Cyberwarfare: A Threat to National Security

Dr. Saba Sahar, Areesha Anwer

Abstract

The rise of emerging technologies and the growing use of internet has led to a more digitized world where cyberspace has become the new battleground for nations to compete with each other. Cyber attacks comprise a range of assaults that can put at risk the critical infrastructure and thereby the national security of a state. Damage by cyber-attacks could be inflicted through cyber espionage, hacktivism, ransomware or cyber terrorism. Cyberspace has a significant effect on the instruments of national power such as diplomacy, economy, military prowess and control over information. Thus, it requires a 'whole of nation approach' at all levels to protect the physical and network security of critical infrastructure which is imperative for national security. Cyber-attacks have become a potent tool in the hands of both state and non-state actors because of their relative cost-effectiveness, difficulty of attribution, anonymity and ambiguous nature.

The study comprehensively identifies the nature of cyber-attacks that endanger the national security of Pakistan. Furthermore, the paper examines the extent of the resilience of the cyber security policy of Pakistan in providing a robust mechanism to contend with the threat of cyber-attacks. This research also provides policy recommendations to enhance the cyber security infrastructure of Pakistan. This research is qualitative and both primary and secondary sources have been used to analyze the research topic.

Keywords: Emerging technologies, Cyberspace, Cyber security, National Critical Infrastructure

Introduction

In the modern age as states rely deeply on networks and digital infrastructure, the number of cyber-attacks has tripled over the last decade especially targeting the financial services industry.[1] Hostile elements seeking to derail information systems can breach cyber security and inflict physical damage on critical infrastructure.[2] In response, states require capabilities to recover from and avoid significant cyber risks including the setting of security standards, technical innovation, sector-specific risk management and the effectiveness of the indigenous cyber security industry. According to a Foreign Policy magazine survey cyber is the "single greatest emerging threat".[3]

Cyber security has the potential to revolutionize our future including our national security as contemporary global communication and connectivity are becoming increasingly dependent on cyber technologies. Pakistan has already embarked upon this path of digital transformation under the slogan "Digital Pakistan." To realize this digital transformation, Pakistan has taken several initiatives including formulating Pakistan's Cyber Security Policy 2021 which attaches top priority to securing Pakistan's cyberspace in its National Security Policy[4]. Pakistan is facing cyber-attacks against targeted

[1] Jennifer Elliott and Nigel Jenkinson, Cyber Risk is the New Threat to Financial Stability, IMF blog 2020

[2]Gabi Siboni and Sami Kronenfeld Iran and cyberspace warfare Military and Strategic Affairs, December 2012 Volume 4, No. 3, available at https://www.inss.org.il/wp-content/uploads/systemfiles/MASA4-3Engd_Siboni%20and%20Kronenfeld.pdf

[3]Peter W Singer and Allan Friedman What everyone needs to know Oxford University Press 2014, available at: https://news.wttw.com/2014/01/15/cybersecurity-and-cyberwar

[4] See National Cyber security policy 2021

individuals, organizations and the government and ranks 79 on the global cyber security index ranking 2020 in terms of measures taken[5]. Therefore, the "whole of a nation" approach is imperative to ensure robust cyberspace. This entails intelligence sharing and developing defensive and offensive cyber capabilities. It also includes innovative up skilling and education schemes and campaigns aimed at heightening public awareness.

Cyber Deterrence

Deterrence theory was developed during the Cold war to address the challenges which emerged after the development of nuclear weapons. Nuclear deterrence was successful in keeping both United States and Soviet Union from engaging in direct conflict. Cyber deterrence should play a similar role in the digitalized world as it seeks to influence an adversary's behaviour by discouraging him from doing any unwanted activities. Hence, many states have embraced cyber deterrence as a driving policy position in addressing attacks in cyberspace.[6]

The existing cyber defence and offence capabilities of states still have gaps that prevent the full protection of cyberspace. Deterrence-by-denial denies the adversary state the incentive to carry out a cyber offensive. Deterrence by denial, at its core, is the ability of a state to decrease the probability of network penetration to the degree that it either disincentivises an attack or grinds an attacker to halt over time. Deterrence by denial strategies endeavours to improve cyber capabilities so that despite adversarial ventures, a cyber-attack might have a low rate of success. Deterrence-by-

