OPEN ACCESS

Margalla Papers

Volume: 26, Number: 2 (2022)

Journal Homepage: https://margallapapers.ndu.edu.pk/site

e-ISSN: 2789-7028 **ISSN-L:** 1999-2297

RESEARCH PAPER

India's Growing Cyber Partnerships and Challenges for Pakistan

AUTHOR(S): Ammad Farooq and Ahmad Ali

Mr Ammad Farooq is the head of the Cyber Security Programme at the Institute of Regional Studies, Islamabad. Mr Ahmad Ali has worked with the Cyber Security Programme at the Institute of Regional Studies, Islamabad. He holds certifications from Stimson Centre and Chatham House. Authors can be reached at ammadengineer@hotmail.com.

KEYWORDS: Cyber Security, Cyber-attacks, Cyber Posture, Pakistan, India.

DOI: https://doi.org/10.54690/margallapapers.26.2.121

BIBLIOGRAPHY ENTRY

Farooq, Ammad and Ahmad Ali. 2022. "India's Growing Cyber Partnerships and Challenges for Pakistan." *Margalla Papers* 26 (2): 49-61.

ARTICLE HISTORY

- **Received:** July 5, 2022
- **Peer Reviewed:** September 5, 2022
- **Revised:** October 8, 2022
- **Accepted:** November 15, 2022

COMPETING INTEREST: The author(s) have declared that no competing interest exists.

DATA AVAILABILITY: All relevant data are within the paper and its supporting information files.

INDIA'S GROWING CYBER PARTNERSHIPS AND CHALLENGES FOR PAKISTAN

Ammad Farooq and Ahmad Ali[*]

Abstract

With the emergence of new technologies, the potential of cyberspace is immense; however, the growing number of cyber-attacks on states' critical infrastructure has highlighted the need for cyber security. Although it is challenging to achieve foolproof security, states can maximise safety in the cyber domain through cyber partnerships with technologically advanced countries. This study finds that India is maximising its cyber security while enhancing its offensive cyber capabilities by concluding agreements with most cyber-secure states. Furthermore, India's cyber capabilities are more focused on Pakistan due to longstanding tensions between the two countries. On the other hand, Pakistan lacks focus on cyber security and has yet to take sufficient measures. Pakistan can maximise its cyber security through technological advancements and taking advantage of friendly countries' expertise in the cyber security domain. Cyber security partnerships will strengthen Pakistan against threats emerging from state and non-state actors. Following a qualitative exploratory research design, this study provides a detailed understanding of India's growing cyber security partnership and cyber posture, besides highlighting Pakistan's approach towards cyber security.

Keywords: Cyber Security, Cyber-attacks, Cyber Posture, Pakistan, India.

Introduction

Information and Communication Technologies (ICTs) play an important role in almost all aspects of modern-day society. It has opened doors of opportunities for people in economic, commercial and social domains leading to socio-economic development worldwide. With the advent of new technologies, the potential of cyberspace appears to be limitless. However, the malicious use of ICTs in cyberspace raises concerns among individuals, organisations and states. It is not only affecting macroeconomic growth and social development by posing financial and security risks to enterprises and individuals but also undermining national security. Additionally, cyberspace refers to as the fifth domain of warfare.[1] Over time, threats associated with cyberspace have increased in number as well as sophistication.

Threats associated with cyberspace are transnational; thus, international cooperation and engagement are vital to counter these threats, such as phishing

[*]Mr Ammad Farooq is the head of Cyber Security Programme at the Institute of Regional Studies, Islamabad. Mr Ahmad Ali has worked with the Cyber Security Programme at the Institute of Regional Studies, Islamabad. He holds certifications from Stimson Center and Chatham House. Authors can be reached at ammadengineer@hotmail.com.

campaigns, data theft, cyber espionage, etc. India is concluding agreements with advanced countries to strengthen the cyber security of its digital assets while enhancing its offensive cyber capabilities. It places Pakistan in a tough spot as it neither prioritizes cyber security nor concludes agreements with like-minded countries to strengthen its cyber security capabilities. Therefore, this study aims to analyse India's growing cyber security partnerships and cyber posture and explore implications and the way forward for Pakistan in terms of cyber security. It also examines the cyber threat landscape and the steps taken by Pakistan to improve its cyber security.

While writing this research paper, several limitations have been faced as the study area is less explored, and scholars have barely worked on related topics, so it is somewhat difficult to find scholarly references. Secondly, it is difficult to find accurate data while analysing India's cyber security agreements with other countries leading to a prolonged writing process. Finally, in some cases, the terms of India's cyber contracts were not made public, so it was somewhat challenging to connect the dots.

