Prophets of Cyber War: Examining the Role of Pakistan's Private Sector in a Strategic Cyber Context

Hammad Salik[1]and Rao Ibrahim Zahid[2]

Abstract

Developed nations have historically leveraged the productivity and efficiency of the private sector to drive R&D and growth in several sectors. This, in turn, has been used as a driver of national economic, diplomatic, and military power. The same is true for the cyber domain, where the private sector has made significant contributions to cyber defence, development of offensive cyber capabilities, and support for cyber operations. Developing nations struggle to follow a similar path due to several challenges. A prerequisite to solving these challenges is an accurate understanding of the strategic problems before tackling them effectively to avoid wasting scarce resources, a viscous constraint for developing nations. The reality states must acknowledge that deterrence has failed to dissuade adversaries from taking aggressive actions in cyberspace. This is a direct result of two factors. One, cyberspace is interconnected, implying that the terrain is continuously updated and contact with the adversary is constant. Two, states have realized

[1] Hammad Salik is a consultant to the Prime Minister's Task Force on Knowledge Economy (Pakistan) and member advisory of the Strategic Warfare Group (SWG).
[2] Rao Ibrahim Zahid is a consultant to the Prime Minister's Task Force on Knowledge Economy (Pakistan) and member advisory Strategic Warfare Group (SWG).

that they can manage strategic gains through cyberspace by conducting cyber offensive operations with effects below the threshold of armed conflict. This is significant as activity below the threshold carries a risk of escalation, which is non-existent. Hence, this is an attractive avenue for states pursuing a redistribution of power in the international system. Developing states such as Pakistan must incorporate the implications of this understanding before designing any national strategy or policy for cyberspace, including policies that can leverage the private sector to meet these Challenges.

Keywords: Offensive Cyber Operations; Private Sector Combatant Groups; Cyber Deterrence; Persistent Engagement, Cyber Strategy

Introduction

The military sector has always been home to significant innovation. World War -II events set out a prime example of how innovations such as radars, jet engines, blood plasma transfusion, cameras, and electronic computers, were born purely out of the necessity to survive. Private corporations are commonly known as "Prophets of War."[3] Such as Lockheed Martin, Northrop Grumman, Raytheon, Amazon Web Services, and Huawei have served as drivers of innovation, economic growth, and national power for developed nations. Although the development and employment of offensive cyber capabilities and operations fall in the military domain, private corporations and defence

[3] Kelly Krebaum, "Capital from Carnage: An Analysis of the Military-Industrial Complex," *ESSAI*, Vol.13, no.1 (2015), 23. Prophets of War" is an expression used to describe the affinity between the military and the private defense sector, which may sway public policy.

contractors have played a pivotal role for developed states. The corporate sector is a critical driving force behind the development of modern cyber security products and tools, with lines blurring between the private, public, and military sectors. Cyber capabilities are being developed rapidly, but the sensitivity of these products and services has led them to be carefully guarded secrets by national governments.

It is only logical then for developing nations to adopt similar practices to augment their cyber capacity and capabilities if they compete. But this is easier said than done as several challenges impede the pursuit of this strategy. A precursor to these challenges is that developing states lack the academic capacity to conduct primary research, which drives an understanding of the challenges themselves. This understanding is critical so that effective solutions can be envisioned. Otherwise, these states may invest scarce resources in solutions that will be ineffective in the long run. Pakistan faces similar challenges, limiting the state's potential to develop and then effectively deploy cyber capabilities that may serve as a driver of national power.

This article first submits the theoretical framework, which serves as the foundational perspective of the analysis of the problem. It then explains the significance of the topic: Why is it significant to understand that a role must be played by the private sector of any state in pursuit of national power in cyberspace? And finally, the article describes the challenges Pakistan faces in embracing a national strategy that successfully realizes the private sector's potential to contribute to national cyber power, which is then leveraged for the propagation of national interests in, from, and through cyberspace.

Theoretical Framework

This theoretical research examines Pakistan's private sector's role in offensive cyber operations through the prism of two theories: *Cyber Persistence* and *Cyber Deterrence*. According to Richard Harknett and

Michael Fischerkeller, cyber persistence theory is based on the premise that "the dominant strategic interaction dynamic in cyberspace is competitive interaction within a definable operational space." [4] The need for this new strategic framework arises from the argument that the strategic framework must align with the realities of the respective strategic environment. A framework cannot be imposed on a strategic environment. But it must be derived from a strategic environment which is possible only after understanding the fundamentals and unique characteristics of the environment. The perspective further implies that these interactions are constant. States are inclined to pursue this strategy because they realize that strategic gains can be achieved through aggressive actions with effects below the threshold of armed conflict. Cyber persistence theory can be viewed as a refutation of the theory of cyber deterrence. The theory of cyber deterrence maintains that a defending state can deter potential hostile cyber activity by influencing another state's decision-making calculus. This influence is based on communicating the ability, and the intention, to impose costs if the adversarial state crosses a specified red line. The potential costs imposed must outweigh any potential gains the adversary expects to reap through aggressive behaviour.[5] The perspective implies that aggressive activity in cyberspace is episodic and can be deterred via coercion. The current dynamics of cyberspace seem to disobey this logic. Extensive empirical evidence indicates that aggressive activity in cyberspace is only increasing in frequency and

[4] Michael Fischerkeller and Richard Harknett, "Cyber Persistence Theory, Intelligence Contests, and Strategic Competition," *Institute for Defense Analyses Alexandria United States,* 2020,Available at: https://apps.dtic.mil/sti/citations/AD1118679 (Accessed on December 12, 2021).

