Cyber Deterrence: Challenges and Strategic Approaches

Mubeen Ashraf[*]

Abstract

In an era defined by the complexities of global connectivity, the strategic interplay within cyberspace presents unprecedented challenges and opportunities. The nuances of cyber deterrence, leveraging theoretical frameworks such as Game Theory and the Stability/Instability Paradox to illuminate strategic decision-making processes and dynamics become intrinsically dense. Deterrence and its fundamentals, cyber deterrence and its types, challenges in mapping key elements of cyber deterrence, and policy options for cyber deterrence all are significant features in devising effective strategies. By analysing the interactions between major cyber powers like the United States, Russia, and China, this paper underscores the intricate balance of deterrence and escalation risks in cyberspace. It highlights how the anonymity and deniability of cyber operations contribute to instability, while advanced cyber capabilities can serve as both deterrents and provocations. The research concludes that cyber deterrence necessitates a tailored approach that is adaptive to the evolving cyber landscape. By addressing the challenges outlined and implementing the recommended measures, effective cyber deterrence can be achieved among state and non-state actors.

Keywords: Cyber Deterrence, Stability/Instability Paradox, Game Theory, Cyberspace, Cyber Power, Cyberwarfare

[*] Ms. Mubeen Ashraf has an M.Phil. in Defence and Strategic Studies from Quaid-i-Azam University, Islamabad, and has worked as a Researcher at Global Foundation for Cyber Studies and Research, Washington D.C, USA. She can be reached at mubeen.0727@gmail.com

IPRI Journal XXIV (1): 62-89
https://doi.org/10.31945/iprij.240104

Introduction

The concept of warfare has been a constant evolving entity, adapting with each technological leap, throughout human history. From the earliest use of rudimentary clubs to the advanced weaponry of the contemporary era, the methods of waging war have undergone profound transformations. In the present digital epoch, a new form of warfare has emerged, characterised by the complex web of connectivity that defines the internet. This evolution has given rise to a compelling notion of information as a potent and influential weapon.

Information has acquired unprecedented significance in contemporary warfare, distinguishing itself from conventional physical armaments such as tanks and bombs. This novel paradigm unfolds within the domain of computers and the internet often referred to as *cyber*. It encapsulates the realm of information warfare which is defined as "an operation conducted to gain an information advantage over the opponent."[1] The objectives of information warfare pivot around disruption, deception, or weakening of adversaries through the manipulation of data and influencing people's thoughts and emotions. In a world interconnected on a global scale, information has metamorphosed into a formidable weapon capable of inflicting substantial harm, all without the need for vast physical resources.

Within its ever-evolving landscape of information warfare, a new class of weapons (cyber) has emerged, comprising viruses, ransomware, and phishing attacks. These digital tools operate stealthily, akin to invisible soldiers causing chaos behind the scenes. Much like infectious diseases, these digital weapons can proliferate rapidly, holding critical data hostage or deceiving individuals into divulging confidential information. It underscores the pressing need for vigilance and robust defenses in a world where physical and digital battles intertwine.

[1] "Information Warfare," *Defence Education Enhancement Programme*, n.d., https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

A compelling example of the potency of cyber weaponry is the Pegasus virus, a spyware developed by NSO group which is an Israeli private company.[2] This malware has been covertly deployed to eavesdrop on phone conversations, read messages, and even assume control of cameras and microphones on targeted devices. Such tools infringe upon privacy and, in some cases, challenge a nation's sovereignty as it has done to Pakistan since the year 2019 by compromising numerous governmental officials' phones and data.[3]

The FBI reports underscoring the severity of the cyber threat, noting that in 2022 alone, cyberattacks caused damages exceeding $10 billion.[4] Despite a decrease in complaints compared to the previous year, financial losses have surged, underscoring the gravity of cyber warfare, which refers to the techniques, tactics, and procedures involved in cyber conflicts in the digital era. These cyberattacks have occurred alongside traditional conflicts, as evident in the Russia-Ukraine conflict. Even non-state groups like Anonymous have declared "cyber wars," fundamentally reshaping the concept of warfare and its repercussions on the world's economies and stability.

In the recent past, during the Cold War, nuclear deterrence played a pivotal role in averting a catastrophic conflict between the United States and the Soviet Union.[5] However, in the contemporary, rapidly evolving world, the principles of deterrence are now being applied to the cyber

[2] Kali Robinson, "How Israel's Pegasus Spyware Stoked the Surveillance Debate," *Council on Foreign Relations,* accessed October 1, 2023, https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.

[3] Stephanie Kirchgaessner, "Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones," *The Guardian,* December 12, 2019, https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones.

[4] Eduard Kovacs, "Cybercrime Losses Exceeded $10 Billion in 2022: FBI," *SecurityWeek,* March 13, 2023, https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/.

[5] GERALD C. BROWN, "Deterrence, Norms, and the Uncomfortable Realities of a New Nuclear Age," War on the Rocks, April 20, 2020, https://warontherocks.com/2020/04/deterrence-norms-and-the-uncomfortable-realities-of-a-new-nuclear-age/.

domain, giving birth to the concept of cyber deterrence. Cyber deterrence is similar to nuclear deterrence, which centers on the perception of consequences and costs. Nations must demonstrate their capabilities and willingness to respond to cyberattacks in a manner that deters potential aggressors. This approach assumes paramount importance because, unlike the well-established international treaties and norms governing nuclear weapons, there exists no comprehensive set of international laws regulating cyber warfare. The absence of such legal frameworks compounds the challenges, making it arduous to mitigate cyber-attacks and their resultant damage.

