
BIPSS
Towards a Secure World
www.bipss.org.bd

# Cyber Security

## The Emerging Threat Landscape

ISSUE BRIEF
A Monthly Publication of the Bangladesh Institute of Peace and Security Studies

Issue 10
January 2012

## Introduction

During the last years, more and more digital products became part of our daily life. We talk to friends over social network sites, discuss with people from all over the world in internet forums and e-mail has widely replaced other communication methods. More and more companies and governments offer digital products and services and most of our data is stored somewhere on a server. But the more we become dependant on digital products, the more we become vulnerable to attacks from cyber space. Cyber attacks can not only cause financial damage or loss of personal data, it is feared that cyber attacks which target hospitals and power plants or other elementary infrastructure of a nation can also cause fatal damages.

## Security threats from cyber space

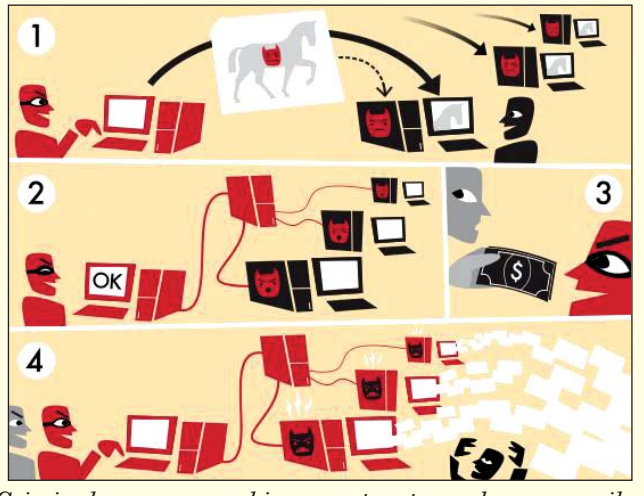
If the whole world is connected via internet, cyber attacks are never just a national threat. Computer viruses, worms and botnets usually affect computers worldwide. So every government and every company who is using electronic data processing has to find a way to secure data, to protect private and confidential data against unauthorized access, to control and limit access to electronic devices and administration, and to fend off attacks on their computer systems. Before thinking about cyber security, an institution has to define what is worthy to protect.[1] A common term that describes these protection measures is *cyber security*. Attacks that try to get unauthorized access to data, networks or computers are so called *cyber attacks*. The topic of cyber war will be discussed later in this paper.

When it comes to cyber security, one of the main questions is: How can unauthorized people get access to internal networks and processes via cyber space? The easiest and simplest way to enter an external computer or network is to take advantage of security gaps. These security gaps can exist within the soft-or hardware used by the governmental institution or company, but the biggest security gap is a system administration that is giving a user too many system access permissions. Giving users extensive system access permission is a big risk. If a user has system access permission and can easily install software and change system settings, intruders can use the lack of knowledge of the person behind the screen to enter a system. With malware attached to e-mails or placed on external storage devices like USB flash drives, intruders can easily enter a system, steal or manipulate data and takeover processes. So the question of cyber security is always also a question of a responsible system administration.

## Zombie computers and Trojan horses – an introduction to malware

Malware like viruses, Trojan horses and worms are working very differently but they are always a serious threat. Most malware is designed to infect Windows system software. If malware is successfully installed and other people are taking over the control of a computer, the computer can become part of a *botnet*. A botnet is usually the description for a "zombie computer network". Without knowledge of the computer owner, his infected computer can become a major part in various criminal activities. In most cases, botnets are involved in attacks on websites or act as sender of spam emails. In the case of attacks on websites or internet services, the army of zombie computers is sending so many requests that the website or service will break down. In some countries, the internet provider will inform the connection holder that his computer is part of a botnet and cut his internet connection until the malware is removed. Usually criminals are owners of botnets and try to get money through it. So there is a big competition along the botnet owners: "The botnet owner community features a constant and continuous struggle over who has the most bots, the highest overall bandwidth, and the largest amount of "high-quality" infected machines (commonly university, corporate, and even government machines)."[2] One of the most famous botnets is the Bredolab botnet, which is believed to be located in Russia or Kazakhstan and was partially shut down in 2010. Bredolab was built up of around 30 million zombie computers and parts of it are still active.[3]

Spam e-mails are not a major safety threat, but their content often include attempts of defraud, dubious offers and phishing attempts.




