National Defence College E-Journal
(NDC E-JOURNAL)
https://ndcjournal.ndc.gov.bd/ndcj

THE DYNAMICS OF CYBERSPACE AND NATIONAL POWER: CONTINUITY AND CHANGE

Khaled M. Khan
Department of Computer Science and Engineering, College of Engineering,
Qatar University, Doha, Qatar.

(Received: 03rd August 2020; Revised: 10th October 2020; Published: 28th October 2020)

Abstract: This paper attempts to provide policymakers with an overview of cyberspace in support of their national power and national security preparedness. In this regard, it presents foundational issues and the dynamic nature of cyberspace that decision-makers often need to deal with in their policy-making process. It discusses the main building blocks of the topic and analyses how nation-states can effectively utilize cyberpower in cyberspace as an instrument of national power. The paper outlines the critical challenges posed as well as opportunities provided by cyberspace that developing countries can explore to consolidate national power. It finally proposes a set of recommendations with national cyber defensive and offensive protocols for nation-states such as Bangladesh.

Keywords: *Cyberspace; cybersecurity; cyberpower; cyber warfare; cyber strategy; national power*

INTRODUCTION

The rapid proliferation of computers and the associated technologies in the digital world has brought about fresh opportunities as well as challenges to nation-states. This digital world, although virtual, is increasingly becoming a vital component of the national power structure in the context of conflicts between nation-states. The main communication melting pot in this digital world is called cyberspace – a man-made intangible digital domain. During the early age of our civilization, the main operational domains of conventional warfare were limited only to land and sea. Nations developed their armies and navies only for these two domains (*Kaspersen, 2015, p. 1*). In the Twentieth century, the invention of aircraft and later, space rockets resulted in two more domains, air and space. Today, we have the fifth operational domain, that is, cyberspace – a virtual world of connectivity (*Schreier, 2015, p. 10*).

Cyberspace exists as a conceptual entity that is based on connectivity to create, store, exchange and manipulate information via autonomous and interconnected networks using computer technologies. Cyberspace is not a physical place - rather, it is a digital environment governed by networks of computers and telecommunication infrastructures (*Wingfield, 2000, p. 17*). However, rapid technological advancements and innovative ideas are constantly changing and reshaping cyberspace; hence, it is dynamic. The degree of change can be considerable, and it could be dramatic (*Kramer, 2009, p. 2*). These changes introduce opportunities as well as challenges. For example, twenty years ago, wireless communication in public places and households were unimaginable. The introduction of wireless network has elevated cyberspace to a different height in terms of efficiency and convenience. However, it also introduces a new set of threats to cyberspace. The recent invention of quantum computing, which is 100 million times faster than existing computers, is a case in point. While this provides a much higher computing power, hackers can also use the same machine to crack securities in a faster manner, thereby altering the cybersecurity landscape to a considerable extent.

This dynamic nature of cyberspace now demands a reassessment of the established national cyber strategy of many nation-states. This is particularly true for developing nation-states like Bangladesh. To utilize cyberspace as a part of national power, it is a prerequisite for developing nation-states to understand the dynamism of cyberspace, and other related areas such as cybersecurity, cyberpower, cyber warfare, and cyber strategy in the context of modern conflict (*Schreier, 2015, p. 8*). This understanding helps nation-states formulate their national cyber strategy considering the evolving nature of cyberspace. Based on the foregoing context, the objectives of this paper are set to:

- Discuss the main building blocks of cyberspace.
- Explore how and why major players in the global arena are aggressively investing on the cyber front.
- Highlight the challenges and opportunities that cyberspace has brought about, and
- Recommend ways for developing nation-states to explore opportunities and tackle challenges to enhance national security.

With these objectives in view, this paper draws upon existing literature from various fields ranging from conventional battles to modern cyber warfare. The recent advances in computing technologies, the contemporary cybersecurity landscape, different security policy frameworks adopted by key players in the global stage as well as prior experience of the author in the field have significantly contributed to the recommendations made in this paper.

The next section is on the vocabulary encompassing the topic of cyberspace. Then, a review of cyber strategies of some nation-states is provided. Next, the paper outlines major challenges as well as opportunities that developing countries can explore along with a set of recommendations for countries like Bangladesh. The paper then closes with some concluding notes.

VOCABULARY FOR THE CYBER REALM

Beyond the daily news of cyber incidents, cyber-enabled coordinated assaults on nation-states are real (*CSIS, 2020*). To tackle such assaults, nation-states should have a good understanding of the full spectrum of the cyber realm such as cyberspace, cybersecurity, cyberpower, cyber warfare, and cyber strategy.

Cyberspace

One can find numerous definitions of cyberspace as there is no officially agreed definition. The metaphor *cyberspace* was probably first popularized in the mid-1980s by Gibson (*1984*) in his science fiction book *Neuromancer*. Later, in the mid-1990s, people began to use cyberspace and information superhighway interchangeably to refer to the global digital connectivity. These metaphors were chosen deliberately to suggest the usefulness, speed, and the nature of the Internet (*Dzieza, 2014*).

Cyberspace is an information superhighway where data move, rest, and are produced (*White, 1994, p. 51*). Origins and destinations of data are entities such as machines, databases, human users, etc. In cyberspace, humans deploy and use man-made technologies to create effects in other operational environments such as air, land, space, and sea. The national cyberspace of a nation-state consists of government, military, financial, telecommunication, and industrial networks; and it is a part of a global information superhighway.