The proliferation of cyberattacks poses a significant threat to national security, critical infrastructure, and organisational stability. Despite advancements in cyber security measures, the complexity and sophistication of these attacks continue to outpace defensive capabilities. Traditional deterrence theories are challenging to apply effectively in cyberspace due to issues such as attribution difficulties, the rapid evolution of cyber threats, and the involvement of non-state actors. With this evolving landscape of cyber warfare, unique challenges are faced that necessitate reevaluation of traditional deterrence strategies. However, it is vital to understand how deterrence should be conceptualised under the emerging circumstances, identify the primary challenges, and design policy options and strategies to ensure effective deterrence regime. Recognising the dynamic nature of this field, this paper employs qualitative data analysis to illuminate the intricate dimensions of cyber deterrence. A comprehensive understanding of the intricate relationship between technology, geopolitics, and security in the digital age is suggested.

Theoretical Framework

In the contemporary world, the landscape of modern warfare has transformed. The use of cyberspace in pursuing objectives by both state and non-state actors has become a commonplace. These actors employ various tools and weapons in cyberspace, distinct from those used in traditional ground wars. To understand the phenomenon of cyber deterrence and the policy options pursued by states and non-state actors to deter adversaries in cyberspace, a collection of concepts is examined. Deterrence itself is a widely debated and applied concept. A specific comprehension of the Stability/Instability Paradox, and Game Theory is more pertinent.

Stability/Instability Paradox

The Cold War era was characterised by paradoxical stability. Though the threat of Mutually Assured Destruction (MAD) averted an all-out war but did not prevent skirmishes. The end of the Cold War indicated the end of strategic equilibrium and increased instability and violence. The limited confrontation between the two nuclear rivals paved the way for a new theoretical base, known as the Stability-Instability Paradox. Glenn Snyder first proposed this in 1965, stating, "Greater the stability of the greater strategic balance, lower is the stability of overall balance at lower levels of violence."[6]

During the same period, cyberspace emerged as a new domain for strategic competition among states like Russia, China, and the US. Drawing insights from the Cold War era, it can be inferred that just as nuclear deterrence creates a paradox of stability and instability, cyber capabilities and deterrence strategies can similarly influence state behaviour in cyberspace, which is particularly relevant in contemporary times.

There is no doubt that the challenge of attribution, anonymity, lack of international norms, and evolving cyber threats can complicate the Stability/Instability Paradox. However, advanced cyber capabilities can work as a deterrent against potential cyberattacks. This is especially true for nations with robust offensive and defensive cyber capabilities that have the potential to retaliate. Similarly, the anonymity and deniability of cyber operations enable states to use proxies and non-state actors for

[6] Robert Jervis, "Why Nuclear Superiority Doesn't Matter," Political Science Quarterly, Vol.94 No.4 (Winter 1979-80). P 617-633 https://www.jstor.org/stable/2149629

cyberattacks, contributing to the instability experienced during the Cold War.

One of the best examples is the cyber relationship between the US and Russia, and the US and China, which illustrates strategic cyber stability while simultaneously highlighting conventional cyber instability.

Game Theory

Game theory proposed by theoreticians including *John von Neumann, Anatol Rapoport, Thomas Schelling* and others, studies strategic interactions among rational players and offers valuable insights when applied to cyber deterrence. It elucidates that engaging in cyber warfare can be a rational choice for actors due to factors such as the difficulty in detecting sophisticated cyberattacks, their relatively lower cost, and the potential for anonymity. While the risk of retaliation remains, as demonstrated by the Stuxnet case, where the possibility of a counter-attack existed, scholars argue that deterrence by punishment in cyberspace can escalate tensions.

For instance, deterrence by punishment, such as through retaliatory cyber-strikes, is inherently escalatory. This is evident in the Stuxnet case. If Israel was behind the operation, it successfully deterred Iran's nuclear programme temporarily. However, once the attack was exposed, Israel and the US faced the threat of retaliation. This highlights the potential for counter-retaliation and the temporary nature of such deterrence.

Another assumption of the Game Theory is that every player has a combination of *plays* that leads to a *well-defined end-state*, which ultimately decides the termination of the game. This assumption being highly relevant to cyber deterrence implies that both the defender and the potential attacker possess a set of strategies that, when executed, lead to specific outcomes in cyberspace. For the defender, these strategies might include the implementation of robust cyber security measures, the establishment of credible retaliatory capabilities, and the communication of clear deterrent threats to adversaries.

The potential attacker, on the other hand, evaluates these defensive plays and adjusts their strategies, accordingly. It can be justified through various examples added in the research such as the US-China 2015 Agreement or the sanctions posed to North Korea after Sony Hack in 2014. Signaling a strong deterrence stance, the well-defined end-state here was to prevent future attacks by demonstrating that such actions would result in severe political and economic consequences.

These claims can be further justified by using *Thomas Schelling's* mathematical *game theoretical model*. This model explores the way states behave under the threat of cyber-attacks and counter-attacks. The *Game of Chicken* is an apt model because it captures the essence of brinkmanship and strategic decision-making under uncertainty and mutual threat, which is highly relevant to cyber deterrence. The model involves two players and in the context of cyber deterrence, the two "players" can be understood as:

- Player A: The state considering launching a cyberattack.
- Player B: The state considering responding to a cyberattack (or a potential cyberattack).

Each player has two strategies:

- Swerve (Deter): Avoid confrontation by adopting alternate measures such as sanctions, increased cyber security, or diplomatic warnings.
- Stay on Course (Retaliate): Engage in or threaten a counter-cyberattack or another form of retaliation.

The payoffs in the *Game of Chicken* are structured as follows, adapted to cyber deterrence:

	Player B: Deter	**Player B: Retaliate**
Player A: Deter	(2,2)	(1,3)
Player B: Retaliate	(3,1)	(0,0)

Game Chicken Model

The matrix shows:

- (2, 2): Both players deter. Mutual avoidance of escalation, maintaining peace but possibly at a strategic disadvantage.
- (1, 3): Player A deters, and Player B retaliates. Player B gains a strategic advantage, while Player A loses face but avoids direct conflict.
- (3, 1): Player A retaliates, and Player B deters. Player A gains a strategic advantage, while Player B loses face.
- (0, 0): Both players retaliate. Mutual destruction or severe escalation leads to significant harm for both the parties.