*Criminals can use zombie computers to send spam emails. (Illustration by Tom Bojarczuk)*

## Private users under attack

The main target of cyber criminals are private people, because cyber criminals are usually focusing on getting money via access to online-banking accounts, e-mail-accounts and credit card fraud. Sometimes private users notice the fraud too late or not at all or feel so embarrassed by the fact that they ordered illegal substances in the internet or sent money to people they just met online that they will not report the incident to the local police. In this article, cyber criminals are defined as people who use the internet for fraud, sabotage, unauthorized access to computers and data theft.

One of the main threats for private users and companies in Bangladesh is scam. Scam is defined as a form of fraud via e-mail. Usually the initiator of the scam is contacting its potential victim out of the blue via e-mail and announces the winning of an award or price, offers a green card or visa, tries to establish a personal or business relationship or announces the admission to one of the top foreign universities. If the sender sees that his potential victim is willing to believe him, he will ask for money to hand over the award, transfer the price, enroll the student at the university or in case of love scam, the sender will pretend to be in an emergency situation or ask for money for a plane ticket to visit his internet love. Worldwide, criminals are making millions of US-Dollars with scam and now scam is becoming a big problem in Bangladesh. Especially new established and successful businesses are seeing themselves confronted with award scam. The scheme is used in a lot of countries worldwide: The sender will announce that the company won an award and the official ceremony will take place in one of Europe's metropolises. Usually the sender of the scam e-mail creates different websites to look more trustworthy. But in almost every case, no one in Europe has ever heard about the award or one of the companies involved in the award ceremony. A little research on the owner of the award websites and its affiliates will show in most cases that all websites mentioned in the scam e-mail are registered on the same person. After receiving an answer from its potential victim, the sender of the award scam will ask for an amount of around 4,000 USD to cover all costs of the award ceremony. At this point the "winner" should be very careful and suspicious. When it comes to scam, people should follow three simple advices: don't trust unknown senders, don't send money or personal data, just delete the e-mail.

Senders of scam usually play with hopes and wishes of their potential victims. They will offer green cards, visas, awards, love, admissions to foreign universities or promise a lot of money. But they always ask for a payment in advance. And after the money is paid, they will ask for more money and in case the victim stops paying, they will disappear. In a lot of cases, victims of scam feel too embarrassed to report the incidents to the police. But usually senders of scam emails are operating from foreign countries, so it is also very difficult for the police and local institutions to fight them. The only thing police and governments can and should do is to create awareness among the citizens.[4]

Activities by cyber criminals that affect governments are the hacking of governmental websites. Sometimes criminals change the content of these websites. In 2010, 20 of the web portals of Bangladesh districts were hacked.[5] The hackers, a common term with negative connotations used to describe people who are using the lack of security in computer systems to enter it[6], placed a message on the district websites saying: "Secure border between INDIA and BANGLADESH If any terrorist send by Pakistan came via Bangladesh route then I will be danger to YOU Cyber War will be started this is demo We don't want more 26/11 in India. GOVERMENT LOOK AT IT ELSE CYBER WAR WILL START ....WE ROOTED [...] YOUR ISP !"

Poorly programmed websites and use of not-up-to-date software make it very easy for hackers. In a lot of cases, hackers are just pointing out the lack of security by placing a message that the website was hacked so that the webmaster of the affected website has a chance to improve its security.

But as uncomfortable a hacked or hijacked website is, these attacks can happen to almost every website but usually they cause little damage except for redirected websites which lead to a *phising* website to steal user data. Phishing describes a process similar to fishing: like a fisherman, criminals lay bait and wait for a victim to bite. The usual bait used for phishing attacks is a copy of a banking, email provider or online payment service website. The phishing website will usually ask for username, password and other sensitive data that is required for online banking or payment. After the user entered his data at the phishing websites, the criminals will try to use his data for a transaction. In this case the economic damage can be enormous. But according to Franz-Stefan Gady, the "real danger to a country's economy arises from advanced persistent threats (APTs) – highly sophisticated and long-planned intrusions often executed with state sponsorship".[8] Espionage is part of the APTs and the following passage will focus on this issue.