[5] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Security,* Vol.7,no.1(2014), 54–67, doi:10.5038/1944-0472.7.1.5.

intensity despite states developing advanced offensive cyber capabilities.[6]

These theories are two competing arguments and represent starkly different strategic imperatives. The strategic framework of cyber persistence theory aligns more accurately with the environment of cyberspace. There is overwhelming evidence of failing cyber deterrence below the threshold of armed conflict.[7] Failure of deterrence in cyberspace can be attributed to low escalation risks and cumulative strategic gains in return for an aggressive activity.[8] It is essential to understand that adopting the correct strategic imperative is crucial for Pakistan to mitigate issues of domestic workforce and retention, oversight of the private sector, cost of economic inefficiency, and the broad definition of the private sector's role.

The Barons of Cyberspace

The precise understanding of how security can be achieved in cyberspace is yet to be determined. However, before we even scratch the surface, this section puts forth a central argument to answer the question: Is cyber a military domain? The fundamental imperative to reach a mature understanding is that cyber is a strategic environment used to conduct military operations that lead to cumulative strategic gains.[9] What influences these organizing principles to drive military cyber strategy is the perspective that deterrence is not the cornerstone strategy for cyberspace. Still, cyberspace instead is an offensive

[6] Fischerkeller, Michael P., and Richard J. Harknett, "What Is Agreed Competition in Cyberspace?," *Lawfare*, February 19, 2019, Available at: https://www.lawfareblog.com/what-agreed-competition-cyberspace(Accessed on December 12, 2021).
[7] Ibid.5
[8] Ibid.4
[9] Larry Welch, "Cyberspace-The Fifth Operational Domain," *Institute for Defense Analyses Alexandria VA*, 2004, Available at: https://apps.dtic.mil/sti/citations/AD1124078(Accessed on December 12, 2021).

persistent strategic environment.[10] Setting the foundation accurately is essential for ensuring that cyber theory and policy are not derived from the construct of cyber war. Fischerkeller & Harknett[11] It is concluded that cyberspace's security strategy must be separated from notions of coercion, conflict, and military crisis. The logic leading to this conclusion is that the cyberspace environment, as stated before, is defined by a persistent nature of activities rather than an episodic nature of actions.[12]

This is based on the genuine possibility that strategic outcomes and behaviour of states in cyberspace are not captured through coercion and conventional deterrence but motivated by competition. Deterrence in cyberspace is not failing across the board, but it cannot avert the exponentially increasing frequency of cyber-attacks conducted below the threshold of armed conflict. We argue that these attacks are exactly the ones causing a cumulative strategic impact by delegitimizing democratic institutions and processes, eroding our national sources of power - our military capability, political cohesion, and economic prosperity. States are now incentivized to make strategic gains (tactically, operationally, and strategically) in, from, and through cyberspace by engaging in offensive activity short of armed conflict. Therefore, raising the argument that Pakistan's military leadership wrongly categorizes cyberspace as an intelligence contest and calls for a drastic shift from previous thinking. The thought process should be informed by the fact that adversaries are conducting well thought out strategic and sophisticated campaigns that undermine instruments of

[10] Michael Fischerkeller and Richard Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis*, Vol.61, no.3 (2017), 381–93, https://doi.org/10.1016/j.orbis.05.003.

[11] Ibid,3.

[12] Fischerkeller, Michael P.., Harknett, Richard J.., Goldman, Cyber Persistence Subject Matter Expert Emily O, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (United States: Oxford University Press, Incorporated, 2022), 11.

national power and cause a redistribution of power in the international system.[13] Adversarial states are degrading the state's power without deploying traditional military resources and avoiding conflict concurrently.[14] This awareness moves away from the conventional understanding that cyber activity falls under cybercrimes and surprise attacks on critical infrastructures. Lonergan points out that "ongoing behaviour in cyberspace suggests that states perceive a strategic utility in leveraging cyberspace for both intelligence and military purposes."[15]

For Pakistan to achieve cyber military superiority, which is sustained cyber initiatives and is quickly becoming central to maintaining dominance in all conventional military areas, two objectives should inform the core strategy. One freedom of action in, from, and through cyberspace while integrating it with broader strategic initiatives and goals and two, denying adversaries the same freedom of action in cyberspace. It is important to note here that we use the term "superiority," a carefully chosen military doctrinal concept, instead of "dominance." Because we recognize that one cannot dominate cyberspace, superiority can be achieved at a particular time and place to operate and deny the same ability to the adversaries of Pakistan.

---

[13] Hammaad Salik and Ibrahim Zahid, "Pakistan and National Cyber Command: A Strategic Competitive Enabler (part I) – OpEd," *Eurasia Review,* January 24, 2022, Available at: https://www.eurasiareview.com/25012022-pakistan-and-national-cyber-command-a-strategic-competitive-enabler-part-i-oped/(Accessed on January 28, 2021).

