WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data and Communication Security of Bangladesh Army: Prevention of Phishing Attacks

Md Mostafizur Rahman

Army Information Technology Support Organization, Dhaka Cantonment, Dhaka, Bangladesh

"Data. We love it. And we also know just how noteworthy it is to sanctuary it innocuous. These days we arecontinued in wherever and the entire interval. Now and again, we may not even realize how persevered in we truly are while our submissions, web hunts, and credit card acquisitions are repetitively stowing our engagements in the circumstantial"

Katie Atkinson, Survey Monkey Blog

ABSTRACT

Data and communication security has implemented many counter measures to protect our own networks for Phishing attacks.Data and communication security in today's world is perceived as one of the core elements of national security.Cybersecurity professionals provide fortification for networks, servers, intranets and computer systems and that is how they safeguard cyber safety.Danger prospect is accumulative at exceptional ways owing to the fast-moving technological changes including proliferation of endpoint devices.Cyber criminal's gives an impression that cyber-attacks are becoming more frequent, more organised, more costly and altogether more dangerous. The use of computers to disrupt the activities of an enemy country, especially unhurried attacks on communication systems.

Key Words : Cyber security, Cyber space, cyber domain, Cyber War, Cyber terror, Cyber sabotage, computer virus, Data, Communication, Security.

Introduction

1. The importance attached to it grew steadily because of series of incidents like data theft, computer virus and other penetration of interacted computer systemthat combinedlydiscriminating the media devotion.Data and communication security has become the latest trend during the last three to four decades. Now a day's cyber security is viewed as a strategic-military issue and to focus on countermeasures like cyber offence and defence or cyber discouragement.
2. The atmosphere of Cyber anxiety has shaped tension in the national and worldwide system consequential increasing militarization of cyber security. Now it is an undoubted fact that the cyber dimension will play a substantial role in the future conflicts with either excessively high cost or ambiguous benefits.The growing erudition of cyber criminals gives an impress that cyber-attacks are becoming more frequent, more organised, more costly and altogether more hazardous. The threat representation based on inherent insecurity of the information organisation and the way it could be manipulated by technologically skilful individuals.
3. In a borderless environment hackers can exploit computer insecurity in various ways; in particular, digitally stored information can be delayed, disrupted, besmirched, destroyed, stolen or reformed.A link was established between cyber threats and critical infrastructures that are the assets whose incapacitation or destruction could have a distressing impact on the national security or economic and social welfare of the entire nation. Now a days, potentially devastating attacks only require a computer with an Internet linking and a handful of Hackers. Trespassers can also leave 'backdoors' to come back at a later time, or use the hijacked machine for attacks on other machines. Though most individual would probably lack the motivation to cause viciousness or severe economic or social harm, large amount of money might motivate them to place their particular knowledge at the disposal of actors with antagonistic intent like radicals or external states.
4. The mainstream critical cyber infrastructures of a nation are owned and operated by the non-military,government and private association. Therefore, ensuring the security of cyber space will warrant the contribution of private actors.It is to be mentioned that 90% of the total cyber deeds are in privet sector hands. In order to safe guard the cyber space we need skilled individuals whether they put on uniform or not. One of the biggest experiments of this field is the rapid evolution of cyber equipment

Security Field in Global

5. Cyber is distinct as the objects that refer to a network area and network area refers to the space of computers that are used to permitdata from one computer to another. It is fundamentally the choice of coverage for a system. The cyber domain is a new conception which became manageable to mankind in the middle of the 20th century; a fifth domain, being added to the well-known four, namely, land, sea, air and lastly, space.

