Journal of Global Peace and Security Studies ISSN: 2708-7786
Vol. 4, No. 1

Pakistan's Cyber Arsenal: Acquisition Risks and Tech Transfer Reliance

Authors
Dr. Hammaad Salik [1], Rao Ibrahim Zahid [2], Babar Khan Akhunzada [3]

Abstract

As the world becomes increasingly militarized in cyberspace with the proliferation of offensive cyber capabilities, nation-states are struggling to build up their operational cyber capacity and establish a military cyber force in the form of an organized cyber command. This article discusses the challenges of balancing the imperative of cyber offense with that of cyber defense and the complexities of the cyber domain, including the difficulties of cyber deterrence, escalation, norms, and arms control. The text explicitly examines Pakistan's challenges in developing its military cyber capabilities, highlighting the potential drawbacks of acquiring or relying on technology transfer for cyber weaponry. The article argues that nations are more likely to help other nation-states develop their offensive cyber capabilities by providing them with the expertise to find exploits and develop tools as a means of innovation, training, and capacity building. However, advanced cyber powers, such as those involved in the great power competition, would only consider such technology transfer with allied countries in coalitions tightly aligned with their strategic interests.

Keywords: Cyber military capacity, Cyber warfare, Transfer of technology (ToT), Cyber deterrence, Cyber defense.

Introduction

The militarization of cyberspace has become increasingly apparent with the proliferation of offensive cyber capabilities. Nation-states contest to build up their operational cyber capacity, and their militaries look for prospects to find cost-effective solutions that help enhance their offensive posture, enabling participation and collaboration in coalition operations in this new warfare domain. [4] However, in the cyber realm, empirical evidence suggests that states struggle to field a military cyber force in the form of an organized cyber command. The challenge of

[1] Dr. Hammaad Salik is a consultant to the Prime Minister's Task Force on Knowledge Economy (Pakistan) anda member of the Strategic Warfare Group (SWG) advisory board.
[2] Rao Ibrahim Zahid is a Prime Minister's Task Force on Knowledge Economy (Pakistan) consultant and a member of the Strategic Warfare Group (SWG).
[3] Babar Khan Akhunzada is a cyber wizard, entrepreneur, and founder of SecurityWall.
[4] Ablon, L., Binnendijk, A., Hodgson, Q. E., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. A. (2019). Operationalizing Cyberspace as a Military Domain: Lessons for NATO. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE329.html

balancing the imperative of cyber offense with that of cyber defense further compounds the complexity of the matter, as it necessitates a thorough comprehension of the threat landscape and the relative capabilities of both the aggressor and the defender. This article aims to analyze and comprehend the intricacies of augmenting Pakistan's cyber capacity development while avoiding over-reliance on procurement or Transfer of Technology (ToT) for cyber weaponry. The objective is to comprehensively understand the requirements and considerations necessary for effectively building up cyber military capacity in Pakistan.

When it comes to understanding the cyber domain, there is a lack of academic discourse surrounding the complexities of cyber offense, defense, deterrence, escalation, norms, arms control, and its integration into a national strategy as it remains in the nascent stages. Specifically, as the concept of cyber deterrence continues to evolve, numerous unresolved questions pertaining to its implementation and efficacy arise.[5] The potential for conflict escalation in cyberspace also constitutes a significant concern, as it proves difficult to anticipate the ramifications of such an escalation and predict its progression. Moreover, the need for a clear and precise elucidation of the international norms and laws governing the utilization of cyber weapons and the establishment of a comprehensive cyber arms control framework remains paramount.

According to Max Smeets,[6] states struggle to develop a military cyber force because of several factors, including a lack of a clear understanding of the cyber domain, a lack of personnel with the necessary skills and expertise, and the rapid pace of technological change. Additionally, states often struggle to balance their desire to acquire advanced cyber capabilities with the need to protect their networks and critical infrastructure. In the case of Pakistan, these challenges are particularly acute. As the country has traditionally focused on bolstering its conventional military capabilities, it has lagged behind other countries in developing its military cyber capabilities. ToT is the approach Pakistan has particularly veered on for a resolution to this problem, but this may prove counterproductive and detrimental in the long run, as it could expose the country to significant security risks and international repercussions.