[14] Michael Fischerkeller and Richard Harknett, "Persistent Engagement and Tacit Bargaining: A Path toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, Available at: https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace(Accessed on January 28, 2021).

[15] Erica Lonergan, "Cyberspace Is Neither Just an Intelligence Contest nor a Domain of Military Conflict; SolarWinds Shows Us Why It's Both," *Lawfare*, May 12, 2021, Available at: https://www.lawfareblog.com/cyberspace-neither-just-intelligence-contest-nor-domain-military-conflict-solarwinds-shows-us-why(Accessed on January 28, 2021).

"Cyber Pearl Harbor" is one of the most common and familiar analogies used by academics and researchers.[16] This analogy is often misused out of context due to a lack of understanding of this strategic environment. One critical point to register here is that we have not witnessed a cyber-pearl harbor.[17]. Hence, it may be safe to argue that states are abiding by the laws of self-defence codified in the United Nations (UN) charter that ministers these activities as equivalent to an armed attack or acts of war, legitimizing the right of self-defence.[18] We conclude that Pakistan may never witness a cyber-pearl harbor during peacetime.[19] Adversarial states have concluded that they do not need to risk escalation by engaging in such activity to diminish Pakistan's national power. They are simply engaging in the aggressive activity below the threshold of armed conflict where escalation risks are non-existent, and the deterrence doctrine is inapplicable. This set of circumstances calls for a strategy of constantly competing against a malicious activity as it cannot be avoided. Such a strategy will require the development of cyber capabilities at scale in Pakistan. This, in turn, will only be possible if the private sector contributes to R&D and support at scale.

[16] Jeremy Straub, "Defining, Evaluating, Preparing for and Responding to a Cyber Pearl Harbor," *Cornell University*, 2021, Available at: http://arxiv.org/abs/2103.07662(Accessed on January 28, 2021)."Cyber Pearl Harbor" is a catastrophic cyber-attack on a nation-state's critical infrastructure that deals a tremendous psychological blow to the general population in addition to causing massive damage".

[17] Valeriano Brandon and Ryan C. Maness, "How We Stopped Worrying about Cyber Doom and Started Collecting Data." *Politics and Governance*, Vol.6, no.2 (2018), 49–60, https://doi.org/10.17645/pag.v6i2.1368.

[18] Gray Christine, "International Law and the Use of Force," *Oxford University Press*, 2004.

[19] Hammaad Salik and Ibrahim Zahid, "Pakistan and National Cyber Command: A Strategic Competitive Enabler (part II) – OpEd," *Eurasia Review*, January 31, 2022, Available at: https://www.eurasiareview.com/31012022-pakistan-and-national-cyber-command-a-strategic-competitive-enabler-part-ii-oped/?cv=1 (Accessed on February 4,2022)

Issues of Domestic Workforce and Retention

Cyber workforce challenges are the most existential for the military sector. Coupling that with offensive cyber operational challenges opens a new Pandora's Box because it requires intense training to create these cyber warriors who can successfully execute these operations. Professional human resources are also needed to develop effective tools and technologies. There is already a significant shortage of cyber security professionals in Pakistan partly because educational institutions have only recently adopted this domain as a core area of technology research and have struggled to keep pace with the growing need for cyber talent.[20]

The current approach to military hiring needs a drastic change from an individual level to a more robust corporate staffing model in which the private sector can be employed to provide crucial contributions by filling staffing needs. It makes sense to vet individuals from a military perspective before allowing them access to sensitive information. However, the most acute challenges that Pakistan's military faces are finding, hiring, and retaining relevant cyber professionals across the spectrum of cyber capability development, support, and operations. This holds for the military more than intelligence agencies or federal ministries because of the secrecy around the cyber domain.[21] Secondly, even if the military can hire and train an individual at its great expense to become highly proficient in offensive cyber operations, retention will always remain a challenge.

[20] APP, "President Alvi Inaugurates Pakistan's First-Ever Cyber Security Academy," *Geo News,* November 23, 2021, Available at: https://www.geo.tv/latest/383844-president-alvi-inaugurates-pakistans-first-ever-cyber-security-academy-in-islamabad(Accessed on December 8,2021).

[21] David Barno and Nora Bensahel, "The 'Force of the Future' and the Fate of the United States Military," *The Atlantic*, November 5, 2015, Available at: https://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/(Accessed on December 8,2021).

Thirdly, the private sector offers more attractive and alluring compensation at the very least two or three times the military's basic compensation.