Cyberspace connects other operational domains because they need to exchange, manipulate, and process vital critical data. Cyberspace provides huge operational effectiveness to other domains in terms of efficiency, effectiveness, speed and convenience. Cyberspace is the only domain in which all tools and tactics of national power such as diplomatic, military, and economic can be concurrently exercised through the manipulation of information (*Schreier, 2015, p. 13*). However, this superhighway of digital connectivity is not free from hazards. The most alarming of such hazards is the security issue in cyberspace.

Cybersecurity

Security is a major issue in cyberspace. Nation-states, criminals and even amateurs can attack the flow of information in cyberspace by making data or systems unavailable, destroying data, stealing data, and gaining control of digital entities of others. Every component of cyberspace such as network, computers, devices, software is susceptible to security problems due to deliberate attacks, accidents, or malfunctions of devices. These components have vulnerabilities which attackers exploit to launch attacks using cyber weapons. A cyber weapon used in a cyber-attack is anything that influences, impacts, or changes elements of systems of others.

Modern conventional military forces are increasingly becoming vulnerable to attacks due to excessive dependence on net-centric weaponry, which utilizes software and network to gain competitive advantages in a conflict (*Andress et al.,* *2014, ch. 1, p. 5*). This capability relies on open systems that require real-time information updates using cyberspace. For example, fifth-generation multirole combat fighters such as F-35 Lightning II, Chengdu J-20, and Sukhoi Su-57 are open systems, meaning these aircraft depend on connectivity to update and integrate real-time information during combat operations. This dependency makes net-centric modern military arsenals a valuable target for cyber-attacks.

In addition to the weaponry systems, even the logistics, military command, and control systems as well as financial systems heavily rely on cyberspace. To defend malicious activities in these systems, nation-states deploy protection mechanisms. The effectiveness of such defence heavily depends on cyberpower of nation-states. To utilize cyberspace for offensive purposes, nation-states need cyberpower too. In the contemporary world, there is a direct link among cyberspace, cybersecurity and cyberpower. Cyberspace is an operational environment where adequate cyberpower of nation-states could address their cybersecurity issues.

Cyberpower

Cyberpower is the capability of an individual, an organization, or a nation-state using cyberspace to explore advantages effectively and efficiently (*Kuehl, 2009, p. 38*). Cyberpower is a measure of someone's capability of using cyberspace (*Schreier, 2015, p. 14*); that is, it is the degree of ability to control, manipulate and influence cyberspace. Cyberpower can be exercised to take advantages as well as cause disadvantages to others (*Kramer, 2009, p. 48*). The magnitude of cyberpower of a nation-state is determined by (i) its technological advancements in cybersecurity, (ii) adequately skilled manpower in the field, (iii) a robust cyber strategy, and (iv) its degree of dependency on imported technologies.

Cyberpower has some unique characteristics. It is *ubiquitous*, *complementary*, and *stealthy* (*Schreier, 2015, p. 16*). *Ubiquity* refers to its ability to simultaneously generate a strategic effect on other four operational domains; so, cyberpower is pervasive. *Complementarity* means that cyberpower can be exercised as a supporting offensive tool along with other military weaponry systems. Finally, *stealthiness* alludes to the difficulty in identifying actual attackers and their motivation. Besides these three, cyberpower has other properties, namely *speed* and *zero proximity*. With cyberpower, attacks can be launched on opponents at lightning speed. It also enables one to launch an attack at *zero proximity* of targets, from anywhere (*Rattray, 2009, p. 255-256*).

Cyberpower, an indispensable complementary component in modern military conflicts, could be used for offensive as well as defensive purposes. From an *offensive* perspective, cyberpower provides a nation-state with the necessary capability to exploit vulnerabilities of target systems to launch an attack. The cyber offensive can be used to punish an opponent as well as to gain political objectives (*Janczewski et al., 2007, p. xiv*). Cyberpower used for offensive purposes may have far-reaching political, tactical, and military implications if executed skillfully. For *defence*, a nation-state utilizes its cyberpower to safeguard its critical digital assets against potential attacks. A nation-state can have cyberspace supremacy over other nations in terms of cyberpower. Cyberspace supremacy is based on the capability of preventing any attempted interference by opponents through detection and mitigation.

In addition to offensive and defensive capabilities, cyberpower can provide a nation-state with improved situational awareness about the theatre of conflict. For example, an *Advanced Battle Management System* (ABMS) based on the Internet-of-Things (IoT) combat concept provides such capabilities (*Janes, 2020*). Cyberspace superiority is the operational advantage in cyberspace that can be translated into an advantage in cyber warfare.

Cyber Warfare

The definition of cyber warfare is still debatable. In a simple term, cyber warfare is a massively coordinated symmetric or asymmetric digital assault on a nation-state by another state actor(s) to damage critical information infrastructure, as defined by USLegal.com. According to the US Department of Defence (DoD), cyber operations in cyber warfare are the exercises of cyberpower where the main goal is to achieve military objectives or impacts in or through cyberspace (*JCS, 2016*). As cyber warfare is becoming more real, many nation-states are actively arming themselves with cyberpower for potential cyber conflicts. An alarming number of nation-states are aggressively investing more intellectual and financial capitals in cyberspace (*Robinson et al., 2013, p. ix*).

