BTTN Journal
p-ISSN 2958-1214
e-ISSN 2958-1222

RESEARCH ARTICLE

Deterrence and the Problem of Attribution in Cyberspace: An Analysis of Vulnerabilities and Options for Pakistan

Akber Khan[1]
Assistant professor, Command and Staff College, Quetta.

Article Info

Article History:
Received:
June 11, 2022
Revised:
December 06, 2022
Accepted:
December 15, 2022

Keywords:
Deterrence, Cyberspace, Attribution, Defense, Capabilities, Strategy

Abstract

This study examines the concept of deterrence and the problem of attribution in cyberspace. Unlike conventional deterrence, deterrence in cyberspace is perplexing, and the problem of attribution makes it even more complex. However, the advancement of technology and its sophistication have made deterrence in cyberspace, as well as attribution, relevant. States in the context of cyber rivalry employ different strategies to deter their rivals in cyberspace, such as threat of punishment, denial by defense, entanglement, etc. This study further argues that the threat of punishment is relatively less effective as compared to denial by defense and entanglement because robust infrastructure and a resilient system would imbalance the cost-benefit equation, making the attack futile and costly. Furthermore, this study suggests that investing in and advancing scientific capabilities, as well as strengthening infrastructure and defense capabilities, would help improve attribution forensics while improving the deterrence capability of states in general, and Pakistan in particular. This would make the attacking states realize that the costs of attacks would exceed the benefits.

[1]Akbar Khan is an Assistant professor at Command and Staff College, Quetta.

Introduction

It is of great concern how scholars of international security assess unconventional deterrence and the problem of attribution in cyberspace, both theoretically and practically, to assess where it is now, where it might be, and how it might impact security dynamics soon. However, in the aftermath of the Cold War, studies predicted that the conception, role, and conduct of conventional deterrence would change immediately. This suggestion had its roots in the rapid advancement in the domain of science and technology and the changing nature of interactions between states. These conceptions pushed the states to behave differently on regional and international stages, giving space to the biggest question: can states deter each other in cyberspace while confronting the problem of attribution? What are the vulnerabilities, and, at the same time, what are the options available for states in general and minor states to strengthen their position in the domain of cyberspace? This is because the risks of cyber-attacks have increased dramatically, putting the security of states at risk.

In the contemporary world, the internet has got such prominence that no state can deny its importance. It has immensely contributed to the world economy and has been playing a lead role in boosting up the economies; however, the trajectory of economies and capabilities of the states are directly proportional, meaning that states can build their military prowess if they have strong and sophisticated economies otherwise it would be nearly impossible for states to what are the vulnerabilities, and, at the same time, what are the options available for states in general and for minor states in particular to strengthen their position in the domain of cyberspace? This is because the risks of cyberattacks have increased dramatically, putting the security of states at risk.

In line with this, the sophistication of the internet is gaining more prominence in contemporary times while bringing forth the vulnerabilities of states. It is estimated that two decades ago, there were only 16 million internet users, and the number of internet users and connectivity has now multiplied exponentially. It is estimated

that more than twenty billion devices have been connected to the internet in the past decade, and analysts predict that this type of connectivity is expanding at an alarming rate, making the concept of cyber-attacks more common.[1] Thus, total dependence on the internet has created new dimensions while posing serious challenges to the security of the states.

Nation-states' reliance on cyberspace for the flow of trade and commerce, support for critical infrastructure such as water, banking, electricity, transportation, communication, and military system command and control has grown dramatically. However, in response to such dependency, malicious acts in cyberspace by states and capable non-state actors have also increased dramatically. The case of the US is an excellent example because the US has been leading in developing cyber technology, which has, in turn, made the US highly vulnerable. If the US faces a lot of cyberattacks despite being a superpower, then what challenges could the minor states face? And how they might deter their adversaries in cyberspace. It is therefore important to analyze the concept of deterrence in cyberspace and its implications for the states in the developing world and their security structures.