India's Cyber Partnerships

Considering that cyber threats cannot be countered without cooperation with other countries, India is partnering with technologically advanced countries to counter cyber threats.[2] Besides defensive cyber capabilities, India is also aspirant to acquire offensive cyber capabilities. In this regard, New Delhi has already signed agreements with several countries, including Israel, the US, France, Singapore, the UK, Qatar, Australia, Japan and Russia.[3] Moreover, the Quadrilateral Security Dialogue (QUAD) also considers cyber security an important area of cooperation.[4] It is important to note that most countries India is partnering with have been placed in the second tier regarding cyber power.[5] These countries are sufficiently capable in seven categories: strategy, doctrine, cyber-intelligence, global leadership in cyberspace affairs, cyber security, cyber resilience and, most importantly, offensive cyber capabilities.[6]

a) Indo-Israel Partnership

In July 2017, Narendra Modi, Prime Minister of India, visited Israel, and both countries were willing to cooperate in the cyber security domain.[7] Since then, several agreements have been signed between India and Israel to enhance cooperation in the cyber domain. Later, during his visit to India in January 2018, Israeli Prime Minister Netanyahu signed a Memorandum of Understanding (MoU) on cyber security aimed at enhancing cooperation to secure the cyberspace of both countries. Cyber security cooperation grew in the year 2020 when the Indian Computer Emergency Response Team (CERT-In) signed an agreement with Israel's National Directorate of Cybersecurity (INCD) to materialise operational cooperation in the domain of cyber security.[8] This agreement aimed at multilayer cooperation, including exchanging technology, capacity building, and strengthening defence against sophisticated cyber-attacks.[9] India and Israel have been nourishing each other's innovation and Research and Development (R&D) abilities. Also, India is a significant market for Israeli products

and technologies. It has been a major source of market potential for Israeli companies, providing them access to a large and growing consumer base.[10]

Israel is way ahead of many countries vis-à-vis offensive cyber capabilities. Most recently, in June 2022, India and Israel signed an agreement to boost defence cooperation, and the statement released by Tel Aviv particularly talked about the exchange of advanced technology.[11] It is important to note that Israel's Niv, Shalev and Omri (NSO) Group developed the world's most powerful cyberweapon 'Pegasus,' which reportedly sold to many friendly countries, including India, the US, and the UAE.[12] NSO Group is a cyber-intelligence company that develops and sells offensive cyber-surveillance technology to governments and law enforcement agencies worldwide. Pegasus spyware has the capability to access the data of any electronic device, record phone calls, and even plant or alter the information on the victim's device.[13] Reportedly, India procured this spyware as part of the Indo-Israel weapons deal signed in 2017.[14] Since 2017, both countries have finalised several agreements to boost defence and cyberspace cooperation. Therefore, considering these agreements and the sale of Pegasus spyware, it is most likely that Israel will exchange offensive cyber capabilities with India in the future.

b) India and QUAD Cooperation

QUAD is an informal arrangement between four countries: the US, Japan, India, and Australia. It aims at cooperation in economics, health, cyber security, and emerging technologies.[15] In May 2022, QUAD members highlighted the need to work together in the cyber domain during the Tokyo summit. This cyber security partnership mainly focuses on cyber resilience to counter cyber threats and protect partner countries' Critical Information Infrastructure (CII).[16] As part of the arrangement, the Computer Emergency Response Teams (CERT) of these four countries would strengthen information sharing and initiate programs to train relevant stakeholders to counter cyber threats.

QUAD cyber security partnership also seeks to formulate joint cyber principles and coordinate cyber security standards for obtaining software.[17] Furthermore, it has not overlooked critical and emerging technologies; thus, another working group was established to cover this area. Many QUAD initiatives, like the supply chain of semiconductors and 5G technology, have a first-hand effect on cyber security. These initiatives focus on strengthening cyber security of member countries and countering cyber threats emerging from China.[18] However, the possibility of cooperation to enhance offensive cyber capabilities is foreseeable, considering that the future of global disputes is likely to have a robust cyber factor.

c) India-Australia Partnership

Apart from a collective cyber security arrangement, India has signed a bilateral agreement with Australia to enhance cooperation in the cyber security domain.[19] Both countries finalised a comprehensive strategic partnership that identified various fields

of cooperation. Under this partnership, foreign ministers of India and Australia signed Framework Arrangement on Cyber and Cyber-Enabled Critical Technologies Cooperation.[20] This cyber agreement focuses on addressing cyber security challenges, promoting digital trade, and harnessing critical technologies, including Artificial Intelligence (AI) and robotics.

d) **India-UK Partnership**

Furthermore, cyberspace cooperation between India and the UK dates to November 2012, when both countries jointly agreed to counter threats to international security emanating from cyberspace.[21] Later in 2015, both countries agreed to establish a cyber security centre as part of the larger defence and international security partnership.[22] In 2018, India signed an agreement with the UK to enhance cyber security cooperation. As a result of this agreement, four working groups were established to cover areas including incident response, digital economy, cybercrimes and cyber diplomacy. Both countries agreed to share technologies and equipment to advance military capacity.[23] In May 2021, the premiers of India and the UK held a virtual summit in which vision 2030 was launched, identifying cyberspace as an important area of cooperation. Later, in April 2022, Prime Minister Boris Johnson visited India and reiterated UK's commitment to strengthen India's cyber security capabilities.[24]

e) **India-US Partnership**

The US has emerged as the top cyber power in the world, with superior offensive and defensive cyber capabilities. In this context, India is partnering with the US not to advance its cyber security but also to acquire offensive cyber capabilities. India-US cooperation in the cyber security domain was initiated in 2001. Subsequently, both countries established India-US Cyber Security Forum that focused on enhancing capabilities for critical infrastructure security. The forum included cyber security, cyber forensics, and collaboration between the US and India Law and Enforcement Agencies (LEAs) in countering cybercrimes. Later, in 2004, the US National Cyber Security Division and CERT-In agreed to jointly develop expertise in artifact analysis, i.e., analysing traces of computer viruses and exchanging information under the umbrella of India-US Cyber Security Forum.[25]

