Journal of Development Policy, Research & Practice

Vol. 3 (January – December 2019)

pp. 23 - 43

Cyber Warfare Trends, Tactics and Strategies: Lessons for Pakistan

Rafay Baloch[*]

ABSTRACT

With the advent of the digital revolution, computer security has gradually evolved from a technology problem to a business and safety problem. Unlike conventional warfare, cyber warfare is inexpensive, effective and obscure, which in case of conflict, offers nation states a combination of cyber tools such as espionage, subversion, disinformation, and propaganda. Cyber warfare may prove decisive in many international conflicts in the future. This paper discusses the evolution of cyber-attack surfaces, adversaries and next generation cyber-attacks, and illustrates the security risks posed by the technological revolution and its impacts. It further discusses the potential solutions, and measures which the Government of Pakistan (GoP) may take to build effective detection and response cyber warfare capabilities. The GoP should consolidate the available cluster of skills and technology to establish a national agency mandated to conduct cybersecurity for efficient critical asset protection and effective response to any kind of cyber-attack.

Keywords: Cyber-attack, cybersecurity, cyber warfare, cyber weapons, digital revolution.

[*] ***Mr Rafay Baloch*** is currently working as Cybersecurity Advisor at the Pakistan Telecommunication Authority. He is an ethical hacker and security researcher who was the first to discover vulnerabilities in the Android operating system. He has been conducting security research for over seven years.

1. INTRODUCTION

1.1. Evolution of Warfare

To clearly understand the true genesis of cyber warfare, one must understand the evolution of warfare since World War I and II. Mutations in battlefield tactics have created entirely new domains in this area. This cannot be better exemplified than the widespread use of airpower, armour and nuclear weapons during World War II. The Cold War inherited these battlefield dynamics keeping an uneasy balance of power between Western allies and the Iron Curtain. It was also during World War II when the invention of the Enigma machine, by the German *Wehrmacht*, laid the foundation of information warfare (Marvin 2015). The machine proved to be a crucial war weapon which provided encrypted communications between battle formations. The British intelligence services took years to decipher and break the Enigma code, made possible due to the inventions of Alan M. Turing. Cyber warfare, in its modern form, surfaced on the strategic landscape after the 9/11 attacks in the United States (US) due to the widespread availability of computers and network communications. It has since become a weapon of choice for state and non-state actors alike for carrying out 'deniable operations' against their intended targets - case in point, the Stuxnet attack carried out against Iran's nuclear facilities in 2010 (Chen and Abu-Nimeh 2011). Now, modern cyber warfare has mutated into a myriad of sub-domains embodying different tiers in one form or another.

1.2. Evolution of Threat Landscape

The threat landscape has evolved based on the motivation of cyber threat actors. The following list highlights key players in the modern cyber domain:

1.2.1. Script Kiddies

The age of information began 30 years ago with the creation of the World Wide Web (WWW) which became the playground of every Information Technology (IT) enthusiast and expert alike. Even at that time, the world was dealing with teenagers writing computer viruses and *script kiddies* using them for fun and popularity.

1.2.2. Organised Crime Gangs

This trend evolved quickly when the Internet started to become a medium for financial transactions - when organised crime gangs started to hack for financial gains and make quick profit.

1.2.3. Nation States

In 2010, a major revolution took place with the world's first cyberweapon completely written out of code dubbed as 'Stuxnet.' The malware was specifically developed to target Industrial Control Systems (ICS) in Iranian nuclear plants for manipulating the rotation speed of centrifuges used for enrichment of uranium (Kelley 2013). Stuxnet reportedly destroyed almost one-fifth of Iran's nuclear centrifuges and has been widely attributed to the US and Israel. Since then, states have actively started taking part in the cyber arms race to accomplish their strategic goals.

1.2.4. Terrorists

The most recent evolution in threat perception is the use of cyber weapons by terrorist groups like the Islamic State of Iraq and Syria (ISIS) to spread propaganda, recruit, raise funds and to carry out cyber-attacks in the pursuit of their agenda (Healey 2017).

2. LITERATURE REVIEW

2.1. Conventional Warfare

During the two world wars, battlefield dynamics revolved around three major domains of warfare: air, land, and sea. The outcome of battles fought in these domains had a marked impact on the result of these wars. For example, the deployment of integrated land and aerial assets by the German military command during World War II against Poland and France proved to be decisive. Similarly, Normandy and Omaha beach landings also proved to be decisive battles. The German Army's invasion of the Soviet Union under the code name 'Operation Barbarossa' was the largest military operation in human history. The operation relied heavily on land and aerial warfare. The age of conventional warfare abruptly ended with the atomic bombings of Hiroshima and Nagasaki by the Americans. It paved the way for another type of war – the Cold War.

2.2. The Cold War

As post-World War II Europe was carved up and divided into the North Atlantic Treaty Organization (NATO) and Warsaw Pact camps, the world held its breath as it teetered at the edge of nuclear oblivion. The rapid nuclear development of the 1950s and 60s created a toxic global atmosphere. Under the new rules, leading nuclear powers could not conceive the idea of direct confrontation, and a new doctrine of 'indirect' confrontation took over the political arena in the form of proxy, political and economic warfare etc. Nowhere is this new way of war-fighting more visible than in Vietnam, the Middle East, Cuba, and Afghanistan. As global uncertainty grew, indirect warfare became a weapon of choice for global powers to fight for tipping the balance of power without getting involved themselves. The Cold War, however, came to an abrupt end in the early 1990s when the Soviet Union was defeated in Afghanistan. Although weakened, Russia under President Putin has sought to rebuild its global influence by creating an adaptive approach to warfare – known now as 'Hybrid Warfare.'

