The Implications of State-sponsored Cyber Attacks in South Asian Countries

Tanvir Hassan Zoha, Sifat-Nur-Billah
Bangladesh University of Business and Technology
Bangladesh

Abstract

The prospect of a state-sponsored or organized-group (e.g., terrorist) cyber-attack is a rising concern for both government and private strategists. In our research we have found that South Asian country governments are apathetic about cyber security. Apathetic does not require state-sponsored hackers to exert too much effort to easily embarrass the governments of South Asian countries. Because the government does not exchange data in the name of protecting confidentiality, so that criminals are taking advantage of this gap to commit even greater crimes. We also found that there is a tendency of hiding cyber incidence, criminal data exchanging, data briefing of name pad and those dark date are available on deep web. In the days to come, using social media will create political problems from one country to another. To save the digital infrastructure of South Asian countries government should take actual professional initiative. Android Security need to increase and also social If the South Asian countries are attacked, It is an unavoidable conclusion that the South Asian countries will retaliate and make every effort to neutralize the offense with active defence.

Keywords: *State Sponsored Hacking, Cyber Security, Malware Attack, Cross border judicially, Cyber War*

1. Introduction

Government funding of violent non-state actors involved in terrorism is state-sponsored terrorism. States can support terrorist groups in a variety of ways, including by sponsoring terrorist organizations, providing training, providing weapons, and hosting terrorist groups within their borders. Due to the pejorative nature of the term, the identification of clear examples is generally subject to political lawsuits and varying concepts of terrorism. Cyber-attacks funded by the South Asian Country governments are on the rise and display no signs of taking hold. The states, considering the threats raised by these attacks owing to the challenge, responsible citizens also flee with impunity, in attributing their origins to cyber-attacks. As a consequence, the current scholarships are almost exclusively focused on survival technical barriers in the technical field. This note shows that there is a legal solution rather than a legal one. Technologically, the issue of attribution can be solved. Second, in spite of data scientists have established barriers to attribution. A collection of instruments for monitoring cyber-attacks and empirically large-scale cyber-attacks state attacks appear to leave behind ample footprints to lead forensic experts to their source (or circumstantial evidence).

Apart from terrorists, state actors are manipulating the exceptional situation by using targeted phishing emails, so-called "spear phishing," for intelligence purposes, seeking to work covertly in cyber space to escape political accountability. Hacker groups that are suspected to be funded by Russia, China and North Korea use customized emails with references to the pandemic in order to infect or pick up malware on their goals. In the pandemic of COVID-19, which reveals once again the national security not only should conventional military threats be handled, the collection of intelligence services online information, so-called Signals Intelligence (SIGINT), is turning its attention to new goals. Political and military organizations are classical SIGINT objectives that might, for example, provide information on the processes of strategic decision-making or military capabilities of a country government. In addition to counterintelligence, i.e., defense against other activities, another significant area of activity of Internet intelligence services is intelligence services and industrial espionage.

Governments are currently keenly interested in collecting information on the proliferation of the corona virus, various national policies on the virus and possible medicines, as well as vaccines. This data will provide crucial strategic advantages in the war against a pandemic. Consequently, in particular, health-care, pharmaceutical and biotechnology institutions and organizations, government organizations in these fields are coming into the crosshairs of intelligence services, as are logistics infrastructures. The main contribution of this paper as follows:

- South Asian country governments should work together to prevent cyber wars.
- To check the cyber operations by non-state actors to ease the potential financial misfortunes that will

 | DOI: 10.20533/ijcc.2046.3359.2022.0026

be caused by state or companies due to such assaults within the future.

- Raise the android security and social media awareness to reduce cybercrimes.

- To implement the blockchain technology in all South Asian country for prevent the cyber attacks

The rest of this paper is organized as follows: Section 2 illustrates the related work. Section 3 introduces the overall design and working procedure. Section 4 describes the conclusion of this paper.

2. Literature Review

Chen et al., [1] addresses APTs as a new threat pattern. The authors present a report on APT, extract and display its characteristics, and examine APT attack methods. Cole et al., [4] refers to APT as a cyber-disease. He outlines what APT is, who it attacks, what it looks like, and how to protect against it. Another writer Yang et al., [5] is an example, The authors proposed a dynamic model for detecting APT and a new security metric called "equilibrium security."

On the other hand, certain studies look at Stuxnet in a variety of ways. Farwell et al., [2] describes Stuxnet, its past, and its capabilities as a weapon in. Karnouskos et al., [3] discusses the characteristics of Stuxnet, its implications, and some ideas for next-generation SCADA/DCS systems. Matrosov et al., [6] provide a thorough analysis of Stuxnet. They go over the Stuxnet aim, the Stuxnet distribution, and the Stuxnet implementation in detail. Kushner et al., [7] reveals the true story of Stuxnet, how it operates, and malware milestones.