The threat of Mutually Assured Destruction (MAD) is complicated in cyberspace due to the inherent uncertainty in attribution and the varying levels of threats. This makes it different from nuclear deterrence, where the threat of MAD creates clear incentives for both the parties. Thus, the complexities and unique dynamics of cyber deterrence necessitate a nuanced approach, making the *Game Chicken* model an essential tool for understanding strategic interactions in this domain.

Deterrence

Deterrence, a fundamental concept of criminology and international relations, serves as a crucial component of various disciplines, striving to prevent unwanted behaviours or actions by instilling fear of potential costs. Derived from the word "deterrere," deterrence encapsulates the idea of discouraging undesirable actions by making them appear unattractive. Academic literature sometimes employs the term "dissuasion" to encompass measures aimed not only at imposing costs but also at denying benefits to adversaries.[7] Since "deterrence" has a broad conceptual scope, using it as an umbrella term will help us comprehend the Stability-Instability theory and its implications.

During the Cold War era, deterrence played a pivotal role in shaping global geopolitics. The superpowers of the time, the US and the Soviet Union remained engaged in a delicate balance of power through nuclear deterrence. The doctrine of MAD is emblematic of this era. The possession of nuclear arsenals by both sides served as a deterrent against the initiation of a full-scale war since the fear of catastrophic consequences, inherent in deterrence, prevented these nations from engaging in any direct conflict. This period showcased the effectiveness of deterrence in preventing large-scale wars between major powers.

The key elements of deterrence theory include concepts of **certainty**, **celerity**, and **severity**. **Certainty** entails the belief that offense will not go unpunished. **Celerity**, or swiftness of punishment, reinforces the deterrence effect by ensuring that offenders face consequences promptly. And, the **severity** of punishment in the Theory of Deterrence, though important, takes a secondary role in comparison to the certainty and swiftness of punishment. These factors collectively underscore the strength and limitation of Deterrence Theory, as their presence or absence significantly influences its efficacy.[8]

Nevertheless, for deterrence to be effective, three essential factors must be present within the society: free will, rationality, and felicity. Free will

[7] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 1, 2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

[8] David Carter, "Deterrence," 2019, https://openoregon.pressbooks.pub/ccj230/chapter/8-3-deterrence/.

gives the choice of offense or defense Rationality enables individuals to understand the potential consequences of their actions, and felicity, the pursuit of pleasure over harm, motivates them to abstain from criminal behaviour. Together, these components emphasise both the effectiveness and limitations of Deterrence Theory, as their existence or absence plays a significant role in shaping its impact.[9]

In contemporary society, we have gained a better understanding of the effectiveness of deterrence. It tends to work well for lower-level offenses where individuals have 'prosocial or voluntary' tendencies though the overall impact is limited and does not prevent from criminal behaviours. Its far-reaching impact continues to generate concerns for the scholars and the policymakers in an ever increasing environment of cyber security and cybercrime. The challenges faced due to cyber deterrence are more complicated in the backdrop of the ongoing debate about the feasibility and precise meaning of cyber deterrence. Broadly, there are two main perspectives. One group contends that cyber deterrence is analogous to traditional deterrence, with its potential for both success and failure, similar to conventional methods. Some of the notable proponents of this view include Dorothy Denning. On the other hand, it is believed that the unique characteristics of cyberspace necessitate a distinct approach to cyber deterrence, as existing literature and frameworks are inadequate for addressing the complexities involved. Based on traditional deterrence principles, it is better to take cyber deterrence as a strategic effort to discourage unwanted activities in cyberspace by influencing the behaviour of potential adversaries.

In the military domain, cyber deterrence can be further elucidated through three specific applications:

1. The use of military cyber capabilities to deter a traditional military attack.
2. The use of military capabilities to deter a cyberattack.

[9] Carter.

3. The use of military cyber capabilities to deter a cyberattack specifically targeting military assets.[10] Among these, the latter two applications are typically given more prominence.

Cyber Deterrence: Navigating the Digital Battlefield

Lately, the digital realm has emerged as a parallel war zone in tandem with growing global connectivity. The specter of cyber warfare looms as a critical concern for every nation-state. One major setback of increasingly interconnected global society is the exposure of vulnerabilities within the digital frontiers. The consequences of cyber-attacks have reverberated through nations and economies alike. According to *The Global Crime Damage* report by cyber security ventures, cyberattacks impose annual damages reaching up to $10.5 trillion,[11] while raising the question of whether cyber deterrence effectively mitigates this threat or not.

In aligning itself with conventional deterrence, cyber deterrence strategies manifest in two primary modes:

a) Deterrence by Denial

b) Deterrence by Punishment[12]

Deterrence by denial hinges on dissuading adversaries from pursuing their aggressive objectives by rendering them infeasible or excessively arduous situations. It seeks to erode adversaries' confidence in the viability of their

[10] Stefan Soesanto and Max Smeets, "Cyber Deterrence: The Past, Present, and Future," in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans Osinga and Tim Sweijs (The Hague: T.M.C. Asser Press, 2021), 385–400, https://doi.org/10.1007/978-94-6265-419-8_20.

[11] Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually By 2025," *Cybercrime Magazine* (blog), December 8, 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[12] Michael J. Mazarr, "Understanding Deterrence," April 19, 2018, https://policycommons.net/artifacts/4828945/understanding-deterrence/5665691/.

actions, reminding them of the prohibitive costs and exertions entailed.[13] This passive deterrence strategy parallels the objective of thwarting attacks before they materialise, akin to traditional security measures such as anti-malware and anti-virus software installations, which serve as cyber counterparts.[14]

In contrast, deterrence by punishment involves concrete, retaliatory responses to an adversary's actions, potentially inflicting greater harm than initially perceived. Active in nature, this strategy encompasses the threat of retaliatory actions against prior adversarial attacks. However, the cyberspace arena introduces distinctive complexities, mainly due to the anonymity preserved by attackers and the attribution conundrum, which often impedes the prompt identification and penalisation of the responsible party.[15] The case of Stuxnet stands as a vivid example, where the covert nature of the attack rendered attribution and consequent punishment a formidable challenge.