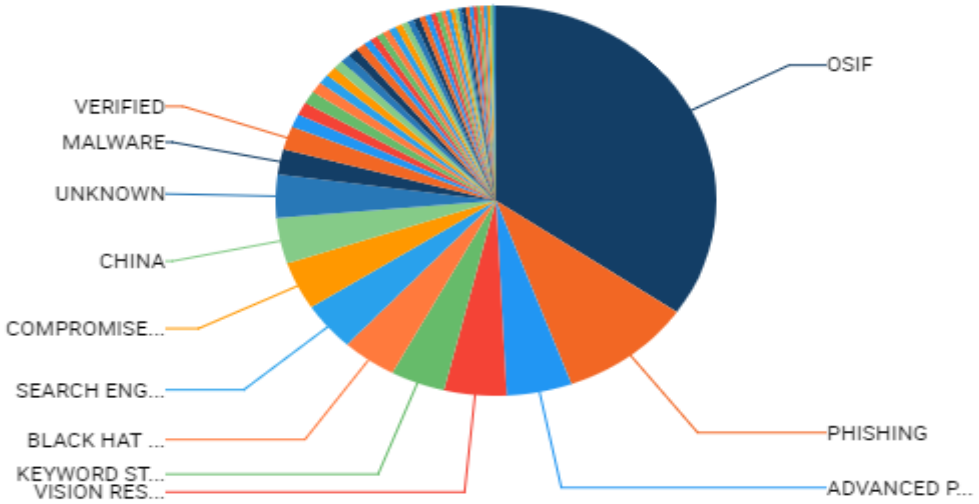
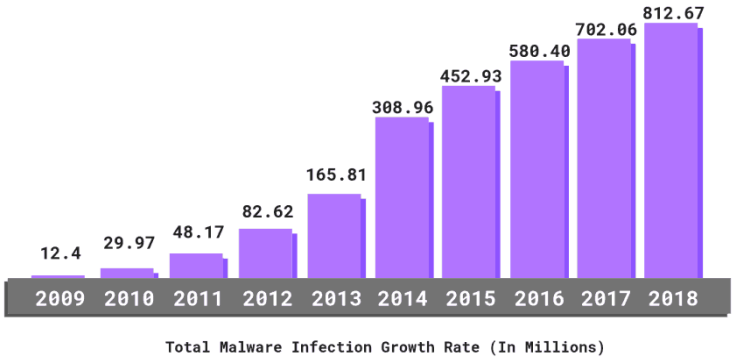


Figure: Security Domain in the World.

Cyber Field isaworld-wide sphere within the information atmosphere consisting of the co-dependent networks of information technology substructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Two main characteristics of cyber domain; first, the boundlessness of that domain. Cyberspace does not have physical or geographicmargins. It exists and plays major and vital roles in each of the other domains. Secondly, the ability to incognito execute any cyber operation in any element, holds no price or risk to the committers. This creates legal glitches, as the operation cannot be attributed to anexplicit individual, organization, or state. This unique distinctive has the most significant and decisive role in making the massive threats.

Cyber Security

6. Cyber security specialists provide protection for networks, servers, intranets and computer systems and that is how they safeguard cyber security.Cybersecurity may be defined as the exercise of defensive information and data from outside foundations on the internet and intranet. But cyber security does not remain constrained within the information domain only, as ICT tools and skills have enabled the utilization of cyberspace in other domains like use of "Internet of things (IoT)" devices for home utilizations or for industrial resolutions. Prevailing perceptions indicate that most of the advanced hardware/ software manufacturers/ developers keep a backdoor open to mine or steal data from devices. Similarly, various social media companies, telecom operators and other digital service providers can also mine data of individuals and organizations.



Furthermore, rapid advancement in hacking tools and skills seems to further increase the threat perceptions against personnel, organizations and state. Besides, there are significant rise of Internet users recorded in the developing countries where awareness about the risk is seemingly low. Besides, fast-moving growth of Information and Communication Technology (ICT) including induction of Internet of Things (IoT), Artificial Intelligence (AI), Big Data Analytics and associated technologies are also posing additional risks to cyberspace.

