Bangladesh Institute of International and Strategic Studies (BIISS)
1/46 Elephant Road, Ramna, Dhaka 1000, Bangladesh

Lecture

on

Securing our Cyber Space: Challenges and Future Directions

14 August 2012

SUMMARY OF THE PROCEEDINGS

1. Introduction

Bangladesh Institute of International and Strategic Studies (BIISS) organised a Lecture on "**Securing Our Cyber Space: Challenges and Future Directions**" at BIISS Auditorium on 14 August 2012. The objective of the Lecture was to identify the insecurities in the cyber space including causes and drivers of cyber crime and evaluate current preparedness for formulating a response strategy to fight the crime and secure our cyber space. **Ambassador (Retd.) Muhammad Zamir**, the Chief Information Commissioner of the Government of the People's Republic of Bangladesh graced the occasion as the Chief Guest. **Major General Muhammad Imrul Quayes**, ndc, psc, Director General of BIISS, chaired the programme. **Colonel Md Nazrul Islam Sarker**, afwc, psc, Research Director of BIISS, introduced the speaker of the programme, **Dr. Kim Kwang Choo**. An Open Discussion was followed by Dr. Choo's lecture.

2. Opening Remarks by the Chair

In the Opening Remarks, **Major General Muhammad Imrul Quayes, ndc, psc,** stated that the convenience of cyberspace to a modern world is indispensable. As dependence increases on technology, so does vulnerability due to its abuse. It has also led to vast quantities of malware

and spyware circulating freely on the internet, and an alarming rise in the number and scale of cyber criminals. Cyber crimes are embarrassing governments and individuals, impairing systems and causing loss of billions of dollars every year. The increased reliance on the internet by business, government and society makes it a prime target for criminals' intent on disrupting economy and way of life. Cyber crime has grown to be larger than illicit drug sales worldwide. At present the cyber crime in our country scenario includes life threatening e-mail to important personalities, malicious mail to foreign diplomatic missions, pornography, fraudulent mail for the realisation of money, inserting porno movies to the well-known websites are a few to name. Much, however, remains unreported, most of which may not have taken a devastating toll yet. How much are we vulnerable to cyber crime, are we aware and are we ready to respond to this threat and what should we do to counter this crime? The Director General of BIISS informed the audience that the lecture will evaluate the vulnerabilities and preparedness to formulate a response strategy to fight cyber crime. The lecture will provide strategies and future directions to counter cyber crime. Finally, he thanked all once again for participating in the Lecture and also requested to provide their valuable comments and suggestions.

3. Introduction of the Speaker by Colonel Nazrul

After the Opening Remarks, Colonel Md Nazrul Islam Sarker, afwc, psc, Research Director of BIISS, introduced Dr. Kim Kwang Choo, a Fulbright Scholar and Senior Lecturer at the University of South Australia. Dr. Choo collaborates with the Australian National Government at the Australian Institute of Criminology (AIC) as an Associate and the Australian National University as a visiting scholar. He has co-authored number of publications in the areas of information security/cryptography, cyber crime and anti-money laundering. His work has been widely cited including in various government reports in Australia and overseas (e.g. UNODC, UN Secretariat and US CRS Report for Congress). He has been an invited speaker for a number of international conference such as 2011 UNODC-ITU Asia-Pacific Regional Workshop on Fighting cyber crime and 2011 (Ministerial-level) Korea-Australia-New Zealand (KANZ) Broadband Summit 2011. In 2009, he was named one of 100 Emerging Leaders (Innovation) in the Weekend Australian Magazine/ Microsoft's Next 100 series. He is also a recipient of various awards and scholarships including the 2010 Australian Capital Territory (ACT) Pearcey Award for "Taking a risk and making a difference in the development of the Australian ICT industry, 2010 Consensus IT Professional Award, 2008 Australia Day Achievement Medallion in recognition of his dedication and contribution to the AIC and through it to the public service of

the nation and the British Computer Society's Wilkes Award for the best paper published in the 2007 volume of the Computer Journal (Oxford University Press).