Notably, while deterrence by denial and deterrence by punishment prove efficacious and admired in conventional settings, their applicability and effectiveness in the cyber realm remain contentious and intricate. Several factors contribute to this complexity. Firstly, the scarcity of documented incidents related to cyber warfare has impeded the establishment of a robust theoretical foundation for cyber deterrence. Secondly, the proliferation of offensive cyber warfare capabilities coupled with an inherent lack of transparency regarding adversarial cyber arsenals compounds the challenge. This opacity extends to the secrecy surrounding

[13] Michael Kassner, "Can Deterrence Counter the Threat of Cyberweapons?," TechRepublic, December 30, 2016, https://www.techrepublic.com/article/can-deterrence-counter-the-threat-of-cyberweapons/.

[14] Scott Jasper, "Deterring Malicious Behavior in Cyber Space," 2015, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-1/jasper.pdf.

[15] Nye, "Deterrence and Dissuasion in Cyberspace."

states' offensive cyber capabilities, which hampers cooperative efforts to fortify cyber defenses.[16]

To further enrich the discussion, it is essential to introduce the Tallinn Manual 2.0 and 3.0. These manuals, developed by a group of international legal experts, offer valuable guidance on the application of International Law to cyber operations, including issues related to cyber deterrence. Tallinn Manual 2.0, published in 2017, provides a comprehensive analysis and interpretations of existing International Law principles in the context of cyber operations. It has been instrumental in shaping legal discussions surrounding cyber conflict, helping policymakers navigate the evolving landscape of cyber threats.[17]

Tallinn Manual 3.0, the latest iteration released in 2021, further refines and expands upon its predecessors, addressing key contemporary challenges, including cyber deterrence. It offers insights into how International Law applies to state behaviour in cyberspace and sheds light on the legal considerations of cyber operations that may be employed as part of a deterrence strategy.

While the Tallinn Manuals play a pivotal role in clarifying legal frameworks in the cyber domain, their weaknesses lie in their adaptability and practicality. International Law, as articulated in these manuals, can be slow to evolve and may not always align with rapidly changing cyber threats and technologies.[18] Additionally, the enforcement of international

[16] John Glaser, "Cyberwar on Iran Won't Work. Here's Why," Cato Institute, August 21, 2017, https://www.cato.org/commentary/cyberwar-iran-wont-work-heres-why.

[17] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.

[18] "The Tallinn Manual," accessed October 1, 2023, https://ccdcoe.org/research/tallinn-manual/.

norms and legal principles in cyberspace remains a complex challenge, as attribution and accountability issues persist.[19]

Moreover, another challenge that is added to the list of achieving an effective credible deterrence framework is to analyse and estimate the motivation and level of risk tolerance of the competitor. Therefore, for effective deterrence complete information about the adversary's cyber capabilities is required which is not feasible for any state. However, it can be achieved if states keep in mind and learn from the damaging impacts of cyber-attacks that have been used in the past and at present to build a suitable framework for cyber deterrence.[20]

Challenges in Mapping the Key Elements of Cyber Deterrence

The intricate landscape of cyber deterrence is explored with a particular focus on the substantial challenges that arise when attempting to define its essential components. As one navigates through the subtleties of cyber deterrence, one will unveil the obstacles and uncertainties that complicate its precise delineation. The objective is to shed light on these challenges, offering a clearer perspective on the complexities surrounding the strategic realm of cyber deterrence and its practical application.

Sensitive Data Sharing

Cyber deterrence often relies on the collection and sharing of sensitive intelligence and attribution data. The challenge lies in striking a balance between the need for transparency in attribution and the protection of sensitive sources and methods. Nations are often hesitant to disclose the full extent of their cyber capabilities or the sources of their intelligence, as this can reveal vulnerabilities or classified information. The reluctance to share sensitive data can hinder efforts to establish certainty in cyber attribution, a fundamental element of deterrence.

[19] Michael Schmitt, "Germany's Positions on International Law in Cyberspace Part I," *Just Security*, T14:15:30+00:00, https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/.

[20] Jyri Raitasalo, "Cyber Deterrence: An Oxymoron for Years to Come," *Global Security Review* (blog), June 7, 2019, https://globalsecurityreview.com/cyber-deterrence-oxymoron/.

Proxy Wars and Attribution Complexity

In cyberspace, attribution is not always straightforward. Cyberattacks are frequently launched through intermediaries, making it difficult to attribute an attack to a specific state actor definitively. State-sponsored hackers may operate from foreign soil or use proxy servers to obfuscate their origins. This attribution complexity introduces uncertainty and challenges the element of certainty in cyber deterrence. Accurately identifying the true perpetrator in a world of proxy wars and cyber mercenaries can be elusive.

Lack of International Rules and Norms

Unlike traditional warfare, cyberspace lacks well-established international rules and norms governing state behaviour in times of conflict. The absence of a universally accepted framework for cyber warfare complicates the determination of what constitutes a severe response or an act of aggression. The lack of clear boundaries can lead to misinterpretations and unintended escalations, posing a challenge to the element of severity in cyber deterrence.

Asymmetry and Non-State Actors

Cyberspace is characterised by significant asymmetry, where even smaller, less-resourced actors can launch disruptive cyberattacks against larger, more powerful states. Additionally, non-state actors, such as hacktivist groups or cybercriminal organisations, can engage in cyber aggression without the constraints of traditional state boundaries. These dynamics challenge the notion of holding assets at risk and raise questions about how to deter non-state cyber threats effectively.