Types of Cyber Conflicts

7. There are different forms of cyber conflict. Different terminologies used to detectcyber conflicts are given below:

a. **Cyber Conflict**. The use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. The term is also used loosely for cyber events of a political nature.

b. **Cyber Terror**. Illegitimate attacks against computers, networks, and information stored therein, to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack should result in causing enough harm to generate the requisite fear level to be considered 'cyber terrorism'.

c. **Cyber Disruption**. The deliberate disturbance of an economic or military process for achieving a particular goal with cyber means.

d. **Cyber Intelligence**. The unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files.

f. **Cyber Misconduct**.A criminal activity done using computers and internet.

g. **Hacktivism**. The combination of hacking and activism, including procedures that use hacking techniques against a target's internet site with the intention of disrupting normal operation.

8. All these conflicts may happen with different degree of devastation except full cyber war. Since the potentially devastating effects of cyber-war are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of weight despite their very low probability. Most experts agree that strategic cyber war remains highly unlikely in the predictable future, mainly due to the indeterminate results such a war would bring. The lack of motivation on the part of the possible fighters, and their shared inability to defend against defenses. It is very difficult to take down multiple, specific targetsand keep them down over time. The key difficulty is to do proper investigation of the cyber target, as well as the need to deal with a variety of varioussystems and at the same time to remain ready for the countermoves by the rival. So the risk of war like cyber-attack of severe proportion is minimal. But cyber-crime and cyber reconnaissance are a different story. They are here now and will remain the biggest cyber risks in the upcoming.

Present Tendencies of Militarization

9. Cyber domain is not only a military domain. It actually incorporates every investor of a country. But worldwide present trend about cyber security is to militarise it with the idea that cyber turbulences are increasingly dangerous and fall under the purview of national security. One of the most common trends of present time is militarization of cyber domain. Well, it is within the purview of national security but unlike other threats, it does not concerns only the security agencies at the first place. Since mainstream of the cyber infrastructures are in the hand of privet sector, they are very well an important part of the Cyber domain and its security.

10. Still sometimes the cyber threat is hyped. You may be very astonished hearing this statement. Butfor us, it is a threat but not at the rate that we perceive it to be. The reason is very simple – we are not digital yet in its true meaning.There is no repudiating fact that different radical, economical and military conflicts have had cyber mechanisms for a number of years now. Additionally, unlawful and intelligence activities involving the use of computers happen every day. Our defence system, weapon systems are not in the cyber space or digital. Countries that have such systems in cyber space are in real threat. We also do have the risk in cyber domain but not like them. The realms that are currently openly discussing the use of the cyber war tools are precisely the ones that are the most vulnerable to cyber warfare attacks due to their high dependency on information infrastructure. But we are not in that group.

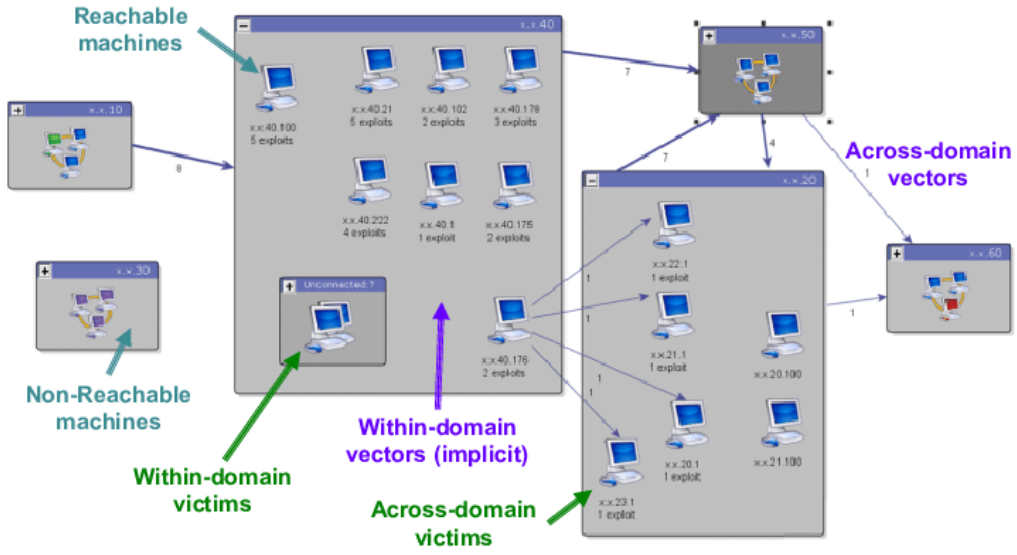


Figure: Cyberspace component and present Trends of Militarization.