Cyber warfare is an integral part of cybersecurity. Cyberspace can be the virtual battlefield of cyber warfare. Cyberpower enables a nation-state to unleash its cyber weapons using cyberspace on others in cyber warfare. We can see that cyberspace, cybersecurity, and cyberpower are the central concepts in cyber warfare. However, there is a difference between cyber war and cyber warfare. Cyber war is a conflict entirely fought through digital means, whereas cyber warfare is the utilization of cyberpower to achieve a political gain against an opponent.

In cyber warfare, the attacking nation-state needs technological advances for an offensive, whereas the defending nation-state requires robust protection mechanisms to mitigate threats to its critical systems. In other words, the attacking nation-state needs technological advances and skill in launching cyber-attacks (*Coughlan, 2003, p. 2*). The defending nation-state requires cybersecurity skill in managing and protecting its critical information and digital infrastructure. One of the goals of cyber warfare is to create uncertainty and doubt in the minds of military commanders and political leaders to slow the decision-making process of the opponent, thereby increasing the chances of errors (*Schreier, 2015, p. 25*). Misleading an opposing nation is always a part of conventional warfare; cyber-attacks can exactly achieve this. However, cybersecurity incidents are not always considered cyber warfare unless these are associated with political purposes.

The success of cyber warfare mostly depends on two things: *means* and *vulnerability* (*Lewis & Timlin, 2011*). The trained workforce and required computing tools are the *means* that can be utilized for offensive as well as defensive objectives in cyber warfare. The *vulnerability* is the weakness of the opponent's system that can be exploited. Given the potentially damaging impacts of cyber warfare, at present, there is no international treaty or pact in place to police these (*McConnell, 2017*). Therefore, every nation-state needs to have its cyber strategy on how to acquire cyberpower and how to utilize it wisely for their national security.

Cyber Strategy

A cyber strategy is a national policy that actively governs the development, deployment and exercising of cyberpower in cyberspace, and prepares a nation-state for cyber warfare to achieve national strategic objectives. It binds cyberspace, cybersecurity, cyberpower and cyber warfare with the strategic goals of a nation-state. Cyber strategy embodies a set of fundamental principles and beliefs by which a nation-state guides its operations in cyberspace to support its national security objectives. To formulate a cyber strategy, policymakers can use the traditional military tactics, techniques, and procedures (TTPs) that their military has been using for a long time (*Andress et al., 2014, p. 70*).

Usually, cyber strategy is defined under the umbrella of national security policy. Once developed, the cyber strategy needs to be validated by analyzing three properties of any military strategy: *ends*, *ways* and *means* (*Lykke, 1989, p. 3*). *Ends* define the objectives or goals in cyberspace, for example, intercepting enemy's command and control messages. *Ways* formulate how the cyber strategy is to be implemented; and *means* spell out the required resources such as manpower, equipment, technology to execute the strategy. Cyberpower without any specific cyber strategy means that it merely exists without any specific purpose.

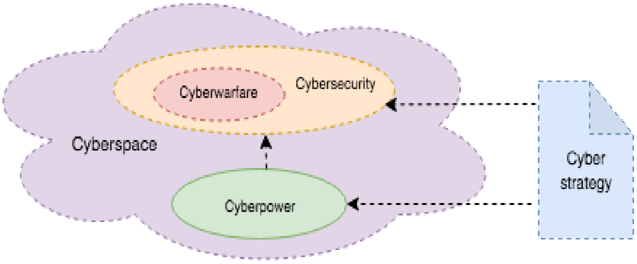

***Figure 1**: A Framework connecting cyberspace, cybersecurity, cyber power, cyber warfare, and cyber strategy.*

Based on the preceding discussion, we can formulate a conceptual framework that connects cyberspace, cybersecurity, cyberpower, cyber warfare and cyber strategy, as shown in Figure 1. According to this framework, cyberspace is a digital operational environment where nation-states, individuals and organizations can exercise cyberpower governed by their cyber strategy, to control, influence and participate in cyber warfare, which is a part of cybersecurity.

CYBER STRATEGIES OF SOME NATION-STATES

Some nation-states continue investing huge resources not only for cyber defences, but also for cyber offences. It was reported in 2016 that the US, the UK, Russia, Israel, and China were believed to be the cyber superpowers because they had acquired significant cyberpower. In a rare acknowledgement, the US announced that its military *Cyber Command* can mount effective cyber-attacks against its opponents at any time (*Breene, 2016*).

The *Cybersecurity and Cyber Warfare: Preliminary Assessment of National Doctrine and Organization* is a useful compendium for various cyber doctrines and strategies (*UNIDIR, 2011*). The report compiled cyber policies of 133 nation-states and pointed out that a total of 33 nation-states included cyber warfare in their national security strategies, and another 36 nation-states did not have any public discussion about cyberspace and security. A similar research sponsored by Sweden was conducted on the cyber-security strategies of ten countries (*Robinson et al., 2013, p. x*). At this stage, we are going to have a quick look at the key aspects of cyber strategies of four nation-states, namely France, the USA, China, and the Russian Federation.