2.3. Hybrid Warfare

Hybrid Warfare leverages the 'indirect warfare' doctrine of the Cold War days and blends it with the most cutting-edge tools offered by the digital revolution to wage information and cyber war. It combines the use of irregular forces, proxy elements, political and diplomatic tools with information operations and cyber warfare to impact global power dynamics. This new doctrine is being called the 'New Way of War'. Cyber space is a rich and fertile ground to invoke social unrest in target countries by using information warfare techniques. For example, during the Arab Spring, the populace was bombarded with false and misleading information, leading to anti-government protests. Many countries in the Middle East and Ukraine were targets of highly sophisticated propaganda campaigns by hostile actors (Erol 2015). Resultantly, unrest grew and a number of countries, such as Egypt, Tunisia, Syria, Yemen, and Ukraine witnessed extended periods of unrest, violence and civil wars which destroyed their economies.

3. EVOLUTION OF CYBER WARFARE

In cyber warfare, the gap between perception and reality is still not evident as it has often been argued that it does not directly result in human casualties. Therefore, the correct terminology would be 'cyber espionage', 'cyber sabotage' or 'cyber terrorism'. However, there are instances whereby casualties have occurred as a result of cyber espionage. One notable example is the conflict between Russia and Ukraine whereby Ukrainian artillery soldiers' mobile phones were infected with malware to pinpoint their locations to target the country's military units. Between late 2014 and through 2016, a known malware family called 'Fancy Bear' was distributed within a legitimate android application on Ukrainian military forums (Martin 2016). The application allowed speedy processing of targeting data for the Soviet-era D-30 howitzer. The 'Fancy Bear' family was also used in the Democratic National Committee (DNC) email hack of John Podesta, Chairperson of Hillary Clinton's presidential campaign of 2016 (DNI 2017).

3.1. Information Warfare

When the Internet had not become commonplace, disinformation and propaganda was conducted through airborne leaflets and loudspeakers. However, with massive adoption of social media platforms such as Twitter and Facebook, states use cyber space to invoke unrest in rival countries.

A striking case was the US Presidential Elections in 2016 during which a combination of cyber-attacks and information warfare techniques were used to sway the opinion of the general public. Although no traceable evidence was found, yet there are certainly examples of several (unsuccessful) attempts to hack voter database registrations which, were widely ascribed to Russia by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). The opinion was backed by several well-known cybersecurity firms such as CrowdStrike, Fidelis, and Mandiant based upon technical similarities between malware samples. Another reported attack was the one compromising John Podesta, Chairman of Hillary Clinton's presidential campaign who received a phishing email on 19 March 2016, purporting to alert him of a 'compromise in the system', and urging him to change his password 'immediately' by clicking on a link. As a result of this phishing email, his password was stolen, and during the election campaign, stolen files and emails were leaked through various platforms such as DCLeaks, WikiLeaks, etc. The content of the emails severely damaged Clinton's campaign, since they contained transcripts of paid speeches and certain controversial comments about Catholic voters. This was utilised by Donald Trump's campaign and led to anti-Catholic sentiment within Clinton's vote bank (Dias 2016).

One of the ways to affect the outcome of an election is to prevent campaigners from casting their vote. In the days leading up to the election, Twitter had to ban several accounts for spreading misleading information to the public (Roberts 2016). The accounts claimed that Clinton's voters could vote by simply sending an SMS to a short code number. This was an attempt to mislead voters and prevent them from voting at all. A report released by the FBI and DHS showed that malware samples used to infiltrate information systems of the Democratic National Committee (DNC) had similarities with the methods used by Russian hackers. Other reports also attributed the DNC hack to Russia, more specifically to two espionage groups 'Fancy Bear' and 'Cozy Bear' (DNI 2017). Russia, despite a weak GDP as compared to other developed countries (especially the US) and with several demographic disadvantages, was able to accomplish much more in the cyber domain which may otherwise not have been possible in the real world. Cyber propaganda undermined the trust of the American public in their country's fundamental democratic process, i.e. elections. According to the early January 2017 polls, it was revealed that 55% of the respondents suspected Russian interference in the US elections, out of which 51% believed that this was done through cyber means (Tim and Rubenstein 2017).

The case of Cambridge Analytica (CA) is also worth mentioning. The data intelligence and analytics company played a crucial role in the US elections while running the presidential campaign for Donald Trump (Paul and Paul 2018). The company focused on micro-targeting using psychographics[1] outpacing Hillary Clinton's campaign which was only using demographics. CA collected voters' data through various demographic and social media sources by exploiting a design flaw in Facebook and using a misleading application on the platform. The data collected was used to construct the psychological profiles of voters based on the OCEAN (Openness, Conscientiousness, Extroversion, Agreeableness, and Neuroticism) model. This model, applicable to 32 different personality types, helped CA construct psychological profiles of millions of voters who were believed to have influenced voters' opinion significantly.

3.2. Cyber Espionage

Cyber espionage is a multipurpose and multidimensional tool. States have long relied on this method to undermine the military and commercial interests of their adversaries by hacking into their defence systems and commercial enterprises. For over a decade, the US has accused China of alleged intellectual property theft such as stealing early age ideas and propriety technology by bringing in competitive products, and claims to have suffered losses worth hundreds and billions of dollars. One such example is theft of confidential data about the F-35 Lightning II joint strike fighter, the most advanced American stealth aircraft manufactured by the Lockheed Martin Corporation (Daniel 2017). Similar document thefts were reported of the F-22 fighter jet, and B2-stealth bombers' nuclear submarine/anti-air missile designs (Gady 2015). With the knowledge that Rivest-Shamir-Adleman's (RSA) SecureID devices are widely used, sensitive parts of Lockheed Martin Networks (Hosenball et al. 2011), defence contractors and government agencies' RSA SecureID devices were targeted using Advanced Persistent Threat (APT) attack vectors (Siobhan and Shara 2011).

