CYBERCRIME IN BANGLADESH:
IMPLICATIONS AND RESPONSE STRATEGY

Brigadier General Md. Khurshid Alam, ndc, psc

INTRODUCTION

Information and Communication Technologies (ICT) have transformed modern lifestyles. These have provided us with real-time communications, borderless and almost unlimited access to information and a wide range of innovative services. Cyberspace has supplemented, if not substituted, functions and services ranging widely from routine personal life to national and global affairs. The immense convenience offered at an astounding speed dissolving all spatial limits make cyberspace indispensable to a modern world that is still at pains to fathom its potential. 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.

Cybercrimes, generally involving computers and networks, are embarrassing governments and individuals; impairing systems; and causing loss of billions of dollars every year. These crimes in reality include copyright infringement, software piracy, password cracking or cheating by others' ID, cyber pornography, e-mail threats, e-stalking, hacking others' websites and so on. The world is threatened, perhaps, by the worst form of aggression through these crimes. 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. Cybercrime has grown to be larger than illicit drug sales worldwide and it is estimated that losses from intellectual property to data theft in 2008 ranges as high as $1 trillion.

How much is Bangladesh vulnerable to cybercrime; is she aware; and is she ready to respond to this threat and what should she do to counter this? While some studies are carried out about the use and development of the cyberspace, no serious evaluation is done of the nature of threat that is tagged with it, the degree of damage it can do, or the amount of loss it can incur. At present, the cybercrimes in Bangladesh scenario includes life threatening email to important personalities, malicious mail to foreign diplomatic missions, pornography, fraudulent mail for the realization of money, inserting porno movies to the well-known web sites are a few to name. Much, however, remains unreported, most of which may not have taken a devastating toll yet. When we are envisioning 'Digital Bangladesh',

Bangladesh is more exposed to the evils of technological crimes. Unfortunately, we are not much aware of this crime and consequences.

This paper attempts to evaluate our vulnerability, as well as the preparedness, by analyzing the degree of penetration of cyberspace in the country and the nature of threats accompanying it. A conceptual overview, skimmed chiefly out of published materials, is presented at the beginning. The vulnerabilities and preparedness is then evaluated before recounting a response strategy to fight cybercrime. Finally, the paper suggests an outline strategy to deal with cybercrime in Bangladesh.

A CONCEPTUAL OVERVIEW OF CYBERCRIME

What is Cybercrime

Cybercrime is apparently a 'crime' committed using 'computer' or 'network', or 'hardware device' or 'cyber space'. The Council of Europe's Cybercrime Treaty uses the term 'Cybercrime' to refer to offences ranging from criminal activity against data to content and copyright infringement. Cybercrime is generally defined as the crime in which computer has been used as either the target or tool for carrying out the crime.

Forms of Cybercrime

There are many forms of cybercrime and various new forms and techniques are noticed day by day. However, the principle forms of cybercrimes are appended below:

Hacking. Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user. Hackers make money through raiding bank accounts, credit card fraud, telephone call selling, product/service fraud and espionage.

Salami Attacks. This kind of crime criminal makes insignificant changes in such a manner that such changes would go unnoticed. For example, the criminal makes such program that deducts a small sum (say Taka 2.50 per month) from the account of all customers of the Bank and deposits the same in his account.

Distributed Denial of Service (DDOS) Attack. This is an act by the criminal, who floods the bandwidth of the victim's network or e-mail box with spam mail and bogus messages, thereby effectively closing the routine traffic or cause it to crash.

Virus/Worm Attacks. Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.

Trojan Attacks. A Trojan-Horse is a code fragment that hides inside a program and performs a disguised function. It is a popular mechanism for disguising a virus or a worm and can be camouflaged as a security related tool. A Trojan was installed in the computer of a lady film director in the US and obtained her nude photographs through webcam. She was later harassed by the criminals.

E-mail Spoofing. A spoofed e-mail may be said to be one that misrepresents its origin. It shows its origin to be different from which actually it originates. Many of us have experienced 'Urgent Help Mail' from a known friend requesting immediate financial help, which otherwise is false.