Escalation Risks

The digital realm is highly dynamic, and cyber operations can escalate rapidly. A retaliatory cyber action, intended as a deterrence measure, can quickly spiral into a broader conflict. Without well-defined rules of engagement and de-escalation mechanisms, cyber deterrence efforts run the risk of inadvertently causing more significant disruptions or conflicts than they aim to prevent. The escalation risks in cyber deterrence are complex and multifaceted, mirroring the intricacies of escalation theory. Understanding and mitigating these risks requires clear communication, well-defined rules, improved attribution capabilities, and a nuanced approach to cyber strategy that considers both state and non-state actors. Failure to address these risks adequately can lead to unintended escalations in cyberspace, with potentially severe consequences for international security and stability.

Having explored the multifaceted challenges in mapping the key elements of cyber deterrence, we now shift our focus to a comparative analysis of deterrence fundamentals. Understanding the intricacies of these challenges will provide valuable context as we examine how deterrence principles apply in both physical and digital realms.

Effective deterrence strategies in cyberspace must consider these diverse motivations and adapt accordingly to deter malicious cyber activities. For example, a comprehensive cyber deterrence strategy may include measures to counteract the various motivations driving cyber threats, such as enhancing cyber security to reduce financial incentives for cyber criminals or engaging in diplomatic efforts to address ideological conflicts in cyberspace.

It underscores the challenges and complexities policymakers and cyber security experts' face when crafting effective deterrence strategies. As we explore the cyber deterrence options, this comparative analysis provides a critical backdrop for discerning how these strategies can be tailored to address the distinctive dynamics of the digital age.

Options for Cyber Deterrence

The application of traditional deterrence principles in the evolving landscape of cyberspace presents a complex challenge. Scholars such as Dr. Joseph Nye and Dorothy Denning remain optimistic about the feasibility of effective cyber deterrence, emphasising the pivotal role of robust cyber security measures and advanced cyber deterrents. These deterrents encompass offensive and defensive cyber weapons, strategically employed to deny and penalise adversaries in response to malicious cyber activities. In light of these evolving dynamics, this section explores various policy responses to the emergence of new offensive cyber capabilities. By examining these options, states can better navigate the concentrated realm of cyber deterrence and safeguard their interests in an increasingly interconnected world.

Sanctions

One traditional and still practiced method to stop an adversary from doing anything undesirable, bigger states tend to impose economic and trade sanctions. Sometimes it also happens that states warn before they impose sanctions and the adversary state restricts itself from carrying out the activity.[21] One reason may be the increased globalisation and the importance of the economy in running state affairs. Once the economic activity is halted, it becomes difficult for smaller states to survive. One way of putting sanctions is through strong international agreements.[22] It is noted that most of the states that are attacking other states in cyberspace are already under sanctions and imposing new ones will not help much. Till now there is no such law developed at the international level that may ease the task and deter the enemy from doing illicit activities. Therefore, for the sanctions to have an impact on the adversary, a new set of laws regarding the increased ratio of offensive cyber weapons is required. However, that was one side of the coin, the other side believes in putting sanctions to deter and punish the adversaries, just as the US did during the Sony Pictures Hack in 2014, by imposing sanctions on North Korea.[23] Considering the effectiveness and limitations of imposing sanctions, the US in 2016, also signed legislation that allows it to employ sanctions on

[21] "Soleimani: What Are Sanctions and Why Do Countries Use Them?," *BBC News*, August 9, 2018, sec. Newsbeat, https://www.bbc.com/news/newsbeat-45128837.

[22] Misha Glenny, "Stuxnet Will Come Back to Haunt Us," *The New York Times*, accessed October 1, 2023, https://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

[23] Julia Edwards and Jason Lange, "U.S. Slaps More Sanctions on North Korea after Sony Hack | Reuters," *Reuters*, January 2015, https://www.reuters.com/article/idUSKBN0KB16T/.

states that are involved in hostile activities in cyberspace.[24] Furthermore, on September 3, 2020, the State Department wrote a detailed letter to the Secretary of Russia Mr. Steven Mnuchin. In the letter, it mentioned Russia's involvement in US 2020 elections and warned about imposing severe sanctions if Russia and its surrogates continued their interference in future.[25] The US expelled Russian diplomats, imposed sanctions and increased cyber security protocols following Russia's alleged interference in the 2016 US elections.[26]

Setting up Protection/Defense

All the defensive tools and techniques that provide security in cyberspace are the deterrents. The ones working on deterrence theory from a cyber perspective also believe that passive deterrence involves all relevant actions to minimise the threats prevailing in cyberspace and building resilient networks is no exception in the process. Although these actions help in better system security engineering and doctrine, however, their effectiveness as a substantial deterrent against cyber-attacks is not much effective.[27]

However, scholars and practitioners feel the cyber security measures at present announce several uncertainties as well. They believe that the accommodation of IoT devices has doubled the risk of exploitation and Mirai Botnet is a live example of that. The reason behind this exploitation

[24] Rustam Goychayev et al., "Cyber Deterrence and Stability," Assessing Cyber Weapon Analogues through Existing WMD Deterrence and Arms Control Regimes, September 30, 2017, https://doi.org/10.2172/1405058.

[25] "Letter from Senate Democrats to Treasury Secretary Steven Mnuchin on Sanctions," *The Washington Pos*t, September 2020, https://www.washingtonpost.com/context/letter-from-senate-democrats-to-treasury-secretary-steven-mnuchin-on-sanctions/9a87d3ad-db47-40a8-b09f-e29d6c7917b3/?itid=lk_inline_manual_7.

[26] Eric Tucker and Aamer Madhani, "US Expels Russian Diplomats, Imposes Sanctions for Hacking," *AP News,* April 2021, https://apnews.com/article/us-expel-russia-diplomats-sanctions-6a8a54c7932ee8cbe51b0ce505121995.