3.3. Cyber Sabotage

Cyberspace offers extraordinary access to potential attackers for using technology to conduct acts of sabotage. The problem has become more challenging with the Fourth Industrial Revolution allowing more and more Supervisory Control and Data Acquisition (SCADA) and Programmable Logic Controller (PLC) systems to connect to networks, hence, introducing new kinds of risk. For example, an unprecedented attack, by a company known as Prykarpattyaoblenergo, caused the shutdown of the

[1] A method of political market segmentation of public demographic to sort them into relatively homogenous groups based on similarities in views. See, Shin (2008).

Ukrainian power grid in 2015 whereby the perpetrators initially gained access to corporate networks through a speared phishing campaign aimed at system administrators (Zetter 2016). The corporate networks were well segregated from SCADA networks using firewalls. However, over months of reconnaissance into mapping out networks, the attackers finally managed to gain access to the Windows Domain Controller. From there, the employees' credentials were dumped out. Out of these, some were for Virtual Private Networks (VPN) that grid workers used to gain access to the SCADA systems remotely. On 23 December 2015, attackers logged into SCADA systems remotely by using hijacked VPN credentials, disabled UPS systems and tripped power breaks remotely resulting in electricity blackouts for about 30 substations leaving approximately 230,000 people without electricity in the middle of winter (Ibid.). To exacerbate the effect, Telephonic Denial of Service (TDOS) was conducted on the electrical grid's customer service call centres in an attempt to deny legitimate complainants from reporting concerns pertaining to blackout in their areas and further caused panic among the citizens. Ukrainian authorities managed to recover from this incident in six hours. However, had this persisted for a longer duration, it could have certainly led to human casualties (Ibid.).

3.4. Cyber Economic Warfare

Cyber warfare, in its economic embodiment, has proven to be a game-changer in 21st Century politics. It can be used to deliver extensive damage to the economy of a target country. The paper has already discussed US allegations against China of targeting its commercial interests through intellectual property theft and cyber espionage. The US has responded by imposing numerous sanctions and directly targeting China's commercial interests. For example, bans have been imposed on Chinese tech giants 'Huawei' and 'ZTE' by the US and her allies on the pretext of backdoors found in Chinese-made equipment (Mengting and Lee 2019). Huawei was also added to the 'US Trade Blacklist' forcing Alphabet Inc. (Google) to suspend provision of updates for Android OS and Google services such as Google Play Store on Huawei's smartphone business outside China and future devices. The US further suspended any future agreement with Chipset manufacturers such as Broadcom, Intel, Qualcomm, Xilinx, Western Digital, etc. Similar bans were imposed by US allies, such as Australia, Canada, and New Zealand on Huawei's telecommunications equipment particularly related to 5G (Kaska, Beckvard, and Minarik 2019). Moreover, the US government is actively working with Australia, Israel and India to hinder Chinese 5G tech investments, especially in Europe.

States have also been targeting their adversaries to realise their budget deficit. One of the largest cyberbanking heist was at the Bank of Bangladesh that took place in 2016.

Around 35 fraudulent transactions close to US$ 1 billion were performed via Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, which financial institutions use to move money around the world. Transactions worth US$ 101 million were traced to Sri Lankan and Philippines' banks (Quadir 2019). Of this, only US$ 20 million was traced and recovered from Sri Lanka. While no substantial evidence could be found, the attack was attributed to North Korea due to similarities with the 2014 Sony Pictures hack and WannaCry ransomware. North Korea's continued ransomware attacks on various financial institutions may be compensating the country's budget deficit. The country was also allegedly involved in the 'NotPetya' ransomware attacks on various Ukrainian companies. NotPetya is a variant of 'Petya' but is different as it works at the administrator level and can dump credentials from the system's memory and encrypt any device in the system it gains access to. Unlike its predecessor, the encryption routine of NotPetya is modified in such a way that it is not technically possible to revert changes made by the malware, which is estimated to have cost companies more than US$ 1.2 billion (£850m). Maersk, the world's largest shipping company, has been a victim of NotPetya ransomware. About 4,000 servers, 45000 endpoints, and 2500 applications had to be re-installed. While the latter was accomplished within ten days of the incident, the attack caused damage of approximately US$ 300 million (Brandom 2017).

The software M.E.Doc is used to file taxes for companies doing business in Ukraine. It is believed that the software update mechanism of M.E.Doc was compromised to infect all machines using it. According to ESET (an antivirus company), the M.E.Doc servers were infected six weeks earlier indicating a carefully planned and well-executed attack (Greenberg 2019). Apart from Wikipedia, Ukraine's critical infrastructure such as the radiation monitoring system at the Chernobyl nuclear power Plantkrainian, ministries, banks, metro systems and state-owned enterprises (Boryspil International Airport, Ukrtelecom, Ukrposhta, State Savings Bank of Ukraine, Ukrainian Railways) were affected. These attacks have been attributed to Russia. It is widely believed that the series of cyber-attacks were part of cyber economic warfare to send a message to Western companies to refrain from doing business in Ukraine.