In 2011, India signed MoU with the US to exchange expertise and critical information on cyber security, which was later renewed in 2018. This agreement included coordination between government organisations responsible for cyber security of their respective countries.[26] Later in 2016, India and the US held the 5th Cyber Dialogue that covered most aspects of cyber security, including assistance in building robust cyber security capabilities, followed by a cyber framework and defence cooperation agreement. The defence cooperation prioritised six areas of collaboration, including cyberspace.[27] As part of this agreement, the US has offered to provide training to Indian military personnel on cyber warfare and the role of AI in future wars.[28] Additionally, two more cyber security agreements were signed between New Delhi and Washington in 2017 and 2018.

The overall framework of India-US cyber partnership includes sharing of information regarding cyber threats and cyber-attacks on time, development of a joint mechanism to eliminate cyber threats practically, promotion of cybersecurity-related R&D, enhancing cooperation among organisations responsible for cyber security, improving capabilities of LEAs to prosecute cyber criminals, strengthening India's CII, conduct joint exercises to test cyber vulnerabilities, and establishment of sub-groups to explore other areas of cooperation under cyber security including the dual-use technologies.[29]

f) India-Russia Partnership

India has strong economic, defence and diplomatic relations with Russia; however, cyberspace is an unheeded domain of cooperation. In 2016, Russian President Putin signed a cyber security agreement during his visit to India. Interestingly, the text of this agreement remains classified; however, experts believe it is an open-ended agreement with cooperation ranging from cyber security to military-to-military cooperation on cyber defence.[30] Russia has strong offensive cyber capabilities, and Kremlin is often accused of cyber-attacks by the US and its allies. However, Russia remains on the frontline when it comes to making an effort to establish international cyber norms. India is likely to benefit from cyber cooperation with Russia in three ways, including strengthening its cyber security capabilities, acquiring offensive cyber capabilities, and finally, India will get a voice in the form of Russia while establishing global cyber norms.

g) India-Japan Partnership

India and Japan are part of QUAD, and cyber security is an important area of cooperation among member states. Apart from this arrangement, both countries have signed a bilateral agreement to enhance cooperation in cyber security. In October 2020, New Delhi and Tokyo finalised a cyber security agreement, which was signed due to the 13th India-Japan Foreign Ministers' Strategic Dialogue.[31] It focuses on capacity building to secure CII, conducting cyber security R&D, and cooperation in the domain of AI and the Internet of Things (IoT). Later in January 2021, both countries signed another agreement to bolster cooperation in the ICT field, including 5G.[32] This agreement was most likely the result of China's tensions with Japan and India and to counter Beijing's monopoly in the 5G technology market. Furthermore, both countries continue to hold cyber dialogues every few years. The most recent, in June 2022, focused on cyber security policies, cyber threat landscape, 5G policies, and capacity-building matters. A study conducted by cyber security firm Comparitech termed Japan the most cyber secure country, and India is likely to benefit from Japan's best practices in the cyber domain.

h) India-EU Partnership

The EU published its cyber security strategy on December 16, 2020, highlighting the importance of strengthening cyber security cooperation with other countries.[33] India is one of the important strategic partners of the EU, which is why the EU and India

continue to conduct cyber dialogues to share best practices and strengthen cyber security cooperation. In fact, two days before the release of the EU's cyber security strategy, the EU conducted a sixth cyber dialogue with India that highlighted the need to develop tools to minimise the threat of cyber conflict.[34] Emerging cyber-related technologies, preventing cyber conflict and capacity building were given significant importance in the dialogue. As a result of this dialogue, the EU and India agreed to continue cooperation in the cyber domain. They decided to hold the seventh EU-India cyber dialogue in the coming years. Furthermore, the EU and India established a Joint ICT Working Group in the aftermath of the fifteenth EU-India Summit held in July 2020. This joint working group was established to enhance cooperation on cyber security, AI, and data governance.[35] Apart from these initiatives, India-EU Connectivity Partnership and India-EU Strategic Partnership: A Roadmap to 2025 highlight cyber security as an important area of cooperation.[36] These initiatives would help India mitigate cyber threats and make it an essential stakeholder in establishing global cyber security laws and norms.