[5]Global Cyber Security Index 2020, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
[6]Cybersecurity: Deterrence Policy, Congressional Research Service report January 18, 2022, https://crsreports.congress.gov/product/pdf/R/R47011

punishment threatens an adversary with costly consequences in an event of a cyber-attack.[7]

The Problem of Attribution

Cyber attribution refers to allocating the responsibility of an attack to an attacker or group of attackers and subsequently, unveiling their real-world identity.[8] Attributing a cyber-attack to the perpetrator is a difficult task as the origin of the attack mostly remains unknown and leaves no physical evidence. Therefore, it is hard to distinguish the cyber assault, that originated from one country against the other was carried out by the state.[9]Cyber-attacks can be masked as an attack by a state when in reality it could emerge from a non-state actor as well. Hence, it is difficult to decipher the origin of the cyber-attack and thus refrains from deterring the enemy.

Joseph Nye describes deterrence by denial as an effective deterrence mechanism in cyberspace. The ambiguity surrounding attribution compels states to resort to deterrence through denial.[10] Thus, deterrence by denial is a key question for policymakers. Maintaining robust cyber infrastructure can help become a shield against cyber-attacks from both states and non-state entities. It is to mention that, this does not fully eliminate the possibility of cyber-attacks. It is hard to deter and punish the unseen enemy. Hitting back at the wrong target may worsen the situation and weaken deterrence.

[7]Cyber Deterrence: The Past, Present, and Future, NL ARMS Netherlands Annual Review of Military Studies 2020,

[8]Klaus-Peter Saalbach Attribution of Cyber Attacks, Springer 2019,https://link.springer.com/chapter/10.1007/978-3-658-25652-4_13

[9]Lorraine Finlay, Christian Payne. The attribution problem and cyber armed attacks, University of Notre Dame Australia, school of law,2019 https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1089&context=law_article

[10]Joseph S.Nye Deterrence and Dissuasion in Cyberspace, *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, doi:10.1162/ISEC_a_00266

This can further incentivize cyber terrorists to take advantage of the situation. Given the time required to recognize the origin of the attack, attribution becomes more challenging for states in the domain of cyberspace.[11]

Offensive Cyber Capabilities

One of the increasing risks for cyber is enormous global digitization. A distinction between offence and defence is blurred in the complex domain of cyber security, mainly due to security paradox.[12] Offensive cyber capabilities are needed because of deterrence as areas of conflict in cyberspace are ambiguous, without a clear starting and ending point. Physical and cyber conflicts are intertwined and, therefore, cyber domains cannot be treated as different from physical ones. Cyber-attacks can subvert the target with catastrophic impacts on critical infrastructure. Resilient cyber capabilities help resist offences and circumvent the harm to other domains of security and critical areas.[13]

Further, opacity, asymmetry and attribution remain a problem in cyberspace. Military offensive cyber capabilities are designed surgically to bring down sophisticated critical civilian and military networks during an armed conflict. In addition, in the latest Cyber Strategy of the United States, the offensive cyber policy is strongly emphasized and it has been said in public that the US Defence Advanced Research Projects Agency (DARPA)

[11]Lorraine Finlay, Christian Payne. The attribution problem and cyber armed attacks, University of Notre Dame Australia, school of law,2019 https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1089&context=law_article
[12]Limnéll, Jarno. Offensive cyber capabilities are needed because of deterrence. Accessed at https://cyberwar.nl/d/20130200_Offensive-Cyber-Capabilities-are-Needed-Because-of-Deterrence_Jarno-Limnell.pdf
[13]Ibid

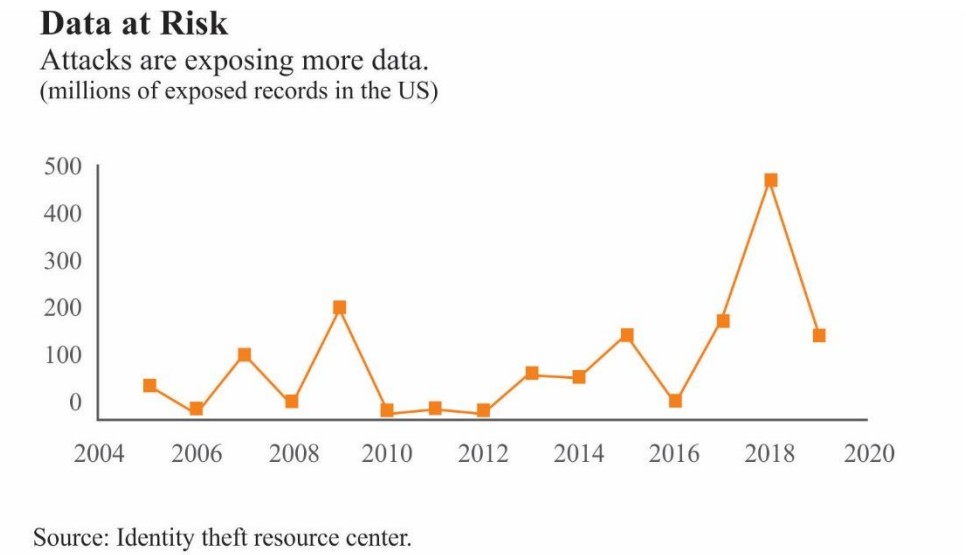
is focusing its research on offensive cyber capabilities. It has also been announced by many countries that a response to a cyber-attack is not limited to the cyber domain, which is understandable.