On top of that, the commercial sector offers flexible working conditions and the prospect of rapid career advancements.[22] States such as the U.S., China, and Israel, have specific and extensive programmes to fill lingering skilled workforce gaps as part of the remedy.[23] Pakistan's military fails to do so. We must find ways to seamlessly move our skilled cyber workforce between the public, private, and military sectors. Furthermore, it fails to invest in the right areas, such as cyber capacity-building efforts, primarily due to economic constraints and ill efforts on its borders by neighboring states. A better understanding of state interests, analysis of the shortfall of cyber capacity, and a broader discussion around the magnitude of the problem in developing and maintaining offensive cyber teams will shed light on whether, how, and in what capacity the private sector can be leveraged for such functions. Suppose the military cannot solve the retention issue timely. In that case, it may find itself in a challenging position to rely on the private sector for exceedingly sensitive support roles to conduct cyber operations. Irv Lachow and Taylor Grossman accurately state, "There is a vast difference between *choosing* to use the private sector and *needing* to use the private sector."[24]

[22] Cory Bennet, "NSA Staffers Rake in Silicon Valley Cash," *The Hill,* Feb. 2018.
[23] Morgan Chalfant, "Army Leaders Launch Program to Recruit More Cyber Warriors," *The Hill*, December 5, 2017, Available at: https://thehill.com/policy/cybersecurity/363349-army-leaders-launch-program-to-recruit-more-cyber-warriors(Accessed on December 8,2021).
[24] Herbert Lin and Amy Zegart, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019), 388.

Oversight Issues in Private Sector

If Pakistan is to employ the private sector for offensive cyber operations, it must first tackle many obstacles. The first and foremost would be to bridge the gap between academia, industry, and the government.[25] Second, as discussed in the earlier section, there is a shortage of cyber expertise not only at the federal government level but also in the private sector. The third is the concern that no proper contracting model exists. Pakistan released its first National Cyber security Policy in 2021, a step in the right direction but policy-wise, highly flawed and missing core constituent components.[26]

Moreover, it barely scratches the topic of public-private partnerships. National-level projects and initiatives fall under the Planning Commission of Pakistan or Public Sector Development Projects, which are awarded to contractors via an open bidding process. Unlike countries like the U.S., where laws and regulations are in place to limit the transfer of technology, enforce export control, and enforce standards over contractors, or China, where state capitalism and control prohibits undesirable outcomes - for Pakistan, establishing technical liaisons in the form of contracting mechanisms and hiring relevant contracting officers as subject matter experts will be a challenge. Cyber-related contracts can be effectively, legally, and ethically managed only by overcoming this challenge.

The complexity, scope, and unique challenges that cyber offensive operations pose, accompanied by the shortage of cyber expertise in Pakistan, give birth to three significant risks. One is the

[25] Muhammad Naseer, "Bridging the Gap between Academia and Industry," *The Express Tribune*, June 11, 2015.
[26] Soumik Ghosh, "Pakistan's New Cyber Policy: Welcome, but Flaws Remain," *Bankinfo Security*, August 12, 2021, Available at: https://www.bankinfosecurity.asia/pakistans-new-cyber-policy-welcome-but-flaws-remain-a-17269(Accessed on December 8,2021).

financial aspect, where a lack of oversight on these projects would deliberately lead to fraud, waste, and abuse, a historical issue faced by all developing nations.[27] The second would be the implementation aspect, where subpar technical expertise and unprofessional leadership often lead to poor project outcomes. Cobb's paradox holds in most cases, where perils of over-commitment and under-delivery with requirements volatility, lack of discipline, process immaturity, and funding instability are quite observable.[28] The third risk that falls in murky waters; is the operational aspect, where a lack of understanding of international and strategic implications of offensive cyber operations coupled with actions undertaken by the private sector may lead to intentional or inadvertent escalations.

International Balance of Power

Private businesses offer advanced cyber tools and weapons for sale to international governments or individuals with strong ties to rogue military regimes for use against other states or their populations.[29] This reality creates alternative patterns of power and authority affecting domestic politics and international dynamics since the cyber environment is often characterized by low barriers to entry for new actors. The proliferation of offensive cyber operations, therefore,

[27] Vaishali Sharma, "Pakistan Debt Crisis Intensifies as Economic Mismanagement Continues Unabated," *The Wire*, February 27, 2021, Available at: https://thewire.in/south-asia/pakistan-debt-crisis-intensifies-as-economic-mismanagement-continues-unabated(Accessed on December 8,2021).

[28] Joseph Carl and George Freeman, "Non stationary Root Causes of Cobb's Paradox," *Defense Acquisition Univ Ft Belvoir, VA,* 2020, Available at: https://apps.dtic.mil/sti/citations/ADA523877(Accessed on December 8,2021).. Cobb's Paradox questions why projects fail despite the management being aware of issues that lead to failure and specific risk mitigation techniques for particular problems

[29] Department of Homeland Security, "Geopolitical Impact on Cyber-Threats-Nation-State-Actors.pdf," *Public-Private Analytics Exchange Program*, 2019, Available at: https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf(Accessed on December 8,2021).

opens up this new seam in cyberspace, which raises a fundamental question: Will the private sector lead to greater global stability by providing a level playing field for states to develop offensive cyber capabilities, or will it further the divide where few cyber powers will dominate others?

Pakistan has limited to almost non-existent offensive cyber capabilities and is highly dependent on the Transfer of Technology in cyberspace. This transfer of technology approach is forced by the lack of technical expertise and economic feasibility.[30] Unfortunately, the development of these capabilities is not embedded in the military structure and broader strategy despite a keen need. In general, states building their entire arsenal of cyber weapons on commercial-off-the-shelf products and services will not be able to compete with advanced players possessing sophisticated cyber capabilities in this domain.