Cyber Security Partnership and Minimising the Threat of Cyber Non-state Actors

Cyber Non-state Actors (CNSAs) have emerged as crucial actors in this globalised world and have a substantial impact on states. Due to the proliferation of cyber technology, CNSAs can threaten a country's national security in many ways. They have political and financial motivations for launching cyber-attacks on the state's critical infrastructure. Although several CNSAs are operating worldwide, some target states for their policies. Anonymous Group is a prime example of that.[37] Anonymous Group is known for targeting states for their policies, and most recently, this group targeted Russian critical information infrastructure for waging war against Ukraine.[38] Similarly, it targeted Iranian cyber infrastructure due to Tehran's mishandling of hijab protests.[39] These instances portray that CNSAs can target states whenever they like, which is problematic as it can lead to a situation where states are unable to protect their infrastructure and data from being compromised. It can have serious implications for the security and stability of states. However, cyber partnerships among states can somehow minimise this threat by understanding the threats they face and developing strategies to counter them.

It is important to note that multiple CNSAs are operating worldwide to undermine states' national security. The most concerning thing is that these CNSAs can decide to attack states according to their assumption of justice. These instances signal that CNSAs have emerged as a threat to states' national security; however, cyber security partnerships among countries can be helpful to minimise this threat. Apart from bilateral cooperation, there is limited international cooperation in the cyber domain due to a lack of international agreement. It is why CNSAs are not held accountable for launching cyber-attacks on other states. However, keeping the lack of international consensus in view, cyber security partnerships with other states can minimise this threat. In case of a cyber-attack on a state, the victim state would be able to request

other like-minded states to put an end to malicious activities being conducted from the state's territory. States can ensure such arrangements through bilateral agreements in the cyber domain.[40] India is concluding cyber security agreements with other states is likely to counter the threat of CNSAs in both ways mentioned above.

India's Cyber Posture

India is increasingly focusing on enhancing its cyber security capabilities and, at the same time, integrating cyberspace with other dimensions of warfare. India's Joint Doctrine for Indian Armed Forces (2017) highlights cyberspace as a crucial national territory along with air, land, maritime and space. [41] This doctrine recognises cyberspace's importance for conducting operations to have an edge over an adversary. In the 2017-Joint Doctrine, India introduced a new military posture by adding a triad consisting of cyberspace, outer space, and special operations. India is preparing to engage its adversaries, particularly Pakistan, in these domains in the sense that cyberspace and outer space will be used to have information superiority so that special operations can be conducted to achieve strategic goals. [42] Additionally, the doctrine discusses establishing the Defence Cyber Agency (DCA), which was later formed in 2019.

In 2018, India released Land Warfare Doctrine (LWD), a supplement to the 2017-Joint Doctrine for Indian Armed Forces. LWD is related explicitly to advancing existing cyber warfare capabilities and developing superior information warfare capabilities. [43] India recognises the importance of cyberspace operations, including degradation or destruction of computer and information systems, so it has been strengthening the security of its digital assets and focusing on building offensive cyber capabilities to undermine its adversaries. According to a renowned internet security company, McAfee, many countries are developing offensive cyber capabilities, and India is one of them.[44] Owing to the longstanding rivalry between New Delhi and Islamabad, Pakistan is likely to be the prime target of Indian cyber-attacks. Additionally, in 2021, an influential think tank, International Institute of Strategic Studies (IISS), released a report saying that Indian cyber capabilities are focused on Pakistan and are very effective. [45] India has considerable cyber capabilities to undermine the security of Pakistan in cyberspace.

Challenges for Pakistan

Pakistan falls into the list of one of the most vulnerable countries to cyber-attacks. The report released by IISS indicates that Indian cyber capabilities are more focused on Pakistan due to longstanding tensions between the two countries.[46] In light of these indications and cyber-attacks on Pakistan, including on the Federal Board of Revenue (FBR), it can be said that Pakistan might face difficulty in countering India's offensive cyber operations.[47] There have been cyber security incidents in the past that pose a direct threat to the national security of Pakistan. India keeps on defacing government websites, especially on Pakistan's Independence Day. It is important to note that a report released by a Chinese cyber security firm revealed that India launched

massive cyber-attacks against sensitive military departments of China and Pakistan to steal critical information.[48] In 2021, India organised a spying operation against high-ranking Pakistani officials using Pegasus spyware.[49] It also indicates that this spyware is being used by Indian intelligence to gather sensitive information. A similar incident happened in 2020 when Indian intelligence agencies tried to steal critical data by targeting networks of the Pakistan military.

The Snowden leaks revealed that Pakistan was the second most spied country by the US National Security Agency (NSA) after Iran.[50] In August 2021, Pakistan's most crucial institution FBR experienced one of the worst cyber-attacks directed towards the institution's data centres.[51] This cyber-attack disrupted FBR services for over seventy-two hours while sensitive data was stolen. The initial investigation of the attack suggested that Indian hackers were involved in such a massive cyber-attack on FBR.[52] According to a study conducted by a cyber security firm, Comparitech, Pakistan was ranked among the least cyber-secure countries worldwide.[53] All these factors suggest that Pakistan is already vulnerable to cyber-attacks, and India's growing cyber capabilities have made a threat to Pakistan's national security more imminent.

