russia after the Solar-Winds attack. However, it is debatable whether economic sanctions would establish cyber deterrence's effectiveness.

Iran Nuclear Facility Attack

In April 2021, while the world powers and Iran were attempting to re-negotiate the Joint Comprehensive Plan of Action (JCPOA), the Natanz nuclear facility in Iran suffered an electrical blackout resulting in damage from the centrifuges housed at that facility.[32] The blackout came a day after Iran disclosed that new advanced centrifuges had been set up at the facility.[33] The Iranian leadership termed the attack at Natanz as an act of nuclear terrorism through the cyber space.[34] It is argued that an explosive device was planted, likely by Israel, near a gas line. However, experts believed that a cyber-attack was used to trigger the incident.[35] Later, an unnamed Middle Eastern intelligence official revealed to the New York Times that Israel had caused the blast at Natanz. Previously, Israel's foreign minister Gabi Ashkenazi had responded obliquely when asked if Israel was behind the incident, saying, "It is better not to mention our actions in Iran."[36]

While most cyberattacks are not considered physical attacks [37]–as

---

30 Guy Faulconbridge, "Flattered Russian Spy Chief Denies Solarwinds Attack - BBC," *Reuters*, May 18, 2021.

31 K. Holt, "US Plans 'a Mix of Actions' against Russia over Solar Winds Cyberattack," *Engadget*, March 8, 2021.

32 Siobhán O'Grad, "What we Know about the Natanz Nuclear Site Attack," *The Washington Post*, April 14, 2021.

33 Ronen Bergman, Rick Gladstone and Farnaz Fassihi, "Blackout Hits Iran Nuclear Site in what Appears to be Israeli Sabotage," *New York Times,* April 13, 2021.

34 "The Usual Culprits," *Tehran Times*, April 21, 2021.

35 David E. Sanger, Eric Schmitt and Ronen Bergman, "Long-Planned and Bigger than Thought: Strike on Iran's Nuclear Program," *New York Times,* July 10, 2020.

36 Ibid.

37 Russell Buchan, "Cyber Attacks: Unlawful uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law* 17, no. 2 (2012): 211–27. He considers that as per Article 2(4) UN Carter if cyber- attacks cause physical

they mostly pertain to the theft of virtual information or sabotage of virtual infrastructure- the Iranian nuclear program has been repeatedly targeted with cyber- attack which caused physical damage. 'Stuxnet' attack at the same Natanz facility a decade earlier remains one of the first demonstrations of cyber-attacks with physical manifestations. Computer codes caused real-world physical damage by interfering with the centrifuges controllers, spinning them at breakneck speeds, resulting in slow-motion explosions, which were not detected until it was too late.[38] It is one of the most sophisticated and targeted operations jointly run by the US and Israel.[39] The Stuxnet attack provided a new understanding of cyber-attacks to the world that cyber-attacks could also cause physical damage.

Vulnerabilities and Challenges in the Cyber Space

Advancements in the cyber space have been occurring at lightning speed in recent years, with more actors realizing that the vulnerabilities inherent in the cyber space can be exploited. In order to develop deterrence against cyber-attacks, one must first understand the vulnerabilities and challenges inherent in the cyber space.[40] Some of the main challenges and vulnerabilities of the cyber space, which States would need to contend with while formulating any potential cyber deterrence policies are elaborated below.

Regulation and Attribution

One of the most significant challenges and vulnerabilities in the cyber space remains that of regulation and attribution.[41] Vulnerabilities

---

damage then it violate the said Article. However, many of the cyber-attacks do not cause physical damage, therefore are thus not captured by Article 2(4). However, it does not mean that cyber-attacks are lawful rather coercive and nevertheless violate the non-intervention principle.

38 To understand the physical damages caused by the Stuxnet, Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Security Studies 22, no.3 (2013): 365-404.

39 Gordon Corera, "Iran Nuclear Attack: Mystery Surrounds Nuclear Sabotage at Natanz," *BBC News,* April 12, 2021.

40 There is a dearth of literature of vulnerabilities and challenges to cyber security. Some of the research papers are analyzed for literature review. J Chen, "On Levels of Deterrence in the Cyber Domain," *Journal of Information Warfare* 17, no. 2 (2018): 32–41; Robert Ghanea-Hercock, "Why Cyber Security Is Hard," *Georgetown Journal of International Affairs*, (2012): 81–89; McKenzie, " Is Cyber Deterrence Possible?"; and also see Sitara Noor, "Cyber (In) Security: A Challenge to Reckon with," *Strategic Studies* 34, no. 2/3 (2014): 1–19.