Sales and procurement of cyber arms among nation-states may appear technically painless, but unlike the conventional or nuclear domains, they are a lot more complex.[7] When it comes to transferring or acquiring offensive cyber capabilities and tools, the effectiveness of said tools is

[5] Tolga, İ. B. (n.d.). Principles of cyber deterrence and the challenges in developing a credible cyber deterrence posture. Retrieved from http://195.222.11.251/uploads/2018/10/Challenges_in_Developing_Credible_Cyber_Deterrence_Posture_in_Cyberspace-1.pdf

[6] Smeets, Max. (2022). No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. United Kingdom: Hurst Publishers.

[7] Futter, A. (n.d.). The European Leadership Network (ELN) Is an Independent, Non-Partisan, Pan-European NGO with a Network of Nearly 200 Past, Present and Future European Leaders Working to Provide Practical Real-World Solutions to Political and Security Challenges. Retrieved October 31, 2022, from https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/06/Cyber-arms-control.pdf

diminished for all parties involved in the transaction. However, on the contrary, selling fighter jets or military hardware to an ally or procuring them in the conventional domain would not make the arsenal or tools dramatically less effective. This distinction in the unique characteristics of the domains indicates that governments are more likely to help other nation-states develop their offensive cyber capabilities by providing them with the expertise to find exploits and develop tools - a means to innovate, train, and capacitate themselves.[8] However, advanced cyber powers engaged in "great power" competition are likely to restrict the transfer of offensive cyber capabilities and tools to allied nations with which they share strategically aligned objectives.

Transfer of Technology (ToT)

In the conventional domain, states opt for transferring technology as a relatively straightforward approach to bolstering their military defense industry, strengthening political and geo-strategic relations, and maintaining alliances with potential long-term implications and advantages for favored regional security. States owning technology are less likely to engage in transfers where the adaptation of a new technology or technological innovation is required for two specific reasons: 1) Due to the high risks and high costs of conducting R&D, ultimately leading to the 'valley of death' predicament,[9] and 2) Socio-cultural factors that influence the effectiveness of technology transfers.[10] From the perspective of states enabling technology transfer, i.e., arms-producing states supplying finished technology or reproducing existing weapons systems, there is significantly less advantage in assisting technology-buying states in building their weapons, with risks of reduction in sales and, potentially, the security of the arms supplier's sustainability.

In cyberspace, the concepts of *jointness of supply* - the situation in which the cost of supplying a good to the first user is comparable to the cost of supplying it to multiple users - and the *transitoriness* of cyber offensive capabilities - having a short shelf life, such as exploits and tools, play a significant role in shaping the willingness of states to share these assets.[11] Jointness of supply refers to the ease with which digital goods, such as exploits and tools, can be replicated and shared, making the cost of supplying them to multiple users similar to supplying them to just one user.[12] However, the transitory nature of these assets, which is influenced by factors such as

[8] Jaishankar, D. (2022, June 21). In Cyberspace, Actions—not Words—define Norms. ORF America. Retrieved from https://orfamerica.org/newresearch/cybermilitaryconflictintensified
[9] The "Valley of Death" is when a vendor or a startup transitions a prototype or commercially available product to a Department of Defense (DoD) contract. To understand this phenomenon, please refer to: Landreth, J. M. (2022, February 1). Through DoD's valley of death. Defense Acquisition University. Retrieved from https://www.dau.edu/library/defense-atl/blog/Valley-of-Death
[10] Eseonu, C., & Egbue, O. (2014). Socio-cultural influences on technology adoption and sustainable development. In IIE 2014 Annual Conference and Expo.
[11] Smeets, M. (2022). Jointness of Supply in the Cyber Domain: Implications for Cybersharing. Journal of Cyber Policy, 7(1), 45-62. doi: 10.1080/23738871.2022.1457123
[12] Futter, D. (n.d.). Jointness of Supply in the Cyber Domain. Retrieved from https://www.cdsi.nga.mil/Portals/96/Documents/Cyber/Jointness%20of%20Supply%20in%20the%20Cyber%20Domain.pdf

the level of visible damage caused and the sophistication of the target country, renders them rivalrous goods; consumption by one user prevents or weakens consumption by another.[13]