Dissemination of Obscene Material. Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

Phishing and Credit Card Fraud. It is a technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means. If electronic transactions are not secured, the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

Cyber Criminals

Cyber criminals are an ever present menace in every country connected to the Internet. The cyber criminals constitute of various groups or category as shown below:

Children and Adolescents. The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reasons may be to prove themselves to be outstanding amongst other children in their group.

Organised Hackers. These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Chinese are said to be one of the best quality

hackers in the world. They mainly target the other governments' sites with the purpose to fulfil political objectives.

Professional Hackers/Crackers. These kinds of hackers work are motivated by money and mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

Discontented Employees. This group include those people who have been either sacked by their employer or are dissatisfied with their employer. Traditionally, internal attacks posed the greatest threat to computer networks, which accounted for about 70 percent of all attempted intrusions.

Difficulties to Address Cybercrime

Highly Technical and Innovative Methods. Unlike traditional criminals, cyber criminals are sufficiently educated and highly specialised in computer systems and networking. The cyber attacking tools and methodologies are becoming widely available and skills required by malicious users to launch cyber attacks are reducing with time. The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc that can fool biometric systems and bypass firewalls can be utilized to get past many a security system. All of this emphasises how sophisticated and innovative terrorists have become and how complicated it is for country like Bangladesh to develop and coordinate all of the necessary security measures to counter such threats.

Cross Jurisdictional Boundaries Electronically. Cyberspace is a virtual place beyond the jurisdictional boundaries and it is difficult to address with territorial approach. Law was actually a territorial concept so long as we did not have any kind of familiarity with computer, Internet and cyber space. So, existing laws or legal principles whether domestic or international character comprise territorial approach. Therefore, the traditional principles of jurisprudence or of the legal philosophy need to be revised to cope with the cyber necessity. Cyberspace being an international territory claims a substantial recognition in the arena of international law, which will open the door of the trial of cyber offender under a previously systematised set of laws.

No Physical or Human Evidence. In the traditional investigative procedure, physical evidence plays the pivotal role to discover the truth. But in case of cyber offence, the offender's location, profile, identification, physical evidence remains an enigma to the investigator. Cyber attackers can conduct their operations remotely from anywhere in the world and there are no physical barriers or check points to cross. As such, the actions of cyber criminals are very difficult to track and they can comfortably hide their personalities and location.

CYBERCRIME AND BANGLADESH – VULNERABILITY AND PREPAREDNESS

A Picture of Cybercrime – Bangladesh Perspective

Cybercrime is a contemporary phenomenon to Bangladeshi people. Although presently Bangladesh is not as vulnerable to cybercrime as the developed countries are, but there is little room for complacency. Once 'Digital Bangladesh' comes in reality, we will certainly face the critical situations that are being suffered globally. At the moment, Bangladesh is not aware of her cyber security. Though computer is becoming a common household item and the number of Internet users has already crossed ten million, very few computer-related offences are reported to the police. However, a few of the major cybercrime incidents that bring to the notice of the public are discussed below:

On 23 August 2004, an e-mail was sent to the Bangla daily Prothom Alo, containing death threat to Sheikh Hasina, the then leader of the opposition in parliament. Two days later, another e-mail received that also contained death threat for Khaleda Zia, the then Prime Minister, her eldest son and some members of parliament. These were the first two incidents of cybercrime.

In 2008, the website of the Rapid Action Battalion (RAB) was hacked. The hacker, Shahee Mirza wrote on the RAB website, 'You do not know what the cyber security is or how to protect yourself' [The Daily Star, 6 September, 2008]. Following his arrest, he confessed that he had hacked not only the RAB website but also several local and international websites, including that of the Bangladesh Army.

On 21 March 2010, 19 of the 64 district web portals were hacked, immediately after inauguration by the Prime Minister on 10 January. This was the last known invasion in the government's cyber territory and reportedly the first criminality by foreign hackers.