Another work from Zhioua et al. [8] provides a technical overview of the attack vectors used by the three most well-known malware, namely Stuxnet, Flame, and Shamoon. They go over their key modules, their advanced spreading capabilities, and how they differ from traditional malware. This paper's main goal is to highlight recent developments influenced by this latest breed of malware.

Our research review shows that there were slight works depleted on State Sponsored cyber-attack vectors used by the Stuxnet, Flame malwares. The State sponsored cyber-attack are not focused on the high security system that how they can prevent the state sponsored cyber-attack which is now happening in South Asian Country. In our research, we will try to show the types of state sponsored cyber-attacks and how to save the digital infrastructure of South Asian countries government to prevent the state sponsored cyber-attacks (see Figures 1 and 2).

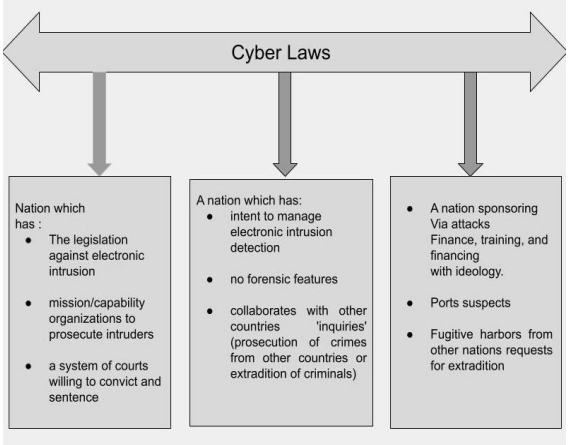

Figure 1. Spectrum of cyber law compliance

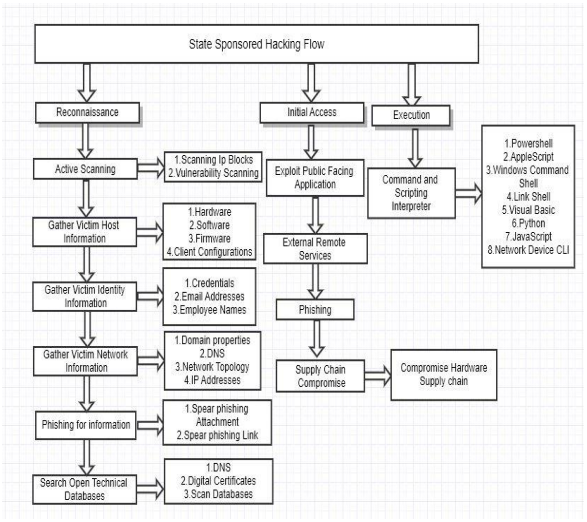

Figure 2. State Sponsored Hacking Flow

3. Methodology

The methodology of the proposed model is discussed in this section. This section is divided into two sections, one for system design and one for process. The sub-sections are arranged sequentially from the model's input to output process, with comprehensive explanations. Furthermore, it depicts the architecture's overall workflow.

3.1. Cyber-attacks in South Asian Countries are on the rise

Cyber-attacks continue to rise at various commercial and service-providing outlets around the world, despite multiple preventive measures. The country has made significant progress in the digital age, especially on the socioeconomic front, and the number of cyber-related incidents is on the rise. The topic of cyber security has become more important as

 | DOI: 10.20533/ijcc.2046.3359.2022.0026

a result of an increase in information technology-related crimes.

Bangladesh e-Government Computer Incident Response Team of the Ministry of Posts, Telecommunications, and Information Technology (BGD e-Gov CIRT), the number of incidents reported with the organization increased to 870 in 2018 from 683 in 2017. In 2016, the figure was 379. Vulnerability accounts for 63.2 percent of the attacks, intrusion or hacking for 5.7 percent, malicious code for 22.5 percent, offensive material for 4.5 percent, and fraudulence, intrusion attempts, service requests, information protection, and others account for the remainder.

The true number of attacks is much higher since many commercial or service-provider outlets do not report such incidents to the state-owned special agency. More recently, the government developed the BGD e-Gov CIRT under the Bangladesh Computer Council shortly after the Bangladesh Bank's reserve heist (BCC). It was created to protect against any potential fatal intrusions.