Cyber Attacks on Critical Infrastructure: An International Approach

"Systems-of-systems" integrated with massive information and communications infrastructures exposes critical infrastructures to significant cyber threats".[14]A cyber-attack on the critical infrastructure of a state is a threat to its national security. In such a case, denial-by-defense will help counter cyber-attacks by both states as well as non-state actors more adequately. However, denial-by-punishment will be more effective to deter states solely as the threat of retaliation can deter the intention of an offensive cyber-attack.

The United States has been working on developing its cyber security policy since the 1990s focusing on countering cybercrime and preventing losses to the corporate sector. However, there has been a sharp and intensifying concern about protecting the country's critical information infrastructure. A key component of the US 2018 cyber strategy is its Cyber Deterrence Initiative (CDI). This states that the US will work closely with allies in responding to cyber-attacks (including through intelligence-sharing), attributing attacks, formulating public statements of support for actions taken and jointly imposing consequences against those responsible.

[14]BélaGenge, István Kiss, Piroska Haller, A system dynamics approach for assessing the impact of cyberattacks on critical infrastructures, International Journal of Critical Infrastructure Protection, Volume 10, 2015.



The figure shows an annual increase in cyber-attacks and data comprised during the mentioned period in the US.

Critical National Infrastructures (CNI) around the world are mostly controlled by private companies. Notably, the private sector controls roughly 90 percent of US critical infrastructure. The threat to critical infrastructure has raised a serious question in the world coalescing into the massive booming business of cyber security, one of the fastest-growing industries in the world. From 2006 to 2020, 156 significant[15] attacks were made on the United States with an average of 11 significant attacks per year.

In 2014 President Xi Jinping initiated a wave of internet-related organizational reforms and new laws and regulations to make China a cyber

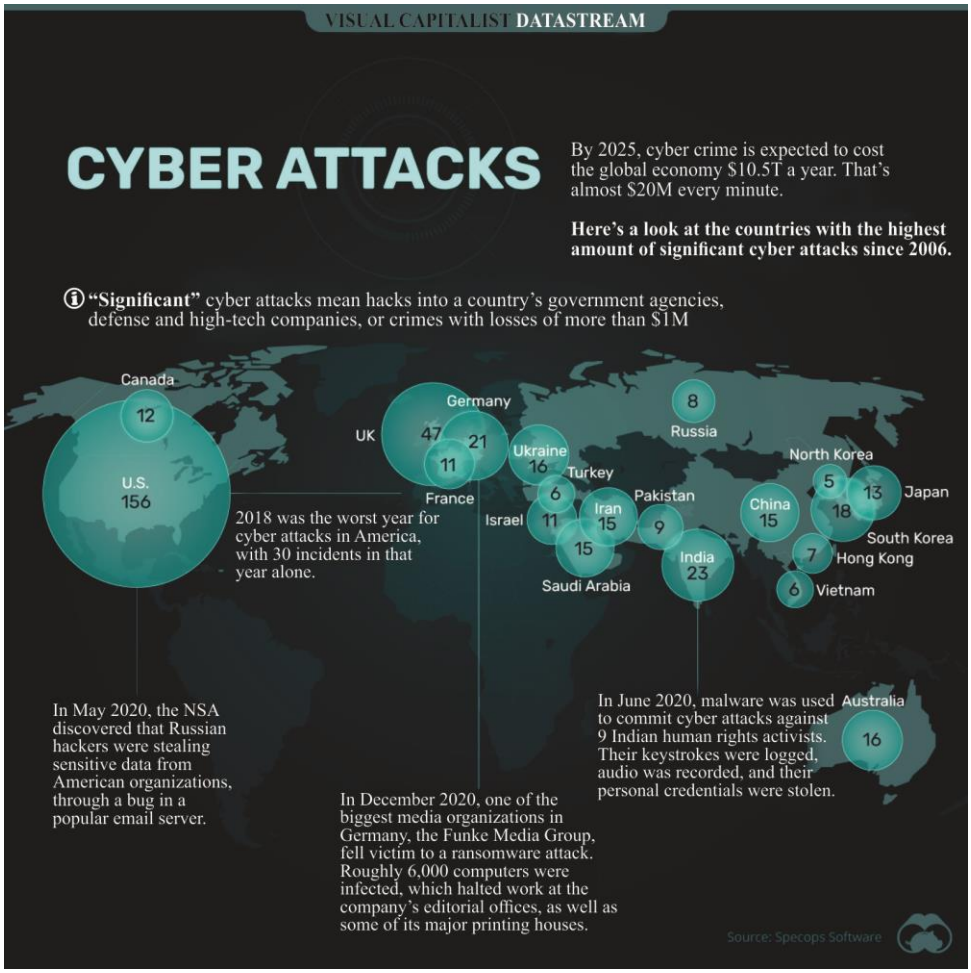
[15]Significant cyberattack refers to hacks into a country's critical infrastructure, each attack costs more than $1 million https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

