Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

Cyber Security

Dhirodatta Subba is an Assistant Professor and Head, Department of Computer Science and Application, Salesian College, Siliguri Campus. He obtained his M. Sc (Mathematics) and M. Tech (Computer Science and Data Processing) from IIT Kharagpur. He worked with Tata Consultancy Services for many years before joining the College. He is associated with editing of the Salesian Journal of Humanities & Social Sciences.

Abstract

The growth of Internet Technology has brought huge benefits to mankind. However, new and more complex issues have arrived: cyber crime, cyber terrorism, cyber espionage, cyber war. The subject that deals with the preventive aspect of handling these issues is Cyber Security. It requires an army of trained professionals to make the country safe from these threats. Due to its importance, University Grants Commission (UGC) has mandated that the subject be taught in the institutes of higher education. It is a vast subject, and in this article effort has been made to introduce it in brief with some basic information regarding sources of threat, forms of cyber attack and elements of cyber security.

Keywords: Cyber security, Cyber space, Cyber espionage, Cyber war, CERT-In.

Introduction

In the recent past we have witnessed some events which are worth mentioning. The first one is about Iran's nuclear program. Many countries in the world had been watching the development with concern as Tehran was determined on producing weapons-grade uranium. The stated intention about the program was for medical research. In his retirement speech to the Israeli Knesset Foreign Affairs and Defense Committee on January 7, 2011, Mossad Chief Meir Dagan stated that Iran would not be able to produce a viable nuclear weapon before 2015. He elaborated that Iran is still far from being capable of producing nuclear weapons and that a series of malfunctions and failures had set the Iranian nuclear weapons program back by several years.[1] Meanwhile, from around June 2010, rumor about Stuxnet, a computer worm, believed to have originated in Israel, was doing the rounds in international media. It made its way into the computers of Iran's nuclear facilities via the laptops used by engineers. The worm first reached the laptops through internet.

> It knew exactly what to do. It did not make the control systems go haywire or stop the machines abruptly, which might have caused suspicion. It just tweaked the controls so as to make the centrifuge yield very little without going defunct. It is said to have increased the speed in order to damage the spindle in the machines over a period of time. The centrifuge

1 URL: http://www.haaretz.com/print-edition/news/outgoing-mossad-chiefiran- won-t-have-nuclear-capability-before-2015-1.335656 (accessed on 14/Apr/2013)

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

machines, during the productive period, worked so inefficiently that they hardly enriched any uranium quantity before going out of order.[2]

Another one that hit the news headlines in April 2010:

Unidentified hackers based in China systematically penetrated computers in sensitive Indian government offices, including the National Security Council Secretariat, electronically stealing documents on Maoists, missiles, and personal and financial information on Indian officials.[3]

Further back, in 2008 South Ossetia war, Russia's initial attack on Georgian soil was preceded by a synchronized cyber attack that crippled Georgian government websites.[4]

These examples give us a sense of how the present and the future looks when we are dealing with the age old issues of conflicts or power game. Cyber world is known as the 'fifth front' by people involved in defense - others being land, air, sea and space. The use of cyberspace depends on physical facilities like undersea cables, microwave and optical fibre networks, telecom exchanges, routers, data servers, and so on.

Sources of Threat

Some of the known sources are as follows:

- **Insider Threat**

  The disgruntled insider is a potential perpetrator of computer crimes. Insiders do have unrestricted access to the system/s; so, they could damage it or steal data for personal gain.

- **Criminal Groups**

  Criminal groups are increasingly using cyber intrusions, attacking systems for purposes of monetary gain. They are responsible for extortion, credit card frauds, tricking employees into giving up their log-in and password information (identity theft) which they use to break into target systems and vandalize them. They are making use of social media sites to gather intelligence about companies to achieve this objective. They are also using innovative techniques through 'spam', 'phishing' and 'vishing' to steal sensitive user information.

2 URL: http://www.telegraphindia.com/1120216/jsp/opinion/ story_15137785.jsp#.UWV_96I9GxA (accessed on 14/Apr/2013)

3 URL: http://www.telegraphindia.com/1100407/jsp/frontpage/ story_12311784.jsp (accessed on 14/ Apr/2013)

4 URL: http://www.crn.com/news/security/210003057/russian-cyberattacks- shut-down-georgian-websites. htm (accessed on 14/Apr/2013)

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

- **Malware Developers**

  Malware (Virus, Worm, Trojan) developers can do more damage to networks than hackers do. Malware attacks are also being launched from social media sites such as Facebook or LinkedIn.