41 Annegret Bendiek and Matthias Schulze, "Attribution: A Major Challenge for

associated with deterrence in the physical domain are amplified in the cyber space due to attribution difficulties. For States' cyber deterrence to be seen and presumed as credible and capable, they have to demonstrate their ability to not only pre-emptively detect the attack but also attribute it to the right actors. "Assumptions about identity, intent, nature or rationality of a typical cyber adversary can be called into question when forming the basis for retaliation."[42] Attribution is a time-consuming and expensive endeavour. It has been proved by the SolarWinds attack as well as solving the mystery of Iran's allegation of an Israel-led cyber-attack on Natanz.

For cross-border cyber-attack investigations, the jurisdictional limitations can further hinder the efforts to establish the attack's origin and the attacker.[43] Going through official lines of communication to request access to data and evidence is onerous and can hamper the investigation when the information needs to be collected as quickly as possible. One of the most pertinent examples, which signify the difficulties related to attribution, is that of the Mariposa botnet, which was involved in denial-of-service attacks and cyber-scamming.[44] The botnet consisted of thirteen million computers being used for malicious activities. Attribution for the botnet was a momentous exercise involving hundreds of human hours and research to track the source IP and the cyber actor.[45]

Emerging Technologies

Today's world is overrun by many emerging technologies, all of which have direct or indirect implications in the cyber space. Artificial Intelligence (AI), Machine Learning (ML), Blockchain Networks, Big Data, Internet of Things (IoT), mega constellations,[46] cloud and quantum

---

EU Cyber Sanctions," *German Institute for International and Security Affairs*, SWP Research Paper 11, December 2021; and also see Amanda G. Hill, *The Ultimate Challenge: Attribution for Cyber Operations* (Maxwell, Al: Air Command and Staff College, n.d).

42 Steve Winterfeld and Jason Andress, *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (. Waltham, MA: Syngress, 2012), 123.

43 Alexandra Perloff-Gilest, "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges," *The Yale Journal Of International Law* 43, no.1 (2018) 191-227.

44 Ali Zerdin, "Cyber Mastermind Arrested, Questioned in Slovenia," *The Washington Times*, July 28, 2010.

45 Steve Winterfeld and Jason Andress. *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Waltham, MA: Syngress, 2012), 123.

46 Russia disrupted Satcom services provided by a Viasat satellite. But SpaceX's broadband constellation Starlink provided internet services in Ukraine. This

computing are few of the many transformative technologies which will have a substantive impact on physical and cyber spaces. As likely as these emerging technologies are radically changing how humans work, communicate and even fight in the future, they are simultaneously capable of disrupting vital services and posing a massive threat to strategically vital networks.[47]

With the advent of 5G technology, the attack surfaces and the number of entry points for hackers increase drastically as more devices with minimal security features are connected to the same grids. Not only do these interconnected devices increase vulnerabilities in the cyber space, but their ability to communicate with each other also remains one of the weakest links in 5G security.[48] AI and ML are other facets of emerging technologies, which will have consequences for the cyber space. These technologies have become critical linchpins in information security as they exponentially increase the speed with which data is identified and analysed. Owing to their ease of use and increasing ease of access, cybercriminals can use AI technologies to go through defences while avoiding detection and subsequent attribution. Therein lies the 'AI/cybersecurity conundrum.'[49] While AI and ML can guard against cyber-attacks, sophisticated cyber criminals can also bypass the security algorithms through data manipulation using the same technologies. This manipulation can remain dormant and undetected until the right time, which will have integrated into the victim's cyberspace.[50]

Cloud Computing Risks

Cloud computing is the availability, on demand, of online servers

---

shows the power of mega constellations providing commercial satellite internet. Mega constellations of internet services are also considered as part of emerging technologies.

47 Robert A. Manning, "Emerging Technologies: New Challenges to Global Stability," *Atlantic Council*, issue brief, 2020, http://www.jstor.org/stable/resrep26000. He argues that Disruptive technologies, also known as emerging technologies pose new risks and challenges to strategic stability across increasingly contested global commons—air, sea, cyber, and space.

48 Fotios Kanellos, "Implications of 5G to Air Power – A Cybersecurity Perspective," in *Joint Air & Space Power Conference 2020 Read Ahead*, Bruce Hargrave (ed) (n.d), https://www.japcc.org/read-aheads/joint-air-space-power-conference-2020-read-ahead/.