[27] Robbie Gramer Mackinnon Amy, "U.S. Envoy Says Former Officials' Call for Russia Rethink Is 'Shameful,'" *Foreign Policy* (blog), September 3, 2020, https://foreignpolicy.com/2020/09/03/trump-putin-russia-west-reset-osce-gilmore-huntsman-russia-rethink-shameful/.

is the extreme insecurity of these devices that are not very costly and, therefore, are given more preference over the secure and costly devices. This has urged the communities to take frequent and reliable actions to protect the companies from becoming victims. So, it is better to follow robust security standards and hold the companies accountable and responsible if any breach occurs.[28] This way increased protection in the vulnerable devices will act as a consistent deterrent. A good cyber defense strategy is essential for states and bigger organisations to counter threats effectively by focusing on the pillars of cyber defense strategy.

Cyber Defence Strategy

In the cyber domain, it is immensely important to protect and secure critical assets of organisations and states. It requires lots of effort and careful yet effective measures to minimise the threat. To defend against an adversary's offensive action, organisations need to develop a cyber defence strategy that helps maintain their cyber hygiene. The different ways to do so include drills, penetration testing, vulnerability assessment etc.[29] Therefore, it is vital to opt for layered defenses that work on three pillars i.e. people, infrastructure and procedures. As mentioned earlier, it is recommended for the companies to look for better solutions and better strategies other than the proposed ones. All the companies should discuss, develop and adopt new and effective strategies that others are using. The aim should be the adoption of cyber security by design and to consider cyber threats as actual threats. Otherwise, companies due to their carelessness will allow the hackers to make use of the critical infrastructure and information.[30]

[28] Kassner, "Can Deterrence Counter the Threat of Cyberweapons?"

[29] David Balaban, "Red Teaming: How to Run Effective Cyber-Drills? | Tripwire," FORTRA, accessed October 1, 2023, https://www.tripwire.com/state-of-security/red-teaming-effective-cyber-drills.

[30] Lili Nguyen, "3 Pillars of Cyber Defence Strategies," Informa Connect, October 2, 2018, https://informaconnect.com/3-pillars-of-cyber-defence-strategies/.

Active Cyber Defense

One vital component for organisations and small enterprises to securely surf online is opting for a robust cyber defense. It is a defense mechanism for a computer network that helps protect critical information and infrastructure of the government units and other private organisations.[31] Cyber defense acts as a cyber deterrent in countering the threat of a malicious attack. Moreover, there are a variety of things that cyber defense focuses on including protection, prevention, detection, and timely reaction to the proposed threats to safely run businesses. It is a long-term guarantee to run the business and to determine the effective utilisation of resources while opting for a security strategy.[32]

Defensive cyber operations are conducted to provide efficiency to the military networks so they may work in an environment that is free from the threats emanating from cyberspace.[33] There are three tracks or methods that are used in shielding the data and preventing cybercrimes; defensive, offensive, and general methods. All three are similar to active and passive defense and deterrence. One utilises the proactive while the other chooses a reactive approach and the third deals with a mixture of both to provide security and safety from cyber threats.[34]

The active cyber defense has numerous benefits as it can take direct (defensive) actions against the adversary by invalidating, terminating, and dropping robust cyber threats. It can also help in identifying and later punishing the actual culprit. The perks of having an improved cyber defense will restrict the adversary from planning a cyber-attack against a state's military (e.g. US, Russia, or China) which they already know will have a hard time if they mess with it. It can be demonstrated without

[31] "Cyber," "Cyber Defense," Techopedia, February 5, 2019, https://www.techopedia.com/definition/6705/cyber-defense.

[32] Adam Bateman, "What Is Cyber Defense?," F-Secure, 2020, https://www.f-secure.com/en/consulting/our-thinking/what-is-cyber-defence.

[33] Col. Mark Taylor, "Defensive Cyber Operations," Military, PEO EIS, n.d., https://www.eis.army.mil/programs/dco.

[34] "Maryville," "Understanding General, Defensive, and Offensive Cybersecurity Tracks"," University, 2020, https://online.maryville.edu/online-bachelors-degrees/cyber-security/understanding-cyber-security-tracks/.

unleashing information that could become a source of exploitation. It is possible to plant deceptive *bait* files to discourage an enemy.[35] This makes active and improved cyber defense into a useful and effective cyber deterrent.

International Norms and Laws

The increased number of cyberattacks in recent years has forewarned the states to opt for strict policies against attacks and attackers. It is observed that national governments can be a strong deterrent. It depends on the effectiveness of their policies and actions when they become a target of cyberattacks. For International Law and norms to work as robust deterrents for cyber weapons used by states, the Tallinn manual has provided a little help.[36] It is still a norm and is not as effective as a treaty or law could be. Moreover, it is not even acknowledged by bigger states like the US and Russia. It, however, provides a framework for many cyber-related aspects that are ignored by the international bodies and states.

There are many examples where states have individually signed different treaties to protect their infrastructure from malicious attacks by the adversary. The usefulness of these contracts is another question but for a limited period, it has worked as well. One example is taken from China and the US agreement in 2015[37] after Chinese military hackers targeted five American companies related to nuclear power, metals, and solar products.[38] This brought both parties to agree on neither stealing nor exploiting each other's secrets. These norms and laws can work as effective deterrents, if taken seriously and respectfully. Other examples of the issue of cyber security include the Budapest Convention and the