4. Lecture given by Dr. Choo

At the beginning of his presentation, Dr. Kim Kwang Choo informed that currently there are more than 2 billion individual online users. More than 26 percent of the total population in Asia is using internet which makes about 45 percent of the world's total internet users. And it is interesting to note that the share of Asian people among the internet users is gradually increasing. He noted that many malicious cyber warms, in most of the cases, are originated in one country and quickly spread across the borders with the help of internet. This cross border nature of cyber crime makes it difficult to identify the origin and the individual or the group who are behind it. Therefore, it is difficult for the law enforcing agencies to apprehend cyber criminals. He further added that cyber attacks are getting more and more sophisticated and difficult to detect. The key points discussed in the Lecture are 1) the nature of cyber crime; 2) motivating factors for cyber crime; 3) actors involved in the crime; 4) the victims of the crime; 5) future direction to face the challenges.

About the nature of cybercrime, he distinguished the motives. It may be financially motivated or state sponsored. However, uncertainty about physical location of origin of the crimes complicates government effort to respond, investigate and the use of retaliatory measures. Cyber threats are increasingly becoming important and strategically relevant in both developed and developing countries.

To define cyber crime, Dr. Choo said that it is a crime where Information and Communication Technology (ICT) tools are used to commit it. The crimes may be like from fraud against individuals, government or any business to online child or young people exploitation. It also includes crimes where ICT is the target. Hacking, for example, is a cyber crime where a person has access to unauthorized data and privileged information. Other examples are interruption of services or Malware (malicious software such as worms and viruses). Malware can be used against government individuals and businesses. He indicated that at present people are increasingly using smart phones. These phones are becoming subject of malware attack.

About motivation of cyber crime, it was said that most of the cyber crimes are committed for making financial gains. Cyber criminals hack password of individual's or business firm's bank account and steal or relocate money from those accounts to their account. Besides this major cause, many of the times young people get involved in cyber crimes out of curiosity to learn about hacking. In addition, some young people hack websites of important organisations to demonstrate their skills. Revenge motivation of former employees of any company or two rival companies may be another cause. Sometimes, ideologically and politically motivated people may take revenge by hacking to establish their cause, for example "Anonymous". Criminal motivation like online sexual exploitation also may be behind any cyber crime. Explaining psychology of cyber criminals, Dr. Choo mentioned that many people do not think that they are committing crime as they are not seeing the victims. During high unemployment time, the rate of cyber crimes increases as people remain jobless and frustrated.

On vectors of cyber attack, he said smart mobile devices are emerging vectors of malwares. Many people use smartphone for financial transaction and business communication. For example, checking bank account and viewing company information. While performing those actions, they consciously or unconsciously save passwords of respective banks or companies on their smartphone devices. If those phones are lost or attacked by any malware, then the criminals have a chance to steal that information and use it for their own purpose. Citing an example of a survey conducted at the University of South Australia, he showed that most of the 3G smartphone users are from age 35 and below (76.4 percent) of total respondents. Undergraduate students are the majority among such users. They use their phones for personal message exchange, social networking, and banking, web surfing and playing online games. Social networking has become an important way for malware creators to attack other computers. Many people aged from 19 to 35 who are net savvy are in risk of becoming cyber victims.

To be safe from cyber attack, it is recommended to avoid saving credit card information on any applications or web browsers. He also suggested for using modern mobile devices which have options for PIN or password protection for opening, and everyone should be very careful about checking unknown emails and downloading something from any un-trusted websites.

Dr. Choo noted that cyber criminals become successful because of their patience and continuous effort. Usually, they are very intelligent and innovative. Global trans-border nature of information web also creates conducive environment for them. In addition, proliferation of

networks has increased the chance of committing cyber crimes. Many organisations and companies are using more layers in their cyber security system that is also increasing loopholes through which the cyber criminals can penetrate their defense system. Hence, cyber security system should be well maintained and regularly updated. For making an effective cyber security system, people need to be innovative. Every country should have a strategic framework in which decision makers, experts from public and private sectors should be involved for better technological solution.

About the cost of cyber crime, it is informed that there may be direct and indirect cost like cost of cleanup, cost of liabilities such as submitting law suits, monetary penalties. Nevertheless, in this age of technology, it is very difficult to conduct our daily activities without internet; therefore the government must find an effective way of securing cyber communication for protecting their people's private and national strategic interests.