This article argues that deterrence in cyberspace is perplexing to some extent, unlike conventional deterrence, because it is quite hard to find the attacker. The attacker may raise false flags to deceive the targeted state, complicating the targeted state's ability to attribute the attack. However, if a state advances in the field of science and technology by building sophisticated infrastructure, then the probability of tracing the attacker could be highly likely. If not, then states would be vulnerable to such attacks.

This article is divided into five sections. To assess the additive value of deterrence and the problem of attribution in cyberspace, I

[1] John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," *Journal of Cyber Policy*, Vol. 1, No. 1 (April 2016), 5–28.

succinctly explain why non-conventional deterrence is perplexing in cyberspace, or why it is difficult to deter a potential rival in cyberspace by making an analogy between conventional deterrence and deterrence in cyberspace, and how failure in attribution in cyberspace becomes an impediment to deterring any aggressor. Second, this article explains the mechanisms of cyber threats and national security architecture, followed by the real problems faced by states in attribution in cyberspace. Failure in attribution is likely to shift the perception of states, and self-deterrent behavior becomes susceptible. Third, I examine different modes of deterrence in cyberspace like those in conventional deterrence. Fourth, I explain options available for states in general and Pakistan to improve their deterrence capability in cyberspace. The final section concludes the article with a brief discussion on the perplexity of deterrence in cyberspace and the issues of attribution.

Deterrence in Cyberspace and Nuclear Deterrence: An Analog

The concept of deterrence has been defined by scholars as the act of dissuading someone from doing something by threatening that the costs of doing so or trying to harm others would exceed the benefits they expect. The same concept of deterrence is applicable to cyberspace, but it is a bit perplexing. The concept of deterrence in cyberspace is difficult to understand because our minds are mostly influenced by the conception of conventional deterrence, especially nuclear deterrence.[2] Throughout the Cold War period, this type of deterrence was critical in deterring potential adversaries; for example, the Cuban Missile Crisis and subsequent interactions between the United States and the Soviet Union demonstrate how nuclear weapons forced rivals to deescalate many potential conflicts. The analogy between nuclear and cyber deterrence, however, is quite misleading because the goal of nuclear deterrence is total prevention of a nuclear attack by nuclear-weapons states. In

[2] Chris Jaikaran, "Cybersecurity: Deterrence Policy" January 18, 2022; Congressional Research. Available at: https://crsreports.congress.gov/product/pdf/R/R47011.

contrast, cyber behavior, in many aspects, is very similar to other behaviors, such as crime on the street.[3] This is why this strategy is not convincing. However, states in the domain of cyberspace employ this strategy to deter potential aggressors, which can be regarded as an imperfect strategy. This is because of the problem associated with attribution in the realm of cyberspace. Similarly, the mechanism that states often employ to prevent harm in cyberspace is complex because of the nature of its employment. States often use threats of punishment, denial, and entanglement as deterrent strategies to deter the potential aggressor, but these strategies can be best employed if the state has technological dominance. Otherwise, a state can only become a victim of cyberattacks.

Cyber Threats and National Security Paradigm

The term "cyber" refers to digital and computer-related activities; however, in the military context, it is referred to as a domain of broader actions, covering important areas such as air, sea, space, and land. This scope can also be broadened to include critical infrastructure.[4] If any state wants to extend the scope of deterrence to cyberspace, then it must be kept in mind that deterrence in the cyber domain requires sophisticated knowledge, a deeper understanding, and an effective strategy. Otherwise, a state can only think about it. Moreover, a response to a cyberattack may not only be a counter-cyberattack, but states can also choose an appropriate military response while calculating the damage done.