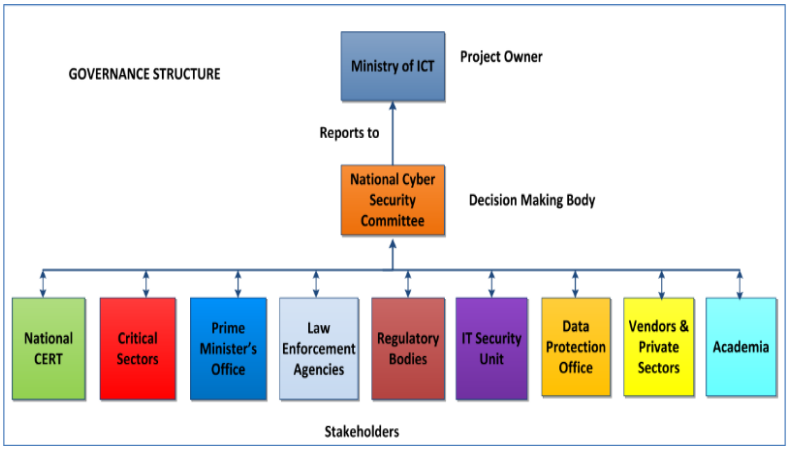

Figure 3. Governance Structure

To prevent the cyber-attacks, all South Asian Countries have to maintain the cyber law compliance. Need to provide the VAPT training for protect the Government National Databases by providing visibility of security weaknesses and guidance to address them.

Collaboration between government, corporate, and private stakeholders is vital to the strategy's success because it requires both key public and private sector players to work together to protect the country's information infrastructure. An effective public-private partnership for cyber protection would allow the detection of threats, suspicious activities, and other anomalies, and react to them, as well as build a more stable network. This collaboration would also pave the way for research and development as well as the identification of security threats. Finally, this will assist stakeholders in better responding to cyber threats.

3.2. Cyber Security Strategic Guidelines

In accordance with the strategic guidelines, a national cyber security strategy is established. This will help to create the conditions for the realization of the national cyber security vision. The steps to achieve the national cyber security priorities will be outlined in a separate action plan. The strategic guidelines' implementation would enhance national and international cooperation. This type of collaboration would support the entire community while also assisting the major players in the cyber security industry. The resilience of society's core functions against cyber security disruptions is based on the long-term development of capabilities, their ease and versatility in use, and the long-term creation of capabilities.

To protect our cyberspace and provide a first line of protection against cybercrime.

Our project aims to establish a cyber-security strategy that avoids cyberspace intrusion and attack by enhancing capabilities, articulating responsibilities, and designing effective responses for both the public and private sectors. By establishing or improving mutual situational knowledge of network flaws, Threats and incidents, as well as the ability to respond rapidly to reduce existing vulnerabilities and avoid intrusions, will all contribute to the safety of our cyberspace. In addition, this strategic guideline focuses on improving law enforcement agencies' ability to detect and prosecute cybercrime. International collaboration and knowledge sharing can be used to practice and improve cyber security against cybercrime.

 | DOI: 10.20533/ijcc.2046.3359.2022.0026

To improve our cyber-resilience and our ability to protect against a wide range of threats.

Scaling up efforts to protect critical infrastructure and networks in order to provide equal assurance of resilience and protection to support national missions and economic stability is one of the strategic recommendations of the National Cyber Security Strategy. The states of the economy in the nation, critical infrastructure safety and robustness, which can impact a nation's ability to function effectively in a crisis if they fail, are becoming increasingly necessary for security and quality of life. Government information infrastructure and networks will be given top priority, and will be secured from cyber-attacks by security assessments and the global and international information security regulations are being implemented. The goal is to identify and recognize critical function disturbances and react in a way that minimizes their negative consequences.

To create an effective partnership model between the government and the private sector in order to advance national cyber security and cyber defense.

The strategic guidelines of the Cyber Security Strategy are reinforced by increased active cooperation among actors with the aim of achieving shared situation awareness and effective cyber threat defense. To make identifying critical IT infrastructures and systems easier, a standard set of criteria will be created. A framework for assessing risk and vulnerability will be established. Encouragement of knowledge exchange and regulation, as well as cooperation between authorities and the business community, would help advance cyber security.

3.3. National Cyber Security Strategy and Action Plan Importance

The ICT sector has an effect on people's lives, as it contributes directly or indirectly to various sociology-economic parameters such as jobs and living standards. It is making a major contribution to Mauritius' transformation into an African cyber-hub. The government has been a key driver for increased adoption and promotion of IT-based products and IT-enabled services in the public sector (e-Government services to citizens), education (e-learning, virtual classrooms), and financial services (mobile banking, Internet banking). The country's IT adoption has increased as a result of these interventions.

Given Mauritius' rapidly expanding ICT sector, ensuring a secure computing environment has become one of the country's top priorities. Cyberspace is vulnerable to a variety of events that could stymie economic, political, and social change, as well as public health, security, and national security activities. Information loss and theft can have a significant impact on reputation, confidence, and brand value.