3.5. Cyber Terrorism

Terrorism movements are always early adopters of new technologies. This dynamic has led to acts of cyber terrorism. This domain includes the recruitment, funding, organisation and propaganda elements of terrorism. In some cases, terrorist groups have been able to carry out high profile cyber-attacks against nation states. One such example is from 2012 when Junaid Hussain aka 'TriCK' (behind the infamous hacking group 'TeaMp0ison') was responsible for several high-profile attacks. These included leaking email addresses and passwords from the United Kingdom's Ministry of Defence, leaking Tony Blair's voicemail to the public, bombarding the MI6 counterterrorism hotline with computer-generated calls (TDOS attack) so that their system was unable to receive legitimate calls, and, wiretapping of MI6 officers (Kovacs 2012). The hacker reportedly fled from custody and joined ISIS. It has been further reported that he conducted numerous other conspicuous cyber-attacks, including releasing US military personnel data to the public. The FBI, however, refuted this claiming that the data was acquired through open-source intelligence techniques (Myers 2015).

For these notable cyber-attacks, 'TriCK' was third on the Pentagon's 'kill list' and reportedly died in a drone strike. This was the first instance where a government responded to cyber-attacks with a real-world intelligence operation. While it is unclear how he was traced, anecdotal evidence shows that he was traced through a link that was sent to him through 'Surespot' which he used for recruitment purposes. However, this theory seems to be flawed as an experienced hacker like him would never make the mistake of clicking untrusted links; and it is highly unlikely that he would connect to the Internet without using a proxy or a Virtual Private Network (VPN). There are also those who believe that his geolocation was traced through one of his close associates using a Skype account he had used. This seems to make sense as there are videos of him on YouTube displaying weapons to his friends.

As far as conventional terrorism is concerned, the Pakistan Armed Forces have achieved significant success in its eradication. However, cyber terrorism remains a potent and persistent threat due to issues such as indoctrination, communication, recruitment, propaganda, and fundraising as well as lone wolf attacks. An unregulated cyberspace offers anonymity and global cybernetic reach. Terrorist groups pose advance level threats because they can exploit the ungoverned cyberspace for disrupting target networks through cyber-attacks and coordinating these in the real world.

3.6. Digital Innovations and Future Threats

Computers and smartphones connected to networks are now integrated with the Internet. The next revolution will see everything connecting to the Internet. The adoption of Internet of Things (IoTs) will take place at a much faster pace than any previous technology revolution and the world has already started witnessing its effects:

> *…8 billion devices connected to the internet, however by 2020, about 50 billion devices worldwide are expected to be connected to the internet. It is estimated that worldwide technology spending on the IoTs would reach USD*

> *1.2 trillion in 2022. Between 2004 and 2014, the average cost of IoT sensors dropped by more than half, from USD 1.30 to USD 0.60, furthermore, the prices are expected to shrink by another 37% to USD 0.38 by 2020 (Dukes 2018).*

This would lead to a situation where all existing devices and appliances like refrigerators, washing machines, and microwave ovens will be based on IoT by default. This will enable manufacturers to collect end-user data from all sorts of IoT devices of daily usage. This also means that there will be new kinds of security and privacy threats to deal with. Security requires trust - trust in the places where the chips are made, where devices are built, and where software is written. Many companies have their software sourced from different countries. Therefore, one may logically ask where the programmers are from. No one can be trusted regarding national security matters, yet citizens have no choice but to trust everyone. While some citizens may be aware of security controls and procedures, how do they get companies to adopt security that protects them? People will not buy an IoT device for the type of Firewall or antivirus it has, but for its features. While there are billions of devices connected to the Internet, one cannot rely on manufacturers alone as they will only add security if consumers demand it or a regulator mandates it.

With millions of devices coming online every day, the attack surface keeps on expanding as well. The security industry cannot work in isolation, rather it has to work in collaboration with other stakeholders. This is where *Threat Intelligence* comes into play. The accumulated data collected through threat collaboration and intelligence-based sharing, after research and analysis, enables states to come up with preventive measures in advance with timely, contextual and coherent planning. Considering the severe impacts of cyber threats, *Cyber Threat Intelligence* has been developed as an efficient solution to maintain international security. Security controls are not fool proof. Further, they need to run on higher level privileges on networks or endpoints so they can inspect and control. This also implies that security vulnerabilities in them may be even more serious.

These technological revolutions pose certain security risks that should be addressed at early adaptation phases with policy directives and regulations to promote these technologies, and at the same time, reduce risk to an acceptable level.

4. IMPLICATIONS FOR PAKISTAN

4.1. National Security

The most visible and pressing implication of cyber warfare for Pakistan is the state's overall national security. Pakistan, being a nuclear state and the producer of advance missile technology, also has a strategic geographic location. This makes the state a potential target for cyber-attacks, not just designed to steal information, but also to sabotage its national assets, such as nuclear reactors, power plants, grid stations, airports, telecom hubs, etc.

4.2. Military

All branches of the Pakistan military remain an active target for cyber warfare both in peace and war. It is, therefore, imperative that military assets, communications, computers, and installations are robustly protected. It is also a requisite that the military should retain the capability to retaliate against a sophisticated cyber-attack. It should be able to safeguard its information and assets from highly advanced threat actors which are fast evolving.

4.3. Economy

Through continuous years of war on terrorism, Pakistan has always been running a fiscal deficit, and struggling for economic stability. The economic sector has become dependent on digitalisation which has not only brought tremendous changes in the economic fabric, but also made it vulnerable to cyber-attacks. Economic disruption is the most critical cyber-attack that a country's economic system can face as the economy is the basic pillar of national security. If Pakistan's economic assets are targeted by cyber-attacks, the economic loss can be appalling. Therefore, the government must develop a National Cybersecurity Policy that applies to the entire economic apparatus of the country – including banks, stock exchanges, industries, etc.