power.[16] China's first national Cyberspace Security Strategy was published in 2016 and was supported by China's first Cyber security Law in 2017. On the industry side, the 'Made in China 2025' strategy, announced in 2015, is of particular significance. Identifying reliance on foreign vendors for its core internet technology as China's biggest cyber risk, this ambitious strategy intended to ensure that 70% of the core internet technology the country depended on would be manufactured domestically by 2025 and that it would become a world leader in such technology by 2030.[17] This is complemented by the Belt and Road Initiative (BRI), in which the Digital Silk Road component is designed to open up markets in the developing world to Chinese technology.[18]

The United Kingdom's critical national infrastructure officially consists of 13 sectors which include Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Each of these sectors is required by the government to produce an annual Sector Security and Resilience Plan, incorporating cyber security issues, while individual companies are responsible for their business continuity and resilience plans.[19] There is a proven system for incident alerting and response, cyber defence exercises involving government and industry and a dedicated national risk

[16]Paul Triolo, Lorand Laskai, Graham Webster, and Katharin Tai, 'Xi Jinping Puts "Indigenous Innovation" and "Core Technologies" at the Center of Development Priorities', New America, 1 May 2018
[17] Ibid
[18]Laura G. Brent NATO's Role in Responding to China's 'Cyber Superpower' Ambitions, horizon scanning, and analysis, Cyberspace strategic outlook 2030 Vol.2, 2022 CCDCOE. P-36-46
[19]Public Summary of Sector Security and Resilience Plans, Cabinet office UK,2017

register.[20]The UK Government's assessment of threats to Critical National Infrastructure (NCI) is based on a continuous cycle of learning lessons from real-world events.[21]



Source: Visual capitalist data streamhttps://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/[22]

[20]Harrop, Wayne; Matteson, Ashley Journal of Business Continuity & Emergency Planning, Volume 7, Number 2, Winter 2013-2014
[21]Public Summary of Sector Security and Resilience Plans, Cabinet office UK,2017
[22]Carmen Ang, The most significant cyberattacks from 2006-2020 https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

The figure shows that the UK is the second-largest victim of significant cyber-attacks after the United States. It is estimated that by 2025 cybercrime is going to cost the global economy around $10.5 trillion which is almost $20 million every minute.[23]

The UK government focuses on improving its resilience by strengthening the capabilities in cyberspace to withstand and recover from disruption. Its approach to security and resilience focuses on Resistance, Reliability, Redundancy and Response and Recovery. [24]

International Dialogue and Agreements on the Use of Cyber Capabilities Under UN Auspices

There are two parallel major UN-sponsored initiatives aimed at addressing the future of cyber security. First, the Group of Governmental Experts (GGE) operating under the auspices of the United Nations was formed in 2004. In period 2019-2021 GGE comprised of experts from 25 member states including five permanent members of the UN Security Council. It is working to promote responsible state behaviour in cyberspace.[25] Second, the Russian-sponsored Open-Ended Working Group (OEWG) was established in 2018. It is tasked to examine the developments in the field of Information and Telecommunications in the context of international security.