Cyber threats may be multifaceted, including sabotage, war, spying, and disruption,[5] and in this regard, international law is silent or has ambiguous rules. However, the United Nations allows states to use force to defend themselves against any potential aggressor only when the threat perception crosses certain limits. Michael Schmitt, on the other hand, claims that "cyber operations do not fit neatly into this paradigm because they are "non-forceful" (that is,

[3] Joseph, S. Nye Jr. "Deterrence and Dissuasion in Cyberspace" *International Security*, Vol. 41, No. 3 (Winter 2016/17), 44–71.
[4] Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011), chapter. 5.
[5] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

"non-kinetic"). [6] This clearly indicates that the international community or organizations have no consensus on the use of force in the domain of cyberspace. There are ample cases of cyberattacks. Some of these attacks are trivial, while others are costly and disruptive in scope. For example, hackers targeted the Pentagon, which reported more than 10 million cyberattacks, ranging from sophisticated to minor. [7] Higher-intensity attacks pose a serious threat to national security, necessitating a comprehensive response from the target state. Computer network exploitation and computer network attack are examples of costly cyber intrusions. These attacks were designed to aggressively disrupt the confidential information and process.[8] In this case, the intrusions involve spying for commercial, political, and economic purposes.[9]

Some of the prominent cyber-attacks that have already been made public have caused significant destruction, including in 2008, Russia invaded Georgia's defense system. In 2010, Iranian centrifuges were targeted by the Stuxnet virus, which potentially caused the destruction of some 1,000 computers and delayed the uranium enrichment process. This attack was attributed to the US and Israel. In contrast, it was argued that Iran retaliated with a counter-cyberattack against the financial institutions of the US in 2012 and 2013. Iran was also blamed for its attack on Saudi Aramco Corporation in 2012, which destroyed almost 30,000 computers. In 2015, the Ukrainian electrical grid was targeted during hybrid warfare, which affected some 225,000 users.[10] These cyberattacks

[6] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, Vol. 56, No. 3 (2011), 573.
[7] Brian Fung, *"How Many Cyberattacks Hit the United States Last Year?" Nextgov*, March 8, 2013, http://www.nextgov.com/cybersecurity/2013/03.
[8] Joseph, "Deterrence and Dissuasion in Cyberspace", 44–71.
[9] National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, D.C.: National Academy of Sciences Press, 2009).
[10] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, D.C.: Atlantic Council, 2013); and Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln: University of Nebraska Press, 2015). On Ukraine, see

raise some important questions about the concept of deterrence in cyberspace. Were these attacks less important, or did they fail to cause significant damage to the targeted states? If the attacks had occurred, then it could be argued that the concept of deterrence has failed in cyberspace. Furthermore, the other side of this picture might be that all these attacks were not devastating and even failed to affect national security substantially. If they had caused significant damage, the targeted states might have retaliated with even more force against the aggressor. But the capability of the states to employ force against the attacker is also an important factor.

The strategic meaning of cyber-attacks is that they can be employed to cause destruction and disruption and to pursue political goals with denial. In this regard, the attacking and target states' capabilities and intentions must be considered to comprehend the concept of deterrence; however, the aforementioned examples clarify the intentions, capabilities, and vulnerabilities as well. To quote some of the examples again here would make the statement clear. For example, In the aftermath of the Stuxnet attacks, Iran disrupted the communications of the US banking system, but was it also sending a signal by hacking the computer system of Saudi Aramco? These techniques are used to remind the target state that its critical infrastructure can be targeted at any time. The Russian and the Chinese intrusions into the US electric system since 2011 may have the same designs.

The Problems of Attribution in Cyberspace

Attribution is a concept that is important when it comes to deterrence in cyberspace. It can be defined as the action of regarding something as being caused by a person or thing. It is a difficult task for any state or individual to locate a person responsible for carrying out attacks in cyberspace. This is why the problem of perfect attribution in cyberspace has consistently remained an issue. In this

Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO, 2015).