Malicious behaviors, on the other hand, can be mitigated by early identification, knowledge sharing, investigation, and well-organized response and remediation. The protection of information technology, as well as the confidentiality, fairness, and availability of information, describe a secure cyberspace.

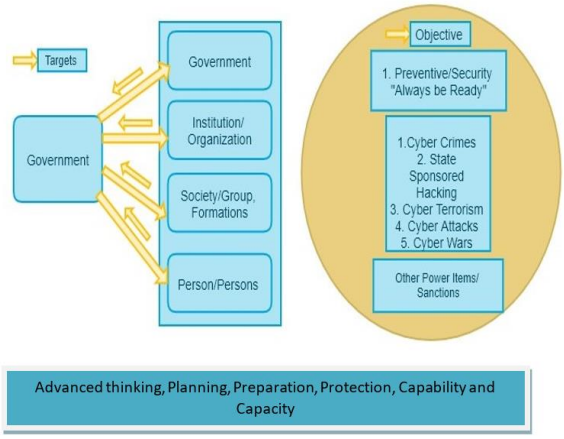

Figure 4. The aim and goals of deterrence

Apart from using cyber security/defence or counter-cyber-attacks/war to stop cyber criminals, terrorists, spies, State Sponsored Hackers, or attackers plotting a cyber-attack or war, the scope of cyber deterrence may include preventing or directing government non-cyber environment operations, such as civil or military formations, as well as other national power elements and sanctions, or only using cyber power (see Figure 4).

4. Conclusion

It is no longer possible to ignore cyber-war as a hypothetical scenario. It's a clear threat that both South Asian countries and the international community should be worried about. While a cyber-war is not as deadly as a nuclear war or other weapons of mass destruction, it has the potential to be equally devastating. Since an all-out cyber war could potentially impact every home and workplace in South Asian country governments, as well as seriously affecting our economy, destroying our infrastructure (lights, power, oil, etc.), undermining our armed forces, and causing a slew of other catastrophic consequences, it is a top priority for South Asian countries. “Securing cyberspace is a difficult strategic task that demands a concerted and concentrated effort from our entire society—the Federal, state and local governments, the private sector, and the American people,” according to the

 | DOI: 10.20533/ijcc.2046.3359.2022.0026

National Cyber Security Strategy. Several government agencies are attempting to work aggressively on sensitive cyber issues. However, in order to effectively combat a cyber-attack, governments in South Asia must focus their resources by ensuring command and control and a concerted cyber-warfare campaign. The primary actors in the cyber-terrorism, namely the Divisions of Homeland Security, Defense, and State (if international cyber space restoration is needed), must promote unity of command and effort; they must seamlessly transfer the lead role among themselves as required for conducting defensive, offensive, and international cyber acts. South Asian governments cannot afford to gamble for a state-sponsored or organized group cyber-attack to figure out the highly complex communication functions and legal implications of cyber security. As soon as possible, the lead agencies for each phase in cyber security should be called.

5. References

[1] Chen, P., Desmet, L., Huygens, C. (2014). "A study on advanced persistent threats", Proc. IFIP Int. Conf. Commun. Multimedia Secure. pp. 63-72, 2014.

[2] Farwell, J. P., and Rohozinski, R. (2011). "Stuxnet and the future of cyber war", Survival, vol. 53, no. 1, pp. -40.

[3] Karnouskos, S. (2011). "Stuxnet worm impact on industrial cyber physical system security", IECON 2011 – 37th Annual Conference on IEEE Industrial Electronics Society, pp. 4490-4494.

[4] Cole, E. (2012). Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization, Newnes.

[5] L. -X. Yang, P. Li, X. Yang and Y. Y. Tang, "Security Evaluation of the Cyber Networks Under Advanced Persistent Threats," in IEEE Access, vol. 5, pp. 20111-20123, 2017, DOI: 10.1109/ACCESS.2017.2757944.

[6] Matrosov, A., Rodionov, E., Harley, D., and Malcho, J. (2010). “Stuxnet under the microscope,” eset, Tech. Rep: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf (Access Date: April 23 2021).

[7] Kushner, D. (2013). "The real story of Stuxnet", IEEE Spectrum, vol. 50, no. 3, pp. 48-53, Mar.

[8] Zhioua, S. (2013). "The Middle East under Malware Attack Dissecting Cyber Weapons," IEEE 33rd International Conference on Distributed Computing Systems Workshops, Philadelphia, PA, USA. pp. 11-16, DOI: 10.1109/ICDCSW.2013.30.

 | DOI: 10.20533/ijcc.2046.3359.2022.0026