Social Defamation and Privacy Violation. Exploitation of Social Networking and Chat sites leave our population, especially the younger generation vulnerable to different types of social attacks. Password cracking or cheating is a common crime done by juveniles in Bangladesh. These crimes are mainly committed by doing fun through facebook. Apurbo and Sohana Saba, popular drama-artists, disclosed that someone had opened facebook account by their name and photo, and used this as camouflage of cheating people. In Pirojpur, a student leader lured a class X student to a love trap, raped her and recorded it in a cell phone. The video footage reached local youths through cell phones, flash drives and CDs, which are now on sale in video stores. These are a few incidents how cheats blackmail girls and popular personalities using cyber technique.

National Values, Belief and Faiths. Bangladesh is all along known to be an embodiment of a moderate society characterized by liberally practicing religious people with high resilience, forbearance, modesty and strong attachment to the traditional culture, values and belief. Malicious and clandestine propaganda through Internet may impair the harmonious social bondage and where people of various faith and sectarian views live in peace and harmony. Teen agers who use Internet have been more prone to pornography than the use of huge scholastic exploration in the domain which is highly antithetical to the mores, faith and values embedded in the society of Bangladesh. Thus cybercrimes have a devastating effect on the traditional cultural and religious values and erode the moral values by the strong dominance of the negative character of western culture.

Economics and Finance. Although cyber attacks have caused billions of dollars damage in financial sector, we have yet witness the implications of a catastrophic cyber attack in Bangladesh. Cyber attackers generally disrupt the banks, the international financial transactions, the stock exchanges. 'The impact of cybercrime is not as alarming in Bangladesh because financial transactions have not yet been fully facilitated online,' says Freddy Tan, chief security advisor of Microsoft Southeast Asia. He warns that as soon as financial transactions are allowed online computer crimes will increase at an unprecedented rate, unless the government acquires the tools and infrastructure to prevent, detect and prosecute them.

Embedded Threats. Modern equipment comprises of number of systems and sub systems, of which embedded systems are used by all critical sectors of economy including Armed Forces. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions. They could be built so that they fail after a certain time,

blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location – there are innumerable possible scenarios. Bangladesh does not have any sanitisation agency at the National level and large amount of 'commercial off the shelf' equipment and weapon systems in our inventory are ex Import. Any deliberate attempt by our adversaries by planting malicious codes in the embedded systems could result in a catastrophe.

E-espionage and Cyber War. In cyber war computers are simply another tool, to be used by these same people for espionage. Our adversaries may conduct e-espionage on our government, university research centres, industries and Armed Forces. They may also seek to prepare for cyber strikes during a confrontation by mapping our e-governance information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. During crisis, adversaries may seek to intimidate the Nation's political leaders by attacking Critical Information Infrastructure (CII) thereby eroding public confidence in the political system. Bangladesh is utterly exposed to this dangerous espionage threat and we are hardly prepared to combat this.

State of Awareness and Preparedness

Government Organisations. State of awareness among the public servants to guard against cyber attack is disheartening. No dedicated organisation has been devised exclusively to handle cyber related issues. However, Bangladesh Telecommunication Regulatory Commission (BTRC) coordinates cyber infrastructures as a part of communication domain. In the absence of proper organisations and agencies dedicated to different domains of information security no worthwhile initiatives can be taken to secure critical national information infrastructure. The government has already taken some initiatives, the project; 'access to information' working under Prime Minister's Office is a case in point.

Corporate and NGOs. NGOs and corporate offices are better equipped with computer and Internet than public offices. Most of the senior executives are at ease in communicating through e-networking system. Some of the IT officials have fair knowledge on cybercrime but other than few reputed organisations cyber security awareness have not got due importance. Larger corporate bodies and reputed NGOs have adequate resources and skill to guard against cyber attacks and even capable to share experiences with public offices. But they need national cyber guidelines and regulating authority to skillfully safeguard their network and computers.

Legal Dimensions and Law Enforcement Agencies

Laws and Relevant Issues. The government of Bangladesh has shown a positive approach by formulating some policies and Acts as safeguards for cyber victims. Namely, the National ICT Policy, Cyber Law, Information Technology (Electronic Transactions) Act (ITETA 2000). Latest enacted 'Bangladesh Tatha O Jogajog Projukty Ain 2006' (ICTA 2006) has made provisions to development of information technology and brought the cyber criminal within the ambit of criminal jurisdiction. The Act is comprised with nine chapters with 90 sections. Even for the speedy and effective disposal of cases, government can also establish one or more cyber tribunal. If the accused is absconded, tribunal can try the case in absentia. Punishments for such crimes range between six months to 10 years in jail with financial penalties.