In addition, since wealthier state governments and militaries are now involved in the back-door exploits markets, it forces poorer and less developed countries like Pakistan out of the exchange. Our analysis concludes with two reasons for the failure to adapt to these conditions. Pakistan has minimal cyber resources and an almost non-existent infrastructure to integrate commercial-off-the-shelf (COTS) offensive cyber capabilities with full-scale military and intelligence operations. Second, cyberspace is a dynamic strategic environment with a rapidly changing technology landscape, and offensive cyber operations require intensive and timely intelligence about the intended target. This means a drastic fundamental change in military intelligence planning, strategy, and operations is required.

[30] Nicola Whiting, "Cyberspace Triggers a New Kind of Arms Race," *SIGNAL Magazine*, January 29, 2018, Available at: https://www.afcea.org/content/cyberspace-triggers-new-kind-arms-race(Accessed on December 8,2021).

Role of Private Sector Actors as Combatants

The concept of 'corporate warriors' in the conventional domain is not novel. Instead, security studies academics have extensively researched this subject matter worldwide.[31] Expanding on this concept in the cyber environment, if Pakistan actively employs the private sector to support offensive cyber operations, we are compelled to raise fundamental questions. How can states legitimately draw the lines when private sector actors act as cyber combatants, making them lawful targets of a retaliatory counter-attack? How can we control escalation dynamics and the spillover effects leading to an all-out cyber conflict?[32] Civilians generally are not considered legitimate targets in military conflicts but rather share *hors de combat* status. States are encouraged to follow the principle of, among other things.[33] However, civilians' direct or indirect participation in cyber hostilities or cyber combatant functions invokes this status, making it legitimate for states to respond with force. To understand the roles of states employing the private sector for offensive cyber operations, such as the U.S. and China, we found the role to be more of intelligence gathering, military planning, development of tools and weapons, and operational support rather than direct participation in hostilities or actual combat operations.[34]

[31] Peter Singer,"Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry," *International Security,* Vol.26*,* no. 3(2002), 186–220.

[32] Martin Libicki and Olesya Tkacheva, "Cyberspace Escalation: Ladders or Lattices?" *Cyber Threats and NATO 2030: Horizon Scanning and Analysis 60,* (2020), Available at: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf#page=67(Accessed on December 8, 2021).

[33] International Committee of the Red Cross, "Rule 1. The Principle of Distinction between Civilians and Combatants," *ICRC*, Available at: https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule1 (Accessed February 3, 2022)

[34] Madelyn Wardle, "Offensive Cyber Operations: An Examination of Their Revolutionary Capabilities," *Wright State University,* 2021, Available at: https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?clear=10&p10_accession_num=wright1620995515559657(Accessed February 3, 2022).

States are already employing private sector services in "proxy war" scenarios in cyberspace. This enables nation-states to deny any state involvement. Iran can be identified, allegedly, as the top offender for leveraging private cyber actors to augment its national cyber capabilities that sometimes even rival the United States, China, Russia, and the United Kingdom.[35] The Chinese government allegedly conducts large-scale espionage activities and intellectual property theft at scale through a wide range of actors.[36] Furthermore, China has positioned itself as a geostrategic competitor with targeted investments in emerging technologies. It uses overt legal behaviour to invest in enterprises to supplant American and European advantage to be in the lead for upcoming technological developments. China is also influencing global design and engineering standards in its favor by positioning itself as the world's leading manufacturer and distributor of Information Technology (IT) equipment.

The Russian government has also allegedly involved the private sector, hacktivist groups, and Advanced Persistent Threats (APTs) in conducting offensive cyber operations, psyops, and subversion activities on its behalf. These activities cause a redistribution of power in the international system by eroding faith in its adversary's national institutions.[37] Russia's cyberspace operations demonstrate its role as more of a geostrategic agitator. Russian private sector actors as combatants can be traced in Russia-Ukraine and Russia-Georgia cyber

[35] Jordan Brunner, "Iran Has Built an Army of Cyber-Proxies," *The Tower,* Available at: http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/(Accessed February 3, 2022).

[36] Ethan Gutmann, "Hacker Nation: China's Cyber Assault," *World Affairs ,* Vol.173, no. 1(2010), 70–79.

[37] Tim Maurer, "Cyber Proxies and Crisis in Ukraine," Cyber War in Perspective: Russian Aggression against Ukraine, edited by Geers, K., *Tallinn: NATO CCD COE Publications,* (2015), 79–86.

war events.[38] The employment of proxies to shift and redistribute the relevant power and maintain plausible deniability of such operations further increases uncertainty in attribution, enabling states to avoid retaliation against their actions.

One important concept that should be central when envisioning the role of Pakistan's private sector as combatants are mentioned in the theoretical framework; 'persistent engagement' adversaries continually engage in low-level attacks, below the threshold of armed conflict, against Pakistan's military, society, and economy, cumulatively eroding its national power sources. "Persistent engagement"[39] Acknowledges the fact that adversaries will not be degraded in a single strike or a single episode. It further implies that threat actors will not cease aggressive activity immediately; hence, the defending state will have to engage adversaries persistently to define acceptable behaviour. The emphasis on "engagement" accentuates its need to be done instantaneously. The fundamental operational impetus of Pakistan's cyber forces should be established on two concepts - enabling and acting.