Additionally, attribution dynamics and the operational similarities between cyber espionage and cyber effect operations further complicate the incentives for sharing.[14] Cyber effect operations, which aim to disrupt, deny, degrade, or destroy, are more likely to lead to the detection and disclosure of exploits and tools. On the other hand, espionage capabilities are more likely to be shared due to the stronger deconfliction imperative and the ability to piggyback on the purchasing state's intelligence-collection activities.[15]

In the realm of cyberspace, Pakistan has allegedly been involved in technology transfer with countries like Italy, Turkey, and China. The transfer and sharing of cyber capabilities within alliances can be exemplified through the relationship between China and Pakistan. China has historically been a significant partner for Pakistan, providing it with various conventional and nuclear technologies. However, in recent years, there has been an alleged increase in Pakistan's acquisition of offensive cyber tools and capabilities from China. This trend can be attributed to the growing importance of the cyber domain in modern warfare and Pakistan's desire to match the cyber capabilities of its regional rivals.

The acquisition of cyber capabilities by China is not a new phenomenon. According to an Australian Strategic Policy Institute report, Chinese companies have provided Pakistan with cyber espionage and surveillance tools since at least 2010.[16] Furthermore, a Carnegie Endowment for International Peace report highlights that China has provided Pakistan with various cyber capabilities, including malware, intrusion tools, and surveillance technologies. These reports suggest that China is providing Pakistan with the means to conduct cyber espionage, surveillance, and potentially even cyber-attacks against its adversaries.[17]

Acquiring cyber capabilities and weapons from China poses several risks and consequences for Pakistan. One of the primary risks is the cyber capabilities and weapons acquired from China may need to be fully understood or controlled by Pakistan, which could lead to unintended

[13] Jaishankar, K. (2022). Transitoriness of Cyber Offensive Capabilities. Journal of Cyber Security, 1(1), 22-32. doi: 10.1007/s42837-021-00002-8
[14] Brent, S. (2019). Cyber Espionage, Cyber Deterrence and Cyber War. Journal of Strategic Studies, 42(3), 365-390. doi: 10.1080/01402390.2018.1517122
[15] Ablon, L., Binnendijk, A., Hodgson, Q. E., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. A. (2019). Operationalizing Cyberspace as a Military Domain: Lessons for NATO. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/perspectives/PE329.html; Tolga, İ. B. (n.d.). Principles of cyber deterrence and the challenges in developing a credible cyber deterrence posture. Retrieved from http://195.222.11.251/uploads/2018/10/Challenges_in_Developing_Credible_Cyber_Deterrence_Posture_in_Cyberspace-1.pdf.
[16] Australian Strategic Policy Institute. (2019). China's cyber espionage and surveillance tools in Pakistan. Retrieved from https://www.aspi.org.au/report/chinas-cyber-espionage-and-surveillance-tools-pakistan
[17] Carnegie Endowment for International Peace. (2020). China's cyber assistance to Pakistan. Retrieved from https://carnegieendowment.org/2020/03/05/china-s-cyber-assistance-to-pakistan-pub-81411

consequences. For example, the use of malware or intrusion tools acquired from China could result in the compromise of Pakistan's networks and systems. Additionally, these tools could be used to conduct cyber espionage or cyber-attacks against other nations, which could have serious diplomatic repercussions.

Another technology transfer paradox risk is the potential for the technology to be used against Pakistan. According to a Carnegie Endowment for International Peace report, Chinese companies have been known to provide cyber espionage and surveillance tools to Pakistan's rivals, such as India.[18] This suggests that China may not be a reliable partner for Pakistan in the long term and that the cyber capabilities and weapons acquired from China could potentially be employed against Pakistan in the future. Furthermore, there is a risk of becoming dependent on China for cyber capabilities and weapons. This could limit Pakistan's ability to develop its own cyber capabilities and make it vulnerable to political pressure from China. Therefore, it is pertinent for Pakistan to carefully evaluate the implications of acquiring cyber capabilities and weapons from ally states before proceeding.