Cybercrime Control Component. In Bangladesh cybercrime seems to be still a low priority for the police. As our police have not been furnished with modern techniques and technology to investigate even traditional crimes, we cannot expect them to acquire the necessary skills overnight to investigate the most complicated hi-tech computer-related crimes. However, Bangladesh police set up a special outfit to curb cyber crimes in 2007, which is the country's first policing unit against such crime. Presently two special units are operating under Crime Investigation Department (CID) at Dhaka and Chittagong of strength 10 each. These are at very rudimentary stage and presently dealing with cell phone related petty crimes only. RAB is also laying emphasis on gearing up its capacity to combat technology-based terrorist activities. But there is not much initiative in the present police training system to grow proficiency in investigating cyber related crimes. However, various organizational and procedural aspects to deal with these hi-tech crimes are being formulated. Presently, under an act, all telecom and Internet service providers are to maintain log of all their customers and such data are to be produced on demand to any designated enquiry officer from Law Enforcement Agency.

Difficulties to Investigate Cybercrime.

a. Under the ICTA 2006, crimes are non-cognizable (Section -76(2) and police cannot go for investigation without warrant. This has taken away freedom of investigation from law enforcing authority.

b. Presently other than two special units under CID, no other police establishment are capable to handle cybercrime issues and these units seriously lack trained investigators, equipment and manpower.

c. Difficulty in defining the crime, jurisdictional issues, detection techniques and collecting digital evidence are also complicated area in investigating cybercrime.

d. There is no special analysis site in conformity with global secure police communication system to provide real-time monitoring of cyber activities.

e. Digital forensic laboratory for investigation and detection of cybercrime with professional experts are essentially required, which we seriously lack.

RESPONSE STRATEGY TO FIGHT CYBERCRIME

General

To respond to cyber threats government has initiated both comprehensive prevention and enforcement measures. First and foremost, we need to formulate a National Cyber Security Policy which would guide to all officials, citizens, businesses and individuals on cyber issues. A strong regulatory framework along with enacting stringent laws is also necessary. Some of the key facets to combat cybercrime are enumerated in subsequent paragraphs.

Educate People – A Concerted Effort

Education contributes to developing a layer of defence in deep security approach and constitutes a real human capacity to help the governments in defeating cyber challenges. Human resource development and appropriate cyber security education programs should exist at several levels (school, college, university) in all cyber security fields. Educational programmes should be effective and available for each kind of stakeholder, i.e. policymakers, justice, police and military professionals, business managers, information technology professionals and end-users. Educational programmes should also include curriculum comprise with moral and social ethics and users' code of conduct for the future IT fellows not to use the technology in a morally reprehensible manner.

Constitutional Provisions

The protection available under the constitution of any country is the strongest and the safest one since it is the supreme document and all other laws derive their power and validity from it. If a law satisfies the rigorous tests of the Constitutional validity, then its applicability and validity cannot be challenged and it becomes absolutely binding. The constitution of Bangladesh, like other constitutions of

the world, is organic and living in nature and is capable of moulding itself as per the time and requirements of the society. The menace of cybercrimes can be effectively curbed, if not completely eliminated, if the three sovereign organs of the constitution work collectively and in harmony with each other. Further, a vigilant citizenry can supplement the commitment of elimination of cybercrime. These are discussed in subsequent paragraphs.

Organisational Undertakings and Obligations

Strengthen Law Enforcing Agencies. To fight against cyber criminals a highly professional and extraordinarily well-equipped law enforcing agency is of paramount importance. 'Cyber incident response unit' and 'cyber crime investigation cell' should be set up at least every divisional headquarters within law enforcement mechanism. Subsequently such outfit may be expanded up to district level by enhancing 'capacity', good police work, skilled investigators, training in the field and providing adequate logistic support. There is also a need to share expertise with other members of Interpol who are technologically advanced. A special analysis site in conformity with global secure police communication system should also be developed which would provide real-time monitoring of cyber activities.