49 "Using Artificial Intelligence in Cybersecurity," *Balbix,* accessed May 15, 2022, https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

50 Maria Bada and Jason R.C. Nurse, "Profiling the Cybercriminal: A Systematic Review of Research," (paper, 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021), 1-8.

for data storage without the physical and active involvement of the user. Cloud computing has revolutionized cyberspace, enabling users to keep large-scale data freeing up their servers at remote locations. It has accelerated the speed of work for businesses and organizations. Given its popularity, cloud computing is expected to reach 947.3 billion by 2026.[51] However, as with most beneficial technologies, there is also a downside – cloud vulnerabilities- in this case. Cloud data centers experience the same threats as traditional data centers. However, given the virtual nature, the vulnerabilities increase. Businesses are shifting their operations to the cloud, making cloud providers a profound target for hackers. In this connection, Distributed denial of service (DDoS) attacks are frequent. A business-oriented website in a DDoS attack remains at the attacker's mercy for days or even weeks, which may result in loss of revenue, brand authority and customer trust.

On the other hand, there is a greater possibility of adversaries gaining access to exploit vulnerabilities in cloud computing. One of the most common and exploitable vulnerabilities is account hijacking, where malicious actors can steal users' account credentials through phishing, key logging, buffer overflow attacks, XSS attacks and brute force attacks.[52] Likewise, cloud data breaches are increasing, especially since securing sensitive data is becoming daunting.

In cloud computing, Application Programming Interfaces (APIs) are convenient and efficient means of sharing information with two or more applications. However, insecure APIs can be another source of cloud vulnerabilities. API's greatest benefit is accessing data from any part of the world and from any device. Hackers are leaving no stone to unearth to gain access to vulnerabilities and exploit authentication via APIs provided ample time. Hackers can exploit insecure APIs to access data and launch potential DDoS attacks.[53] With more and more private and public sector organizations increasing their dependence on APIs, the data becomes more vulnerable.[54] Additionally, exploitation of cloud system vulnerabilities, deliberate or accidental, by potential malicious insiders, including current and former employees, contractors and partners, cannot be ruled out.[55]

---

51 "The Top 5 Cloud Vulnerabilities to Watch Out for in 2022," *Alert Logic Staff*, January 20, 2021, https://www.alertlogic.com/blog/top-cloud-vulnerabilities/

52 Ibid.

53 Danko Kovacic, "API Security: The Complete Guide," *Bright*, April 4, 2022, https://brightsec.com/blog/api-security/; and also see "What is a DDoS Attack?" *Cloudflare*, accessed May 15, 2022, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

54 Ibid.

55 Atulay Mahajan, Sangeeta Sharma, "The Malicious Insiders Threat in the Cloud," *International Journal of Engineering Research and General Science* 3,

Proportionality of Punishment

Warfare in the cyber space also raises unique complications about applying the International Humanitarian Law (IHL), especially regarding the use of force against civilians and proportionality of punishment.[56] Many experts believe that the Tallinn Manual only describes how the IHL might be applicable in the cyber space.[57] However, even under Tallinn Manual, the issues of distinction and proportionality for the protection of civilians are not addressed adequately. For example, the scope of what constitutes a civilian versus a military object remains unclear in the cyber space,[58] especially regarding data and functioning of cyber systems. Additionally, the definition of attack, as per IHL and Tallinn Manual, does not fully account for non-kinetic effects, which are likely to be greater in the cyber space.[59] Likewise, the assessment for damages as well as the calculation of damages remains vague in cyberspace. Encompassing all these factors is the lack of guidance for assessing the value of a cyber-attack for the response or punishment to be proportional.[60]

Addressing Vulnerabilities through Cyber Deterrence

Deterrence as a concept has developed and endured since the advent of the first weapons. It became a more concrete concept following the advent of the nuclear age when States developed nuclear weapons to deter the adversary from initiating aggressive action.[61] Whereas the deterrence theory has a historical lineage, dating back centuries, cyber deterrence is still in its nascent stages.[62] Most of the academic literature on

---

no. 2 (March-April 2015): 245-256.

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

57 Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution," *Minnesota Journal of International Law* 26, no. 2 (2017): 419-460.