regard, Richard Betts agrees that deterrence in cyberspace is quite problematic because of the issues of attribution.[11] This conception may be elaborated further, such that it is quite difficult for a targeted state to identify a person sitting in front of a computer and projecting a virus, and the virus is even unidentifiable. However, any sophisticated mechanism might be applied to identify such malware, but this could be costly and take significant time. Contrary to this, states that are far behind in the field of science and technology and whose technical experts do not meet such standards are even more vulnerable. This suggests that the problem of attribution and states' capabilities in identifying potential attackers in the cyber domain are inextricably linked. Moreover, if we consider the case of states possessing nuclear weapons for direct attribution, Israel remains the only undeclared nuclear-armed state despite possessing nuclear weapons. The isotopic identifiers of the nuclear weapons are well-known, and these can be identified if sincere efforts are made. Such conceptions are not applicable in cyberspace because the malicious codes are difficult to identify as compared to the isotopes of nuclear weapons.

Cyberattacks can be carried out in three different ways, such as through networks, supply chains, and human beings working inside.[12] All these vectors are considered appropriate ways to carry out cyberattacks against potential rivals, aiming to pursue their strategic and political objectives. Joseph Nye claims that "… every serious intrusion into the American military networks has involved human error."[13] Similarly, another example is the Stuxnet attack on the Iranian centrifuges, which were disconnected from the internet. Despite this disconnection, Iran failed to protect its centrifuges from attack. Furthermore, supply chains and human agents are also good means to reach the point. The company supplying electronic requirements and human agents could potentially bridge the gap in the air and cause devastation. The attackers using the internet are

[11] Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terror," *Political Science Quarterly*, Vol. 117, No. 1 (Spring 2002), 19–36.
[12] Joseph, "Deterrence and Dissuasion in Cyberspace", 44–71.
[13] Ibid., 50.

difficult to trace because they can easily hide themselves by raising false flags. They can also use others as proxies for this purpose while maintaining complete denial. To trace the actual position, the target state needs to allocate significant time and resources, which can be unbearable for states that are weak economically and technologically. This is why attribution in the realm of cyberspace is a matter of great concern in international politics. The difficulty in getting prompt and clear information about the attacking parties and their deniability makes the attribution more complicated.

Moreover, to acquire sufficient information about the attackers, states must enhance their technical capabilities with sound economics. Otherwise, states would not be able to identify the attackers and would face not only hardships but would also put their national security and survival at high risk. Powerful states can extend their deterrence against the attacker even based on imperfect attribution, but vulnerable states can only become victims, risking their national security structure.

Deterrence and Dissuasion: The Means

Cyberattacks can potentially be reduced and prevented by employing some mechanisms with full force. These mechanisms are: threat of punishment, denial by defense, entanglement, and norms. The first two mechanisms play a leading role when it comes to deterrence and dissuasion in cyberspace; however, the latter two are equally important, but their application in cyberspace totally depends on the state’s prowess.

Punishment

The biggest problem here is the identification of the attacker. If the identity of the attacker is uncertain, then threats of punishment would be less effective; however, if the attacker is identified, then the conception of punishment would be effective. Another critical issue in this case is how long a state can engage a belligerent attacker's key assets and what the impact of the threat of punishment might be. Deterrence by punishment is a phenomenon that is employed to deter any state from taking any aggressive step that

makes itself stronger and capable of punishing the culprit. For example, Pakistan has nuclear weapons, and it can use them to punish any aggressor if it attacks.

Despite the difficulties in deterrence by punishment, it is critical in deterring attackers in cyberspace. Studies have identified steps that can make retaliatory attacks more feasible in cyberspace. For example, Libicki argues that diplomatic, economic, cyber, physical, and nuclear force are the effective steps that can be employed to deter the attacker in sequence, keeping in mind the increasing belligerence and calculating the damage done.[14] In this context, nuclear arsenals may be the final resort to act against the offender in series.[15] Moreover, deterrence in cyberspace and conventional deterrence work hand in hand, and the former is actually part of the latter. This is how states that are frequently targeted in cyberspace should employ a mixed strategy of deterrence to deter their rivals. The US armed forces have adopted this offensive strategy over time, for example.[16] Despite adopting retaliatory steps to counter the cyberattacks, the problem of attribution is the greatest obstacle on the way of deterrence through punishment. If the problem of attribution is resolved and states identify the attacker, then deterrence through punishment would work, and states might take escalatory steps in sequence.