11. The military notion of striking back is therefore useless in most cases.Now days it has become difficult to attribute a cyber-attack to a specific country or organization. Military counter measures require an opponent that is clearly identifiable as an attacker. For this, deterrence and retribution do not work well in cyber space. When an intrusion is detected, it is often impossible to determine whether it was an act of destruction, computer crime, terrorism, foreign intelligence activity or some form of strategic military attack. The only way to determine the source, nature and scope of the incident is to investigate it. This might take years with highly uncertain results.
12. The power in this domain is shared with privet sectors. Much of the proficiency and many of the possessionsmandatory for taking better practicalprocedures are located outside administration.Whatever cyber threats are there, cyber space is partly controlled or controllable by state actors. The military or any other state entity, does not own dangerousorganizations in its eternity. Protective them as a military mandate is impossible, and conceiving cyberspace as an occupation zone is an illusion. Military alone cannot defend the cyber space of their country because the logic of national precincts does not apply.
13. Investing too much time or spending increasing amounts of money on them will not make the country's cyberspace more secure – these are uncertainly developed technology where no one knows who industrialized what and how far.Future conflicts between nations will most certainly have a cyberspace constituent, but this will just be an accompanying element of the battle. Regardless how high we judge the risk of a large scale cyber-attack, military type countermeasures will not be able to play a substantial role in cyber security. Military alone cannot take on a considerable role in ensuring the cyber security of the whole country. So the conventional thinking of upkeep the territory of the country will not work here.

Cyber Security Scenery of Bangladesh

14. At first we need to see – what is the cyber landscape of Bangladesh, because that will show where armed forces fit in. We need to understand cyber security in global and Bangladesh perspective first and then finally in armed forces perspective.
15. The cyber security risk likelihood is increasing at unprecedented ways owing to the fast-moving technological changes including propagation of endpoint devices. Moreover, technology is widely exploited to speed up the transfer of information, which is creating amazing opportunities at one end and unfolding greater risks at the other end. The cyber security risk vectors thus involve many uncountable actors including hardware manufacturers, software developers, mobile operators, hackers, information brokers and so on. Such changing delicacies have varying degree of meanings at global and national viewpoints.
16. At national level, cyber securityscenery is measured through various indices; some of these are Global Cyber security Index (GCI), National Cyber security Index (NCSI), ICT Development Index, Network Readiness Index etc. The 2020 statistics show that Bangladesh ranks 78th in GCI, 68th in NCSI, 147th in ICT Development Index and 112th in Networked Readiness Index. The indices manifest requirements of significant improvements in cyber security fields at national tier. The International Telecommunication Union (ITU) measures the cyber security standards of the member states basing on five pillars namely legal, technical, organizational, capacity building and cooperation. Bangladesh has scored 0.525 and ranked 78. It ranked 15 out of 38 countries in Asia Pacific region.
17. The present condition clearly suggests that we need improvements and our government also acknowledged and endorsed it. As such lot of steps has already been takento improve the overall situation.
18. The globalization, evolution of ICT and proliferation of Internet in every spheres of life system cause an avalanche alteration of the information system causing wide range of security challenges in managing the information domain. Beginning with the privacy compromise and data theft, the challenges extend to information breaches, software piracy, cybercrimes, adulteration, forgery in e-commerce and so on.