58 Susan W. Brenner and Leo L. Clarke, "Civilians in Cyber Warfare: Conscripts," *Vanderbilt Journal of Transnational Law* 4, no. 4 (October 2010): 1011–1076.

59 Pascucci, "Distinction and Proportionality in Cyberwar."

60 McKenzie, *Is Cyber Deterrence Possible?*and also Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 817–85.

61 Ahmad Khan and Ali Ahsan, "Deterrence in Indo-Pak Context: A Critical Appraisal," *Policy Perspectives* 13, no. 1 (2016): 53–76.

62 McKenzie, *Is Cyber Deterrence Possible?*; Mark Montgomery and Erica Borghard, "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence," *Joint Force Quarterly* 102, (July 1, 2021); Stefan Soesanto and Max Smeets, *Cyber Deterrence: The Past, Present, and Future* (The Hague: T.M.C. Asser Press, 2020); Max Smeets, "Cyber Deterrence Is Dead. Long Live

the subject has only been produced in the past fifteen or so years. One school of thought believes that cyber deterrence practices outpace the development of the theory. "Tactics, strategy, doctrine, and policy are developed and used even before corresponding theories are properly understood."[63] For any deterrence to be effective, actors need to understand their adversary's values and willingness to take risks when faced with a potential threat. However, deterrence in the cyber space lacks a model of punishment, unlike nuclear deterrence.

Communication and credibility of one's threat are also important factors for effective deterrence. Traditional deterrence models, especially nuclear deterrence, presume a stable bi-polar relationship between adversaries with roughly equal capabilities, power and the expectation and will to avoid nuclear warfare at all costs. In the traditional concept of deterrence, referent States are needed. The referent States are considered rival or adversary States. In conventional concept, a referent State is easy to recognize, unlike in cyber deterrence, where attributing an attack is a primary challenge. One fine example is the SolarWinds hack, where major nuclear labs and administrations, including intelligence agencies' computer networks, were hacked. Unfortunately, a response did not come up because of the attribution challenge. President Biden and President Putin discussed the SolarWinds attack during Biden-Putin Summit in Geneva on 16 June 2021. However, awkward conversations over the subject did not let the issue be included in the joint statement issued by the White House.

The cyber space does not contain any elements that make traditional deterrence work, especially the issue of including a State as a referent object.[64] In the traditional model, two States are considered referent objects. The model does not include a non-State actor as a referent object in a deterrence model. In the cyber space, prominent challenges in the non-State actor led to attacks on a state's critical infrastructure.

Unlike traditional deterrence models, the cyber space is rife with an infinite number of asymmetric, constantly in flux, multilateral and bilateral relations between states and non-State actors, which make the development of a clear hierarchy of action and reaction a much more

---

Cyber Deterrence!" *Council on Foreign Relations*, February 18, 2020, https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence

63 Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43, no. 2 (2019): 245-280.

64 David J. Betz, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (London and New York: Routledge, 2017); Joseph S Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3: 44-71; Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102-135.

difficult task.[65] The availability of cyberspace to a wider group of actors complicates and undermines the stability, communication and clarity of threat for deterrence.[66] However, deterrence in the cyber space is still being termed as one of the few plausible means of preventing or defending cyber-attacks. The establishment of effective cyber deterrence requires the development of newer theories and their implementation mechanisms. Like traditional deterrence, cyber deterrence would only be successful if the adversary is dissuaded from taking aggressive action in the cyber space. Also, like traditional deterrence, the adversary can be dissuaded from action through deterrence by denial and punishment.

Deterrence by Denial

Traditionally, deterrence by denial seeks to stop the adversary from taking any action by convening them that their actions will not yield the desired results. For this type of deterrence to succeed, there needs to be no doubt in the adversary's mind regarding the futility of their action.[67] For deterrence by denial to work in the cyber space, one's defences must be made so strong that the possibility of a successful cyber-attack becomes low. Although, establishing it in cyberspace is extremely low. Still, as with all deterrence, the communication of strong defences needs to reach the adversary for deterrence to be effective.[68] Typically, deterrence by denial is achieved by having multiple layered defences, also known as the defence-in-depth concept. For deterrence by denial in the cyber space, the defences could include intruder detection systems, firewalls, encryption, and training and awareness of the practitioners. The possibility of breaching these defences cannot be ruled out unless assured cyber deterrence is established and communicated. Resilience against cyber threats as well as the flexibility of defences, are two of the key factors of deterrence by denial by the cyber space. Additionally, management and minimization of a cyber-attack's potential consequences are likely to augment the deterrence by denial by making the adversary weigh the costs and benefits of an attack.