Denial by Defense

Deterrence by denial is one of the strategies that states employ against their rivals, aiming to prevent any potential attack from the aggressor. In other words, it is a mechanism that can only be employed after building significant military prowess. And without a strong military architecture, states may not be able to apply the concept of deterrence by denial. Moreover, deterrence by denial is to some extent problematic because the equation between offense

[14] Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica, Calif.: RAND Corporation, 2009), 26-29.
[15] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford University Press, 2014), 144–146.
[16] Ibid. 144–146.

and defense is not balanced yet. It means offense distorts defense by blurring the dividing lines between them.[17] In line with this, cyber defense can be improved by investing heavily and adopting new and emerging technologies. For instance, if a state recovers the hacked data or reduces the chances of doing so, making it more difficult and futile for the attacker, this could deter the attacker. The resilience in defending or making the attack more difficult may provoke the attacker to think about the costs and benefits of attacks. Thus, showing resilience while investing heavily in the defense sector and in educating the population is essential to minimizing the chances of notorious actions against critical infrastructure. This strategy would make the attack not only difficult, but also futile and costly for the aggressor. As a result, deterrence by denial becomes more likely.

The concept of deterrence by denial is also applicable once the target state dominates the political situation by destroying tangible and intangible resources. This technique would potentially push the aggressor back while disrupting the cost-benefit equation,[18] which is a driving factor in carrying out cyberattacks. Additionally, if the attacking state is weak and unfamiliar with the sophistication of modern technologies, then the capable target state can minimize the chances and even prevent its critical infrastructure from being attacked. However, the opposite of this conception may devastate the target state. States can also enhance deterrence by denial by improving the performance and sophistication of their critical infrastructure, for example, their health system. Regularizing and updating the system continuously will make it harder for the attacker to carry out cyberattacks. In this way, deterrence by denial can make the attacks futile, disadvantageous, and costly. Moreover, enabling and assisting alliances to protect their infrastructure and update their systems may enhance extended deterrence making deterrence by denial in cyberspace more likely.[19] Thus, deterrence by denial in cyberspace works if the defender makes its

[17] Ablon, Libicki, and Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, Calif.: RAND Corporation, 2014), 31.
[18] Joseph, "Deterrence and Dissuasion in Cyberspace", 44–71.
[19] Franklin D. Kamer, Robert J. Butler, and Catherine Lotrionte, *Cyber, Extended Deterrence, and NATO* (Washington, D.C.: Atlantic Council, May 26, 2016).

unconventional defense system sophisticated to such an extent that the adversary might think a hundred times before carrying out any attack. In addition, the defending state should enhance its defense and undermine the offensive capabilities of its rival, ensuring that the attack would be futile and counterproductive for it.

Entanglement

Conventional and non-conventional deterrence have been playing a central role in deterring rival states. In this context, besides punishment and denial by defense, two other important conceptions of deterrence are of great importance, which are strong means of dissuasion in cyberspace—entanglement and normative anathemas. Just like the other forms of deterrence, entanglement makes the attacking state perceive that the costs of doing so may exceed the benefits, and this kind of behavior could be counterproductive.[20] Such a mechanism contributes to deterrence. If the chances of getting benefits do not exceed the costs, then the chances of attacks are less likely. The following example demonstrates how entanglement works in cyberspace. The Chinese government was reluctant to carry out a cyberattack on the US power grid, fearing greater retaliation from the US and greater economic costs in return because of the increasing economic interdependence suggesting that interdependence could result in mutual destruction.[21]