- **Foreign Intelligence Services**

  Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Foreign intelligence services are actively using cyber tools as part of their information gathering and espionage tradecraft; target being sensitive government and private sector information for the purpose of gaining strategic, economic, political, or military advantage. The theft of innovations which are the fruits of costly investments in research and development is an immense strategic and economic loss to the targets.

- **Foreign Military**

  Although cyber war is not so lethal in the sense of human loss or property destruction, the consequences could be equally severe, especially, if the level of automation is high in the country as the system of governance as well as business and industry could be brought down to a state of total collapse, even if temporarily.

- **Terrorists**

  Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. There are reasons to expect terrorists to use cyber attacks to disrupt critical systems in order to harm targeted government or civilian populations. The knowledge of making bombs, lethal weapons, and even weapons of mass destruction (WMD) are freely available in the internet.

- **"Hacktivists"**

  Politically motivated attacks on publicly accessible web pages or email servers. Groups and individuals seek to overload email servers and to hack into web sites in order to send a political message. While these attacks generally have not altered operating systems or networks, they still damage services, and by denying the public access to websites containing valuable information, they infringe on others' right to communicate.

- **"Recreational" Hackers**

  Virtually every day there is another report about "recreational hackers" or "crackers" who penetrate networks for the thrill of it or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill and

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

computer knowledge, the recreational hacker can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. These types of hacks are numerous and may appear on their face to be benign, but they can have serious consequences.

Forms of Cyber Attack

Following are the commonly found techniques:

- **Hacking**

  It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some technologies like packet sniffing, tempest attack, password cracking and buffer outflow facilitates hacking.

- **Web Defacements and Semantic Attacks**

  Website defacements are the most common form of politically motivated cyber attack. The most serious consequences of web defacements result from "semantic attacks," which change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated.

- **Domain Name Server (DNS) Attacks**

  Computers connected to the Internet communicate with one another using Internet Protocol (IP) addresses. Computers consult domain name servers (DNS) to map the name of a website (e.g. xyz.com) to its numerical IP address (64.12.50.153). If the DNS provides an incorrect numerical address for the desired website, then the user will be connected to the incorrect server, often without the user's knowledge. A DNS attack can thus be used to disseminate false information or to block access to the original website.

- **Distributed Denial of Service (DDoS) Attacks**

  Distributed Denial of Service attacks subject web and email servers to overwhelming numbers of communications from other computers. The high volume of communications can slow or crash the target system. Hackers often multiply the force of their DDoS attacks by using malicious code to take control of other users' machines and using these "zombie" machines to send additional communications to targeted servers. The hijacked computers are also called 'botnets'.

- **Syntactic Attacks using Malicious Code**

  Worms, Viruses, and Trojan horses are types of malicious code. The computer infrastructure is damaged by modifying the logic of the system in order to introduce

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

delay or make the system unpredictable. It is a cost-effective way to significantly disrupt the information infrastructure. Malware is getting smarter and has evolved from simple code that can be identified by its signature to one that can change its signature, making it very difficult to detect. Major commercial anti?virus programs are not always able to identify them.

- **Exploitation of Routing Vulnerabilities**

  Routers are the "air traffic controllers" of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing disruptions from malicious activity have been rare; but the lack of diversity in router operating systems leaves open the possibility of a massive routing attack. The malicious reprogramming of even one router could lead to errors throughout the Internet.

- **SQL Injection Attack**

  SQL (Structured Query Language) is the language of computer database. Whenever one fills out a form to purchase a product through a website, the entries are translated into SQL and entered into a database. If a particular web form has been poorly designed, an attacker can enter information to trick the database into revealing information it was not intended to, for example, vast customer lists including email addresses and credit card information.

- **Defamation**

  E-mails could be used for spreading disinformation, threats and defamatory elements. Similarly, social networking sites could be used.

- **Use of Cryptology**

  Financial institutions and governments have been using encryption for secure data transmission. But the availability of high frequency encrypted voice/data links has made the task of tracking communications by bad elements and terrorists difficult. It is a herculean task to decrypt the information being exchanged.

- **Compound Attacks**

  By combining methods, hackers could launch an even more destructive attack. Politically-motivated hackers will seek to attack high-value targets, including networks, servers, or routers whose disruption would have symbolic, financial, political or tactical consequences.

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

What is Cyber Security?

"Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."[5]

"Cyber security involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a nation, or its people."[6]

Elements of Cyber Security

The following are the general characteristics of cyber security framework:

Application Security

It is the use of software, hardware, and procedural methods to protect applications from external threats. Following are some examples:

- Application firewall that limits the execution of files or the handling of data by specific installed programs
- Anti-virus software
- Spyware detection/removal programs
- Configuration and patch management
- Following security protocols for Web applications during development
- Performing hostile security test

This involves breaking into own system through the web application - simulated attack.

- Penetration tests
  These are regular scans for vulnerabilities which can uncover problems and make one aware of software that needs to be patched. Thorough scans can be performed by third party consultants like Qualys, or with use of software like.

Information security

- User access authorization
- Encryption/decryption programs
- Database logs

5 URL: http://whatis.techtarget.com/definition/cybersecurity (accessed on 11/Apr/2013).

6 URL: http://www.paloaltonetworks.com/community/learning-center/ what-is-cyber-security.html (accessed on 11/Apr/2013).

- Auditing process
- Web Application Firewall (WAF)
  This new breed of firewall watches for attack signatures and stops them before they reach the application. It comes either as an appliance, made by companies like Imperva or Barracuda Networks, or as a cloud-based service, like CloudFlare.

Network security

- A router that can prevent the IP address of an individual computer from being directly visible on the Internet
- Conventional firewalls
- Network security monitoring for detection and prevention of intrusions
- Auditing process

Disaster recovery / business continuity planning

- One possibility is that of moving some of the infrastructure to the cloud for its ability for network resources to scale elastically in order to mitigate the attacks. Google's AppEngine, Amazon's EC2, RackSpace's Cloud, CloudFlare - they have the infrastructure in place to continue to run even under what would be a withering attack to a traditionally hosted site. This approach allows sites to use only the resources they need under normal conditions, but still not be overwhelmed when an attack occurs.

End-user education

- Insuring all employees/users, not just the IT staff, are aware of safe computing practices by way of training, newsletters, posters and simulations.
- Introducing the subject in regular courses of academic and engineering institutes so students get the knowledge early on.

Issues Involved

Following are some of the key issues:

- Complications associated with cross-border law enforcement
  A typical cyber investigation can involve target sites in multiple states or countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Moreover, attribution and identification is extremely difficult as identities of the perpetrator can be easily masked, making it easy for the possibility of denials.

- Slow realization
  Malware is getting smarter and has become very difficult to detect, even for major

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

commercial protection software. Often, cyber attacks are silent and go unnoticed for long periods.

- Lack of International Standard/convention
  With regard to Cyber attack, Cyber war, and appropriate countermeasures, till date there is no common convention agreed upon by all nations. Globally, the issues are still under debate.

- Constantly evolving nature of security risks
  To deal with such environment, advisory organizations are promoting a more proactive and adaptive approach. In USA, for example, the National Institute of Standards and Technology (NIST, a unit of the Commerce Department, formerly known as the National Bureau of Standards), issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments. International Organization for Standardization (ISO) has its own guideline. These guidelines are expatiated on in the NIST 8007 and ISO 270028 publications.

How are we doing?

On 9th June, 2000, our parliament passed the "IT Act 2000".[9] It addressed issues primarily related to electronic commerce. In 2008, Parliament passed amendments to the IT Act, with added emphasis on Cyber Terrorism and Cyber Crime, with a number of amendments to existing sections and the addition of new sections, taking into account cyber threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act.

Indian Computer Emergency Response Team (CERT-In): CERT-In is the most important constituent of India's cyber community. It is modeled along similar agencies in the Western countries. Its mandate states, '*ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance*'.

Under the IT Amendment Act 2008, only CERT-In is mandated to serve as the national agency in charge of cyber security. The Act also provided for a national nodal agency for protection of CII (Critical Information Infrastructure).

7 URL: http://www.itl.nist.gov/lab/specpubs/sp800.htm (accessed on 14/Apr/2013).

8 URL: http://www.iso27001security.com/html/27032.html (accessed on 14/Apr/2013).

9 URL: http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf (accessed on 15/Apr/2013).

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

As for National Policy on cyber security, the Department of Information Technology issued a discussion draft on National Cyber Security Policy[10] on 26th March 2011, and invited comments on it. Among the publicly available feedbacks are following:

- Observations from Takshashila Institution were provided back in May 2011.[11] It contained many suggestions for improvement.
- Institute for Defense Studies and Analysis (IDSA) has done a thorough job of assessing the cyber security challenges facing the country in the study report. It includes some feedback by way of references to the original document.[12] It recommends setting up of a central command for handling cyber war, as it is considered to be the fifth front.
- Data Security Council of India (DISC), setup as an independent Self-Regulatory Organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same, has presented its viewpoint from the Industry perspective: "While CERT-In is doing an excellent job in the government sector, same needs to be replicated for the private sector through establishment of appropriate agencies within each of the identified private sectors, that co-ordinate with CERT-In and / or National Nodal Center that may be created. DSCI feels that in this policy, there should be a recommendation for establishment of National Nodal Center, which will co-ordinate the efforts of both the public and private sectors and will also assign roles and responsibilities."[13]
- Dr. Marri Channa Reddy Human Resource Development Institute of Andhra Pradesh also provided some input. Table A in the next page is a summary of procedural recommendations at four levels: Country, Network, Corporation and User.

Chart-1 (page 69) in the following section is a representation of government organizations that would work in collaboration with one another, as proposed in the draft security document.

Department of Electronics and Information Technology initiated the Legal framework.[14]Many other entities are involved in the work.[15]

10 URL: http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf(accessed on 15/Apr/2013).

11 URL: http://www.takshashila.org.in/wp-content/uploads/2010/03/TPACyberSecurity-RJSKN-1.pdf (accessed on 15/Apr/2013).

12 IDSA, IDSA Task Force Report, 2012. URL: http://idsa.in/system/files/book_indiacybersecurity.pdf (accessed on 15/Apr/2013).

13 DSCI Comments on National Security Policy_Final.pdf, URL: http://www.dsci.in/taxonomy/term/591 (accessed on 15/Apr/2013).

14 URL: http://deity.gov.in/content/cyber-laws (accessed on 15/Apr/2013).

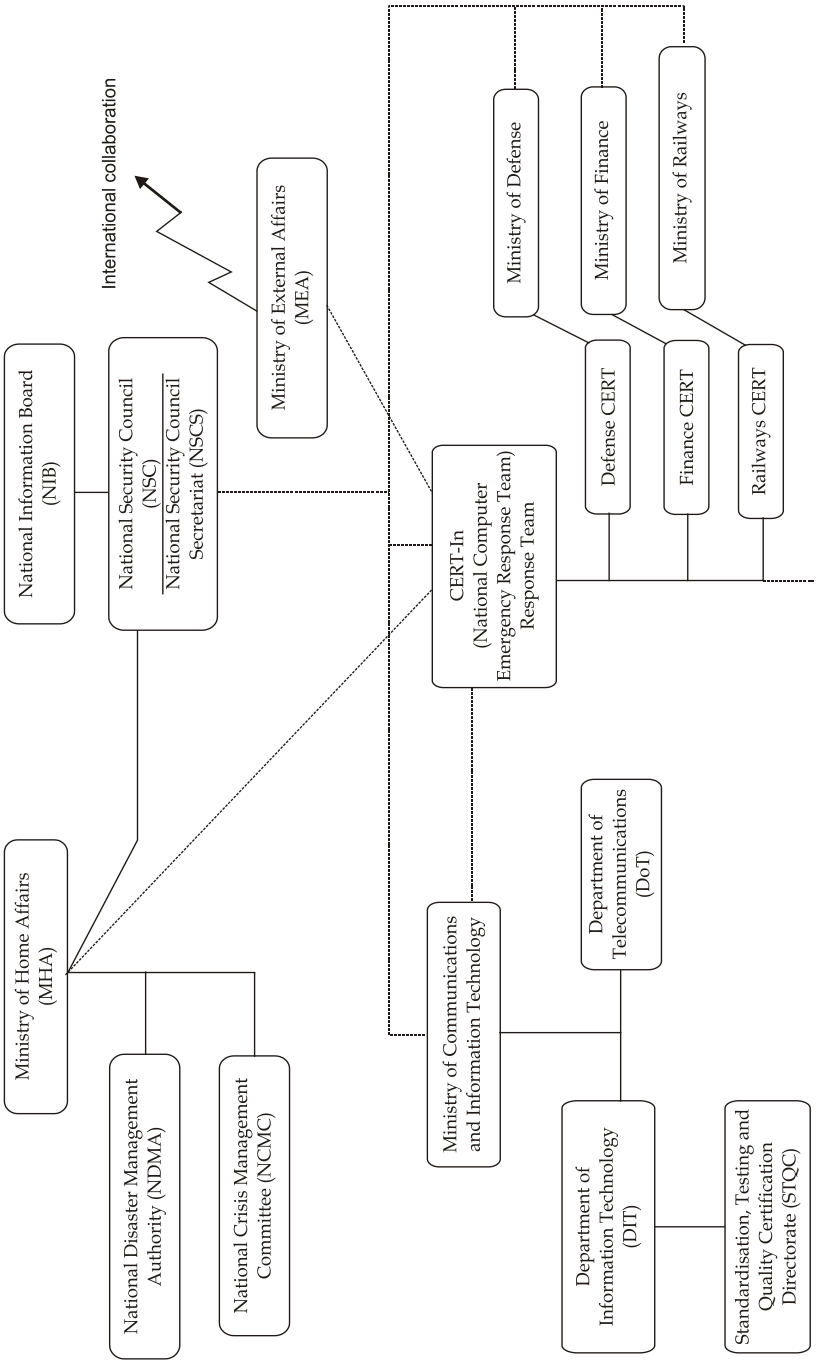
15 URL: http://www.cyberlawsindia.net/; http://www.caaa.in/Image/cyber%20laws%20overview.pdf (accessed on 15/Apr/2013).