Dr. Choo briefly described about Routine Activity Theory, which can be applied for reducing cyber crime. This is a series of regular activities that emphasis on regular monitoring, surveillance and upgradation of cyber security system. It will make cyber crime difficult, time consuming and costly so that the criminal will lose incentives. It is very important to encourage people through various programmes and competition for making innovative programs that will increase cyber security. He put emphasis on information sharing among the agencies in order to make threat assessment based on accurate information and to develop validate effective measures and mitigation controls. Dr. Choo asked the government agencies for taking a leading role to create a market for the cyber security software. They should ensure more innovative and improved security measures. Government agencies can also play as a supporting role to the private software development and hardware development. Cooperation on knowledge and technology exchange among the governments is the demand of time.

5. Open Discussion

Brigadier General (Retd.) M Mofizur Rahman noted that although cybercrime is expensive to commit, it is done pervasively by the hackers. Collective measures and preventive measures are taken in many countries to counter this crime. He raised a question as to what degree the preventive measures can be taken in case of hard ware and soft ware. And then he asked

about the legal part of cyber space and whether there is any common definition by the UN so that preventive measures can be taken in a unified way.

Faisal Mahmud, a Journalist from the Independent news, also raised some relevant questions: Is not online security more expensive? Regarding i-phone, what about black berry and Samsung? To what extent does Choo's lecture fit in Bangladeshi culture as his research is accomplished on Australian society?

In reply, Dr. Choo noted that there is no common solution to check cyber crime. It is fact that cyber crime prevention is very expensive. So, everybody looks for cheaper option. He added that it is not people are unaware of software and hardware security; it is also related to prevention of virus and its annual subscription. Regarding anti-virus in particular, it was commented that it is a regular process as the program has to update once a day. Even, to run the program in future, it requires a new license. Citing the example of Australia, he referred that some banks have offered anti-virus with free of charge to the customers. As people cannot afford this, bank could secure the customers and it could be a method of collective measure for the other countries as well.

About the legal part of cyber space, he replied that there are many international organisations like the UN, UNODC, and the Council of Europe as well as international telecommunication organisations which have taken a number of legal initiatives. The Council of Europe, for instance, has convention of laws which Australia is yet to ratify. With regard to the common law of cyber crime, Dr. Choo informed that there is no unified law to prevent cyber crime. Each country is different and therefore, they have different levels of development. Even, cyber laws are different between Australia and the US, the two technologically advanced countries.

Regarding various initiatives that already taken, he mentioned that there are a number of international bodies who have already taken the initiatives. For example, NATO has taken the initiatives to formulate cyber norms as it is an ongoing issue. Within the norms, they try to develop the answers of certain relevant questions including: what is cyber behaviour? What constitutes cyber war? How cyber activity can be classified?

About the definition of cyber crime, he said that still it is difficult to say who is right and who is wrong as there is no common classification of cyber space. He added that people have an idea about nuclear weapon, but it is unclear how cyber terrorism or cyber war looks like. Also, it is very early stage for the international community to deal with these notions. Even the ICT

developed countries like Canada, USA and Australia are still not dealing with the cyber treaty at a large scale. On the other hand, cyber treaty has been developed in many Asian countries for the last few years. Thus, due to lack of proper definition, countries are dealing with the terms of cyber terrorism or cyber crime in their own way.

Mohiuddin Ahmed from University Publication Limited (UPL) informed that Bangladesh has the copy right laws and a bit of cyber laws. But, the country is far away from dealing with cyber crime properly. Bangladesh government has taken a number of initiatives to digitalise the country for its technological advancement within five years or ten years. As far as motivation of cyber crime is concerned, the main reasons behind this are curiosity, fame seeking, illicit financial motivation, revenge, and so on. He then enquired how Bangladesh could develop cyber laws where rampant piracy of physical books is very common crime.

Based on his query, **Dr. Choo** replied that copy right is related to moral ethics. Recently, Bangladesh Bank introduced credit card and a number of books can be purchased through amazon.com. He informed that Australia has copy right laws and E-book system and Bangladesh could introduce as it has no restriction regarding credit card. He suggested that Bangladesh needs to develop anti piracy law as early as possible.

Dr. Mostafizur Rahman, Chairman, Institute of Development Strategy (IDS), mentioned that in our country we are not totally vulnerable to cyber space crime so easily. For us this is an advantage at this moment. According to him, most of the countries try to develop their own security. He pointed out that if we educate our children from right now in computer science, they will gradually develop and it will be helpful for us in future. He added that our software developers are now getting recognition internationally which means they are capable. So, we have to protect our own network and secrecy. We have to develop our own capability in software and hardware.