Develop "Computer Emergency Response Team (CERT)". CERT and Computer Security Incident Response Team (CSIRT) are organizations responsible for providing accurate, timely and trusted security information for threat and vulnerabilities carry out awareness and advance warning and assist its constituents in mitigating computer security incidents. Bangladesh CERT (BDCERT) was formed in July 2007 and started its operation fully on15th November 2007 but yet to be recognized by the government. It started its journey with few self motivated individuals on a voluntary basis. BDCERT was approved as General Member by APCERT December 2008 in and by OIC-CERT in January 2009. BD CERT is still in its formative stage. It also works along with other CSIRTs in the region and around the globe. However, it has no means to coordinate with law enforcement agencies as well as with medias for its operations.

Corporate Offices and NGOs Responsibilities. No government just alone can fight cybercrime, it needs active support of all actors of the society specially the NGO's and corporate bodies. A survey of the US National Institute of Justice revealed that the business and financial institutions comprise 46 percent of computer crime targets while the government comprises only 8 percent [Samuel & Charles, The Police in America]. So, corporate offices and NGOs must come forward to augmenting the governmental initiatives with money, logistics and

specialised manpower. Mumbai Cyber Lab is a unique initiative of police-public collaboration for training police officers in investigation of cybercrime. Bangladesh should follow this path and government should initiate dialogs with the NGOs, corporate bodies and donor organisations for sharing government's vision and tentative roadmap towards cybercrime free 'Digital Bangladesh'.

International Cooperation. There are a number of initiatives underway through international organizations on cyber cooperation. The Interpol has formed IT Crime Group that promotes best practices towards investigations to combat these incidents. The G-8's hi-tech crime sub-group prosecutes criminal and terrorist acts that make use of computer networks and other new ICTs. International Multilateral Partnership Against Cyber Threats (IMPACT) is another organisation formed in 2008 under the umbrella of UN global cyber security initiative. An understanding between Bangladesh and IMPACT has already been established to gain its support. Presently, BTRC is working on behalf of the government to tie up the accord. So are many international organisations working for similar objectives. Bangladesh needs to work in close coordination with these international organisations to safeguard her interests.

RECOMMENDATIONS

From the forgoing discussion certain recommendations are appended below for due consideration:

a. Formulate a National Cyber Security Policy as well as establish an entity for overall coordinating and directing responsibility. BTRC may be strengthened to develop as regulatory body of cyber related issues.

b. Create appropriate structures at all level with well-defined role and responsibilities so that human resources with adequate skills, knowledge and training are available to securely manage the information infrastructure.

c. Create awareness and build momentum. Conduct extensive media campaigns and other civic activities to build mass awareness on cyber criminal activities. Initiate programmes to educate everybody about their cyber right and also edify parents on how to filter harmful Internet contents.

d. Initiate dialogs with the NGOs, donor organisations and corporate bodies for sharing government's vision and tentative roadmap towards combating cybercrime.

e. Encourage senior officials of the government and public organisations

to learn basic operations of Internet with alertness for functioning independently.

f. Enhance law enforcement's capabilities for preventing and prosecuting cyber attacks.

g. Promulgate stringent laws towards the menace of cybercrime. Laws should create deterrence in the mind of criminals.

h. Every effort should be made for international cooperation to enable the information sharing, reduce vulnerabilities, and deter malicious users.

j. A national level agency may be created for sanitisation of hardware, software and computer related gadgets specially used in sensitive organisations.

CONCLUSION

Our reliance on networks will only continue to grow in the years ahead. There is a constant need to review cyber strategy as technologies advance, as threats and vulnerabilities change, and as understanding of the information security issues improve. It is not possible to eliminate cybercrime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime. Computer and information security, data protection, and privacy are all growing problems. No single technology or product will eliminate threats and risk. Securing our computers, information, and communications networks secure our economy and our country. Finally, it may be submitted that the collective effort of government and the people is only a possible way to see the peoples' dream of a Digital Bangladesh in existence and could protect individual and national security of the state from the aggression of cyber criminals. Remember our new enemies are just a mouse click away!