## The mystery of cyber espionage

Cyber espionage is not just a threat for companies. Also governments and facilities of strategic importance can be affected by it. Cyber spies who act on behalf of a government can enter the networks of another government and get access to sensitive information and other data that a government would usually not publish.

The simplest way to enter a network is the use of Trojan horses, especially if the network is suffering from a lack of security measures. As soon as one user opens an infested email, the Trojan horse can become active. Cyber spies could alternatively send phishing emails which look like emails from a trustworthy sender but lead the user to a website that is infected with malware or have malware as email-attachment. According to a Wall Street Journal article from June 2011, this happened to a member of the US-cabinet. After opening an e-mail with a Trojan horse as attachment, unauthorized people had access to all of his email communication for months.[9] Of course not just foreign intelligences could have an interest in this kind of information, also political opponents within the country or curious citizens with hacking skills may do it.

During the last years, China was often suspected of carrying out big cyber espionage attacks.[10] This is not the first time that China is suspected of carrying out cyber attacks: "In 1998, computer networks in the Pentagon came under sustained 'attack' for several days. Solemn officials came to the conclusion that China was the attacker and they began to contemplate having the Department of Defense launching some kind of cyber counterstrike when a little more investigation showed that the attacker was not the Peoples Liberation Army but bored teenagers in Cupertino, California."[11]

China denies the involvement in cyber attacks against the US and draws attention to the fact that China itself is a victim of major cyber attacks.[12] But even if the source of cyber attacks remains often a mystery, China is not the only country that is accused of accomplishing cyber attacks. So the following passages will focus on major cyber incidents on national level.

## Terrorism and cyber space

One scenario that is often discussed in news papers is the threat of terrorists who could use the cyber space for their attacks against civil societies. In some scenarios, it is feared that terrorist hackers could take over the control of nuclear power plants, embankment dams or airports. But James Andrew Lewis points to the fact that "Cyber terrorism is not a threat at this time. Terrorists have not launched a single cyber attack. This is probably because it currently takes a large, well-resourced and time-intensive effort to use cyber tools for disruption or attack."[13]

Even if terrorists are not able to carry out cyber attacks at this time, they could profit from a lack in cyber security if e.g. counter-terrorism strategies or data that terrorists could use for planning an attack are easily available on unclassified networks with internet connection. So when it comes to cyber security, governments and companies should keep in mind what damage their sensitive data could create if it falls into wrong hands.

As mentioned above, cyber attacks need deep knowledge and a cost-intensive and time-consuming development process. At the same time, a major blackout or unavailability of websites is not something that causes major attentions rather fear, loss of human lives and panic – are things terrorist attacks usually focus on. No doubt, the cyber space is very interesting for terrorist organizations to spread their propaganda and communicate with their followers worldwide, but the outcome of a cyber attack at this time is usually not something that terrorists would prefer to get attention by and enforce their claims. But this could change if terrorists focus more on cyber attacks due to counter-terrorism and high safety measures and if at the same time, more and more countries become digitized.

## Cyber war – the future of warfare?

Cyber war needs to be distinguished from other cyber attacks and "cyber warfare will almost certainly have very real physical consequences".[14] Together with the common definitions of war, this leads to the conclusion that there was no cyber war so far. But it is completely wrong to think about a cyber war as a war between countries that is just taking place in cyber space. It is very doubtful that cyber war will replace traditional war in the near future. On the contrary cyber war will become an addition to other tactics in war, so we should think of "cyber war as an adjunct to military operations."[15] In that case, cyber war can also affect countries that cannot take part in cyber war strategies.

According to Shimeall, Williams and Dunlevy[16] there are two categories of cyber war:

A) *Limited cyber war* which focuses on the information infrastructure with little or no real-world action accompanying the attack

B) *Unrestricted cyber war* which causes major destruction because this kind of war makes no distinction between civilian and military targets and attacks air-traffic control, emergency-service management, water resource management and power generation. This kind of cyber war can cause an extent of destruction which is massive, long of duration and a threat to human life.