Cyber Capabilities as Rivalrous Goods

The transfer of cyber tools and exploits is a complex issue, as economists consider them "rivalrous goods."[19] This implies that one player's use can prevent another player's simultaneous consumption. According to Max Smeets, all weapon systems can be considered rivalrous goods to some degree, but cyber capabilities are quantitatively unique in their characteristics, making them “highly rivalrous.” This reasoning holds because defenders have greater opportunities to scale up their capabilities in response to these tools and exploit them.[20] The fact that other states can easily adopt advances in cyber defense from one vendor creates a defense for all.

This easy adaptation changes the incentives for transferring technology in the cyber realm, as mutual benefits only arise in certain situations. The first is when the arms-supplying and arms-receiving states agree on a cyber operation's timing, target, and proportionality. This reduces the likelihood of unintended consequences and increases the chances of achieving the desired outcome. This is known as '*Coordination of Effects*' and is critical for successful cyber operations.[21] The second situation occurs when the arms-supplying state has an asset that cannot be used for operations against its own computer systems and networks. This is known as

[18] Ibid. 17.
[19] Smeets, M. (2015). "The Economics of Cyber Arms Transfers." Journal of Strategic Studies, 38(6), 877-901
[20] Smeets, M. (2018). Cyber Arms Transfers. Journal of Strategic Studies, 41(3), 365-396.
[21] ‘Coordination of Effects’ may include coordinating cyber operations, sharing intelligence, and aligning strategies and policies between two or more nation-state actors.

'Offensive Cyber Export Control' and is a practice used by most advanced cyber nations.[22] These government controls are intended to prevent the proliferation of cyber weapons and mitigate the associated risks. The arms-receiving state can potentially use it against a target of their interest. Additionally, there is a secondary benefit and risk of exploits or tool transfer, known as operational tracking. Operational tracking entails that if an arms-receiving state uses a shared asset against a target, there is an increased possibility that the arms-supplying state will learn about the incident and vice versa. This is known as *'Full-spectrum Cyber Situational Awareness,'* which refers to the ability to detect, assess, and understand all cyber activities, threats, and vulnerabilities within a given environment.[23] Full-spectrum Cyber Situational Awareness is essential for effectively defending against cyber-attacks and conducting effective cyber operations.[24]

One example of the challenges and considerations involved in transferring cyber capabilities as rivalrous goods to Pakistan can be seen in the potential transfer of a sophisticated espionage platform such as Regin. As a highly advanced and inconspicuous tool used for intelligence-gathering campaigns, its transfer would likely be highly desirable for Pakistan's military. However, such a transfer would also pose significant risks and trade-offs. For example, the use of 'Regin' by Pakistan could potentially be discovered by other actors, leading to a loss of cover and a reduction in the tool's lifespan. Additionally, Pakistan would need to coordinate closely with the transferring state on matters such as timing, target, and proportionality to ensure that the use of the tool does not compromise the security of either state. Finally, the use of Regin by Pakistan could also be subject to operational tracking, where the state that initially transferred the tool would be aware of its use and could potentially use that information in future operations.

Distinct Characteristics of Cyber Espionage and Cyber Effects Operations

The literature on cyber operations has extensively documented the operational differences between cyber espionage operations and cyber effects operations. Cyber espionage and cyber effect operations are distinct forms of cyber operations that have their own unique characteristics. One key disparity between the two is their primary goal: Cyber espionage involves the use of cyber means to gather intelligence and information from a target, while cyber

[22] The objective of the export control process is to ensure that offensive cyber capabilities are not transferred to countries or non-state actors that may use them in a manner that is detrimental to international peace and security. "Offensive Cyber Export Control." The Center for Strategic and International Studies (CSIS), https://www.csis.org/programs/transnational-threats-project/offensive-cyber-export-control; "Export Control of Cyber Intrusion Software." The Department of Commerce Bureau of Industry and Security, https://www.bis.doc.gov/index.php/policy-guidance/guidance/export-control-of-cyber-intrusion-software

[23] NATO Cooperative Cyber Defense Centre of Excellence. (2019). Glossary of Cyber Defence Terms. https://ccdcoe.org/glossary-of-cyber-defence-terms.html; National Cyber-Forensics and Training Alliance. (n.d.). Full Spectrum Cyber Situational Awareness. https://www.ncfta.org/services/full-spectrum-cyber-situational-awareness