The Cyber Strategy of France

On January 18, 2019, France unveiled its cyber strategy, consisting of a *defensive cyber policy* and a partially unclassified *offensive doctrine*. This strategy confirms that the French approach to cyberspace demonstrates a separation between offensive and defensive cyber operations. Its defensive strategy is limited to reacting to and attributing attacks on its systems and data. The offensive strategy is based on stealthy operations targeting the enemy's cyberspace. The offensive strategy seems to emphasize pre-emptive neutralization of enemy's systems (*Laudrain, 2019*).

France has made it clear that it will launch offensive operations on its opponents if necessary. The French offensive doctrine places great emphasis on the principle of risk balancing against the possibility of an escalation in an asymmetric conflict, or the risk of collateral damage on civilian infrastructures (*Laudrain, 2019*). The main factors for choosing such an offensive doctrine are probably driven by relatively low operating cost, zero proximity and stealthy characteristics of cyberpower in cyberspace along with its technological advancements and capability.

The Cyber Strategy of the United States

The US cyber strategy includes the *Comprehensive National Cybersecurity Initiative* (CNCI), *National Cyber Incident Response Plan* (NCIRP), Homeland *Security/Presidential Directives* (HSPDs) and *National Institute of Science and Technology* (NIST). This strategy focuses on creating and sharing situational awareness of network vulnerabilities and threats and deploying protection mechanisms against the identified vulnerabilities and threats. These defensive objectives were adopted due to weaknesses of the US digital infrastructure.

In 2018, the US Senate Intelligence Committee pointed out that the US was unprepared for cyber espionage and cyber warfare. It was also acknowledged that the opponents of the US were working with a different playbook, and the US failed to put together a comprehensive cyberspace policy (*Fish, 2018*). The main reasons for such unpreparedness include out-dated cyber strategies of the US, a large number of its private cyberspace, the existence of several nation-states and non nation-state actors, the low-cost entry by other nation-states into cyberspace, and continued difficulty in attributing the source of cyber-attacks (*Weber, 2018*).

Considering these weaknesses, later in 2018, the US Department of Defense (DoD) reviewed its cyber doctrine. Since then, the US *Cyber Command* has been taking a more aggressive approach by getting into the enemy's national cyberspace. The offensive principle is based on the notion of persistent engagement so that the opponent never rests (*Pomerleau, 2018*). This line of offensive thinking is pretty much close to the approach taken by France discussed earlier. Both France and the US have acknowledged that offensive cyber operations are not ruled out in conflicts (*Taillat, 2019*). However, the DoD always acknowledges the reality that it is impossible to maintain permanent global cyberspace superiority due to the dynamic characteristics of cyberspace. Unlike the French approach, the US cyber strategy integrates offensive and defensive cyberspace operations.

The Cyber Strategy of China and the Russian Federation

In contrast to the openness of the US and French cyber strategies, it is virtually impossible to locate details about cyber strategies of China. In 1999, Chinese strategists prepared a document called *Unrestricted Warfare*, which discussed some insightful thoughts about the value of network warfare (*Liang & Xiangsui, 1999*). This policy document suggests that China is more aggressive in utilizing cyberspace due to its large skilled manpower. Many suspect that China officially and unofficially maintains many skilled cyber hacker groups or cyber warriors. In a time of cyber conflicts, these could serve as a reserve militia and engage in cyber warfare. Patronizing cyber warriors by China would be a part of cyberpower.

In the case of the Russian Federation, its cyber strategy hints at the fact that they are in an 'information war' with the Western nations (*McConnell, 2017*). Russia does not use the term cyber security, instead, they only talk about information security, which makes it challenging to reach cybersecurity agreements with other nation-states. The Russian Federation has adopted several high-level information security strategy documents in the national and international contexts. However, information about the adopted strategy and policy is not publicly available (*Lewis & Timlin, 2011; Robinson et al., 2013*).

Reasons for Investing in Cyberpower

The cyber strategies of four major countries discussed in the foregoing section suggest that the key players in global power politics have taken cyberspace quite seriously. They have aimed to utilize cyberspace as much as possible as a part of their national security framework. Interestingly, many such nation-states have adopted cyber offensive along with defensive measures as their national security policy. A deeper analysis of various cyber strategies of different nation-states suggests that specific reasons have driven these nation-states to adopt their aggressive cyber strategy. Some of these reasons are outlined below:

- Firstly, nation-states have realized that they may experience cyber-attacks of varying scales today or tomorrow. To address such potential threats, they have kept their pre-emptive options open for cyber offensive on their suspected opponents.
- Secondly, one of the main reasons for adopting offensive strategy is a lack of international act or treaty to prevent, deter, or even stop cyber warfare. In cyber conflict, the involved nation-states had to handle this with their available means without being policed by any international organization like the United Nations.
- Thirdly, these nation-states find cyber-attacks on other nation-states mostly covert, meaning the attacking nation-states could not be attributed. The ability of the attacking nation-state to hide its identity makes cyber offensive more attractive. This characteristic of cyberpower makes it difficult for the defending nation-state to determine how, when, and where to retaliate and respond (*Weber, 2018*).
- Fourthly, to wage cyber warfare on a nation-state, the attacking nation-state does not need to be at closed proximity of the victim state. Cyberspace has removed the distance, time, and space between opponents regardless of their actual physical proximity. This capability is attractive to many.
- Fifthly, obtaining and maintaining cyberpower is less costly compared to advantages gained in terms of offensive as well as defensive capabilities.
- Finally, cyber offensive is easier than defence in cyberspace. Cyber conflict favors the attacker; cyber-attacks may inflict massive systems-level destruction on a society-wide scale (*Schreier, 2015, p. 104*).