To date, six working groups of GGE have been created and the core achievement has been the recognition that international law applies to

[23] Carmen Ang, The most significant cyberattacks from 2006-2020 https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

[24] Public Summary of Sector Security and Resilience Plans, Cabinet office UK,2017https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

[25] Dan Efrony The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence

cyberspace and the introduction of non-binding and voluntary norms of responsible state behaviour.[26] The more recent working group of GGE concluded its work in May 2021 by adopting a consensus report. The report recognized the application of International Humanitarian Law (IHL) to cyberspace, precisely it acknowledges that IHL applies to cyber operations during an armed conflict. The 2021 report stresses that "states need to take responsible steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law." [27]

Building on the 2015 GGE report, the latest report of 2021 expands on principles of international law that are relevant in cyberspace. It accelerates the prohibition of the threat or use of force against the territorial integrity or political independence of another state, respect for human rights and fundamental freedoms and non-intervention in the internal affairs of other states. EU has emphasized that "the critical infrastructures are no longer confined to the borders of states, but are increasingly becoming transnational and interdependent," GGE report highlighted the lack of protection and regulation of such infrastructure, linking this unsettled issue to capacity-building and calling for closer interstate and public-private cooperation. [28]Overall, GGE re-emerged as the main inclusive process for the application of international law to cyberspace and demonstrated progress from its previous rounds.

[26]Adina Ponta, Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes, Insights, American Society of International law, July 2021 Vol: 25, Issue:14
[27]Ibid
[28]Ibid

Unlike GGE, OEWG deliberated in public and member states could submit public contributions to its deliberations. In March 2021 OEWG passed the unanimous resolution and produced a report adopted by 68 participating states. This was the first report on cyber security of this scale with direct governmental participation. During the first round of OEWG, several countries emphasized the threat of misinformation and foreign inference in their electoral processes. Although, the report only gives a brief reference to the election interference to the underlying critical infrastructure.

In the first section, the report focuses on the rising number of hostile cyber operations which destabilize public services such as "medical facilities, financial services, energy, water, transportation and sanitation." The second section deals with rules, norms and principles. It recommends the development and implementation of norms of responsible state behaviour and the exchange of best practices for the protection of critical infrastructure. The third portion backs the GGE statement that international law including the UN charter applies to cyberspace. The fourth portion of the report says the confidence-building measure (CBMs) are policy tools aimed at mitigating threats and building trust & communication channels and have been traditionally promoted in tackling international security issues such as nuclear non-proliferation or disarmament. The fifth section identifies CBMs to develop trust while capacity building is also the focus of the report outline. Finally, the report identifies the importance of regular institutional dialogue under the auspices of the United Nations.[29]

[29]Adina Ponta, Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes, Insights, American Society of International law, July 2021 Vol: 25, Issue:14

Currently, OEWG is working on a second mandate 2021-2025 with an organizational session held in June 2021. The first substantive session of OEWG was held in December 2021 followed by the second substantive session held from 28 March to 1 April 2022 in New York.[30]The OEWG group discussed the existing and potential threats in the ICT sphere and data security rules, norms and principles of responsible behaviour of states in cyberspace. It also addressed the question of how international law applies to the use of ICTs by states, confidence-building measures and capacity building. The next OEWG substantive session will be held on 25-29 July 2022.[31]

It is to note that despite the wide mandate given to each group – the GGE and OEWG – by the UNGA resolutions that establish them, both reports reveal a cautious approach. They mainly focus on voluntary, non-controversial issues such as encouraging states to enhance their cooperation in capacity building and Confidence Building Measures (CBM) to meet the challenges in tackling existing and potential threats.

Cyber terrorism refers to "premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs and data that result in violence against non–combatant targets"[32]

In 2002, the US Centre for Strategic and International Studies defined cyber terrorism as "the use of computer network tools to shut down critical

[30]UN OEWG and GGE, https://dig.watch/processes/un-gge
[31]UN OEWG and GGE,https://dig.watch/processes/un-gge
[32]Maura Conway, Reality Bites: Cyber terrorism and terrorist use of the internet, first Monday, peer-reviewed journal on the Internet, 2002,https://firstmonday.org/article/view/1001/922

national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population".[33]

Cyber terrorism is a more attractive and cheaper method for terrorists than traditional methods because they do not need to invest money and buy weapons. Additionally, compared to conventional forms of terrorism, cyber terrorism needs less physical preparation, fewer mortality risks and greater mobility, making it more appealing for terrorist groups to attract and keep adherents.