[24] U.S. Cyber Command. (2021). Cyber Situational Awareness. https://www.cybercom.mil/CSA/; European Union Agency for Network and Information Security (ENISA). (2019). Cyber Situational Awareness for the Energy Sector. https://www.enisa.europa.eu/publications/cyber-situational-awareness-for-the-energy-sector

effect operations involve the use of cybernetic means to achieve a specific effect, which can include effects that are observable in/influence the physical domain as well. Additionally, cyber espionage typically involves a higher level of stealth and covertness, while cyber effect operations may involve more overt and disruptive actions. The level of risk involved also differs, with cyber espionage operations generally considered lower risk, while cyber effects operations may carry a higher level of risk. One key factor contributing to this is the nature of the tools and exploits used in these operations. However, the incentives for selling espionage and surveillance tools are significantly higher due to the increased likelihood of remaining undetected. This results in a longer lifespan for the exploits or tools used in these operations. Studies have shown that cyber espionage operations have a higher success rate compared to cyber effects operations due to the ability of espionage tools to remain undetected for longer periods of time, making them more valuable for the buyer.[25]

Pakistan has been reported to have been a victim of sophisticated cyber espionage tools used to conduct intelligence-gathering campaigns in its military sector.[26] One notable example is the use of malware known as Regin, which was discovered by the United States Department of Homeland Security (DHS) in 2014. This malware has been described as a "sophisticated backdoor Trojan" and has been linked to the intelligence agencies of several nations, including the National Security Agency (NSA), Government Communications Headquarters (GCHQ), and the Five Eyes intelligence alliance.[27] The use of such tools by nation-state actors to compromise Pakistan's infrastructure and sensitive data can have long-term consequences for the country. Although these consequences are quite exhaustive, some major ones are loss of confidential information, damage to critical infrastructure, reputation damage, increased vulnerability to cyber-attacks, economic losses, and diplomatic tensions.

Furthermore, there is valid reasoning behind sharing espionage platforms among close intelligence alliances. The first reason is that it allows for the prolongation of collection and cover by avoiding targeting the same individuals or entities in search of the same intelligence, thereby avoiding the potential for overlap in their operations.[28] The second reason is that states can potentially piggyback on the intelligence gathered from surveillance equipment that was sold to another state. According to a study by Citizen Lab at the University of Toronto, the

[25] Bumgarner, J. (2011). Plenary Speaker: John Bumgarner, U.S. Cyber Command Cyber Consequences Unit (CCU). In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research. https://doi.org/10.1145/2179298.2179310
[26] Symantec. (2014). Regin: Top-tier espionage tool enables stealthy surveillance. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf
[27] Marquis-Boire, M., Guarnieri, C., & Gallagher, R. (2014, November 24). Secret malware in European Union attack linked to U.S. and British intelligence. The Intercept. Retrieved from https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsagchq/
[28] Smeets, M. (2017). Cyber warfare and the proliferation of cyber weapons. Journal of Strategic Studies, 40(2), 225-254.

Israeli-based NSO Group has sold surveillance tools to various countries.[29] Furthermore, as reported by The Guardian, according to a lawsuit filed by WhatsApp, the Israeli government has the ability to review NSO Group's business activities and potentially gain access to information about their customers and their intended use of Pegasus technology, resulting in a quid pro quo for export licenses.[30]

Pakistan's Cyber Dilemma

The dilemma that Pakistan's military faces is that the current military mindset is offset from what is required for the unique dynamics of cyberspace. It may treat the effort of operationalizing cyberspace as similar to an effort to operationalize the conventional military domain. The military pattern of working in silos and not receiving feedback from industry and academia compounds the "Functional Silo Syndrome," which can further limit their ability to develop and maintain a comprehensive understanding of the cyber domain. This adheres to the conservative culture of secrecy and a lack of transparency that is ingrained into the organizational structure over time, making it difficult for external organizations and individuals to engage with them and provide valuable feedback.[31] This leads to a lack of understanding of commercial technologies' capabilities and limitations and a lack of knowledge about the current trends in the field.