These nation-states are fully exploiting the opportunities that are available in cyberspace. They are leveraging and transforming the opportunities in full into their national power.

CHALLENGES AND OPPORTUNITIES FOR DEVELOPING NATION-STATES

No nation-state can afford inaction in the digital era these days. A militarily strong nation-state cannot easily underestimate a militarily weaker opponent with considerable cyberpower. However, developing countries usually face some common challenges in formulating their cyber strategy; these are outlined here:

- *Lack of clear vision of cyber affairs at the national level.* Most developing nation-states do not have any cohesive national policy regarding cyberspace and cyber preparedness.
- *Heavy reliance on imported hardware and software.* A considerable number of nation-states depend on imported computing technologies, which are used in their critical entities such as defence, financial and government organizations. This dependency is a serious threat to their national security.
- *Inadequate budget allocation for cyber operations.* Governments are reluctant to grant adequate funds to relevant organizations for cyber issues due to a lack of understanding of cybersecurity seriousness at the national level.
- *Absence of an appropriate national structure to deal with cyber warfare.* Many nation-states do not have any national level institute that could govern cyber issues at the highest national level.
- *Absence of persistent cybersecurity culture within government bodies.* Most developing nation-states do not have a regular threat monitoring policy on their critical infrastructure such as banks, telecommunication networks, government organizations, and energy sectors.
- *Perceived resistance to change and reassessment of national security issues in light of the new reality.* Governments of developing nation-states seem reluctant to initiate any drastic change to the existing policy and government apparatus.
- *Difficulty in adopting rapidly changing technologies in a timely manner.* Most of these nation-states spend considerable amount of time in making decisions on technology transfer and adoption of new technologies.
- *Lack of research and development initiatives for home-grown digital products.* Research and development is virtually non-existent in most developing nation-states.
- *Lack of efforts to tap into expertise available in the nation-state.* Many developing nation-states already have a sizeable segment of their population who are skilled in computing and cybersecurity. These nation-states do not have any policy in place to tap into these ingenious talents.

Despite these challenges, cyberspace also offers opportunities for developing countries as well.

- *Acquiring cyberpower can be relatively less costly* than conventional military weaponry systems. The entry into cyberspace is relatively cheap because inexpensive dual use computing technologies enable nation-states to utilize cyberspace. For example, a low-cost laptop used for daily routine tasks can be used to launch an attack on an opponent in cyberspace.

- *Developing skilled manpower* is a common challenge for developing nation-states. Proper training and motivation could make a large portion of population skilled in cyberspace and in cybersecurity.
- *Identifying talents in computing technology*, especially in programming and networking, could boost the cyber capability of nation-states. Most developing countries have a treasure of such untapped talented manpower.
- *Developing home-grown technology* could provide much better defence. The ingenious technology invented by local talents could be used to exploit vulnerabilities of other countries to gain supremacy and influence over their rivals. A right policy could initiate this most important ingredient of cyberpower.

Need for a Cyber Strategy

It is evident from the preceding analysis that no nation states can afford to be lagged when it comes to take advantages of the cyber world. However, the question remains: how should developing countries like Bangladesh move forward? The immediate step would be to develop and follow a comprehensive *cyber strategy* that defines a national security goal including the major milestones with specific timeframe required to reach the goal by leveraging the perceived opportunities to gain cyberpower. The milestones are intended to address the challenges posed to the nation-state. Examples of milestones in the strategy could include the following:

- Formulation of a set of principles that serve the interests of the nation-state best. These could be based on the TTPs of the nation-state.
- Establishment of a *robust governing regime* with adequate power and skill to manage cyber affairs.
- Plan for a systematic approach to *building national capacity* in cyber security by identifying and training talented personnel in the nation-state.
- Creation of *mass awareness* about cybersecurity at the national level.
- Development of *home-grown innovative* digital technologies.

These are the keys in a cyber strategy to achieve sufficient cyber strength that can boost national power. The reasons behind the massive cyber-armament of some key nation-states discussed earlier are also worth considering. Those nation-states are actively seeking to further acquire and consolidate cyberpower to utilise fully the advantages offered in cyberspace. Similarly, developing nations can learn from their experience. Despite some challenges, developing countries such as Bangladesh can leverage the opportunities that are already available to them to explore.

Protocols for Cyber Operations

Considering the challenges, opportunities coupled with the identified reasons for key nation-states arming themselves with cyberpower, this section frames some specific recommendations at the operation level for senior military tacticians, planners, and political leaders of developing nation-states like Bangladesh to go forward. Two distinct generic protocols are recommended here; one for offensive, and the other for defensive operations. Either of the two pyramid-shaped protocols embodies ten specific steps in sequential order, grouped into four successive stages: *Plan*, *Operations*, *Resources*, and *Innovation*. See Figures 2 and 3.