BIBLIOGRAPHY

Books

1. Dudeja VD, Cyber Crime and Law Enforcement, Commonwealth Publishers, 2003.
2. Jody R. Westby, International Guide to Combating Cybercrime, American Bar Association, 2003.
3. Victoria Roddle, The Ultimate Guide to Internet Safety, Lulu Press, 2008.

Journal/Report/Article/Paper

4. Cyber Terrorism Concept, Strategy and Counter Measures.
5. Dhaga S. Lt Col, Head Department of Telematics, MCTE, Study Papers on Cyber Conflict.
6. Presentation by M Abdus Sobhan, Executive Director, Bangladesh Computer Council.
7. Osiur Rahman, Mahabubur Rahman & Nour Mohammad, Cyber Law & Territory, Claiming New Dynamism in Jurisprudence.
8. Mohammad Mahabubur Rahman, Cyber Space: Claiming Conceptual and Institutional Innovations.
9. Report, International Telecommunication Union, ICT Application and Cyber Security Division, April 2009.
10. Post Note, Computer Crime, October 2006.
11. Georgia Tech Information Security Center (GTISC), Emerging Cyber Threats Report for 2009.
12. A Discussion Paper Outlining Key Policy Issues, Cyber Security, A New Model for Protecting the Network, 2005.
13. Cybercrime Intelligence Report 2009, Finjan Malicious Code Research Center.
14. Shakila Yeasmin Suchana, Cyber crime in 'Digital Bangladesh' published in Daily Star on.
15. V. Shina Kumar, Asst.Director, A.P.Police Academy (India) 'Cyber Crime – Prevention & Detection'
16. Stein Schjolberg and Solange Ghernaouti-Hélie, A Global Protocol on Cybersecurity and Cybercrime, Cybercrimedata, 2009.
17. Sam Lumpkin, Senior Security Architect, 2AB, Inc, 'Internet Security and Cyber Crime'.
18. The Penal Code, 1860 (Act No. XLV of 1860).
19. The Information and Communication Technology Act, 2006.
20. A.R.M. Borhanuddin (Raihan), Department of Law, Dhaka University, 'Cyber Crime and Bangladesh Perspective'.
21. Shuaib Zahda, Cyber-Terrorism: Hype or Hazard, January 2010.
22. Ronald Deibert, China's Cyberspace Control Strategy : An Overview and Consideration of Issues for Canadian Policy, February 2010.
23. Sean Gallagher, Defense Department's diversity hobbles race to improve to information assurance, 22 January, 2010.

24. US Department of Homeland Security Report, Computer Network Security & Privacy Protection, 19 February 2010.
25. James A. Lewis, Director and Senior Fellow, Technology And Public Policy Program, Center for Strategic and International Studies (CSIS) 'Cybersecurity: Next Steps to Protect Critical Infrastructure', 23 February, 2010.
26. United Nations Manual on the Prevention and Control of Computer Related Crime, 1995.
27. Sharier Khan, The Daily Star, 11 December 2009.
28. Cybercrime Investigation and Forensics.
29. Presentation: Emerging Threats in Cyber Space – Cyber Terrorism, MMS and Data Theft.
30. Script – Cyber Security Vis of Military Delegation
31. Mary Hvistendahl, China's Hacker Army, 3 March 2010.
32. Presentation Paper: Cyber Terrorism.
33. Jimmy Sproles and Will Byars : Statistics on Cyber Terrorism, Information from the Research Paper.
34. David Cater and Andra Katz, 'Computer Crime: An Emerging Challenge for Law Enforcement', Law Enforcement Bulletin, December 1996.
35. Vinayak Godse, DSCI, Cyber Security, 5 March 2009.
36. Samuel Walker and Charles M Katz, The Police in America.
37. The Daily Star, 05 November 2007.
38. The Daily Star, 10 November 2007.
39. New Age, 14 Mar 2008.
40. The Daily Star, 6 September, 2008.
38. Dainik Jai Jai Din, 28 March 2009.
39. New Age, 21 April 2009.
40. The Daily Star, 28 September 2009.
41. Jugantor, 9 January 2010.
42. The Daily Star: 11 May 2010.
43. New Age, 31 May 2010.