Country	Network	Corporate	User
• Policy directives on data security and privacy protection - Compliance, liabilities and enforcement (e.g. Information Technology Act 2000) • Standards and guidelines for compliance (ex: ISO 27001, ISO 20001 & CERT-In guidelines) • Conformity assessment infrastructure (enabling and endorsement actions concerning security product - ISO 15408, security process - ISO 27001 and security manpower - CISA, CISSP, ISMS-LA, DISA etc.) • Security incident - early warning and response (National cyber alert system and crisis management) • Information sharing and cooperation (MoUs with vendors and overseas CERTs and security forums). • Pro-active dealing with malicious activities on the net by way of net traffic monitoring, routing and gateway controls Lawful interceptions and Law enforcement. • Nation- wide security awareness campaign. • Security research and development focusing on tools, technology, products and services.	• Compliance to security best practices (ex. ISO27001), service quality (ISO 20001) and service level agreements (SLAs). • Pro-active actions to deal with malicious activities, ensuring quality of services and protecting average end users by way of net traffic monitoring, routing and gateway controls • Keeping up-to-date with security technologies and processes (configuration, patch and vulnerability management) • Conformation to legal obligations and cooperation with law enforcement activities, including prompt actions on advisories issued by CERT-In. • Use of secure product and services and skilled manpower. • Crisis management and emergency response.	• Compliance to security best practices (ex. ISO27001. • Pro-active dealing with malicious activities, protecting average end users by way of net traffic monitoring, routing and gateway controls • Keeping up-to-date with security technologies and processes (configuration, patch and vulnerability management) • Conformation to legal obligations and cooperation with law enforcement activities, including prompt actions on advisories issued by CERT-In. • Use of secure product and services and skilled manpower. • Crisis management and emergency response. • Periodic training and upgradation of skills for personnel engaged in security related activities • Promotion of acceptable users' behavior in the interest of safe computing both within and outside	• Maintain a level of awareness necessary for self-protection. • Use legal software and update at regular intervals. • Beware of security pitfalls while on the net and adhere to security advisories as necessary. • Maintain reasonable and trust-worthy access control to prevent abuse of computer resources

Table : Actions At Different Levels

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

Chart 1: Stakeholders : Government Organisations



Thus the legal aspect is also getting refined with collaboration of different groups.

As of writing this article, final policy document has not been released; but the government, the industry, the academia and legal experts are converging, and it is expected to be available soon.

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

Conclusion

More and more nations are realizing that their national security, as well as economic prosperity, will depend on their ability to protect themselves in cyber space (which includes the internet, wider telecommunications networks and computer systems). The complex nature of cyber space requires a multi-faceted approach involving a close partnership between Government, industry and academia for ensuring the security of information systems and assets of the country. While the government, the industry, the academia and the law schools are working on the multi-dimensional aspect of capacity building, national and international cooperation, research and development, education and awareness, issues relating to privacy and freedom of expression - we come to the humble realization that cyber security is everyone's responsibility, every contribution is important, though it may seem like a drop in the ocean.[16]

16 **Recommended reading**
1. URL: http://en.wikipedia.org/wiki/Cyber_security_standards
2. URL: http://www.denyall.com/company/whitepaperrs_en.html?gclid=CMCElrGF3bYCFU8a6wodNm4A_Q
3. URL: https://www.prometric.com/en-us/clients/cybersecurity/Assets/default.html?cshp
4. URL: http://www.cybersecurityindex.org/
5. URL: https://www.eff.org/cybersecurity