4.4. Internal Stability

Continuous internal conflicts in the form of religious, sectarian, and inter-provincial differences have made Pakistan prone to propaganda. These fault lines have always been exploited by hostile state and non-state actors alike. This is particularly concerning now that social media and online space have become a battleground of ideas and a hotspot of malicious narratives. If left unattended, it can have long-term consequences for Pakistan's internal stability, politics, and cohesion.

4.5. Foreign Relations

Cyberspace also offers great opportunities for countries like Pakistan to expand its diplomatic footprint, effectively promote and rebuild its foreign relations and international image with the effective use of digital diplomacy.

4.6. Cyber Terrorism

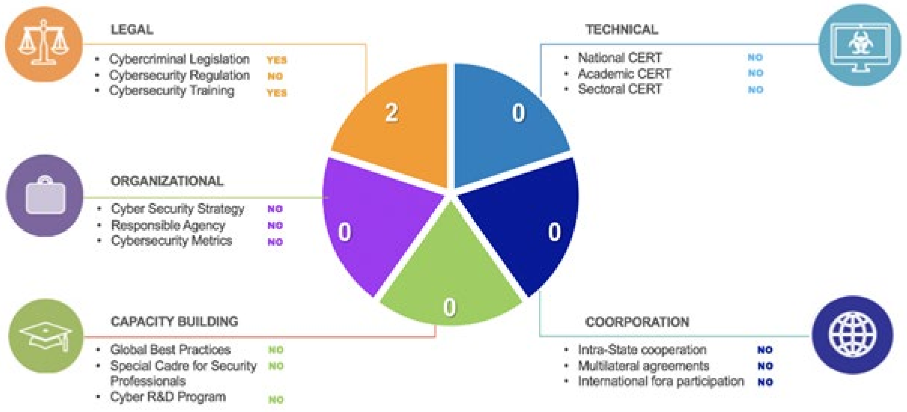
Terrorists use the digital information medium to sow and spread the seeds of extremism, terror, and violence quietly. Pakistan must device an Anti-Terrorism Cybersecurity Policy, integrated and aligned with the National Action Plan, to address national security issues. Lack of coordination between security agencies make Pakistan a soft target for cyber terrorism. To address this, the government needs to organise its cybersecurity activities around a well-structured security infrastructure. Technical, legal, social and military involvement is necessary for developing anti-terrorism cybersecurity laws, and to enforce these laws, multidisciplinary infrastructure is needed (Robinson et al. 2015). 'The person-in-the middle (PIM) is a key factor in helping to defeat cyber terrorist operations. Not only must the cyber terrorist get by cyber defense systems but they must also overcome the final human defender. In many ways, it is the final PIM that makes cyber terrorism operations so unreliable. 'Cyber terrorism as a technical operation has a finite set of attack points. Defend these cyber defense points and you will mitigate or defeat the ability of the cyber terrorist to conduct these types of technical attacks' (O'Hara 2004, p. 18).

4.7. Cybersecurity Research and Development

With the evolution of technology and increasing digitalisation, the attack surface has increased and so has the sophistication of cyber-attacks as nation states have begun a cyber arms race. A strategic roadmap for global cybersecurity Research and Development (R&D) can help prioritise commercial investments and balance trade-offs. Regardless of business size, technology tools are still vulnerable to cyber threats. The only way to curb the menace of cyber-attacks against infrastructure, holistic cybersecurity approaches must be a fundamental part of digital transformation in order to build resilient systems and to stay ahead of the curve through cybersecurity R&D. For digitalisation, non-vulnerable software perception is ideal, but it is really hard to manage the risk associated with vulnerabilities. Developing systems security requirements, testing systems resiliency, software assurance through languages and standard practices can help the software industry to reduce risks (Benzel 2015). Therefore, a 'Strategic Plan for Cybersecurity R&D' that includes security containers, privacy-preserving data sharing, consensus algorithms as an approach to data, human behaviour modelling, and experimental science research at the national level, is required for various virtual organisations. This will provide guidance to the government for funding programmes, policies and collaborations over the next decade.

5. PAKISTAN’S CURRENT CYBERSECURITY LANDSCAPE

Figure 1: Pakistan’s Current Cyber Landscape



Source: ITU 2019.

According to the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) 2018, Pakistan ranked 94th in terms of cybersecurity. The GCI’s ranking is based on commitment of ITU member states in terms of cybersecurity against five pillars: legal, technical, organisational, capacity building and cooperation. It is pertinent to mention that Pakistan dropped from 66th to 94th in 2018 (ITU 2019, p. 59). The major factor behind this drop is failure to show any progress in the aforementioned commitment areas, whereas other countries have started demonstrating their commitments towards GCI’s five pillars. There are other key indicators such as Comparitech Reports, which rank Pakistan as the 7th worst country in terms of cybersecurity. Their statistics reveal that 25% of mobile devices operating in Pakistan are infected with malware (The Tribune 2019). This is not surprising because due to lack of awareness on the subject of cybersecurity at grass-root level and ungoverned cyberspace, the general public falls prey to all kinds of digital viruses.

Due to the absence of strong technical bodies such as national Computer Emergency Response Team (CERT) and sectoral CERTs, different sectors such as telecommunication, banking, oil and gas, defence, etc., are working in isolation to curb cyber-attacks, whereas security always works best in collaboration. Any successful cyber-attack in one sector, such as telecommunications or banking, may also affect the military, as these sectors happen to be the very basis of national infrastructure rendering services to public/private sectors. The Pakistan military, on the other hand, lacks integrated tri-services or 'Inter-Services Cyber Command' (ISC2), to effectively detect and respond to sophisticated cyber-attacks and hybrid warfare.

Furthermore, due to the absence of a National Cybersecurity Strategy and Policy, national objectives and priorities on this issue are not well-defined. Such a strategy allows countries to tackle risks which might have the potential to undermine digitalisation and rapid innovation, economic growth and social benefits from cyberspace.