So far, both kinds of cyber wars are an addition to military operations and a sheer cyber war scenario is nothing that can be expected in near future. It is obvious that a country with lax cyber security is more vulnerable for cyber attacks, cyber espionage and also cyber war especially if the country is not able to protect its infrastructure from cyber attacks and cyber war or not capable of carrying out a counterattack. But as seen on the example of Stuxnet, a cyber attack usually base on a long-drawn-out development process and so it is questionable if one day cyber attacks will redeem other military tactics that allow more flexibility and short-term use.[17]

## Major cyber incidents on national level

In 2010, the computer worm named Stuxnet was discovered. It is one of the most mysterious cyber attacks that have happened so far. Some observers[18] see in the Stuxnet attack a cyber war incident.

Stuxnet targeted only Siemens industrial software based on Microsoft Windows. One of the main targets that were using this kind of software was Iran which led to rumors about the place of origin of the worm. The computer worm infected laptops at the Bushehr nuclear reactor and led to delays in the launch of Iran's first nuclear power plant. At first the worm managed to stay invisible which led to the conclusion that it was a "marksman's job".[19] However, the development of

Stuxnet is assumed to base on deep knowledge and a cost intensive development process which distinguishes Stuxnet from other worms that were sometimes created by a single person.[20] The fact that the attack primarily targeted Iran's nuclear reactor led to speculations about the involvement of the United States and Israel. But Stuxnet remains a mystery, also because the worm did not cause any serious damage to the infected systems. But it seems like Stuxnet was not created for espionage, Stuxnet was made for sabotage: "It indicates that [Stuxnet's creators] wanted to get on the system and not be discovered and stay there for a long time and change the process subtly, but not break it […] The malware intercepts commands sent to the drives from the Siemens SCADA software, and replaces them with malicious commands to control the speed of a device, varying it wildly, but intermittently. The malware, however, doesn't sabotage just any frequency converter. […] Stuxnet targets only frequency drives from these two companies [Iran-based Fararo Paya or Finland-based Vacon] that are running at high speeds – between 807 Hz and 1210 Hz. Such high speeds are used only for select applications. Symantec is careful not to say definitively that Stuxnet was targeting a nuclear facility, but notes that 'frequency converter drives that output over 600 Hz are regulated for export in the United States by the Nuclear Regulatory Commission as they can be used for uranium enrichment'."[21]

Stuxnet found its way into the networks on infected hardware. A similar incident took place in 2008, when infected USB flash drives led to the infection of computers in the U.S. Central Command (CENTCOM) with the worm Agent.btz. But the worm could not create any damage or open doors to unauthorized access to classified information because usually laptops with classified data are just having a thin connection to the internet.[22] This incident remained a mystery too and the source of the worm could not be tracked.

Also the recently reported computer virus on drones used by the US will probably remain a mystery. According to wired magazine, the virus and its keylogger are "logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones".[23] But as in the case of infected U.S. Central Command computers with Agent.btz, the virus came not from the internet: "Predator and Reaper crews use removable hard drives to load map updates and transport mission videos from one computer to another. The virus is believed to have spread through these removable drives."[24] So the question of whether the virus is able to send information to someone outside the classified network remains but it is quite doubtful that something like this happened because as said above, usually classified networks are just having a thin connection to the internet. In this case a virus can enter a network very easily on an infected flash drive but it is almost impossible for a virus to communicate with its sender. But flash drives are not only a security risk because they could bring malware into a computer network. They are also a security risk because they can lead to loss of data if users store sensitive data on the flash drive and take the flash drive when they are leaving the office.

Another example for a cyber attack on national level is a serial of cyber attacks against institutions in the United States. These attacks are summed up under the name Titan Rain. Since 2003, there were a number of coordinated attacks against computer networks in the US: "[…] these hackers wanted all the files they could find, and they were getting them by penetrating secure computer networks at the country's most sensitive military bases, defense contractors and aerospace companies."[25] The identity of the hackers remained unknown. But sure is that the attacks were well coordinated and the hackers used a tool that seemed to be designed just for this cyber espionage: "This was a scanner program that "primed the pump," according to a former government network analyst who has helped track Titan Rain, by searching vast military networks for single computers with vulnerabilities that the attackers could exploit later."[26]