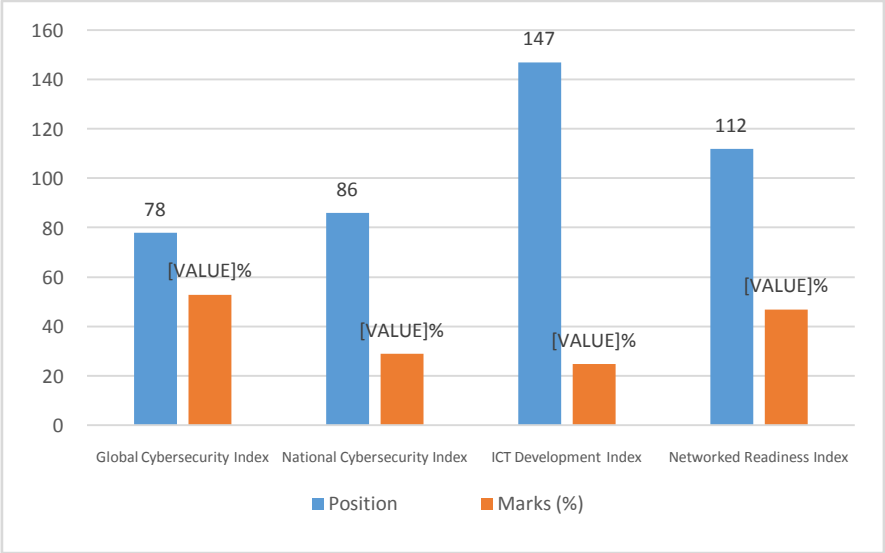


Figure: Cybersecurity situation of Bangladesh

19. Bangladesh scored 56.92% in ITU assessment during developing GCI. A good number of acts, rules, policies and strategies have also been developed to ensure cyber security of Bangladesh. The 'Digital Security Act-2018' has been placed which focused on handling cybercrimes. Legal measures include cybercriminal legislation, cyber security regulation and containment.

20. Technical measures include formulation of national/ sectoral computer emergency response team (CERT), cybersecurity standards implementation framework for organizations, standardization body, technical mechanisms and capabilities deployed to address spam, use of cloud for cybersecurity purpose, child online protection mechanisms etc. Bangladesh established national CERT at Bangladesh Computer Council and in its central bank, yet all major financial institutions and sensitive organizations are still away from such essential facilities, including armed forces.
21. Organizational measures include strategy, responsible agency, cyber security metrics etc. Bangladesh scored 60.19% in ITU assessment during developing GCI. Bangladesh has already developed cyber security strategy in 2014 and Information Security manual in 2016. The cyber security strategy needs up gradation owing to fast moving changes in the sector.