The concept of enablement concentrates on the synergy between Government institutions and departments, international partners and allies, and the corporate sector by contributing to threat intelligence, early warning systems, information sharing mechanisms, and human resources. Therefore, enabling and equipping Pakistan's cyber forces with the ability to compete and win in cyberspace. The argument driving

[38] Geers, Kenneth, "Cyber War in Perspective: Russian Aggression Against Ukraine,"*CCDCOE*, Available at: https://play.google.com/store/books/details?id=UJ2mnQAACAAJ, (Accessed February 3, 2022).

[39] Jacquelyn Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare,* May 10, 2019, Available at: https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy(Accessed February 3, 2022).

this idea is that no one entity can practically hold all the authorities, capabilities, resources, and most critically, all the acuity required for operational persistence. The second concept, acting - emphasizes when authorized to execute a spectrum of offensive and defensive mission-critical operations. This notion permits competition in, though, and from cyberspace to yield outcomes like discomfiting the adversary, inducing mistrust in their capabilities, forcing a redistribution of resources required by the need to shift from an offense centric to a defence-centric operational outlook, jeopardizing the cohesion and coordination among institutions, strategic planning, and actual operations. This should act as the blueprint for Pakistan's cyber forces (operational war fighters) on how they should be operationalized in the cyber environment and cooperate with other institutional components of Pakistan

The Cost of Economic Inefficiency

The Public Sector Development Programme (PSDP) report of 2021-2022 includes six projects focused on the word "cyber".[40] Examining the PC-Is of these projects, we identified the absence of a consistent and coherent nature of cyber security risk assessment and investment optimization research from the documentation. Furthermore, the feasibility of the projects from technical and financial perspectives and the metrics by which security can be measured and evaluated to validate the investment decisions were also incorrect or absent. National-level projects and initiatives need to align with the implications of cyberspace, which imply the constant nature of the contact, universal interconnectedness, the dominance of persistence which is strategic as a factor motivated by the terrain of cyberspace, and accurate analysis of the environment, which suggests that: cyberspace is a terrain which frequently iterates and to defend and

[40] Planning Commission-Ministry of Planning, "Public Sector Development Programme 2021-22," *Development & Special Initiatives, Government of Pakistan*, 2021, Available at: https://www.pc.gov.pk/uploads/archives/PSDP_2021-22.pdf (Accessed February 3, 2022).

grow national power, actors must be persistently engaged, and the initiative of this competition must be seized and retained. An effort to gain initiative when competing will be necessary to achieve security in this strategic space.

These initiatives may be the tactical, operational, and technical outcomes of accurate anticipation of adversarial actions in the context of exploiting cyber vulnerabilities.[41] The core strategic question that leadership in Pakistan should ponder while examining National level projects should be: How do we secure national assets and achieve cyber superiority while being in constant contact with the adversary, ally, private sector, and individuals, all of whom are operationally persistent? The measure of effectiveness in evaluating these projects should be the anticipation of exploiting cyber-related vulnerabilities, and the decision-making model should indefinitely be constant and flexible. Concurrently, an understanding is required of the escalation dynamics of the strategic cyber environment and its ramifications for national interests advanced through winning or supporting de-escalation outcomes. The capabilities development these national initiatives should include must be adaptive to preempt the exploitation of vulnerabilities: Across the spectrum from resiliency, defence, active defence, and offense (tactical, strategic, and operational).

It is worrisome that the design and objectives of these projects do not align with the strategic requirements of cyberspace. Therefore, they will eventually not align with the national needs of Pakistan. This pays homage to the challenge discussed earlier; a correct

[41] Combined Action Group, "How Understanding Cyberspace as a Strategic Environment Should Drive Cyber Capabilities and Operations," *U.S. Cyber Command & NSA*, 2018, Available at: https://nsarchive.gwu.edu/sites/default/files/documents/6560991/National-Security-Archive-2-USCYBERCOM-How.pdf (Accessed December 16, 2022)

understanding of the strategic cyberspace environment is required to make the right investment decisions

The proliferation of Cyber Weapons and Global Stability

Understanding the proliferation of cyber capabilities via the private sector is a tenor for policymakers and academics because of their resultant effects on global stability, implications in fueling the cyber arms race, and exploring critical facets of the ecosystem that facilitates the proliferation of offensive cyber capability.[42] Theoretically, cyber proliferation leads to a greater likelihood of cyber conflicts, conflict escalations, restricting a state's freedom of action, erosion of strategic power, and systematic redistribution of national power. However, substantial empirical data is unavailable around this domain; much of cyberspace is shrouded in secrecy, challenging data collection.[43] The lack of a clear proliferation framework in cyberspace and increasing destabilizing potential of cyber capabilities contributes to making this debate often moribund. The study undertaken by Anthony Craig[44] demonstrates the correlation between cyber threats and the development of military cyber capabilities to understand the proliferation of cyber weapons. States susceptible to cyber threats are most motivated to develop the operational capacity to defend and retaliate against any future aggression.