Pakistan's Approach towards Cyber Security

In recent years, Pakistan has taken several necessary steps to enhance its security in the cyber domain. In this context, Pakistan released its first-ever and much-needed National Cyber Security Policy (NCSP) in 2021, including various action points; however, a few steps have been taken to implement NCSP practically. Apart from this, Pakistan adopted the Prevention of Electronic Crime Act (PECA) in 2016, which covers a variety of cyber security matters, but the issue lies with an enforcement mechanism.[54] Two private CERTs are already operating in Pakistan, and Khyber Pakhtunkhwa province has also established a cyber emergency response centre to counter the growing cyber threats. Furthermore, Pakistan has established the National Centre for Cyber Security (NCCS), which promotes research in the field of cybersecurity.[55] Also, in February 2022, Pakistan approved the Cloud First Policy and the Personal Data Protection Bill, another crucial step to move the country into the digital world.[56] In 2021, Pakistan Telecommunication Authority (PTA) launched a CERT portal for the telecom sector. PTA also established Cyber Vigilance Division responsible for regulating unauthorised IP addresses, capacity-building in the industrial sector, and providing guidelines to counter cyber threats. Pakistan is also taking steps to embrace new technologies. For the first time, in 2019, Pakistan utilised blockchain technology in the banking sector to attract remittances. In 2022, the State Bank of Pakistan (SBP) directed all banks to embrace blockchain technology to make financial transactions instant and secure.[57]

Similarly, the Special Technology Zones Authority (STZA) is a government-run agency established in 2019. The mission of STZA is to promote the development and adoption of advanced technology in Pakistan. STZA provides a wide range of services to blockchain, AI and cyber security companies. It serves as a facilitator for companies to

gain access to local markets, resources, and networks. STZA has helped develop Pakistan's technology sector through its services and created attractive investment opportunities.[58] Furthermore, STZA has been instrumental in developing Pakistan's cyber security policy. Its services have helped to promote innovation and development in the country and have enabled Pakistan to become a more attractive destination for investors in technology.

Apart from these initiatives, academia is also working towards securitising cyber security in Pakistan. Think Tanks of Pakistan continue to organise seminars, roundtable discussions and conferences on cyber security and what steps Pakistan can take to ensure its cyber security. It is important to note that private and public entities highlight cyber security issues in Pakistan, but none of these have discussed cyber partnerships with advanced countries. Despite all these initiatives, the most crucial aspect, i.e., collaboration with developed countries in the cyber domain, is not the top priority of relevant stakeholders in Pakistan.

Pakistan has barely concluded any cyber security agreements with other countries; thus, cybersecurity cooperation is seemingly not the top priority on Pakistan's agenda. Although Pakistan released its comprehensive NCSP in 2021, it lags in implementing it. NSCP advocates concluding agreements with friendly and capable states to maximise cyber security; however, the primary hurdle in achieving this objective is the lack of a central organisation responsible for secure cyberspace. Pakistan has also not been able to establish a national CERT which makes prospects of cyber security partnerships with other countries very limited.[59] Cyber Governance Policy Committee (CGPC) is responsible for national cyber security issues; however, things are considerably vague regarding this committee's members and functions. Pakistan's limited focus on cyber security is another reason for the lack of cooperation with other countries. Apart from this, political instability is also a factor due to which the cyber security domain has not been given the necessary importance.

Way Forward for Pakistan

It is a fact that no country can achieve foolproof security against cyber-attacks. However, what countries can do is maximise cyber security to limit attacks on their digital assets. Maximisation of cyber security is the only way for Pakistan to counter Indian threats in cyberspace. Pakistan is unlikely to maximise its cyber security without cooperation with other countries having advanced cyber security capabilities. The foremost step that Pakistan should take is to establish a point of contact in the form of national CERT so that there is no restraint in materialising cyber security cooperation with other countries. Secondly, the Ministry of Information Technology and Communication (MoITT) and the Ministry of Foreign Affairs (MoFA) should coordinate and identify like-minded countries with advanced cyber security capabilities so that Pakistan can initiate negotiations with them to materialise cyber security agreements. China and Russia can be suitable options for cyber security cooperation as both countries have been identified as major cyber powers after the US.

Thirdly, Pakistan should not miss the opportunity of becoming an important stakeholder in establishing international cyberspace norms by keeping itself distinct from organisations and countries that are working towards negotiating a treaty to establish rules and norms for secure cyberspace. Fourth, the Pakistan military should not overlook the developments of the Indian military in cyberspace as India is preparing to equip its forces to wage cyber warfare. Pakistan army has recently raised cyber command; however, it is necessary to include the air force and navy, making it a tri-services command. Fifth, Pakistan should establish a blockchain centre like NCCS to explore this technology as it can create secure and immutable records of data and transactions, making it difficult for hackers to access or alter data. Finally, considering the possible exchange of offensive cyber capabilities between India and other states, particularly Israel, Pakistan must look for alternate options like China, Russia, the US, EU and the UK to acquire cyber capabilities to counter India's apparent pre-eminence in this domain.