Thus, the concept of entanglement prevents a state from taking aggressive steps against its rival, fearing that it could be counterproductive to its own interests in times when the international economic system is highly interdependent. Scholars such as Joseph Nye and Robert Keohane had developed such a complex interdependence mechanism to reduce the likelihood of belligerent states carrying out cyberattacks, the concept of economic interdependence across different sectors was proposed in

[20] Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).
[21] Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011), chapter 3.

this regard because economic interdependence and any potential disruption can cause damage to both parties involved.[22]

Entanglement is associated with self-restraint, but it should not be treated as an illusionary case. Regarding this conception, Jervis has argued that "because actors can perceive things that are not there, they can be deterred by figments of their imagination—self-deterrence, if you will." This could be justified by the example that the British had a fear that Germany would wipe out London at the start of a world war.[23] In line with this, one cannot ignore the significance of entanglement in any case, and the term "self-restraint" or "self-deterrence" should not compel one to ignore its importance. Thus, the cost and benefit equation may not be balanced, and assessment of this equation may result from a rational approach. Additionally, states learn over the course of time how to protect their core interests, assess the actual value of their assets, and balance costs and benefits. In this way, states can evaluate the potential risks of cyberattacks by realizing the increasing importance of the internet within the domain of economic interdependence.

Normative Anathemas

The last mechanism that can be employed to deter rivals is norms; however, this concept is closely associated with the soft power and reputation of a state. If a state is quite weak and cannot influence others with its soft power, then this concept may not be effective in deterring others. Contrary to this, a state with strong norms and traditions may be quite cautious about its reputation. Thus, such norms can potentially deter rivals by imposing costs relating to their reputation, causing more damage to their soft power than the reputation they gain from an attack. This can be further explained by giving the example that, if a powerful state attacks a weaker state with nuclear weapons, this could potentially affect soft

[22] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, N.J.: Princeton University Press, 1984).
[23] Robert Jervis, "Deterrence and Perception" *International Security*, Winter1982/1983, Vol. 7, No. 3, 1-28, (p. 14).

power and distort the image of the powerful state; in this case, attribution is important for normative anathemas to work.

The expansion of norms helps in raising the costs of corrupt practices, and normative anthems may work in creating deterrence when it comes to cyberattacks.[24] Some of the steps taken voluntarily by states, for example, the proliferation security initiative with an aim to strengthen the normative values, did enhance the norms over the course of time. Moreover, norms work like a lifecycle, starting small and then expanding their sphere of influence and costs.[25] Moreover, the world is moving towards norm building with respect to cyberspace, though it may take time.[26]

Context of Deterrence in Cyberspace and Options for Pakistan

Pakistan is a developing country and lags far behind in the field of science, technology and innovation as compared to other states. The developed and even developing states have been investing more in this growing field, especially in artificial intelligence, to meet and address future challenges. As a result, these countries, such as the United States, China, Israel, Germany, and others, have significantly improved their cyber security and potentially increased their ability to conduct cyberattacks against their competitors. In this intense security environment, one of the options available for Pakistan is that it must aggressively invest in developing its capabilities in the realm of cyberspace; otherwise, it can become a potential target soon. This is because Pakistan is facing a lot of security challenges, especially in the cyber space, which are becoming more complex and difficult to deal with. Due to this, Pakistan has been trying to improve its deterrent force

[24] Brandon Valeriano and Ryan C. Manness, *Cyber War versus Cyber Reality: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 63.
[25] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization*, Vol. 52, No. 4 (Autumn 1988), 887–917.
[26] Mazanec, *The Evolution of Cyber War*, 205–206.

capabilities in the realm of cyberspace; however, there are huge gaps between its capabilities and the challenges that Islamabad has been facing for decades. Despite this, Pakistan has not succeeded in mitigating and filling the existing gaps. Pakistan has conventional infrastructure, nuclear weapons, and limited scientific capabilities which are not sufficient to create deterrence by denial or punishment.[27]

The most difficult task for weak states is the identification of the attacker because of their poor scientific infrastructure. This is because the attackers, including non-state actors, raise false flags, which make it difficult for states to find out their actual position. This is why high-quality attribution in cyberspace for weak states is quite difficult, and, in the case of Pakistan, it is highly relevant, making its deterrence capability fragile.