Another important issue is the absence of cyber resilience, presence of which would allow national infrastructure and services to continue to function even under adverse circumstances, such as an event of a foreign cyber-attack aimed at disabling global network access. Russia successfully conducted tests for establishing a parallel internet by disconnecting from the global network to ensure that local services continue to function in case of adverse consequences of global disconnection from the Internet (Wakefield 2019). Before this, Russia ensured all critical infrastructure/government services had been deployed on local infrastructure.

Last but not the least, the shortfall of competent cybersecurity resources in Pakistan is yet another major problem. This is due to various reasons such as the absence of an established career into the profession, lack of capacity building and accreditation for teaching professionals and lack of opportunities for retaining a high potential workforce in cybersecurity.

6. KEY RECOMMENDATIONS

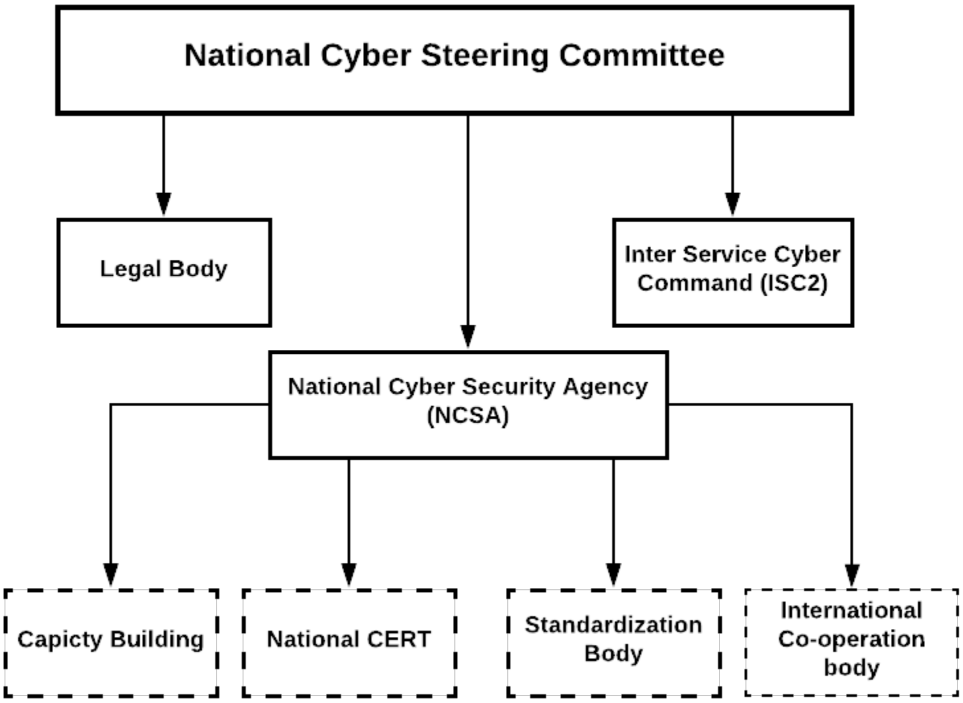
6.1. National Cyber Steering Committee (NCSC)

Strategy and policy enable a country to establish a wide range of objectives, expectations, priorities, and goals to be achieved in a specified timeframe. A National Cybersecurity Steering Committee (NCSC) should be formed under the Prime Minister's Office. It should be the focal authority for international cooperation, legislative matters, offering ease of coordination and enforcement and provide input in strategic decisions.

The Committee should also be delegated the responsibility of formulating a Cybersecurity Strategy and Policy. The developed policy should highlight areas in which Pakistan can develop its capabilities and devise methods to use the instruments developed for the purpose. It should be comprehensive, including both civil and military domains, and take into account global trends and postures on the use of cyber warfare and create policy in conformity with established international norms.

The strategies and policies developed by the NCSC ought to be aimed at improving the security and resilience of national infrastructure, including civilian and military space and e-services. The NCSC should also be responsible for governing the Digital Pakistan Initiative and ensure adequate measures are being taken for effective implementation. It can be comprised of three sub-bodies: National Cybersecurity Agency (NCSA), a legal body, and Inter-Services Cyber Command (Figure 2):

Figure 2: Structure of National Cyber Steering Committee


National Cyber Steering Committee
Legal Body
Inter Service Cyber Command (ISC2)
National Cyber Security Agency (NCSA)
Capicty Building
National CERT
Standardization Body
International Co-operation body

Source: Author’s own.

6.1.1. Legal Body

The legal body should be responsible for formulating laws and regulations in the cyber domain. It should also carry out legislative reforms by improving existing cyber laws. Pakistan currently has a cybercrime law called ‘The Prevention of Electronic Crimes

Act, 2016' (PECA) (GoP 2016). However, it does not have any data protection legislation for ensuring privacy and protection of consumer and citizens' data. Effective data protection legislation would ensure adequate measures for safeguarding citizens' data being taken by public and private organisations. A data protection law will hold the senior management liable and accountable for a breach in case of negligence and will mandate disclosure of breach within a specific timeframe.

6.1.2. Inter-Services Cyber Command (ISC2)

Since the most critical and sophisticated cyber threats may be directed against Pakistan's military services, it is recommended that the Ministry of Defence should establish an 'Inter-Services Cyber Command' (ISC2). The ISC2 should be made under a tri-services model, drawing service members from the Pakistan Army, Air Force, Navy, and Military Intelligence Services. It should be responsible for protecting military cyberspace and tasked with developing policies, strategies, and technologies to protect and defend military assets deployed across the entire spectrum of Pakistan's military services.