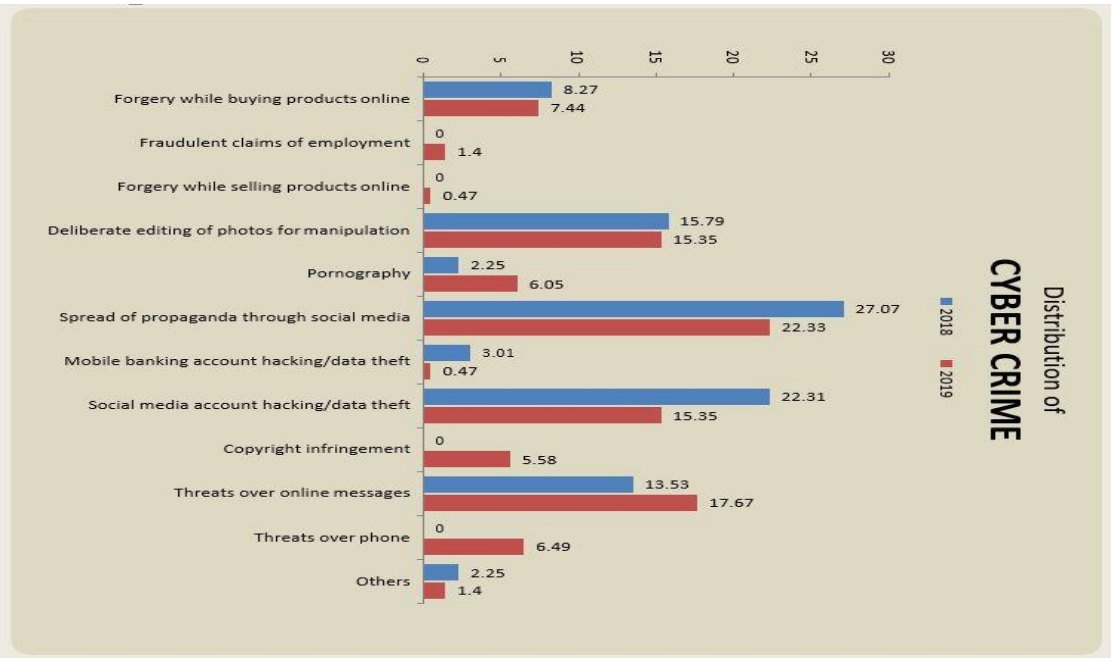


Figure:Cyber Security Scenery of Bangladesh

22. Capacity building includes public awareness campaigns, cyber security standards and certification for professionals, cyber security professional training sequences, national education programs and academic curriculum, cyber security research and development programs, incentive mechanisms, home grown cyber security industry.
23. Bangladesh scored 42.66% in ITU assessment during developing GCI indicating rooms for improvement. A good number of government ministry, departments, law enforcing and intelligence agencies including NGOs and private entrepreneurs are working with the issue with no structured coordination mechanism.

What all the other army have

24. The field includes cryptographic security, transmission security, emissions security and physical security of Communication Security (COMSEC) equipment and associated keying material. COMSEC is used to protect both classified and unclassified traffic on military communications networks, including voice, video, and data.Understanding the importance and severity of cyber security different countries' armed forces have adopted various courses of action. In United State, they have a separate command, United State Cyber Communication headed by a four star general. Total 16500 personnel are working under this command.

Cyber Warfare: Implications for Bangladesh

We are still far behind most of the countries when it comes to the capability of conventional or kinetic warfare. It is understandable that the size and competitiveness of our economy, as well as the sophistication of our technology, is not comparable to those of our big and advanced counterparts. We have to invest billions of dollars to develop a modern-day twenty-first-century army. Which is too costly for a nation like us. But the good news is that we can still compete and in some cases surpass advanced nations if we focus our attention on cyberspace, Cyber security and cyber warfare. It does not cost billions to build an impressive cyber army. It is quite cheap if we consider and contrast it with the mounting cost of conventional military hardware. But we are not implying that we do not need to upgrade regular military equipment; we must procure advanced military hardware when our economy permits us, as those are the core elements of our conventional deterrence, but an additional cyber capability can significantly enhance the strength and compensate for the weakness of our conventional combat capabilities. In the next ten to twenty years, everything, irrespective of military or civilian technology will be fully digitalized. In a time of crisis or war with other countries, we can exploit this very vulnerability of increased digitalization.

So to obtain the benefits of the information age, in addition to developing a state-of-the-art cyber army; we must establish a separate cyber command, capable of defensive as well as offensive operations.

Future Trends of Cyber Threat

The damage potential of a successful cyber attack is constantly decreasing by augmenting the resilience of information networks and critical infrastructures. A challenge for the military, both today and in the future, will be growing and retaining sufficient high quality cyber trained people in our armed forces.The probability if cyber war and large scale attack now and in future is very low though there prevail a very widespread fear of cyber war. Most countries simply follow the threat perception of US, even though the strategic context and disparity in power positions warrant a different threat assessment.

Cyber Threat in the World

The globalization caused digital transformation which impacted the cybersecurity. Most of the authors raised the privacy problem and thereby connected the security. But how the privacy problem affects, cybersecurity of the state is needs further study. Moreover, the current policy and strategy aims to support the Bangladesh Vision 2021 and hence could not delineate guidelines for future challenges. Furthermore, the insecurity environments being unfolded from the ongoing induction of IoT, AI and associated technologies have not been addressed. Of significance to note that there is hardly any policy/ strategic guidance to tackle the cyber insecurity being yielded by the tech giants, hackers and other actors

Implications for Armed Forces

25. Upto this point we have an idea about cyber landscape of Bangladesh as a whole which equally qualify to be true for the armed forces. We have also seen what the other armies of the world are doing. Basing on that now we need to address several cyber related issues for our armed forces.