Mr. Mohiuddin Ahmed again mentioned that the issue of copyright violation is basically a question of morality. WTO has already 85 laws related with this. Regarding the issue of banks not accepting or issuing credit card, he mentioned that Bangladesh Bank recently started to issue credit card for purchasing goods. Bangladesh Bank has no restriction in issuing and accepting credit card for business purposes. He said that we need to diversify the Anti-Piracy laws.

In replying **Dr. Choo** said, in case of Bangladesh, whether the country accepts or not accepts the credit card depends on the commercial providers. Besides, there are different types of payment methods. Some business providers may not interested in about the online business which is very popular in the developed countries.

Benuka Ferdousi, Research Officer, BIISS raised a question about the extent of annual global financial loss caused by cyber crime and which countries are mostly affected.

Dr. Mahfuz Kabir, Senior Research Fellow, BIISS, raised the issue of Julian Assange and Wikileaks, asked how to count the moral incentive of cyber crime.

Answering the question of Mostafizur Rahman**, Dr. Choo** said that it is right that the younger generation prefer science and technology now a days but the concern is that the moral education of ICT is not incorporated in the under graduation or post graduation level. Therefore, many students do not know about the basic core of ethics of IT professionals. Hence, they should teach ethics and moral education about what is right and what is wrong in cyber space.

About the last two questions, **Dr. Choo** commented that certainly, cyber crime is a profitable business. Still it is difficult to find out the amount of loss caused by cyber crime. He noted that a terrorist of one country can be a holy person of another country. Therefore, government needs to be aware of software and hardware issues as well as all kinds of supply chain security issues.

6. Addressed by the Chief Guest

Ambassador (Retd.) Muhammad Zamir, Chief Information Commissioner, Government of the People's Republic of Bangladesh mentioned that the potential benefit of a reliable and secure cyber space environment is very important. Today, while we are talking of national security in terms of traditional land, air and sea space domain, we have forgotten that cyber space is really becoming more important than all of the other together. Raising the issue of his participation at the Internet Freedom, Media Freedom and Cyber Security Conference at Stockholm, he mentioned that the use of technology can have both positive and negative impacts and provided the statistics that it took 50 years for the number of landline phone users to reach 1 billion and, on the other hand, for the mobile phone users, it took only 5 years to reach 5 billion in terms of number. According to him, the private sector has played a significant role in creating the architecture of the internet and unlike other public goods; it owns much of the internet.

Companies have created the technology, they run, market and provide access to it and to a great extent regulate it. The sector sets its own rules about the volume and kind of trafficking within the infrastructure it owns. He mentioned that the PPP principle will not be so useful for the non-developed countries of South Asia. Regarding the issue of government's role, he said that the government has sometimes taken steps to suppress and ensure that has not been misused. He mentioned that keeping the aims and objectives of the government in view, Ministry of Science and Information & Communication Technology (MoSICT) has formulated some policies on protection of its growing cyber world from the unsolicited consequences. The National ICT Policy, Cyber Law, Electronic Transaction Act are already adopted by the highest authority. Appropriate education on Computer Alert and Emergency Response are underway by the different agencies including government, civil society/NGOs and private sector. The Chief Guest also pointed out that cybercrime is a crime which according to the Council of Europe's Cybercrime Treaty refers to offences ranging from criminal activity against data to content and copyright infringement. The principle forms of cybercrimes are hacking, distributed denial of service (DDOS) attack, virus/worm attacks, Trojan attacks, e-mail spoofing, dissemination of obscene material, phishing and credit card fraud, etc. He suggested that as a follow-up after this Lecture, BIISS might organise a seminar or workshop with the stakeholders involved with this issue and its various aspects, what the stakeholders feel about it and to find a least common denominator on how to move forward. We need to have in every print and electronic media space and time on tackling issues related with cyber crime.

7. Closing Remarks by the Chair

In the Closing Remarks, **Major General Muhammad Imrul Quayes**, ndc, psc, mentioned that the knowledge of cyber technology can be used in both positive and negative ways. We must make sure that we use it in a proper way and make best dividend out of it in order to make sure that it contributes in the development of the society and country. We also must safeguard so that it is not used against any individual, institution and country.