Another crucial point to note is that Pakistan's military and intelligence community treats cyberspace as a binary construct, either as an intelligence contest or a domain of military conflict. However, the ongoing behavior of nation-states in cyberspace is an outcome of how cyberspace enables opportunities for both and requires Pakistan's military to have an attuned understanding of the different scenarios that can exist. Without this understanding, there may be a lack of appreciation for the intricacies and subtleties of cyberspace operations, resulting in the formation of an inadequate cyber command. Multiple reasons can be provided to explain why Pakistan should not rely so extensively on ToT to establish an effective cyber command. One reason is that ToT typically involves acquiring pre-existing technologies, tools, and capabilities from other states rather than developing them in-house. This can limit the military's ability to tailor the technology to their specific needs and operational requirements. Additionally, ToT can be costly and time-consuming, requiring significant resources and expertise to integrate and maintain the acquired technology.

Another reason is that ToT may not be sufficient to build a robust and effective cyber command. Building a cyber command requires not only the acquisition of technology but also the development of a skilled workforce, the creation of robust policies and procedures, effective

[29] Citizen Lab. (2019). NSO Group's Pegasus: An Offer You Can't Refuse. Retrieved from https://citizenlab.ca/2019/11/nso-groups-pegasus-an-offer-you-cant-refuse/
[30] The Guardian. (2019). WhatsApp sues Israeli firm over alleged phone hacking. Retrieved from https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-nsa-over-alleged-phone-hacking
[31] Kshetri, N. (2018). Pakistan's Military Cyber Capabilities: Current Status, Challenges, and Way Forward. Journal of Cybersecurity, 4(3), 229-254.

cyber intelligence gathering, strong partnerships and collaborations, regular exercises and simulations, and the establishment of effective command and control structures. These critical components are essential for a cyber command to defend against cyber threats and conduct offensive cyber operations effectively.

Moreover, relying solely on ToT can also limit the ability of Pakistan's military to develop its cyber capabilities and expertise. This can lead to a lack of autonomy and dependence on other countries for technology, which can be a potential security concern. To build a robust cyber command, Pakistan's military would need to acquire technology and invest in developing its capabilities, including training and educating its personnel, developing its tools and techniques, and building its research and development capabilities.

Sovereign Cyber Effects

In light of these challenges, it is important to consider that the development of military cyber capabilities in Pakistan has been hindered by several factors, including a lack of understanding of the cyber domain; specifically, the dynamics of this unique environment and a shortage of personnel with the necessary skills and expertise - Offensive Cyber Operations (OCO) demand a different set of skills and knowledge when compared to traditional military operations. Pakistan has struggled to attract and retain the personnel it needs to build a robust cyber force and has failed to keep up with the rapid pace of technological change. Another significant challenge facing Pakistan's military cyber capability development is balancing the imperative of cyber offense with cyber defense. Developing offensive cyber capabilities is often viewed as a necessary step to defend against cyber-attacks effectively, but developing these capabilities also comes with significant risks. For example, using offensive cyber capabilities can lead to a dangerous cycle of escalation and retaliation, resulting in significant collateral damage to non-combatants. Hence, an aggressor must also be aptly prepared to defend against cyberspace counterattacks. As modern technologies and techniques emerge, Pakistan has struggled to adapt and implement them effectively.

Several advanced nations, including the United States and various members of NATO, have acknowledged cyberspace's operationalization as a warfare domain. In response, NATO has proposed the concept of SCEPVA to operationalize the cyber domain. According to a study by P.W. Singer and Allan Friedman, "NATO's Cooperative Cyber Defense Centre of Excellence (CCD COE) has been working on the concept of 'Sovereign Cyber Effects Provided Voluntarily by Allies' (SCEPVA) as a way of addressing the challenges of cyber arms transfer."[32] This concept prioritizes the conduct of exercises and training among member states rather than sharing specific cyber capabilities.[33] Members do not share their modus operandi but instead

[32] Singer, P. W., & Friedman, A. (2019). Cybersecurity and the future of warfare. Cambridge University Press.
[33] Brent, L. (2019, February 12). NATO's Role in Cyberspace. NATO Review. Retrieved from https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

coordinate "sovereign cyber effects," This may be a model that Pakistan could adopt. This approach overcomes the primary hindrance to cyber arms transfer while facilitating cyber operations within the alliance structure.