a. Bangladesh government has already published its Cyber Security Strategy in 2014. But we do not have any strategy as yet. We must have a Cyber Strategy or at least some guiding principalthat should guide us in shaping our Cyber efforts.

b. Armed forces need legal documents of its own for resolving legal and policy issues related to cybersecurity. Present MBML does not have specific legal frame work to address the Cyber Issues.

c. Armed forces must have a policy guideline on Cyber issues.There should be clear instructions to prevent malicious contents those lead to internal chaos such as fake news, hate speech, online radicalization. The documents shall outline issues related to data security schemes, safe and comprehensive use of cloud, spam control, standardization of data centersetc.

d. Structured education and training would be essential for sustainable capacity building. Cyber security education should be included in all the mandatory courses. We need educated IT users. Concerned directoratewould ensure progressive syllabus for various courses so as to develop adequate awareness and thus significantly reduce cyber victims.

e. Bangladesh has already established national CERT under BCC and one sectorial CERT for Bangladesh Bank. Accordingly we need to establish CERT for us. Besides, certified data centers should to be established for the protection of critical information. Cyber security experts are to be employed for the protection of critical information infrastructure and local CERTs along with AI.

f. All armed forces must have cyber force with experienced and skilled personnel to safeguard their own information domain. There are several self-trained hackers and spammers in the country who support cybercrime victims with various degrees of rewards.

g. Strong prevalence of social media worldwide is a common phenomenon. Members of armed forces are no difference. While social media has a positive impact on modern culture, it also has major adverse effects on national security.

h. The existing government-owned transmission networks suffer from many adverse limitations where reliability and security are at question. Private transmission networks on the other hand provide relative better service with no security guarantee.

h. Finally organizational restructure. We need to have organizational setup for supporting the cyber issues.

Established the Army Cyber Group

26. Bangladesh Army has implemented many counter measures to protect their own networks for Phishing attacks. Most of the attacks come from mail with attachment and links. So, we should aware users not to do any of the said topics unless it comes from a valid sender. Bangladesh Army has implemented a Security Operation Centre inside Army Data Centre and the activities are:

a. Enhance protection of information assets.
b. Step ahead of attackers.
c. Increase security visibility.
d. Security investigation and incident management.
e. Preventing threats by early detection.
f. Expertise on cybersecurity.

27. Beside this Army Information Technology Support Organization (AITSO) was established as temporary basis inside Dhaka Cantonment for

Information Technology support from Army Headquarters down to Formation Headquarters, Brigade and under command units and training institutions. Finally AITSO was raised 04 January 2021 and it's has a wing named "Information Security and Cyber Support wing (ISCS)". The Information Security and Cyber Support Wing of AITSO will look after the Internal Security of Network, Data centre and limited scale of forensic. This wing has four internal groups are mentioned below:

a. Cyber Operation Group.

b. Cyber Intelligence Group.

c. Digital Forensic Operation Group.

d. Information Security Group.

28. Finally, Army Cyber Group has established with 70 manpower but it's activities not started yet. The functionality of Army Cyber group will start very soon. The Army Cyber group will be fully functional to support the Bangladesh Army.

Conclusions

29. Today due to high internet penetration, cyber security is one of the biggest need of the world as cyber security threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free. More attention to both the capacity and capability of t cyber security workforce is needed. Even large organizations with top talent and significant resources devoted to cyber security have suffered major cyber security compromises, and organizations that do not have such levels of talent or resources face even greater challenges. More highly skilled workers in cyber security roles would help the nation respond more robustly to the cybersecurity problems it faces. All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work.

30. Cybersecurity is not solely a technical endeavor, a wide range of backgrounds and skills will be needed in an effective national cyber security workforce. Cybersecurity is a function of organizational policies and process as well as technologies. As a result, people are needed who understand the organizational context—mission requirements, business processes, and organizational culture.Cybersecurity work often involves teamwork and collaboration across organizational boundaries. Soft skills, which include the ability to work in teams and facility with oral and written communication, are essential in many roles.