Cyber terrorists break into computers that control dams or air traffic control systems, wreaking havoc and endangering not only millions of lives but national security itself. [34]

It ought to be mentioned that, most of the critical infrastructure of Western countries is networked through computers. Therefore, mostly electric power grids and emergency services are vulnerable to cyber terrorist attacks because computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses. One such example is the Tamil Tiger Guerrilla fighter's attack on the computer systems of the Sri Lankan State in 1998. The Sri Lankan embassies around the world were flooded with the message that "We are the Black Internet Tigers and we are going to disrupt your communications systems." Similarly, in 2003, a Japanese cult named Aum Shinrikyo ("Supreme Truth") conducted a

[33]Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace, United Nations office on drugs and crime, module 14, https://www.unodc.org/e4j/en/cybercrime/module-14/index.html

[34]Gabriel Weimann, Cyberterrorism: How real is the threat? United States Institute of Peace, special report,2004 https://www.usip.org/sites/default/files/sr119.pdf

complex cyber-attack including obtaining sensitive information about nuclear facilities in Russia, Ukraine, Japan and other countries as part of an attempt to attack the information security systems of these facilities.[35]

Cyber Espionage

Cyber espionage can be described as a method of intelligence collection, particularly to obtain or access information that is not normally publicly available. The techniques of cyber espionage include using human resources (agents) and technical means by hacking into computer systems.[36]

A pitfall attached to taking retaliatory measures in cyberspace is the problem of attribution. Cyber-attacks carried out by state A maybe retaliated by state B if the origin of the attack is known. However, a cyber-attack by non-state actors can not necessarily be traced back to its attribution. Pakistan has also remained a target of cyber espionage. The Intercept 2016 Report states that US National Security Agency NSA spied on the top officials of Pakistan through Second date malware.

Since cyber espionage is carried out for spying and collecting intelligence such tactics are usually carried out by states hence the chances are that the cyber offender is a state actor and the likelihood of tracing the origin of such an attack is possible in some cases. To deter cyber espionage, offensive policy measures should be adopted. This will increase the response mechanism and will deter the possible cyber-attacks faced by Pakistan.

[35] Cyber Crime and Cyber Terrorism Investigator's Handbook; Chapter 13
[36] Ibid

Hacktivism

There is no universal definition of hacktivism but it has been described as the intentional access to systems, websites and/or data without authorization. The techniques also include the signing of online petitions, hashtag campaigns, creating a campaign website, recruiting volunteers and obtaining funds from members and supporters.[37]

Hacktivism has entered mainstream social media such as Twitter and Instagram. Protected by their anonymity, hacktivists can be less inhibited in expressing ideas or abuse and can be much more impervious to criticism and debate, than people who hold similar beliefs but express and defend them publicly. In short, hacktivism can appear more shadowy work of fringe groups and outsiders, than traditional forms of activism.[38]Anti-state elements often use such techniques to malign the other state. For example, the use of fake hashtags against Pakistan; # statekilledKarimabaloch #statekilledusmankakar and the migration campaign that India ran against Pakistan through the srivasta group.

Ransomware

Ransomware is a type of malware and malicious software, used to commit cybercrimes. When a computer or a network is attacked with ransomware, the malicious software blocks access to the system and encrypts its data. Thus, cybercriminals demand ransom money from the victims of cyber-attacks to release their data. In terms of national security, ransomware

[37]Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace, United Nations office on drugs and crime, module 14, https://www.unodc.org/e4j/en/cybercrime/module-14/index.html

[38]Tom Sorell, Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous, Journal of Human Rights Practice, Volume 7, Issue 3, November 2015, Pages 391–410,

attacks are a red line for the states, because they can block the critical data of important national institutions and the blocked data could be used against the victim state. [39]

One of the significant ransomware attacks on the United States was witnessed in May 2021 when the hackers took down the Colonial Pipeline which led to fuel shortages across the East Coast. Charles Carmakal, senior vice president at cyber security firm Mandiant said in an interview that the Colonial Pipeline was hacked by a private network account which allowed the hackers to remotely access the company's computer networks. According to a Bloomberg report, the Colonial Pipeline transports almost 2.5 million barrels of oil daily from the Gulf Coast to the Eastern Seaboard. The ransomware attack resulted in a blockade of the gas stations and higher fuel prices.[40]