---

65 Betz, *Cyberspace and the State*; also see Goodman, "Cyber Deterrence."

66 Jon Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," In *Coercion The Power to Hurt in International Politics*, Kelly M. Greenhill and Peter J. P. Krause, eds., (London: Oxford University Press, n.d); Meer, "State-level Responses to Massive Cyber-Attacks," and also see, Edward Geist, "Deterrence Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no.4 (Winter 2015): 44-62.

67 Michael C. Williams, "Rethinking the 'Logic' of Deterrence," *Alternatives: Global, Local, Political* 17, no. 1 (1992): 67–93; and also see Michael J. Mazarr, "Understanding Deterrence," *RAND Corporation*, 2018.

68 Robert Morgus, "Deterrence by Denial: The Missing Element of U.S. Cyber Strategy," *Lawfare* (blog), March 11, 2020, https://www.lawfareblog.com/deterrence-denial-missing-element-us-cyber-strategy.

Deterrence by Punishment

Deterrence by punishment is the alternative to the deterrence by denial concept. Deterrence by punishment works by letting the adversary know that the punishment in retaliation for action will be dire. In this case, the threat of retaliation and punishment must be perceived by the adversary as more costly than any potential gains. Therefore, for the threat of retaliation to work, attribution of the action must be established.[69] In the case of the SolarWinds attacks, the attribution challenge reduced the chances of punishment. Although the Biden Administration announced sanctioning Russia after the SolarWinds attack, the key question here is whether economic sanctions establish assured cyber deterrence. Answering this question is a tough job as such measures so far cannot persuade State and non-State actors not to commit any future course of aggression in cyberspace. However, it may be noticed that if the US being an economic power, decides to put economic sanctions on a country; then it might contribute toward a cyber compellence. Still, such measures may not work against those States whose economic systems are invariably different from the world economy influenced by the US economic power.

Deterrence by punishment in the cyber space works on the same principles. However, the issue becomes complicated owing to the difficulty of attribution in cyberspace.[70] In the cyber space, deterrence by punishment can be exerted through retaliatory strikes against the perpetrators and potential pre-emptive strikes should the adversary's intentions become clear. It is risky to assert deterrence by punishment, but other means, including putting under economic sanctions, have also failed to achieve the desired outcome. While these are non-kinetic means of punishment, kinetic means, such as the attack against tangible targets, economic strangulation, and diplomatic brokering, may also be employed as deterrence by punishment.[71] The complications with such actions remain the attribution factor and proportionality of the response options. For an effective cyber deterrence strategy, both denials of objectives as well as fear of proportional retaliation needs to factor into the adversary's calculation of whether the cost of the cyber-attack is worth the perceived benefits. Once again, the Solar Winds and Stuxnet and other Iran's cyber-attack allegations on Israel can be exemplified where the issue of attribution restricts the power to retaliate similarly. In Iran's case, Israelis

---

69 Anthony Ellis, "A Deterrence Theory of Punishment," *The Philosophical Quarterly* (1950-) 53, no. 212 (2003): 337–51.

70 Liam Nevill and Zoe Hawkins, "Deterrence by Punishment in Cyberspace," in *Deterrence in Cyberspace: Different Domain, Different Rules* (Canberra: Australian Strategic Policy Institute, 2016).

71 Western literature argues that there are kinetic means to be employed in the cyber-domain. But once again the issue of attribution may lead to dissolution of such an approach.

were not persuaded by the veiled threats of being militarily attacked by the former.[72] However, one proposed model could be to wait and see and launch a non-kinetic retaliatory cyber-attack to at least cause physical damage with tremendous economic loss.

Factors for Effective Cyber-Deterrence

Cyber deterrence remains difficult to execute, while an integral and necessary element of cyber-security, owing to several factors. Several facets must align in order for the deterrence strategy to be effective. These include communication, signalling, attribution and proportionality of retaliation.[73] Without these factors, the adversary may not receive and process the intended purpose, thus inflating the risks of misunderstanding and misinterpretation, leading to potential escalation and physical altercation.[74]