[35] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

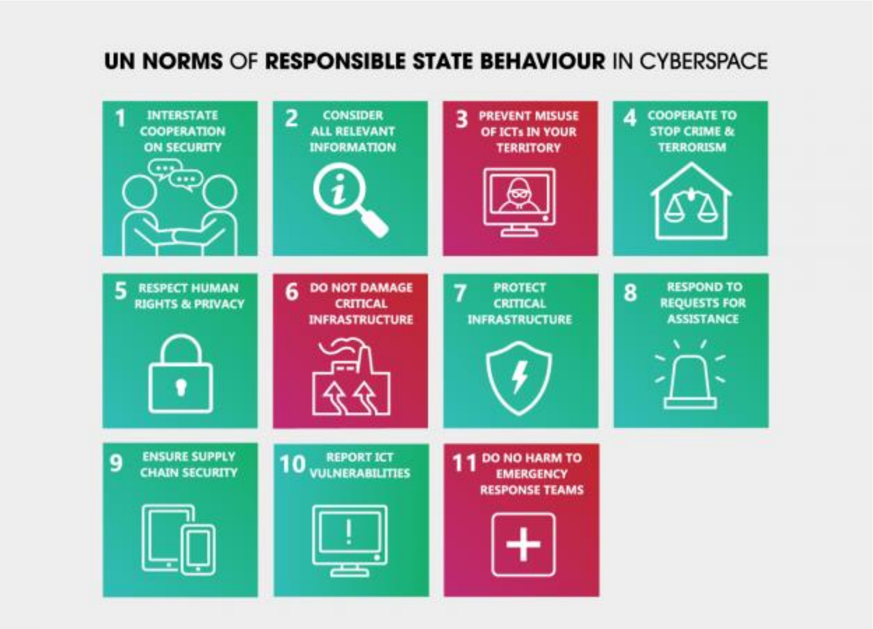
[36] Tim Stevens, "(PDF) Cyberweapons: Power and the Governance of the Invisible," ResearchGate, 2017, https://doi.org/10.1057/s41311-017-0088-y.

[37] John W Rollins et al., "U.S.–China Cyber Agreement," 2015, https://sgp.fas.org/crs/row/IN10376.pdf.

[38] Ashley Fantz, "Chinese Hackers Infiltrated U.S. Companies, Attorney General Says," CNN, May 19, 2014, https://www.cnn.com/2014/05/19/justice/china-hacking-charges/index.html.

African Union Convention on Cyber Security and Personal Data Protection. Also, one of the most relevant to the defense of cyber weapons is proposed by NATO with the name of Cooperative Cyber Defence Centre of Excellence (CCD COE).

Since 2004, there are six Groups of Governmental Experts (GGEs) on cyber security, including representatives of 15 to 25 member states, and the latest convened in 2023 by the United Nations. The GGE is responsible for studying existing and potential threats linked to the digital space and looking at collective measures that could be implemented to address them. The US has been a member of GGE and from the forum, 11 norms of behaviour in cyberspace have been drafted and that include:


UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE
1 INTERSTATE COOPERATION ON SECURITY
2 CONSIDER ALL RELEVANT INFORMATION
3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY
4 COOPERATE TO STOP CRIME & TERRORISM
5 RESPECT HUMAN RIGHTS & PRIVACY
6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE
7 PROTECT CRITICAL INFRASTRUCTURE
8 RESPOND TO REQUESTS FOR ASSISTANCE
9 ENSURE SUPPLY CHAIN SECURITY
10 REPORT ICT VULNERABILITIES
11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

Source: *Australian Government's website*

This drafting of such norms with Russia, USA, Australia, and Switzerland being a part of it holds some peace in cyberspace and if it works, norms can work as effective cyber-deterrents.

Stockpiling of Cyber Weapons

Another effective tactic for cyber deterrence is by increasing the capability of cyber weapons. Having stockpiles of cyber weapons is not just enough. The real task is to convince the adversary about the cyber weapons one owns. The problem comes when a state has to reveal their cyber capabilities. Unlike nuclear weapons, tanks, and missiles, cyber weapons if described and hinted will lose their effectiveness. They are superseded as soon as the kind of vulnerability that is being exploited becomes known because it is a software-based coded weapon and software flaws can be fixed over time. However, fake demonstrations can also be arranged if a state wishes to unleash its capabilities.[39] Since it is hard to detect the real state or group who have developed and deployed a cyber-weapon, this option is still favourable but at the same time alarming.

Counterattack

This technique fits into the deterrence by punishment category, where to shut the enemy down, a state retaliates, and it is not always sure that the damage will be less or more than perceived. In other words, the counter-attack can be both automated and non-automated. In an automated attack, there is a surety that the opponent will suffer, and damage will be caused, while in a non-automated attack, the effect will be widely visible. Another notable point regarding the retaliatory attack is that it is not necessary to answer a cyber-attack with another cyber-attack; however, it is up to the states to look for a suitable response. This is the liberty that states enjoy as part of their defense, as stipulated by International Law.

Amid Russia's recent move to elevate its nuclear readiness, the potential for severe cyber retaliation looms. Conversely, NATO has affirmed that any cyber assault on its members will invoke Article 5 of the NATO Charter, enabling a comprehensive response. Historically, the US and its allies have predominantly relied on publicly attributing attacks to Russia

[39] Elizabeth E. Wanic and Neil C. Rowe, "Assessing Deterrence Options for Cyberweapons - Ppt Download," 2019, https://slideplayer.com/slide/15159973/.

and imposing sanctions on implicated individuals. However, with sanctions largely exhausted, the possibility of counter-cyber-attacks emerges as a viable alternative.

Recently, there have been several incidents concerning the US, Iran, Russia, India, Pakistan, the UK, and many others where either a threat of nuclear war against a severe cyber-attack or a threat, of a cyber-attack in response to other illicit activities is noted. However, in the case of an offensive sophisticated cyber weapon that is used against any state for a certain period, it limits the retaliation factor for some reasons. Firstly, super cyber-weapons like Stuxnet make it difficult for the victims to detect, if there is any abnormal activity present in the system that is compromised, and even if they do, the utmost task is to mitigate the threat. Secondly, attribution is a grave concern in cyberspace operations, and so is the case for cyber weapons. They take some time to develop and are carefully designed to deceive the opponent. Both cases require enough time and, therefore, the probability of retaliation is decreased and highly depends on its timely detection.