Cyber-attacks on Pakistan

With the expansion of cyberspace in the sectors of finance and energy, the threat of cyber-attacks has increased noticeably. Reportedly Pakistan's finance and energy sectors were the frequent targets of cyber-attacks.[41]. Since cybercrimes are a risk to systematic financial stability, the attacks on the critical infrastructure of any state are a matter of its national security. It is important to note that cyber-attacks taking place in one country/organization or a company can have repercussions worldwide. For example, a cyber-attack hit Careem app in 2018 that resulted in a

[39] What is ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

[40] William Turton and Kartikay Mehrotra, Hackers Breached Colonial Pipeline Using Compromised Password, June 2021

[41]K-Electric suffered a targeted ransomware attackhttps://www.hackread.com/netwalker-ransomware-hits-pakistan-power-supplier-k-electric/

compromise of information of 14 million users from several countries. Consequently, information such as email address, trip details, customer identity and phone numbers became a target.[42]

National Cyber Security Policy of Pakistan 2021

In July 2021, the federal cabinet of Pakistan approved the first National Cyber security Policy of Pakistan. The policy emphasizes the development of a response framework to deal with the threats of cyber terrorism and cyber-attacks. It further elaborates on a national cyber vision to have a protected, robust and enhanced nationwide digital ecosystem for national security and socio-economic progress.[43] Further, the policy mentions the development of an integrated digital eco-system to protect the crucial digital assets of states. The policy envisions active defence against cyber-attacks and internet-based services as well as adequate response measures in case of acts of aggression against national sovereignty[44].

Following are the focus areas of Cyber security policy of Pakistan 2021:

a) Establish a governance framework
b) Address the importance of information systems and critical infrastructure
c) Promote data governance and protection

[42]Rubab Syed, Ahmed Awais Khaver & Muhammad Yasin Cyber Security: Where does Pakistan stand? Sustainable Development Policy Institute SDPI February 2019 https://www.think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1
[43]Ministry of Information and technology, National Cybersecurity policy of Pakistan, July 2021.https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf
[44]Ibid

d) Promote online privacy
e) Establish an information assurance framework
f) Create cyber security awareness
g) Capacity building
h) Achieve independence/indigenization
i) Emphasize the national/global cooperation framework
j) Emphasize the adoption of a risk-based approach[45]

In essence, Cyber Security policy 2021 is aimed at protecting the cyberspace of Pakistan by developing a robust cyber security defence. The policy places cyber-attacks at par with attacks on the core aspects of national security. However, policy mainly focuses on defensive approach which is also imperative for securing cyberspace but it should also adopt an offensive approach to deterring cyber-attacks. It ought to be mentioned that this kind of approach cannot be considered a panacea against cyber-attacks. The policy measures, therefore, should be a blend of both offence and defence to comprehend cyber threats.

The Resilience of the National Cyber Security Policy of Pakistan 2021

The 2021 cyber policy mentions establishing a structure to safeguard the cyberspace of Pakistan. It is a positive step towards the security of cyberspace. The policy states that an interactive digital ecosystem will be developed to safeguard digital assets from cyber-attacks. Moreover, special courts will be established at the national level to resolve cybercrime matters. One of the principal rules of cyber security is safeguarding the Critical Infrastructure (CI) and Critical Information Infrastructure (CII). The policy

[45]Muneeb Imran, Pakistan's Cybersecurity Policy in 2021: A Review, Industry news, November 2021 https://www.isaca.org/resources/news-and-trends/industry-news/2021/pakistans-cybersecurity-policy-in-2021-a-review

document maintains enforcement of cyber security risk management methodologies, developing a mechanism for the protection of CII and enforcement of the use of digital certifications and their accreditation including accreditation of national security standards in developing national security standards for public and private sectors.[46]

This establishes that the policy is indeed resilient as it comprehensively covers the existing and possible cyber threats to the CI and CII of Pakistan. In addition to that, the policy covers domestic cyber threats like cybercrimes as well. The number of existing and possible cyber threats to the digital infrastructure of Pakistan is not small. Cyber-attacks in the past were carried out by both states as well as non-state actors. Ransomware, malware, hacktivism, cyber espionage, cyber terrorism and other cyber-attacks have also affected Pakistan. This necessitates vigilance in all areas of the policy. The policy mechanism should not only follow defensive, but rather a combination of defensive and offensive approaches to better contend with the threats of cyber-attacks. The National Security Policy of Pakistan (NSP) 2022-2026 was officially released on January 14, 2022. The NSP highlights present and future threats faced by Pakistan in its neighbourhood and emphasizes the "whole-of-a-nation" approach to deal with these threats at all levels including land, air, sea, cyber and space.[47]