It should also be responsible for training military service personnel at their respective academies and institutions to conduct cyber hygiene and to operate safely in the digital domain. The ISC2 may be involved in state-of-the-art R&D to effectively defend Pakistan's weapon systems, military industrial complex, and technologies against cyber-attacks. It should develop policies and capabilities to establish cyber deterrence to ensure that potential adversaries are made aware of Pakistan's capabilities and its intent to counter any cyber-attacks directed against the military.

6.1.3. National Cybersecurity Agency (NCSA)

The NCSA should be responsible for protecting civilian cyberspace by implementing the Cybersecurity Strategy & Policy. It may be aimed at protecting critical infrastructure and improving resilience by providing services such as standardisation of cyber policies, incident handling services, and encouraging dual military-civilian cyber R&D. To accomplish the aforementioned tasks, the following sub-bodies are proposed under NCSA:

National CERT

PECA section 49 describes the Federal Government prerogative for establishing one or more CERTS (GoP 2016). Keeping this in view, a national CERT should be created which to serve as a focal point for reporting all the security incidents against national infrastructure. It should provide incident handling support, early security warnings, and carry out security posture assessments by conducting red teaming and blue teaming exercises across critical infrastructure. Sectoral CERTs for respective sectors (telecom, finance, energy, oil and gas, banking, etc.) may also be formed for better collaboration of threat intelligence data. All sectoral CERTs may report tactical and operational intelligence data to the National CERT. Along with sectoral CERTs, academic CERTs may also be formed to provide research component and serve as a knowledge base.

International Cooperation Body

This body may be responsible for international cooperation and coordination. For this purpose, special coordinators may be assigned for promoting technical cyber cooperation in the form of bilateral and multilateral agreements, formulating strategic partnerships and development of collaborative frameworks under the National CERT. The body should also ensure Pakistan's participation in international cybersecurity forums such as the Forum of Incident Response and Security Teams (FIRST).

Standardisation Body

This body should be responsible for formulating, coordinating and interpreting technical cybersecurity standards. Since Pakistan lacks a cybersecurity baseline framework, it will set expectations for minimum security controls, policies, procedures, and processes that must be in place for safeguarding an organisation's information systems and ensuring security alignment with organisational goals.

Capacity Building Body

This institution should be responsible for reducing shortfall of cyber individuals, retaining high potential cyber individuals, development of indigenous products and special incubation centres for cybersecurity, and raising cyber awareness at the national level. Pakistan's cyber industry, if tapped accurately, can bring massive economic growth and may also aid in complimenting the development of other technological industries.

To facilitate economic growth, cyber innovation and incubation centres may be developed for funding of cybersecurity start-ups to facilitate the development of cutting-edge cybersecurity products. An integrated tech infrastructure with public-private collaboration may also be formed to promote cybersecurity. The ecosystem should be built on key competencies in high-tech research and entrepreneurship, and should be designed to bring together academia, students, and the private sector to promote development in cybersecurity.

To curb the shortfall of cybersecurity individuals, a special programme on the pattern of Unit 61398 PLA China (DeSombre 2016) can be formulated. The individuals admitted to the programme should undergo three years of specialised and extensive cybersecurity knowledge and skill development training led by academic and industry experts.

To offer an established career in cybersecurity, the government should announce separate service cadre for recruitment of such individuals where criteria for qualification may be relaxed, and preference may be given to individuals with skillsets and aptitude over academic qualifications and grades.

The sub-body should also take measures to introduce cybersecurity education and training at the grassroots level. Students, aged 14-18, may be trained under Science, Technology, Engineering, and Mathematics (STEM) programmes during summer sessions. The initiative may act as a feeder programme for joining the special programme mentioned above. The government would need to establish funds to retain these high potential individuals.

ACKNOWLEDGEMENT

The author is highly indebted to Muhammad Tariq, Komal Batool, Shahid Raza, Erum Ranjha, Zikrat Jamil, Rashid Khan, Kamran Khan and Hammad Shamsi for their assistance in bringing various sections of this paper together.

REFERENCES

Benzel, T. 2015, ‘A Strategic Plan for Cybersecurity Research and Development’, *IEEE Security & Privacy,* vol. 13, pp. 3-5.

Brandom, R. 2017, ‘It’s Already Too Late for Today’s Ransomware Victims to Pay Uup and Save their Computers’, *The Verge*, 27 June, <https://www.theverge.com/2017/6/27/15881110/petya-notpetya-paying-ransom-email-blocked-ransomware>.

Chen, T. M. and Abu-Nimeh, S. 2011, ‘Lessons from Stuxnet’, *Computer*, vol.44, no. 4, pp. 91-93.

Daniel, J. 2017, ‘Chinese Theft of Sensitive US Military Technology is still a ‘Huge Problem,’ says Defense Analyst’, *CNBC*, 9 November, <https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html>.

DeSombre, W. 2016, *Getting Harder to Catch Analyzing the Evolution of China’s Cyber Espionage Campaigns against the United States through a Case Study of APT1,* Tufts University, Massachusetts.

Dias, E. 2016, ‘Hillary Clinton Campaign Pushes Back on “Anti-Catholic” Charge’, *TIME,* 5 October, <https://time.com/4528532/hillary-clinton-campaign-pushes-back-on-anti-catholic-charge/>.

DNI 2017, ‘Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution’, Office of the Director of National Intelliegnce, National Intelligence Council, 6 January, <https://www.dni.gov/files/documents/ICA_2017_01.pdf>.

Dukes, E. 2018, ‘The Cost of IOT Sensors is Dropping Fast’, iOFFICE, 11 September, <https://www.iofficecorp.com/blog/cost-of-iot-sensors>.