- *Plan*: The first four steps in this stage spell out the preparation for the cyber actions defined in the next stage.
- *Operations*: This stage includes three steps dictating what to be executed.
- *Resources*: This involves two steps relating to cyber capacity building.
- *Innovations*. This stage deals with the innovative aspects of cyber technology, that is, the relentless effort to develop home-grown independent cyber weapons and defensive technologies to support *zero trust* principle, which means that no foreign-made or supplied digital products such as computers, programs, network devices and smart-phones should be trusted.

All these steps are governed and executed by the principles defined in the national cyber strategy. We now briefly outline the two protocols.

Cyber Defensive Protocol

This proposed protocol is intended to be used for defensive purposes. It has ten steps, as depicted in Figure 2.

1) *Identify critical assets*: This step involves identifying three types of critical assets of a nation: (i) *Critical systems* such as computers and servers; (ii) *Critical networks* such as sensitive national intra-organizational network topology and corporate network layout; and (iii) *Critical data* such as sensitive information and authentication data.
2) *Assess vulnerabilities and threats*: Conduct monitoring and testing of the identified critical assets using practices such as ethical hacking, intrusion detection, penetration testing and vulnerability analysis.
3) *Deploy protection mechanisms*: Deploy protection mechanisms such as defence-in-depth, intrusion prevention, appropriate access control regime and intelligent firewall to mitigate threats identified in the critical assets.
4) *Monitor critical assets*: Assess the impact and effectiveness of the deployed defensive measures to mitigate identified threats.
5) *Implement disaster recovery*: It is essential to have a disaster recovery plan if attacked. The recovery plan should dictate the resources that need to be deployed in the aftermath of an attack.

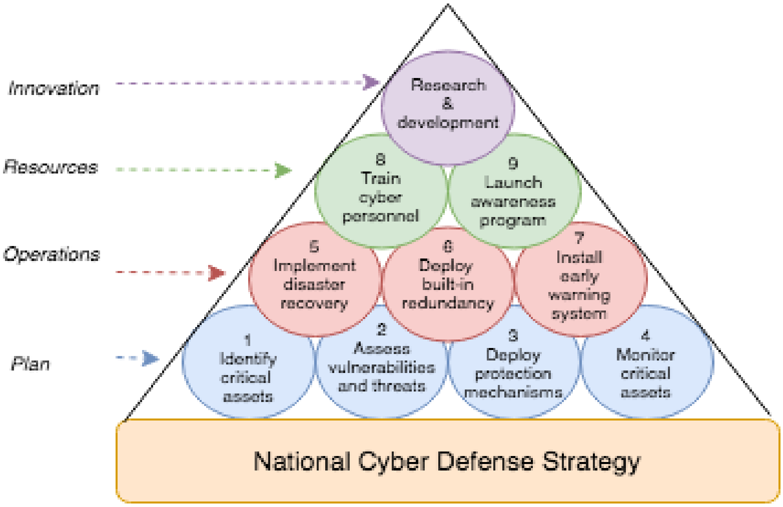
Innovation
Resources
Operations
Plan
Research & development
8 Train cyber personnel
9 Launch awareness program
5 Implement disaster recovery
6 Deploy built-in redundancy
7 Install early warning system
1 Identify critical assets
2 Assess vulnerabilities and threats
3 Deploy protection mechanisms
4 Monitor critical assets
National Cyber Defense Strategy

Figure 2: *Cyber Defence Protocol*

6) *Deploy built-in redundancy*: To be a resilient nation-state, the identified critical assets should be supported with cutting-edge technologies like self-healing capabilities, built-in redundancies, and autonomic computing.
7) *Install early warning system*: These systems are essential because once a system is attacked, other systems or other parts of the system are automatically alerted by early warning systems.
8) *Train cyber personnel*: A nation-state may already have a sizeable, trained cybersecurity workforce serving in government and non-government organizations or as self-employed or free-lancers. They need to be included in a national cybersecurity resource ledger. Once the nation-state is at cyber warfare, these people can be sought for technical assistance. Covertly patronizing cyber warrior groups could also be an option.
9) *Launch awareness program*: During a cyber conflict, a nation-state needs support from its population to enhance its defensive efforts. The population could only contribute if they have elementary knowledge of cybersecurity. Massive Open Online Courses (MOOCs) on cybersecurity could be offered to the population free of charge. Regardless of age or educational background, every citizen should avail himself or herself of these online short courses. This results in a cyber security-aware nation.
10) *Research and development*: A nation-state should have a cyber *R & D* wing at the national level to innovate home-grown ingenious cyber defensive technologies. This supports the *Zero Trust* objective. Most hardware, software and control systems used these days by developing nation-states are manufactured by others. This makes developing countries too vulnerable due to possible hidden malware-spyware in those products.

Cyber Offensive Protocol

The cyber offensive protocol, as shown in Figure 3, also includes ten steps that are self-explanatory.

1) *Identify target assets*: This step selects the target system(s) of the opponent and finds rationale for selecting those targets.
2) *Find out vulnerability*: To launch attack, it is necessary to find out vulnerabilities of the target systems.
3) *Devise offensive protocol*: It includes selecting the timing of the attack, evaluating the current political environment, mode of attack, etc.