All these attacks had in common that they remained invisible for the common population of a country. This was different in the 2007 cyber attacks on Estonia. These attacks were not a silent espionage attack. In Estonia, hackers were "disabling the websites of government ministries, political parties, newspapers, banks, and companies" and even NATO became active and decided to send one of its cyber terrorism experts to Tallinn.[27] A patriotic pro-Kremlin youth organization claimed responsibility for organizing the cyber attack "as an act of personal protest."[28]

Some sources assume that cyber attacks were responsible for the blackouts in parts of Rio de Janeiro in 2005 and 2007.[29] But there is no official approval of this theory and even if cyber attacks caused the blackouts, it is very unlikely that a state actor is responsible for this kind of attacks.

## Digital Bangladesh as national security challenge

According to the Digital Bangladesh vision of the governing Awami League, Bangladesh is believed to become a completely digitized country with universities, schools, madrasahs, hospitals and governmental institutions connected to the internet by 2021.[30] At the same time, companies are said to offer more and more online services so that online shopping, online banking and e-mail communication are believed to become more available and more important. But as simple as that sounds, with increasing online activity, criminals will find their way to the digital world too. In digitized countries, phishing, hacking and stealing of personal data are daily fare. In addition, threats to governmental institutions and companies can affect the daily life of an entire population.

When we start to think about cyber security in Bangladesh, one main question comes up: how is cyber security possible in a country where 90% of the software is pirated software?[31] Especially because it can happen that pirated software comes already with Trojan horses or other kinds of malware. Of course licensed software[32] is not the key to cyber security, but up-to-date software and protection software are very important presumptions to keep a network safe. Especially when a pirated Windows version is used: "Microsoft rolled out an updated Windows Genuine Advantage (WGA) system to help combat the high rate of piracy of its Windows platform. One of the side effects of this policy is that people using illegal copies of Windows will be more likely to disable automatic updates from Microsoft. The fear is that a subsequent update may adversely affect their experience with Windows in a similar way the "black screen" that affected many users in China operating illegal copies of Windows. Without automatic updates, it is highly unlikely that many of these users are manually installing critical updates [...]"[33] If not updated, the security gaps remain and malware can attack the system.

But getting up-to-date software even with a small budget is possible. The recently introduced laptops developed by Doel are using Linux software or Google Android. Open Source Software can be a good alternative if other software is not affordable. But even this software needs experts with deep knowledge about networks and security. So the first important step to improve cyber security is education. Only deep knowledge in networks and software can help to protect networks from cyber threats. As well as computer education in schools and universities, the role of private companies is very important. So a government should invest in its youth and try to get as attractive as possible for software companies who can take part in the education of future computer experts.

Major parts of Bangladesh's institutions and facilities are still offline. But to fulfill her Digital Bangladesh 2021 vision, Prime Minister Sheikh Hasina emphasized: "Every part of the country will be brought under e-governance, while the telecommunication system is being modernised to cut the digital divide"[34] Attacks like in Estonia in 2007 showed that e-governance[35] infrastructures can be easily attacked. At the same time, the privacy of the citizens will become an issue if their personal data will be stored on computers which can be attacked by cyber criminals. On the one hand, the government will have to protect the data of its citizens; on the other hand the government will have to protect its own data and communication from cyber spies and terrorists. But as mentioned above, sensitive facilities have usually classified networks without or with thin internet connection. So malware is usually not a major threat to classified networks because without internet connection and contact to its sender, a Trojan horse cannot open doors to unauthorized access.

Another question of cyber security is the use of electronic voting machines in Bangladesh. Experiences from other countries show that electronic voting machines can cause a lot of difficulties and bias the election outcome. The German based hacker association Chaos Computer Club (CCC) demands a prohibition of electronic voting machines because according to a study published by CCC, electronic voting machines can suffer from a lack of privacy and be very easily manipulated.[36]

Another cyber threat that can lead to serious damage to Bangladesh's economy is the situation of cyber security in the banking sector. Bangladesh is far from online banking and widespread usage of credit cards, but a globalized world will make online financial transactions and worldwide accepted credit cards more and more important for companies and customers. The rise of electronic payment methods will raise questions about online security and banks will see themselves confronted with the question of who will be responsible if cyber criminals empty a bank account or misuse stolen credit card information.