[42] Robert Morgus and Max Smeets and Trey Herr, "Countering the Proliferation of Offensive Cyber Capabilities," *The Global Commission on the Stability of Cyberspace,* 2017, Available at: https://cyberstability.org/wp-content/uploads/2017:12(Accessed December 16, 2022)

[43] Kello Lucas, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol.38, no. 2 (2013), 7–40, https://doi.org/10.1162/isec_a_00138.

[44] "Understanding the Proliferation of Cyber Capabilities," *Council on Foreign Relations*, Available at: https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities (Accessed Feb. 2, 2022)

However, this is just one of many factors. States have also realized that they can make strategic gains below the threshold of armed conflict, placing interventions such as arms control agreements and traditional counter proliferation models as an infeasible path.[45] Richard Harknett and Michael Fischer keller make a valid point and best describe this as tacitly "agreed competition."[46] This competition will lead to consistent expectations of acceptable and unacceptable behaviour in the strategic cyberspace environment by facilitating actions and interactions between adversaries fueled by a strategic opportunity.[47] This opportunity is one of advancing national interests while circumventing any escalation risks. Similar actions to advance national interests would otherwise present a cost in the physical domain. This approach will lead to greater global stability by providing a level playing field for states to develop offensive cyber capabilities and create an environment of cyber restraint and stability by promoting the gap between acceptable and unacceptable behaviour. Other non-favorable outcomes would be tilted towards greater instability where few cyber powers will dominate others. Despite the balance of power distribution by wide accessibility of capabilities, this will also lead to greater instability due to the lack of deterrence.[48]

Conceptualizing the Development of a Cyber Effective Private Sector

As stated in earlier sections, Pakistan must concentrate on two core concepts for developing a cyber-effective private sector: enablement and acting. The private sector must be cultivated so that it can enable other stakeholders to act in, from, and through cyberspace, for the

[45] Ibid.17.
[46] Ibid.11.
[47] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity,* Vol. 5, no.1(2019), 34, https://doi.org/10.1093/cybsec/tyz008.
[48] Herbert Lin and Amy Zegart, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019), 395

entire spectrum of cyberspace operations. In instances where enabling resources are needed, such as threat intelligence, early warning systems, information sharing mechanisms, development of code, and human resources, and the private sector should be positioned to act as a practical resource cache and promote cyber security workforce development to build a robust and sustainable pipeline of skills. At the same time, actions of the private sector itself should be limited to national cyber defence, national cyber capacity-building efforts, cyber emergency response, and national cyber resilience. If the private sector is directly involved in any offensive cyber operations, it may likely become the target for a counterattack in cyberspace.

At the core, the private sector's development must be envisioned at the national policy level. A revision of the national cyber policy is required to better align with the current cyberspace environment and meet the challenges faced by Pakistan. In 2007, when Estonia was subjected to unprecedented cyber-attacks, policymakers recognized it as an opportunity to redraft the national security strategy and the national cyber security policy.[49]These policy transformations led to the emergence of national organizations such as the Estonian Informatics Centre (EIC), CERT-EE, and the Department of Critical Information Infrastructure Protection (CIIP).[50] These organizations led to a revolution in the Estonian cyber landscape, and the country is now considered Europe's Cooperative Cyber Defence Centre of Excellence in (CCDCOE). Similar public sector initiatives in Pakistan will pave the way for developing an enabling private sector. Furthermore, the policy should focus on developing and enforcing minimum cyber security standards, security by design practices, and industry best practices for

[49] Czosseck, C., Ottis, R., & Talihärm, A.-M, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *International Journal of Cyber Warfare and Terrorism (IJCWT)*, Vol.1, no.1 (2011), 24–34, https://doi.org/10.4018/ijcwt.2011010103

[50] Ibid.47.

any private and public sector entities that operate IT infrastructure in any shape or form. This will increase the country's demand for cyber security resources, especially human resources. To meet this demand, the public sector should finance and license private sector cyber security organizations (start-ups) so that they are awarded the status of 'cyber auditors.' These start-ups may provide cyber auditing, cyber risk assessment, penetration testing, and risk mitigation services to other private firms and public sector entities on behalf of the public sector. These services will be required by private firms and public entities so that they may meet national policy requirements. This will also lead to skilled cyber human resources training and development.

Another area that should be stimulated to improve the private sector in terms of cyber effectiveness in Pakistan is academia and scholarship. A prime example of private sector academia contributing to combating national cyber challenges is the National Centre of Academic Excellence (CAE) initiative in the U.S. Currently, two iterations of the CAE programme are being nurtured by the U.S. government; the CAE-Cyber Defence (CAE-CD) and the CAE-Cyber Operations (CAE-CO). The fundamental difference between the two is that CAE-CD programmes focus on cyber policy and risk mitigation skills, whereas the latter focuses on cyber operational skills and training.[51] The academic requirements and modules of these programmes are specifically designed by the Department of Homeland Security and the National Security Agency so that graduates of these programmes can be inducted into the pursuit of national cyber objectives. Iran follows a similar programme of nurtured cyber academics, allegedly. There are speculations that the Islamic

[51] Crumpler, William, and James A. Lewis, "The Cybersecurity Workforce Gap," *Center for Strategic and International Studies (CSIS)*, January 29, 2019, Available at: https://www.csis.org/analysis/cybersecurity-workforce-gap(Accessed December 16, 2022).