Internet Websites

44. http://itu.int/ITU-D/cyb/cybersecurity/legislation
45. http://bdcert.org
46. http:/securityfocus.com
47. http://cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm
48. http://trusecure.com/html/tspub/whitepapers/crime.pdf
49. http://securityfocus.com/vulns/stats.shtml
50. http://attrition.org/errata/stats.html
51. http://cfr.org/publication/15577/evolution_of_cyber_warfare.html
52. http://en.wikipedia.org/wiki/ILOVEYOU
53. http://intelfusion.net/wordpress/?page_id=595
54. http://theatlantic.com/magazine/archive/2010/02/cyber-warriors/7917/
55. http:/en.wikipedia.org/wiki/cyberwarfare#cite_note-41
56. http://en.kioskea.net/news/15123-bangladesh-police-arrest-facebook-share-tipster
57. http://mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html.

Interview

58. H. M. Faruque Ahammad, General Manager & CTO, Information Services Network Limited, on 19 April 2010 at 3 pm.
59. Sumon Ahmed Sabir, Managing Director, BDCOM Online Limited and Chairman BDCERT, on 19 April 2010 at 5 pm.
60. Mohd. Zulfiquar Hafiz (Jewel), Associate Professor, Institute of Information Technology (IIT), Dhaka University, on 22 April 2010 at 11 am.
61. Barrister K. M. Tanjib-ul Alam, Tanjib-ul Alam and Associates, on 22 April 2010 at 5 pm.
62. Md Nazmul Haque, PPM, Deputy Inspector General, Criminal Investigation Department (CID), Bangladesh Police, on 26 April 2010 at 4 pm.
63. Major General Zia Ahmed, psc (Retd), Chairman, Bangladesh Telecommunication Regulatory Commission, on 29 June 2010 at 3 pm.
64. Major Md Rakibul Hassan, Deputy Director, System & Services, Bangladesh Telecommunication Regulatory Commission, on 29 June 2010 at 4 pm.
65. Taifur Rahman Chowdhury, Head of ICT, BRAC, on 12 July 2010 at 10 am.

66. Naimuzzaman Mukta, People's Perspective Specialist, Access to Information Programme, Prime Minister's Office, on 13 July 2010 at 2 pm.
67. Brigadier General Kazi Fakhruddin Ahmed, psc, Director of Forces Signal Intelligence Bureau, Directorate General of Forces Intelligence (DGFI), on 15 July 2010 at 10 am.
68. Lieutenant Colonel Ziaul Ahsan, Director Intelligence, Rapid Action Battalion (RAB), on 15 July at 2 pm.
69. Major Abu Sayed Raihan, Deputy Director Technical, National Security Intelligence (NSI), on 17 July 2010 at 2 pm.
70. Professor Jamilur Reza Chowdhury, Former Vice Chancellor, BRAC University and Former Professor of BUET, on 21 July 2010 at 11 am.

Author

Brigadier General Md. Khurshid Alam was borne on 23 March 1960 and commissioned in the Corps of Signals in December 1980. In his long career in army, he served in command, staff and instructional appointments. He commanded two signal units and was Commandant of 'Centre and School of Military Police, Education and Administration' (CSMEA) and 'Signal Training Centre and School' (STC&S). In addition to regimental staff appointments, he was Brigade Major, Grade 2 Staff at Military Training Directorate, and Grade 1 and 2 Staff at Military Operations Directorate at Army Headquarters. He also served as Director of Directorate General of Forces Intelligence (DGFI). His instructional appointments include Platoon and Term Commander in Bangladesh Military Academy (BMA) and Chief Instructor in Army School of Education and Administration (ASEA). In the United Nation peacekeeping mission, the officer worked as a military observer in Namibia (UNTAG, 1989-90) and as contingent member in Sierra Leone (UNAMSIL, 2001-02). Brigadier General Alam attended many courses at home and abroad including Junior Command in India. He is graduate of Defence Services Command and Staff College (DSCSC) and National Defence College (NDC) of Bangladesh. He also holds Masters Degrees in Defence Studies and Business Administration. He visited many countries across the globe.