This strategy is often favoured by many countries and applies effectively, including the Indo-Pak cyber conflicts. Pakistan and India have, indeed, been engaged in a complex cyber relationship over the years, characterised by a mix of cooperation, competition, and the development of cyber deterrence strategies. It can easily be traced back to the first cyber-attack in India after its nuclear testing in 1998, which was carried out by a foreign organisation. This was followed by several cyber-attacks in Pakistan in 1999. These incidents from the past may not have a direct link with each other. However, since then, counter-attacks have become a recurring pattern for both states, whether in the form of website defacements or the gathering of personal information through cyber espionage.[40]

[40] Marie Baezner, "(PDF) Regional Rivalry between India-Pakistan: Tit-for-Tat in Cyberspace," Center for Security Studies (CSS), ETH Zürich, August 2018, https://www.researchgate.net/publication/326866504_Regional_rivalry_between_India-Pakistan_tit-for-tat_in_cyberspace.

The recent example is of Russia-Ukraine where a full-fledged military operation is launched against the Ukrainians for multiple reasons. However, it is not the first military operation against Ukraine. It started in 2014, and since then Ukrainians have worked hard to improve their cyber defenses to protect critical infrastructure from tremendous cyber-attacks. However, the situation is different as the critical infrastructure is at risk by both cyber and non-cyber forces from Russia. The Russians have defaced multiple Ukrainian government websites and disrupted various digital activities in the country by meddling with the financial systems and wiping off sensitive data. The risk of counter-attack is ever increasing, and sometimes it aggravates the situation, while at other, it might work as a deterrent and prove useful for an aggressor.

Recommendations

The following recommendations are proposed to enhance cyber deterrence strategies and address the evolving challenges in cyberspace.

- **Invest in Cyber Attribution Technologies**
  States and organisations should invest in advanced technologies and methodologies for cyber attribution. Enhancing the ability to identify the true source of cyberattacks is crucial for strengthening the certainty element of cyber deterrence.
- **Strengthen the Foundation of Cyber Deterrence**
  Invest in research and data collection to build a stronger foundation of cyber deterrence by documenting cyber incidents, responses, and communication between states. A comprehensive understanding of past events is essential for formulating future strategies.
- **Promote International Norms and Laws**
  Actively promote and adhere to international norms and laws, such as those outlined in the Tallinn Manual, to provide a structured framework for responsible state behaviour in cyberspace. Encourage other nations to adopt and respect these norms.

- **Public-Private Partnerships**
  Foster public-private partnerships to bolster cyber defenses. Collaboration between governments and the private sector can lead to more comprehensive and resilient cyber security measures, acting as a deterrent to cyber threats.
- **Enhance Cyber Defense Strategies**
  Develop and share robust cyber defense strategies that focus on active cyber defense measures, including automated responses, honeypots, and deceptive tactics. A strong defense can serve as a significant deterrent against cyber threats.
- **Utilise Sanctions and Economic Measures**
  Implement sanctions and economic measures against malicious cyber actors. International cooperation and agreements are crucial to ensure the effectiveness of these measures in punishing cyber aggressors.
- **Strategically Stockpile Cyber Weapons**
  Strategically stockpile cyber weapons while maintaining a high level of secrecy. The convincing demonstration of cyber capabilities can deter potential adversaries, aligning with your original point.
- **Regular Cyber security Drills**
  Conduct regular cyber security drills and exercises to test the readiness of organisations and states in responding to cyberattacks. These drills can help identify weaknesses and improve cyber deterrence capabilities.
- **Adapt to the Evolving Cyber Landscape**
  Continuously adapt to the evolving cyber landscape by staying informed about emerging cyber threats and technologies. Flexibility and adaptability are essential in crafting effective cyber deterrence strategies.
- **Engagement with Non-State Actors**
  Recognise the role of non-state actors in cyberspace and engage with them through legal means. Developing mechanisms for

holding non-state cyber threats accountable can enhance deterrence efforts.

- **Adaptive and Comprehensive Strategy**
  Develop a comprehensive and adaptive cyber deterrence strategy that takes into account the evolving nature of cyber threats. This strategy should encompass prevention, detection, response, and recovery elements.

Conclusion

The research provides a thorough examination of deterrence in the context of both traditional and cyber environments. The realm of cyberspace has, indeed, introduced unique challenges and complexities when it comes to the concept of cyber deterrence. The staggering financial damages caused by cyber-attacks underscore the urgent need to address this issue. While traditional deterrence theories have been effective in conventional domains, applying them to cyberspace is a highly debatable and complex endeavour. One of the fundamental challenges in achieving effective cyber deterrence lies in the absence of a strong foundation of incidents and communication in the cyber warfare landscape. The increasing offensive cyber capabilities and the lack of transparency among states regarding their cyber arsenals further complicate the matter. Additionally, the asymmetry of power in cyberspace, the presence of non-state actors, and the rapid escalation of cyber operations add to the complexity. Hence;

- Cyber deterrence necessitates a tailored approach that recognises the unique characteristics of cyberspace, including attribution challenges and evolving threat landscapes.
- International cooperation and the development of legal frameworks specific to cyber operations are vital for establishing norms and rules governing state behaviour in the digital domain.
- Active cyber defense measures offer a potent means of countering cyber threats effectively, contributing to deterrence efforts by enhancing the credibility of responses.

- In deterrence, the accumulation of advanced cyber weapons has become crucial in the digital age. This mirrors the historical trend in the nuclear arena, where maintaining deterrence capabilities remains essential, irrespective of ethical debates or arms races. This parallel extends to cyber security, emphasising the need for defensive cyber capabilities. Iran's pursuit of top-tier cyber capabilities exemplifies this shift. Just as Pakistan's nuclear programme is aimed to secure its defense, defensive cyber capabilities seek to protect critical infrastructure and deter potential digital threats.

As society continues to grapple with the transformational impact of the digital age, it becomes imperative for policymakers, cyber security experts, and international stakeholders to collaborate in refining and optimising cyber deterrence strategies. It is, thus, pertinent to safeguard our interconnected digital future.■