Revolutionary Guards Corps (IRGCs) Electronic Warfare and Cyber Defence Organization have tailored academic cyber training programmes offered at the Shahid Beheshti University and the Imam Hossaein University.[52]

Pakistan's military departments and the public sector should adopt a similar strategy. A needs analysis of the cyber skills required to meet cyber challenges must be conducted. This analysis should guide the development of academic programmes that focus on policy and strategy and cyber operational skills. Cyber operational skills include exploitation techniques, secure coding principles, risk mitigation techniques, operating system internals, low-level programming languages, Linux-based systems, networking, computer architecture, data, and cryptography.[53] These programmes should then be sponsored at existing academic institutes, and graduates of these programmes must be offered positions where these skills are required. An attractive career path and remuneration schedule should also be

[52] Gundert, Chohan, and Lesnewich. n.d. "Iran's Hacker Hierarchy Exposed." *Recorded Future Blog*, May 9, 2018, Available at: https://vxug.fakedoma.in/archive/APTs/2018/2018.05.09(1)/Iran's%20hacker%20hierarchy%20exposed.pdf(Accessed December 16, 2022).

[53] George I. Seffers, "National Security Agency Program Fills Critical Cyber Skills Gaps," *Signal Magazine*, June 1, 2014, Available at: https://www.afcea.org/content/national-security-agency-program-fills-critical-cyber-skills-gaps(Accessed December 16, 2022); Chris Krebs, "Why So Many Top Hackers Hail from Russia," *Krebs on Security*, June 22, 2017, Available at: https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/(Accessed December 16, 2022); "Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats*," Intelligence and National Security Alliance*, September ,2015, Available at: https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf(Accessed December 16, 2022);"Cybersecurity Skills Gap Analysis," *Workforce Intelligence Network for Southeast Michigan* , July, 2017, Available at:https://winintelligence.org/wp-content/uploads/2017/07/ FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf; Laura Lee, "Circadence responses to NIST RFI on Cybersecurity workforce education or training," *NIST*, August 2, 2017, Available at: https://www.nist.gov/sites/default/files/documents/2017/08/02/circadence.pdf (Accessed December 16, 2022).

established to motivate individuals to join these programmes. Regarding retention, it should be noted that rather than salary and benefits, cyber professionals rate employers on their ability to offer continuous learning/training opportunities and an exciting work environment. This is especially true for employees working in the cyber operations area, as they require constant certifications and training to keep their skills up to date.[54] For this purpose, public-sponsored certification programmes should also be designed and offered to high-performing individuals.

The public and military sectors should also draw some inspiration from the private defence contractor model in the U.S. This will again entail a needs analysis of the software, tools, and IT platforms required by Pakistan, such as CERTs, Cyber Threat Intelligence (CTI) Platforms, Information Sharing, and Action Coordination Platforms, Sensors, Early Warning Systems, Cyber Deception Platforms, Pen-Testing Tools, Vulnerability Disclosure Platforms etcetera. These needs should be converted into contracts awarded to the private sector. IT firms should be vetted and then motivated to execute these projects. These actions will kick-start the process of including the private sector in the cyber landscape of Pakistan. Once such contracts are filled, the private will have a direction to work in and continue developing more effective and efficient products and services. Pakistan must take several such steps to ensure a cyber-effective private sector. However, the process can only be initiated through changes at the policy level and by ensuring that the public sector finances policy implications.

[54] Timlin, Katrina, and Franklin S. Reeder. n.d, "Recruiting and Retaining Cyber security Ninjas," *CSIS,* Available at: https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas (Accessed June 23, 2022).

Conclusion

As a nation, we need to realize that cyberspace is a very dynamic environment with one critical trend in recent years: The rise of the private sector in developing, maintaining, and protecting national computer assets while also affecting the full range of cyber operations - offensive and defensive. Pakistan's "cyber power" cannot be wielded by one sector, but it must be propagated through different sectors that are tirelessly creating and maintaining Pakistan's cyberspace. Pakistan must escape the deterrence mindset and develop a new strategic perspective for cyberspace. This new perspective must identify the implications of constant contact and interconnectedness. The objective of such a strategy should be to gain the initiative in cyber strategic competition.

We observe boundaries between the public and private sectors. We recognize that these boundaries make sense because they are foundational to our constitution. We must realize that these boundaries are artificial, and our adversaries do not acknowledge these constraints. We also tend to have an intellectual mindset that views peace and warfare as a binary construct. Peace is normal, whereas warfare is an aberration. Pakistan's adversaries view this as a seamless struggle across the entire cyberspace continuum, which will inhibit our ability to act. If we do not follow the trends and the workforce retention and investment patterns of nations that have developed advanced cyber capabilities, we will be excluded from this competition for good. Comprehending these factors and implications will play a pivotal role for Pakistan's government and industry in the coming days. We must overcome the challenges and employ private sector actors to take on more significant roles in offensive cyber operations.