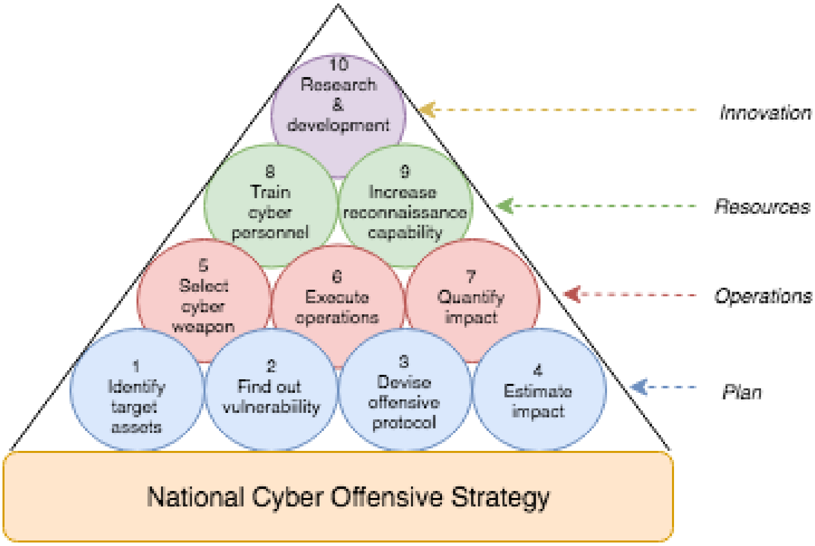

Figure 3: *Cyber Offensive Protocol.*

4) *Estimate impact*: It is quite vital to estimate and assess expected damage on the target system, anticipated reactions, and collateral damages.
5) *Select cyber weapon*: The choice of cyber weapon is to be made in this step along with reasonable justifications for the selected weapons.
6) *Execute operation*: This step fires the cyber weapon on the target system.
7) *Quantify impact*: Gather information about the post-attack scenario and the impact of the attack.
8) *Train cyber personnel*: The step is identical to that we have already discussed in relation to the defence protocol.
9) *Increase reconnaissance capability*: It involves activities such as capacity building for cyber espionage, reconnaissance, and surveillance on the enemy's digital systems.
10) *Research and development*: This step involve researching, innovating and developing home-grown niche technologies for advanced *offensive* operations based on the principle of *Zero Trust*.

Governing Cyber Affairs

Management of cyber affairs requires a thoughtful approach. Different nation-states have taken different approaches and management models of response to cyber warfare at the national level. For example, in some nation-states, the police department is responsible for dealing with cybercrime; national security agencies look after cyber espionage and surveillance activities; an inter-departmental committee tackles issues related to cyber warfare (*Robinson et al., 2013*). The task of formulating a national cyber strategy is usually allocated to a national coordinating authority composed of military and non-military government agencies. In some cases, newly created offices, and in others, the existing departments are assigned the cyberspace affairs. All these vary from nation to nation. There is no uniform structure followed by nation-states.

For example, the US has the *National Cyber Security Division* under the Department of Homeland Security, and *Cyber Command (CYBERCOM)* is under the Department of Defense. France has created *Strategic Commission for the Defense of National Information Systems* under the Ministry for Homeland Security and the National Agency for Information System Security. Germany has formed the *National Cyber Response Centre* under the Federal Office for Information Security and the National Cyber Security Council.

CONCLUSION

The paper has discussed the dynamic nature of cyberspace and the major building blocks related to cyberspace along with some case studies of cyber strategies. It has also pointed out possible reasons why some nation-states have invested aggressively for cyber offensive operations. The paper has identified major challenges and opportunities that developing nation-states could explore. It has finally tabled a set of recommendations for developing countries to consider on how to obtain cyberpower by leveraging opportunities and addressing challenges.

Rapid technological innovations and operational creativity have transformed cyberspace into an influential phenomenon of the national power structure of nation-states. Denying this reality by a nation-state may result in not-so-good consequences. We have seen in this paper a global cyber arms race among some nation-states. Cyberspace is not technically flawless, many security vulnerabilities plague cyberspace. These are difficult challenges. The emergence of cyberspace not only raises challenges but also provides opportunities for developing nation-states. Developing nations can aim to utilize this dynamic space and tackle the challenges for national interests.

Cyberspace has several intrinsic properties suggesting its evolution in the future may differ considerably from its current state. Decision-makers are therefore advised to formulate cyber strategies for a dynamic context. This approach requires developing a cyber strategy that is sufficiently flexible to adapt to changes in the future. The power of human invention of technologies ultimately influences the dynamism of cyberspace.

We can postulate that any future conflict between nation-states will likely use cyberspace as a part of their theatre of conflict. In this context, developing nation-states cannot afford to opt out of national cyber preparedness by underestimating the notion that cyberspace can be used as a theatre of conflict. Nation-states need practical-oriented cyber strategy aligned with their national security priority, policies, and interests. The ultimate objective of developing nation-states is to formulate their cyber doctrine – a comprehensive manual that guides their cyber affairs.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to the Department of CSE, College of Engineering, Qatar University. He also presents his appreciation to the Editors, coordinators, and the reviewers of the *NDC E-JOURNAL* for their insightful inputs to improve the manuscript.

REFERENCES

Andress, J., Winterfeld, S., & Ablon, L. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Second edition, Elsevier, The Netherlands.

Breene, K. (2016). Who are the cyberwar superpowers? *World Economic Forum*. [Online] Available at: *https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers* (Accessed: July 30, 2020).

Coughlan, S. (2003). *Is there a common understanding of what constitutes cyber warfare?* The University of Birmingham School of Politics and International Studies.