Important steps to improve the situation of cyber security in Bangladesh are the classification of digitized data and networks, the implementation of

Open Source solutions wherever other products are not affordable and the set-up of a taskforce which will focus on the broad implementation of cyber security and the analysis of cyber attacks. At the same time efforts should be launched to create more awareness of cyber threats among the citizens and to prevent that Bangladesh will become a safe haven for cyber criminals and botnets. With an increasing access to internet connections and computer education, cyber criminals and their techniques will also become more sophisticated. In addition topics like cyber stalking and cyber mobbing will become bigger threats for young people who disclose too much of their personal data on the internet without being aware of the fact that everything ever written or published in the internet will remain there forever. So not just police and policy makers should focus on the consequences of cyber crime, also parents should pay more attention on what kind of personal information their child is sharing with strangers in the World Wide Web. At the same time, victims of cyber stalking and cyber mobbing should have contact people who will help them with getting over the harm caused by the violation of their privacy.

## Conclusion

Even though more and more digital products became part of our daily life and made us vulnerable to attacks from cyber space, cyber attacks are not a threat to the national security at present. In most cases cyber attacks cause financial damage or loss of personal data. So far there was no cyber attack on the infrastructure of a state that was carried out by another state or a terrorist organization. As mentioned above, cyber attacks need deep knowledge and a cost-intensive and time-consuming development process. Even though the cyber space could be important for the communication between extremist organizations and their followers; it is very unlikely that terrorists will switch their focus to cyber attacks any time soon. But this does not mean that the cyber space is a safe place. As defined earlier, cyber security describes the ability to protect data which is worthy to protect. If users, companies and governments fail to define confidential data and at the same time fail to adopt different security measures, the data is easily available to unauthorized access. But as mentioned earlier, private user are under attack of cyber criminals too and should be aware of the risks from cyber space and it should be within the responsibilities of a government to inform the citizens about the risks and threats of cyber attacks or loss of personal data. At the same time a government has to define the level of the cyber threat within the country and choose adequate measures to face the cyber threat.

***Definitions of Malware***

| Malware | Function | Damage |
|---|---|---|
| Computer virus | A program that usually replicates itself via host files on the computer and other devices connected to the network. Usually the virus needs to get started by a user. | Some computer viruses create damage by manipulating data, but usually viruses are just stealing capacity, cause error messages and make the computer system ineffective. |
| Computer worm | To get infected by a computer worm, it is usually just necessary to be connected to the internet or an infected storage medium. Worms are able to find lacks of security and install themselves on the computer without user involvement. | A worm can affect the computer by causing crashes and work as a gate opener for Trojan horses. |
| Trojan horse | A Trojan horse is a door opener for unauthorized access to a computer and usually a user has to open the Trojan horse to start the process. But sometimes worms can place a Trojan horse in the auto start function of system software. | Trojan horses can allow unauthorized persons to get access to data, takeover the control of a computer or track keyboard entries to steal passwords. |

# End Notes

1 cf. Cole, Eric 2009: The network security bible. Indianapolis: Wiley Publications, Chapter 1.

2 http://www.broadbandreports.com/faq/trojans/1.0_Trojan_horses, (accessed on 10 October 2011).

3 Leyden, John: Undead Bredolab zombie network lashes out from the grave - Someone's still pulling the strings. http://www.theregister.co.uk/2010/10/29/bredolab_botnet_death_throes/, (accessed on 10 October 2011).

4 The Australian Government offers a very informative website regarding this issue: http://www.scamwatch.gov.au

5 Star Online Report: Bangladesh district portals hacked. http://www.thedailystar.net/newDesign/latest_news.php?nid=22785, (accessed on 3 October 2011).

6 But the term hacker describes also people who are focusing on cyber security to improve it.

7 Star Online Report: Bangladesh district portals hacked. http://www.thedailystar.net/newDesign/latest_news.php?nid=22785, (accessed on 3 October 2011).

8 Gady, Franz-Stefan: Statistics and the 'Cyber Crime Epidemic'. http://www.ewi.info/statistics-and-cyber-crime-epidemic, (accessed on 5 October 2011).