[46]Ministry of Information and technology, National Cybersecurity policy of Pakistan, July2021. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

[47]Rabia Akhtar, Pakistan's new national security policy: a step in right direction, Atlantic council, January 2022 available at: https://www.atlanticcouncil.org/blogs/southasiasource/pakistans-new-national-security-policy/

Policy Recommendations

It is imperative to note that policy measures must be implemented in their earnest to achieve the desired policy goals. Likewise, the framework given in the National Cyber security Policy requires prompt implementation given the sharp rise in cyber-attacks and cybercrimes in Pakistan and all over the world. Investments must be made in the ICT sector and emerging technologies to enhance the digital infrastructure of Pakistan, which will serve as a barrier to cyber-attacks.

The National Cyber security Policy 2021 must be updated with the relevance of time and technological advancement and an accountability mechanism must be put in place to monitor the development and goals achieved in the given time.

A whole-of-Government Approach – including diverse ministries, public agencies and public administration, must be taken, to not only provide a common solution to a problem but also work to implement those solutions at the national level. National vulnerability assessment centres and national crime and coordination centres should be established and there should be a collaboration with the private sector and international cyber security research organizations.

Cyber deterrence cannot be carried out by the government alone but with the assistance of the public too. Civilians are on the front lines of cyber warfare. Therefore, it is important to create general public knowledge about cyber warfare and the actions that must be taken individually. This would lead to creating an effective cyber deterrence.

Cyberwarfare is a novel domain of warfare, a challenge requiring an immediate global response to escape any catastrophe. This can be done

through extensive international cooperation. Multilateral discussions on such issues help formulate rules and norms for such threats. Hence, there is a need for Cyber regulation and an agreed battlefield on a cyber treaty. The malicious cyber-attacks have impacted the global supply chains of the services sector. This issue can also be addressed by creating global norms and treaties to manage a global supply chain.

Cyber deterrence works when the enemy is convinced of a counter offensive in cyberspace. It is, therefore, important to have a policy and declaration of offensive capabilities and readiness to communicate the rules of engagement. This awareness prevents conflicts. Many countries have said that a response to a cyber-attack will not be limited to the cyber domain. The US, China, Russia and other countries are incorporating professional people possessing cyber expertise to cope with such threats.

Conclusion

There have been several challenges to national security given the rise of emerging technologies notably in cyberspace. Currently, adversaries are carrying out jeopardizing tactics against each other by targeting sensitive areas unable to be retaliated through physical force. Conflicts in the foreseeable future will not only be fought by the armies on battlefields but also by the malicious codes possessing the capability to subvert the critical infrastructure of a country. Any such assault could paralyze the mobilization of armies and the resources needed at the time of war. Therefore, cyber security measures and strengthening resilience in the system through policy implementation and investments in emerging technologies is the pivotal factor in national security.

It exhibits the prominence of safeguarding the infrastructure which is fundamental to national security. The importance of cyber security also highlights the growing potency of cyber incursions and better ways to target critical institutions of a state. Therefore, it needs to be recognized that cyber security is national security.

Dr. Saba Sahar *is Associate Director at the Centre for International Strategic Studies Sindh (CISSS). She has served as Research Assistant at the Department of the International Relations University of Sindh. Before joining the University of Sindh, Dr. Saba worked as a visiting faculty member at the National University of Modern Languages Hyderabad. She writes on current issues in English newspapers and appears as an analyst on T.V programs related to international events. She holds a doctoral degree in International Relations from Department of International Relations University of Sindh. Her areas of interest include cyber warfare, 5th generation warfare and Artificial Intelligence. She can be reached at* ***saba_solangi@hotmail.com***

Ms. Areesha Anwer *is Research Officer at the Centre for International Strategic Studies Sindh (CISSS). She holds a Master's degree in International Relations from the University of Karachi. She is the author of 'Establishing Deterrence in Cyberspace' published in The Express Tribune. Her areas of interest include hybrid warfare, cyber security, emerging technology and security studies.*