Conclusion

In a nutshell, ICTs are playing an important role in socio-economic development. However, at the same time, such technologies' malicious use threatens individuals, businesses and states. It is difficult to achieve foolproof cyber security; however, maximising security against cyber threats is possible. Many countries, including India, are doing that by concluding agreements with technologically advanced countries. India has signed over 39 multilateral agreements and 54 MoUs on cyberspace with various countries, including the US, Israel, Japan, the UK, Australia, and Russia.[60] Additionally, India is part of informal security arrangements like QUAD that see cyber security as an important area of cooperation. This kind of cyber partnership is essential for security against hostile states and non-state actors in the cyber domain. India is maximising its cyber security and taking initiatives to acquire offensive cyber capabilities. It is likely that India's already existing cyber agreements with other countries also include assistance in building offensive cyber capabilities. India's cyber posture suggests that New Delhi integrates the cyber domain in military operations to engage its potential adversaries. Experts believe that India's cyber capabilities are focused on Pakistan. There is no doubt that India has been involved in several cyber-attacks on Pakistan, which is why Pakistan needs to take proactive measures in the cyber domain.

References

[1] "War in the fifth domain," *The Economist*, July 1, 2010. Available at https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain (Accessed August 2022).

[2] Leilah Elmokadem and Saumyaa Naidu, "Mapping of India's Cyber Security-Related Bilateral Agreements," *The Centre for Internet Society*, December 29, 2016. Available at https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016 (Accessed August 2022).

[3] Ibid.

[4] Ibid.

[5] "Cyber Capabilities and National Power: A Net Assessment," *International Institute for Strategic Studies (IISS)*, June 28, 2021. Available at https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two (Accessed August 2022).

[6] Mark Pomerleau, "Who can match the US as a cyber superpower? No one," *C4ISRNET*, June 29, 2021. Available at https://www.c4isrnet.com/cyber/2021/06/28/who-can-match-the-us-as-a-cyber-superpower-no-one/ (Accessed August 2022).

[7] Madhulika Srikumar, "India and Israel's cyber security partnership could be a potential game changer," *Observer Research Foundation (ORF)*, July 10, 2017. Available at https://www.orfonline.org/research/india-israel-cyber-security-partnership-potential-game-changer/ (Accessed August 2022).

[8] Divyanshu Jindal, "Why India-Israel Cyber Partnership Worries Pakistan & China," *Modern Diplomacy*, July 11, 2022. Available at https://moderndiplomacy.eu/2022/07/11/why-india-israel-cyber-partnership-worries-pakistan-china/ (Accessed August 2022).

[9] Jessica Haworth, "Israel and India sign cybersecurity agreement to protect against Covid-19 cyber-attacks," *The Daily Swig*, July 22, 2020. Available at https://portswigger.net/daily-swig/israel-and-india-sign-cybersecurity-agreement-to-protect-against-covid-19-cyber-attacks (Accessed August 2022).

[10] Divyanshu Jindal, "Why India-Israel Cyber Partnership Worries Pakistan & China," *Modern Diplomacy*, July 11, 2022. Available at https://moderndiplomacy.eu/2022/07/11/why-india-israel-cyber-partnership-worries-pakistan-china/ (Accessed August 2022).

[11] "India, Israel agree to enhance defence cooperation," *The Indian Express*, June 2, 2022. Available at https://indianexpress.com/ article/india/india-israel-agree-enhance-defence-cooperation-7949268/ (Accessed August 2022).

[12] Dana Priest, Craig Timberg and Souad Mekhennet, "Private Israeli spyware used to hack cellphones of journalists, activists worldwide," *The Washington Post*, July 18, 2021. Available at https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ (Accessed August 2022).

[13] Hala Marshood and Jai Vipra, "Pegasus and How the Israeli State Militarises Cyber Technology," *News Click*, August 17, 2021. Available at https://www.newsclick.in/pegasus-how-israeli-state-militarises-cyber-technology (Accessed August 2022).

[14] "India bought Israeli Pegasus spyware as part of weapons deal: NYT," *Al Jazeera*, January 29, 2022. Available at https://www.aljazeera.com/news/2022/1/29/india-bought-israeli-pegasus-spyware-as-part-of-weapon-deal-nyt (Accessed August 2022).

[15] Aamna Rafiq, "Quad Partnership for Emerging Technologies and Cybersecurity," *Institute of Strategic Studies, Islamabad*, August 22, 2022. Available at https://issi.org.pk/issue-brief-on-quad-partnership-for-emerging-technologies-and-cybersecurity/ (Accessed August 2022).

[16] The White House, *FACT SHEET: Quad Leaders' Tokyo Summit 2022* (Washington D.C.: Press Release, 2022). Available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/ (Accessed November 2022).

[17] Ibid.

[18] Krutika Patil, "Quad and Cybersecurity," *Manohar Parrikar Institute for Defence Studies and Analyses*, June 22, 2022. Available at https://idsa.in/idsacomments/quad-and-cybersecurity-kpatil-220622 (Accessed August 2022).

[19] Shristi Pukhrem and Siddharth Singh, "Australia-India Relations: What to Expect From the Modi-Morrison Virtual Summit," *The Diplomat*, June 03, 2020. Available at https://thediplomat.com/2020/06/australia-india-relations-what-to-expect-from-the-modi-morrison-virtual-summit/ (Accessed August 2022).