Communication

Communication remains one of the essential elements of any deterrence strategy, be it traditional, nuclear or cyber. There is a need to effectively communicate to the adversary what is acceptable and where the redlines are, crossing which would result in a reaction. In the cyber-space, communication holds a vital function since the space is rife with ambiguity. Addressing malicious activities in the cyber space, where actors are unknown to each other, broken communication pathways can further complicate the ability to send clear indicators for potential de-escalation. However, effective communication in the cyber-space would require the establishment of norms and a common lexicon, both of which are difficult to achieve, given today's global environment.[75]

Signalling

Signalling is another important aspect of deterrence and is closely linked to communication. Signalling has been used to dissuade and compel certain actions by adversaries in many areas, including the decision to go to or avoid war, crisis management, economic negotiations and diplomatic

---

72 Arie Egozi and Brad D. Williams, "Iran Threatens Israel after Cyber Strike on Nuke Facility," *Breaking Defence,* April 12, 2021.

73 Eric Sterner, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly* 5, no.1 (Spring 2011):62-80.

74 Will, “Cyber Deterrence." and also see, Sandeep Baliga, John L and Helen Kellogg, Deterrence with Imperfect Attribution, *Kellogg School of Management, Northwestern University*, accessed May 15, 2022, https://economics.mit.edu/files/14938.

75 Brian Harding, "Cyber Deterrence," (Dissertation., Air War College, Air University, 2016).

relations. Signalling remains a vital element of any deterrence strategy to showcase intent to the adversary. Without signalling, the possibility of deterrence by punishment would run the risk of escalating tensions because of being misconstrued and misinterpreted. Signalling in the cyber-space can be achieved overtly through diplomatic and established channels of communication or covertly through media and other cyber means.[76]

Attribution

As already established, attribution remains one of the cyber space's most vital and difficult aspects. With the advent of newer stealth technologies in the cyber-space, savvy nefarious actors employ multiple techniques to hinder the correct identification of the attacker and the attack's correct point of origin. Despite the difficulties, attribution remains vital for any deterrence strategy to work as the main premise of deterrence, especially deterrence by punishment, is the fear of greater retaliation.[77]

Several problems are associated with quick and accurate attribution, including the possibility of misattribution, availability of data, analysis of the attack patterns, time, identification of motives etc. Nevertheless, attribution remains one of the most important factors for deterrence by punishment to be successful in the cyber-space.[78] On the other hand, attribution may not always be necessary to engage the deterrence by denial strategy. Non-destructive pre-emptive actions, including defence-in-depth and augmentation of their security systems, are measures that states take for cyber-security. Even without attributing the action to a particular adversary, these measures allow actors to augment their deterrence. Successful cyber-deterrence strategies should blend the technical, cognitive and behavioural investigation of the adversary to identify and take appropriate actions correctly.[79]

---

76 *Cybersecurity: Deterrence Policy* (Washington DC: Congressional Research Service, January 18, 2022).

77 Michael Farrel, "Attribution and its Role in Deterrence," *Institute for Information Security & Privacy*, accessed May 15, 2022, https://www.ntsc.org/resources/ntsc-blog/

78 Jan Dyment, "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence," *Security Intelligence* (Blog), December 28, 2018, https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/.

79 Sandeep Baliga, "Deterrence with Imperfect Attribution," *American Political Science Review* 114, no. 4, (November 2020): 1155-1178.

Conclusion

The traditional concept of deterrence rests on its three manifestations; capabilities, communication and credibility. The traditional deterrence concept resides on clearly defined referent states, which is not the case in cyberspace, leaving little space to orchestrate an assured cyber deterrence model. However, this does not conclude that maintaining cyber deterrence is difficult. Primarily, a punishment model in the traditional concept of deterrence is based on deterrence by denial or deterrence by punishment. This tells varied response options- kinetic and non-kinetic. In the contemporary world, challenges and vulnerabilities faced by the States germinate a need to establish deterrence in the cyber world to ensure State's survival. The study concludes that cyber deterrence is unlike nuclear deterrence and works only at a limited level primarily due to attribution and increasing cost-benefit ratio. Cyber deterrence manifests a limited punishment model, works at a limited level, and requires tremendous input to outweigh any possible outcome. The study concludes that the examples of SolarWinds and Iran's allegations of Israel's cyber-attack on its nuclear installation indicate that capabilities are not yet able to create enough credibility for cyber forces. States have launched cyber-attacks on other states but escaped retaliation due to lack of attribution. However, credible cyber forces are not yet prepared to launch a preventive or defence counter cyberspace attacks. The adversaries have yet not denied benefits or persuaded of any course of aggression as the States establishes only limited cyber deterrence.