9 cf. Crovitz, L. Gordon: China Goes Phishing. Google uncovers Beijing's escalating cyber warfare. http://online.wsj.com/article/SB10001424052702303657404576363374283504838.html, (accessed on 6 October 2011).

10 cf. Nakashima, Ellen: Lawmaker calls for international pressure to stop China's cyber-espionage. http://www.washingtonpost.com/world/ national-security/lawmaker-calls-for-international-pressure-to-stop-chinas-cyber-espionage/2011/10/04/gIQAAR26LL_story.html, (accessed on 6 October 2011).

11 Lewis, James A.: Computer Espionage, Titan Rain and China. http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf, (accessed on 6 October 2011).

12 Ibid.

13 Lewis, James Andrew: Rethinking Cybersecurity - A Comprehensive Approach. http://csis.org/publication/rethinking-cybersecurity-comprehensive-approach, (accessed on 22 October 2011).

14 Shimeall, Timothy / Williams, Phil / Dunlevy, Phil: Countering cyber war. http://www.nato.int/docu/review/2001/0104-04.htm, (accessed on 12 October 2011).

15 Shimeall, Timothy / Williams, Phil / Dunlevy, Phil: Countering cyber war. http://www.nato.int/docu/review/2001/0104-04.htm, (accessed on 12 October 2011).

16 Ibid.

17 Therefore cyber security is becoming a major part in defense strategies and policy planning of several countries and organizations like NATO.

18 cf. Beaumont, Peter: Stuxnet worm heralds new era of global cyberwar. http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar, (accessed on 6 October 2011).

19 cf. Broad, William J. / Markoff, John / Sanger, David E.: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all, (accessed on 3 October 2011).

20 cf. Gross, Michael Joseph: Stuxnet worm. A Declaration of Cyber-War. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104, (accessed on 3 October 2011).

21 Zetter, Kim: Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage, http://www.wired.com/threatlevel/2010/11/stuxnet-clues/, (accessed on 12 October 2011).

22 cf. Shachtman, Noah: Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack, http://www.brookings.edu/opinions/2010/0825_pentagon_worm_shachtman.aspx, (accessed on 6 October 2011).

23 Shachtman, Noah: Exclusive: Computer Virus Hits U.S. Drone Fleet. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/, (accessed on 8 October 2011).

24 Ibid.

25 Thornburgh, Nathan: The Invasion of the Chinese Cyberspies. http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html, (accessed on 8 October 2011).

26 Thornburgh, Nathan: Inside the Chinese Hack Attack. http://www.time.com/time/nation/article/0,8599,1098371,00.html, (accessed on 8 October 2011).

27 Traynor, Ian: Russia accused of unleashing cyberwar to disable Estonia http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, (accessed on 8 October 2011) http://www.nato-pa.int/default.Asp?SHORTCUT=1782

28 CBSNews: Cyber War: Sabotaging the System. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml, (accessed on 8 October 2011).

29 CBSNews: Cyber War: Sabotaging the System. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml, (accessed on 8 October 2011).

30 cf. Siddiqi, Hafiz: Managing Digital Bangladesh 2021, http://www.thedailystar.net/newDesign/news-details.php?nid=79698, (accessed on 1 October 2011).

31 According to the 2010 Piracy Study published by Business Software Alliance, http://portal.bsa.org/globalpiracy2010/downloads/study_pdf/2010_BSA_Piracy_Study-Standard.pdf, p. 3, (accessed on 10 October 2011).

32 Licensed software includes Open Source software.

33 Danchev, Dancho: Does software piracy lead to higher malware infection rates? http://www.zdnet.com/blog/security/does-software-piracy-lead-to-higher-malware-infection-rates/4605, (accessed on 10 October 2011).

34 Ethirajan, Anbarasanhttp Bangladesh unveils $130 'Doel' laptops,http://www.bbc.co.uk/news/world-south-asia-15261076, (accessed on 22 October 2011).

35 The digital communication between government and its citizens.

36 cf. http://wahlcomputer.ccc.de/

**Tk. 25.00**

House 405, Road 6, DOHS, Baridhara, Dhaka 1206
Tel: 88 02 8414284-5, Fax: 88 02 8411309, E-mail: info@bipss.org.bd
**www.bipss.org.bd**