Pakistan is thinking about its vulnerabilities in cyberspace and trying to fill the existing gap between its actual capabilities and vulnerabilities; however, the progress in this regard is not encouraging. Pakistan is ranked 7th in the list of states that are highly vulnerable to cyberattacks.[28] Some of the major obstacles are highly relevant in this context. Economic constraints, the government's failure to develop a solid educational policy, a growing trust deficit between institutions, poor governance, and poor academic performance, and so on. Pakistan should, without any hesitation, investigate these issues as early as possible as the world rushes to construct critical infrastructure in response to rising cyberattacks. Spending on cybersecurity is expected to reach 133.7 billion dollars by 2022. Despite facing consistent cyberattacks, Pakistan's investment in cyber security is significantly negligible or at an embryonic stage. For example, in 2018, the banking sector of

[27] Sannia Abdullah, Pakistan's Full-Spectrum Deterrence: Trends and Trajectories, *South Asian Voices*, April 23, 2020. Available at: https://southasianvoices.org/pakistans-full-spectrum-deterrence-trends-and-trajectories/.

[28] The cyber-attacks which are frequently observed against Pakistan include website defacing, data theft from banks and government offices, and denial of service attacks (DoS). The services of state bank of Pakistan were hacked for twenty-one days in 2008.

Pakistan was attacked, and the data of ten banks was available for sale on the dark web.[29]

Furthermore, Pakistan should strive to integrate the state's intelligence agencies in order to obtain the most accurate information about the attackers' whereabouts, as well as build and complicate the infrastructure. Some institutions have taken some steps in this direction, but a strong mechanism is urgently needed. Additionally, Pakistan needs an integrated institutional framework, which could potentially bridge the gap between the institutions and interconnect critical infrastructure and concerned agencies to create cohesion and cooperation. Islamabad should try its level best to educate its masses in general and cybersecurity experts. Sensitization regarding cybersecurity should be the highest priority of the state, and any laxity in this regard could be devastating for Pakistan's security.

If Islamabad invests heavily in the cyber domain and boots up the pool of talent, then its ability to counter aggressive cyberattacks will increase exponentially. However, this should not only be the objective of the government; non-state organizations must also focus on this to improve their capabilities to counter malicious activities. This could further boost the confidence of the state and would be considered a collective effort to defeat Pakistan's enemies. In line with this, advances in science and technology would aid in improving the forensics of the attribution, thereby increasing its deterrence capability.

Furthermore, Pakistan should concentrate on the offense-defense paradigm about its security in cyberspace. In this case, Pakistan should make the rival realize that the cost of attacking would exceed the benefits. This can only be done if it makes its fortification strong enough. This is because the cost-benefit equation pushes the attacker to carry out attacks if this equation is tilted toward benefits. Furthermore, the real assessment of the

[29] Abdullah Rehman Butt and Amna Tauhidi "*Cyber Vulnerabilities of Pakistan*" February 2020. Available at https://casstt.com/post/cyber-vulnerabilities-of-pakistan/147. Accessed on May 8, 2021.

resources and attacking capabilities of the attacker can deter the rival, provided that the attacker is identified. Pakistan should strengthen its surveillance capability. If it does so, then it can hunt the attacker prior to an onslaught. In this way, Pakistan can go beyond its conventional borders to keep itself safe.

The possible option available for Pakistan is to boost its cyber defense. The cyber defense should not be limited to certain sectors, but it should encompass all sectors and make their system sophisticated to such an extent that the attacker should think before targeting any sector inside Pakistan. For example, by ensuring sophisticated cyber hygiene, Pakistan can make its deterrence capability more credible. In this way, Pakistan can not only deter its rivals, but also potentially prevent cyberattacks.[30] If it fails to employ a sophisticated health model, for example, the costs of destructions could go beyond the imagination.