CSIS. (2020). *Significant Cyber Incidents*. Center for Strategic and International Studies. [Online] Available at: *https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents* (Accessed: September 11, 2020).

Dzieza, J. (2014). A history of metaphors for the internet. *The Verge*. August 20. [Online] Available at: *https://www.theverge.com/2014/8/20/6046003/a-history-of-metaphors-for-the-internet* (Accessed: September 11, 2020).

Fish, D. (2018). Warner: U.S. Needs a New Doctrine in Cyberspace. *Decipher*. [Online] Available at: *https://duo.com/decipher/warner-us-needs-a-new-doctrine-in-cyberspace* (Accessed: July 20, 2020).

Gibson, W. (1984). *Neuromancer*. Publisher ACE.

Janes. (2020). US Air Force performs first Advanced Battle Management System demonstration. *Janes*. [Online] Available at: *https://www.janes.com/defence-*

news/news-detail/us-air-force-performs-first-advanced-battle-management-system-demonstration (Accessed: July 24, 2020).

JCS. (2016). Dictionary of Military and Associated Terms (JP 3-0), Joint Chiefs of Staff, Joint Publication 1-02, *Department of Defense*, Washington D.C. Amended. on 15 February 2016. [Online] Available at: *https://fas.org/irp/doddir/dod/jp1_02.pdf* (Accessed: July 17, 2020).

Janczewski, L. & Colarik, A. (2007). *Cyber Warfare and Cyber Terrorism*, Hershey, Idea Group Inc.

Kaspersen, A. (2015). *Cyberspace: the new frontier in warfare*. World Economic Forum.

Kramer, F., Starr, S., Wentz, L. (2009). *Cyberpower and National Security*. National Defense University Press. USA.

Kuehl, D. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. Kramer, D., Starr, S., & Wentz, L. Eds Cyberpower and National Security.

Laudrain, A. (2019). France's New Offensive Cyber Doctrine. *The Lawfare Institute*, Brookings. [Online] Available at: *https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine* (Accessed: July 23, 2020).

Liang, Q, Xiangsui, W. (1999). *Unrestricted Aarfare. People's Liberation Army (PLA).* Literature and Arts Publishing House, Beijing.

Lewis, J. & Timlin, K. (2011). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. Center for Strategic and International Studies. Washington D.C., CSIS, UNIDIR.

Lykke, A. (1989). Defining Military Strategy. *In Military Review*. US Army Command and General Staff College.

McConnell, B. (2017). Tomorrow's Challenge: Cooperation in the Cyber Realm. *EastWest Institute*. [Online] Available at: *https://www.eastwest.ngo/idea/tomorrow's-challenge-cooperation-cyber-realm* (Accessed: July 13, 2020).

Pomerleau, M. (2018). DoD releases first new cyber strategy in three years. *Fifthdomain*. [Online] Available at: *https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy* (Accessed: July 17, 2020).

Rattray, G. (2009). An Environmental Approach to Understanding Cyberpower. In *Cyberpower and National Security*, Franklin D. Kramer. Stuart H. Starr & Larry K. Wentz, eds., Dullas, VA, Potomac Books.

Robinson, N., Gribbon, L., Horvath, V., Cox, K. Rand. (2013). *Cyber-security threat characterization –A rapid comparative analysis*. Rand Corporation.

Schreier, F. (2015). *On Cyberwarfare*. 2015 DCAF Horizon Working Paper No. 7.

Taillat, S. (2019). Signalling, Victory, and Strategy in France's Military Cyber Doctrine. *War on The Rocks*. [Online] Available at: https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine (Accessed: July 14, 2020).

UNIDIR. (2011). *Cyber security and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization.* Center for Strategic and International Studies.

Weber, R. (2018). Revised DoD cyber doctrine highlights limits to U.S. powers. *Inside Defense.* [Online] Available at: https://insidedefense.com/insider/revised-dod-cyber-doctrine-highlights-limits-us-powers (Accessed: July 23, 2020).

White, H. (1994). The Role of Information Intermediaries and the Superhighway. In *Information Superhighway: The Role of Librarians, Information Scientists, and Intermediaries*. Helal, A., Weiss, J, Eds. Essen University Library.

Wingfield, T. (2000). *The Law of Information Conflict: National Security Law in Cyberspace*. Aegis Research Corporation.

AUTHOR

Dr. Khaled Khan is an Associate Professor in the Department of Computer Science and Engineering, Qatar University. Before this, he served Western Sydney University (Australia) as a Senior Lecturer and the Head of postgraduate programs for several years. Dr. Khan received his BS and MS in computer science and informatics from the Norwegian University of Science and Technology. He received his Ph.D in computing from Monash University, Australia. He has a second bachelor degree from the University of Dhaka.

He also completed some intensive courses such as Cybersecurity Risk Management offered by Harvard University; a course on the Economics of Blockchain provided by Massachusetts Institute of Technology (MIT); and another course on Blockchain technology offered by the University of California, Berkeley.

Dr. Khan has published more than 100 technical papers, four books, and holds a U.S. Patent. He was the founding *Editor-in-Chief* of the International Journal of Secure Software Engineering (IJSSE) from 2009-2017. He is a senior member of IEEE.

E-mail: *khaled.sydney@gmail.com*