[20] Department of Foreign Affairs and Trade, Joint Statement on a Comprehensive Strategic Partnership between Republic of India and Australia (Canberra: Press Release, 2020). Available at https://www.dfat.gov.au/geo/india/joint-statement-comprehensive-strategic-partnership-between-republic-india-and-australia (Accessed August 2022).

[21] Rahul Roy Chaudhury, "India–UK cybersecurity cooperation: the way forward," *International Institute of Strategic Studies (IISS)*, November 22, 2019. Available at https://www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation (Accessed August 2022).

[22] UK Government, *UK-India Defence and International Security Partnership* (London: Press Release, 2015). Available at https://www.gov.uk/government/news/uk-india-defence-and-international-security-partnership (Accessed August 2022).

[23] Ministry of External Affairs, *UK-India Joint Statement during the visit of Prime Minister to UK* (New Delhi: Press Release, 2018). Available at https://www.mea.gov.in/bilateral-documents.htm?dtl/29829/UKIndia+Joint+Statement+during+ the+visit+of+Prime+Minister+to+UK+April+18+2018 (Accessed August 2022).

[24] "India and UK commit to cyber partnership for vision 2030," *Economic Times*, April 25, 2022. Available at https://telecom.economictimes.indiatimes.com/news/india-and-uk-commit-to-cyber-partnership-for-vision-2030/91066308 (Accessed August 2022).

[25] Rahul Prakash, "India-US cyber relations," *Observer Research Foundation (ORF),"* January 14, 2014. Available at https://www.orfonline.org/research/india-us-cyber-relations/ (Accessed August 2022).

[26] U.S. Department of Homeland Security, *United States and India Sign Cybersecurity Agreement* (Washington D.C.: Press Release, 2011). Available at https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement (Accessed November 2022).

[27] Joshua T. White, "After the foundational agreements: An agenda for US-India defense and security cooperation," *Brookings*, January 2021. Available at https://www.brookings.edu/research/after-the-foundational-agreements-an-agenda-for-us-india-defense-and-security-cooperation/ (Accessed November 2022).

[28] Shishir Gupta, "Indian military personnel to train in US on cybersecurity, command in the offing," Hindustan Times, June 30, 2021. Available at https://www.hindustantimes.com/india-news/india-military-personnel-to-train-in-us-on-cybersecurity-command-in-the-offing-101625025032655.html (Accessed November 2022).

[29] US Embassy & Consulates in India, *Framework for the U.S.-India Cyber Relationship* (New Delhi: Press Release, 2016). Available at https://in.usembassy.gov/framework-u-s-india-cyber-relationship/ (Accessed November 2022).

[30] Arun Mohan Sukumar, "India and Russia sign cyber agreement, pushing the frontier for strategic cooperation," *Observer Research Foundation (ORF)*, October 15, 2016. Available at https://www.orfonline.org/expert-speak/india-and-russia-cyber-agreement/ (Accessed November 2022).

[31] Kallol Bhattacherjee, "India, Japan finalise text of cybersecurity pact," *The Hindu*, October 07, 2020. Available at https://www.thehindu.com/news/national/india-japan-finalise-text-of-cybersecurity-pact/article32791549.ece (Accessed November 2022).

[32] Ronendra Singh and Amiti Sen, "India, Japan sign MoU to enhance cooperation in ICT, including 5G tech," *The Hindu*, January 15, 2021. Available at https://www.thehindubusinessline.com/info-tech/india-japan-sign-mou-to-enhance-cooperation-in-ict-including-5g-tech/article33582217.ece (Accessed November 2022).

[33] Hannes Ebert, "Prospects and Perils for EU-India Cybersecurity Cooperation," *The German Marshall Fund (GMF)*, accessed October 28, 2022. Available at https://www.gmfus.org/news/prospects-and-perils-eu-india-cybersecurity-cooperation (Accessed November 2022).

[34] Ministry of External Affairs, *6th India-EU Cyber Dialogue* (New Delhi: Press Release, 2020). Available at https://www.mea.gov.in/ press-releases.htm?dtl/33308/6th_IndiaEU_Cyber_Dialogue (Accessed November 2022).

[35] European Commission, *India-EU Working Group advances joint commitment for digital collaboration* (Brussels: News and Views, 2021). Available at https://digital-strategy.ec.europa.eu/en/news/india-eu-working-group-advances-joint-commitment-digital-collaboration (Accessed November 2022).

[36] Cormac Callanan, Anirban Sarma and Basu Chandola, "Enhancing Global Cybersecurity Cooperation: European and Indian Perspectives," *Observer Research Foundation (ORF)*, October 19, 2022. Available at https://www.orfonline.org/research/ enhancing-global-cybersecurity-cooperation/ (Accessed November 2022).

[37] Pierluigi Paganini, "Non State Actors In Cyberspace: An Attempt to a Taxonomic Classification, Role, Impact And Relations With A State's Socioeconomic Structure," *Center for Cyber Security and International Relations Studies*, June 2022. Available at https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf (Accessed November 2022).