Pakistan should try its best to adopt the model of interdependence, but the equation of interdependence should not be imbalanced. This should be mutual, and the concept of interdependence makes the attacker believe that the attack could also be counterproductive for its own interests because power and interdependence work together.[31] Thus, the concept of interdependence instills fear in the adversary that the attack will harm its own interests and impose more costs than benefits. Economic interdependence can be one of the effective ways to avoid cyberattacks. Any state that tries to boost its economy by building economic alliances with other states through market interactions, research, manufacturing, development, and exchanges would probably also engage in cyberspace interactions, which could benefit both parties. Furthermore, it is extremely difficult to separate markets that rely on technology from those that do not.

[30] Chris C. Demchak and Peter Dombrowski, "Thinking Systemically about Security and Resilience in an Era of Cybered Conflict," in Jean-Loup Richet, ed., *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (Hershey, Pa.: Information Science Reference, 2015), 367–382.
[31] Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).

This is important for the parties involved to understand how to make their state's institutions safe.

Moreover, the deeper economic interdependence for flow of goods and cash between states in the domain of conventional interactions would help states to build a strong and robust interdependence in cyberspace.[32] This strategy is taking strong root in the sense that states are signing free trade agreements and becoming more dependent on each other for many reasons, such as resource scarcity, technological disparities, cash flows, the banking system, etc. These have the potential to bind states and work for mutual benefits. If any state carries out any malicious activity against another state, then it could cause mutual destruction. This further suggests that these types of mutual interactions can tie states together to foster mutually positive norms and behaviors.[33]

Pakistan should try its best to boost up its reputation among the international community and should join international organizations dealing with the cybersecurity issues and other interconnected organizations.[34] Such an approach reinforces the perception that, as a member of an alliance, dealing with cybercrime would ensure that all the members have common interests, and the protection of any member's interests would be considered the protection of all members. Additionally, Pakistan should make its system, infrastructure, and defense much stronger and more sophisticated, making its adversaries believe that the attacks would not cause substantial damage to the critical infrastructure. This can only be done if it ensures the production of brilliant experts in cyber security, educates its entire population in the true sense, and reduces the existing gaps between technology and institutions.

[32] Aaron F. Brantly, "Entanglement in Cyberspace: Minding the Deterrence Gap," *Democracy and Security* 16, No. 3 (2020), 210-233.

[33] Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and Public Policy* Vol. 22, No. 6 (2003), 461-485.

[34] For example, the Budapest Convention on Cybercrime. The US has already started a campaign to join the forty-nine nations. Any new alliance system can be built with an aim to deal only cybercrimes. In the same vein, Pakistan should endeavor to build and join such alliances system dealing with cybercrimes.

Conclusion

Deterrence in cyberspace is quite perplexing because of the nature of rival engagement and the problem of attribution. However, the growing technology and its sophistication have made deterrence in cyberspace relevant, and this could get even more prominence in the foreseeable future in the presence of a complex web of adversaries. Moreover, states employ various mechanisms to deter their rivals in cyberspace, and, among those strategies, the threat of punishment is relatively less effective as compared to others, for example, denial by defense and entanglement. This is because states can build infrastructure and military prowess to such an extent that attacks by other states or non-state actors are considered futile and costly. In other words, if an attack is carried out, then it may not cause damage to the target state. But instead, it would be counterproductive. Moreover, the combination of these strategies could further reinforce the concept of deterrence in cyberspace.

Pakistan is a developing country and lags far behind in the fields of science and technology. Investing in and expanding its scientific capabilities would help improve attribution forensics while increasing deterrence capability. Also, for Islamabad, it must invest heavily in making its infrastructure resilient and building a formidable defense, realizing that the costs of attacks would exceed the benefits. In this way, Pakistan can keep itself safe in the domain of cyberspace and improve its capabilities relating to deterrence in cyberspace.