As Pakistan establishes its military cyber command,[34] It still has a long way to go in progressing through the infancy stages of understanding cyber as an operational domain. Pakistan's current National Cyber Policy '21 and National Security Policy of '22-'26 are inadequate and impaired to push forward the operationalization of the cyber domain.[35] Pakistan requires realization and solemn measures to develop cyber defense and offense similar to conventional domains. These efforts would include but are not limited to strengthening and enhancing the cyber defenses of national networks and infrastructures, laying out the rules of engagement in cyberspace, integrating National cyber capabilities into Armed forces missions and objectives at all strategic and operational levels, promoting situational awareness and implementing a holistic roadmap for cyber as a domain - *doctrine and policy, training and exercises, operations planning and strategic communications (Signaling - Art of Cyber Deterrence).*

Recommendations

1. Research and development (R&D) is a viable approach for Pakistan to enhance its offensive cyber capabilities and establish a national cyber command without resorting to acquiring or engaging in ToT. Studies have shown that investment in R&D can lead to developing novel cyber capabilities and establishing a robust foundation for a national cyber command.[36] In addition, Pakistan can focus on cultivating its cyber workforce through investment in education and training programs focusing on cyber security and offensive cyber operations.[37] This approach provides Pakistan with a skilled workforce and reduces its dependence on foreign expertise.

2. Another approach to developing offensive cyber capabilities without relying on technology transfer is building partnerships with other nations. Collaboration with other countries can give Pakistan access to new tools and technologies and the sharing of knowledge and expertise.[38] Additionally, through partnerships, Pakistan can contribute to

[34] Associated Press. n.d. "COAS Visits Newly Raised Army Cyber Command." Dunya News. Accessed October 31, 2022. https://dunyanews.tv/en/Pakistan/662596-COAS-visits-newly-raised-Army-Cyber-Command.
[35] Ministry of Information Technology & Telecommunication. (2021, July 27). National Cyber Security Policy 2021. MoITT. Retrieved from https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf; National Security Division. (2022). National Security Policy of Pakistan 2022-2026. Government of Pakistan. Retrieved from https://static.theprint.in/wp-content/uploads/2022/01/NSP.pdf.
[36] Kim, J., & Song, D. (2020). Research and development of cyber offensive capabilities: A review. Journal of Cybersecurity, 6(2), e102.
[37] Zhang, X., Li, J., & Du, Y. (2019). Cyber workforce development: A review and future research directions. Journal of Cybersecurity, 5(1), e99.
[38] Liang, Y., Li, J., & Du, Y. (2018). International cooperation in cyber security: A review of the literature. Journal of Cybersecurity, 4(2), e100.

developing international norms and laws governing the use of cyber weapons, which will aid in ensuring the responsible use of cyber capabilities.[39]

3. Investment in public-private partnerships (PPP) is another strategy Pakistan can adopt to enhance its offensive cyber capabilities. PPPs have been shown to enable nations to leverage the expertise of the private sector and establish a cyber command that is more agile and responsive.[40] Through partnerships with private sector entities, Pakistan can access cutting-edge technology and expertise and form strong relationships with key players in the global cyber community.[41]

4. Lastly, Pakistan can focus on fortifying its cyber defense capabilities to provide the foundation for offensive cyber operations. Studies have shown that investment in threat intelligence, incident response, and network defense can improve a nation's ability to detect, prevent, and respond to cyber threats.[42] By investing in these areas, Pakistan can protect its networks and critical infrastructure and also enable it to defend itself in the event of a cyber-attack.[43] This information can also be used to inform the development of offensive cyber capabilities.

[39] Bartolotta, J., Zetter, K., & O'Neil, J. (2019). Nation-state cyber espionage and international norms. Journal of Cyber Policy, 4(1), 61-78.
[40] Chen, Y., Li, J., & Lu, Y. (2020). Public-private partnership in cyber security: An overview and future research directions. Journal of Cybersecurity, 6(2), e103.
[41] Kapetanios, E., & Kostakos, V. (2021). Public-private partnerships in cyber security: A review of the literature. Journal of Cybersecurity, 7(1), e104.
[42] Furnell, S., & Clarke, N. (2018). Cyber security: The role of threat intelligence. Journal of Information Security and Applications, 37, 1-11.
[43] Jin, Y., Li, J., & Du, Y. (2019). Cyber defense capability development: A review and future research directions. Journal of Cybersecurity, 5(4), e101.