[38] Dan Milmo, "Anonymous: the hacker collective that has declared cyberwar on Russia," *The Guardian*, February 27, 2022. Available at https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia (Accessed November 2022).

[39] Ryan Browne and Natasha Turak, "Hacktivists seek to aid Iran protests with cyberattacks and tips on how to bypass internet censorship," *CNBC*, October 5, 2022. Available at https://www.cnbc.com/2022/10/05/how-anonymous-and-other-hacking-groups-are-aiding-protests-in-iran.html (Accessed November 2022).

[40] Sico van der Meer, "How states could respond to non-state cyber-attackers," *Clingendael Netherlands Institute of International Relations*, June 2020. Available at https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_ non-state_June_2020.pdf (Accessed November 2022).

[41] Aamna Rafique, "Indian Cyber Posture: Implications for Pakistan," *Institute of Strategic Studies, Islamabad (ISSI),* October 2, 2019. Available at https://issi.org.pk/issue-brief-on-indian-cyber-posture-implications-for-pakistan/ (Accessed November 2022).

[42] Ibid.

[43] Ahmad Ali, "Indian Land Warfare Doctrine & Recent Developments: Implications for Pakistan," *Institute of Strategic Studies, Islamabad (ISSI)*, August 5, 2021. Available at https://issi.org.pk/issue-brief-on-indian-land-warfare-doctrine-recent-developments-implications-for-pakistan/ (Accessed November 2022).

[44] Muhammad Riaz Shad," Cyber Threat Landscape and Readiness Challenge of Pakistan," *Strategic Studies* 3, no. 1 (2019). Available at https://www.issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf (Accessed November 2022).

[45] Shubhajit Roy, "Focused on Pakistan rather than China, India in Tier 3 as cyberpower: Report," *The Indian Express*, June 28, 2021. Available at https://indianexpress.com/article/india/focused-on-pakistan-rather-than-china-india-in-tier-3-as-cyberpower-report-7378610/ (Accessed November 2022).

[46] Ibid.

[47] Ibid.

[48] "India launched cyberattacks against China, Pakistan: report," *The Express Tribune*, November 24, 2021. Available at https://tribune.com.pk/story/2330871/india-launched-cyberattacks-against-china-pakistan-report (Accessed November 2022).

[49] Asif Shahzad, "Pakistan seeks U.N. probe of India's use of Pegasus spyware," *Reuters*, July 23, 2021. Available at https://www.reuters.com/technology/pakistan-seeks-un-probe-indias-use-pegasus-spyware-2021-07-23/ (Accessed November 2022).

[50] Greg Miller, Craig Whitlock, and Barton Gellman, "Top-secret U.S. intelligence files show new levels of distrust of Pakistan," *The Washington Post,* September 2, 2013. Available at https://www.washingtonpost.com/world/national-security/top-secret-us-intelligence-files-show-new-levels-of-distrust-of-pakistan/2013/09/02/e19d03c2-11bf-11e3-b630-36617ca6640f_story.html (Accessed November 2022).

[51] Shahbaz Rana, "FBR reels under a major 'cyberattack'," *The Express Tribune*, August 15, 2021. Available at https://tribune.com.pk/ story/2315712/fbr-reels-under-a-major-cyberattack (Accessed November 2022).

[52] Sohail Sarfraz, "Indian hackers behind attack on FBR website: Tarin," *Business Recorder*, September 10, 2021. Available at https://www.brecorder.com/news/40119330 (Accessed November 2022).

[53] "Pakistan ranked among least cyber secure countries," *The Express Tribune*, February 13, 2019. Available at https://tribune.com.pk /story/1909680/pakistan-ranked-among-least-cyber-secure-countries (Accessed November 2022).

[54] Ahmad Ali, "Cyber Security Policing: Analysing National Cyber Security Policies of India and Pakistan," *Institute of Regional Studies*, August 2022. Available at http://www.irs.org.pk/Spotlight/SP08012022.pdf (Accessed November 2022).

[55] Ibid.

[56] Kalbe Ali, "Federal cabinet approves Cloud First Policy, Personal Data Protection Bill," *Dawn*, February 16, 2022. Available at https://www.dawn.com/news/1675330 (Accessed November 2022).

[57] Salman Siddiqui, "Pakistan adopts blockchain technology to attract remittances," *The Express Tribune*, January 9, 2019. Available at https://tribune.com.pk/story/1884203/pakistan-adopts-blockchain-technology-attract-remittances (Accessed November 2022).

[58] Special Technology Zones Authority. Available at https://www.stza.gov.pk (Accessed November 2022).

[59] Muhammad Riaz Shad, "Does Pakistan's First Cybersecurity Policy Go Far Enough?," *The National Interest*, June, 10 2022. Available at https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/doespakistan %E2%80%99s-first-cybersecurity (Accessed November 2022).

[60] Leilah Elmokadem, "Mapping of India's Cyber Security-Related Bilateral Agreements," *The Centre for Internet and Society*, accessed October 6, 2022. Available at https://cis-india.org/internet-governance/files/Cyber Security Agreements_ Infographic_04.pdf (Accessed November 2022).