Erol, M.S. 2015, ‘Hybrid Warfare Studies and Russia’s Example in Crimea’, *Gazi Akademik Bakış,* vol. 9, no. 17, pp. 261-277.

Gady, F.S. 2015, ‘New Snowden Documents Reveal Chinese Behind F-35 Hack’, *The Diplomat*, 27 January, <https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/>.

GoP 2016, *The Prevention of Electronic Crimes Act, 2016,* Government of Pakistan, <http://www.na.gov.pk/uploads/documents/1470910659_707.pdf>.

Greenberg, A. 2019, ‘A Brief History of Russian Hackers’ Evolving False Flags’, *The Wired*, 21 October , <https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/>.

Healey, J. 2017, *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities,* Committee on Armed Services, House of Representatives, One Hundred Fifteenth Congress, First Session, H.A.S.C. No. 115-8, Washington, D.C.: U.S. Government Publishing Office, <https://www.govinfo.gov/content/pkg/CHRG-115hhrg24680/pdf/CHRG-115hhrg24680.pdf>.

Hosenball, M. Eckert, P. and Maler, S. 2011, ‘China Under Suspicion in U.S. for Lockheed Hacking’, *Reuters*, 3 June, <https://www.reuters.com/article/us-lockheed-china/china-under-suspicion-in-u-s-for-lockheed-hacking-idUSTRE7517B120110602>.

ITU 2019, ‘Global Cybersecurity Index (GCI) 2018’, International Telecommunication Union, <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>.

Kaska, K. Beckvard, H. and Minarik, T. 2019, ‘Huawei, 5G and China as a Security Threat’, Estonia: Cyber Defence Centre of Excellence (CCDCOE), <https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf>.

Kelley, M. B. 2013, ‘The Suxnet Attack on Iran’s Nuclear Plant was “Far More Dangerous” than Previously Thought’, *Business Insider*, 20 November, <https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>.

Kovacs, E. 2012, ‘MI6 Call, Possibly to FBI, Leaked by TeaMp0isoN (Audio)’, *Softpedia News*, 12 April, <https://news.softpedia.com/news/MI6-Call-Possibly-to-FBI-Leaked-by-TeaMp0isoN-264168.shtml>.

Mengting, L. and Lee, C. 2019, ‘US Blacklist on Huawei: Leverage for the US-China Trade Talks?’, Singapore: S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, 7 June, <https://www.rsis.edu.sg/rsis-publication/cms/rsis-wto-parliamentary-workshop-us-blacklist-on-huawei-leverage-for-the-us-china-trade-talks/#.XpTED8gzbIU>.

Martin, D. 2016, ‘Russian Hacking proves Lethal after Ukrainian Military App Hijacked’, *CBS News*, 22 December, <https://www.cbsnews.com/news/russian-hacking-proves-lethal-after-ukrainian-military-app-compromised/>.

Marvin, T. R. 2015, ‘World War II Information Security: Hacking the Enigma’, *Kaspersky*, <https://www.kaspersky.com/blog/ww2-enigma-hack/8628/>, accessed 23 December 2019.

Myers, R. 2015, ‘British Hacker Suspected of Cyber Attack on US Central Command Twitter Account’, *Mirror*, 13 January, <https://www.mirror.co.uk/news/world-news/british-hacker-suspected-cyber-attack-4974855>.

O’Hara, T. F. 2004, ‘Cyber Warfare/Cyber Terrorism’, USAWC Strategy Research Project, Masters Thesis, Carlisle, Pennsylvania: U.S. Army War College.

Paul, L. and Paul, H. 2018, ‘Leaked: Cambridge Analytica’s Blueprint for Trump Victory’, *The Guardian*, 23 March, <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory>.

Quadir, S. 2019, ‘Bangladesh to Sue Manila Bank over $81 Million Cyber Heist: Cenbank Governor’, *Reuters*, 30 January, <https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-to-sue-manila-bank-over-81-million-cyber-heist-cenbank-governor-idUSKCN1PO19J>.

Roberts, J. J. 2016, ‘Sneaky Ads on Twitter Tell Voters to Text Votes for Hillary Clinton’, *Fortune*, 3 November, <https://fortune.com/2016/11/03/text-vote-hillary-clinton/>.

Robinson, M. Jones, K. and Janicke, H. 2015, ‘Cyber Warfare: Issues and Challenges’, *Computers & Security,* vol. 49, pp. 70-94.

Shin, J. 2008, ‘Psychographics in Politics’, *Encyclopedia of Political Communication*, vol. 1, pp. 665-665, DOI: 10.4135/9781412953993.n549.

Siobhan, G. and Shara, T. 2011, ‘Security “Tokens” Take Hit’, *The Wall Street Journal*, 7 June, <https://www.wsj.com/articles/SB10001424052702304906004576369990616694 36>.

The Tribune 2019, ‘Pakistan Ranked Among Least Cyber Secure Countries’, 13 February, <https://tribune.com.pk/story/1909680/8-pakistan-ranked-among-least-cyber-secure-countries>.

Tim, M. and Rubenstein, P. S. 2017, ‘American Voters Back Sanctions for Russian Hacking, Quinnipiac University National Poll Finds; Israel, Palestinians Not Sincere About Peace, Voters Say’, Hamden: Quinnipiac University, <https://poll.qu.edu/national/release-detail?ReleaseID=2417>, accessed 25 April 2020.

Wakefield, J. 2019, ‘Russia “Successfully Tests” Its Unplugged Internet’, *BBC News*, 24 November , <https://www.bbc.com/news/technology-50902496>.

Zetter, K. 2016, ‘Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid’, *Wired*, 3 March, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.