THE CYBER CRIMES - MODERN THREAT FOR THE NATIONAL INFORMATION INFRASTRUCTURE

Mr.sc. Ahmet NUREDINI, **PhD Candidate**
European University of Tirana
ALBANIA

ABSTRACT

The National Information Infrastructure is the nationwide interconnection of communications networks, computers, databases and consumer electronics that make vast amounts of information available to users. The national information infrastructure also comprises the critical infrastructure, which is deemed critical because its incapacitation or destruction would have a debilitating impact on the national security, and the economic and social welfare of the nation. The history of information security begins with computer security. The need for computer security is the need to secure physical locations, hardware and software from threats. As global networks expand the interconnection of the world's information system, the smooth operation of communication and computing solutions becomes vital. However, recurring events such as cyber crimes illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems. The approach how criminals commit crimes has also changed. Digital general approach has opened new opportunities for criminal behavior. Computers and different networks can be used to attack victims or to prepare global violent acts such as terrorist particular among other. In absence of technology and trained personnel to deal with this new threat known as cyber crime, the security agencies are challenged by specialized cyber offenders which are known as hackers because apart from managing to break into state institution websites they are able to have unauthorized access to information classified as state secret and top-secret.
Due to the global nature of the security of information, the general action in preventing and combating threats from cyber crime, consists on building bridges of cooperation and coordinated action of all countries in order to set international standards in the field of defense the security of information systems. In this paper, among others I will present the definition of the cyber crimes, global aspects of the National Information Infrastructure, components of the security of information, cyber crime strategy and recommendations.

Keywords: Information, security, threat, computer, crime, cyber.

INTRODUCTION

Digital technologies and internet have transformed our everyday lives. We use them to access information, conduct business in our organizations, keep in touch with family and friends, and engage with state institutions. The internet offers huge potential for people. But with greater openness and dependency comes also potential risks. Our use of the internet has created new opportunities and motivation for cyber criminals. Organised criminal groups are increasingly using digital technologies to facilitate their criminal activities, to commit crimes, in this regard specifically cyber crimes.

In every state is very important the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.

Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. One of the threats are cybercrimes.

Advancements in modern technology have helped countries develop and expand their communication networks, enabling faster and easier networking and information exchange. Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide. Every day, 294 billion emails and 5 billion phone messages are exchanged. Most people around the world now depend on consistent access and accuracy of these communication channels.[1]

The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet-based networking, cyber crime and digital attack incidents have increased around the world.[2] These attacks classified as any crime that involves the use of a computer network — include financial scams, computer hacking, pornographic images from, virus attacks etc. The first major instance of cyber crime was reported in 2000, when a mass-mailed computer virus affected nearly 45 million computer users worldwide.[3]

THE DEFINITION OF THE CYBER CRIME

Today in global terms, we are facing with many challenges: terrorism, organized crime, drugs, human trafficking, migrant smuggling, corruption. One of the serious and danger crimes are cyber crimes.

Cyber crime is a clear and present danger that has turned into a silent global digital epidemic. Cyber crime encompasses a wide range of offences, including hacking of computers, data and systems, computer-related forgery and fraud such a phishing and harming, content offences via dissemination of pirated content. It has evolved from the mischievous one-upmanship of cyber vandals to a range of profit-making professional criminal enterprises in a remarkably short time. And there is a rapidly growing nexus between cyber crime and a variety of other threats, including industrial espionage, foreign intelligence services and terrorism.[4]

Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state or private property within another state including: intentional access, interception of data or damage to digital or digitally controlled infrastructure and production and distribution of devices which can be used to subvert domestic activity.[5]

Cyber attacks using malicious software have increased at an alarming rate in the last years. Most of the attacks are aimed at the financial sector and are hosted on financial sector computers. Cyber crime is on the rise: large-scale fraud attacks, consumer data breaches and politically-motivated Distributed Denial of Service attacks on financial institutions and others are costing these businesses billions of dollars every year. Much of this growth stems from

[1] The cost of cybercrime, Detica, February 2011.

[2] It is time for countries to start talking about arms control on the internet, Economist, July 1, 2010.

[3] Message Labs Intelligence: 2010 Annual Security Report, Symantec.

[4] Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security", 2015, pg.9.

[5] UN Security Council, Resolution 1113, 5 March, 2011.

the maturation of the criminal digital underground and its ‘’industrial’’ approach to cyber crime. Traditional fraud detection systems have focused on determining which online customer requests are atypical or unexpected. The industrialization of fraud requires banks to develop or enhance visibility to improve awareness of the criminal enterprise and its processes. This level of placing individual transactions or requests in a broader context is sometimes referred to as ‘’situational awareness.’’[6]

The traditional category of informatics crime included and cyber crime committed through misuse of information technology has and continues to endure changes, as a result of continuous transformation of technology. Terrorist organizations have greatly expanded their presence on the internet. In 1998 fewer than half of the thirty organizations designated as foreign terrorist organization by the U.S. Department of State even maintained web sites. By the end of 1999, nearly all terrorist groups had established a presence on the internet. By 2005, the US State Department's list of terrorist organizations had established presence on the internet. The exact numbers of websites supporting terrorism activity have diminished since then and may have dramatically increased.[7]

The UK Government has warned that the threat of cyber crime is more of a concern than nuclear war. That alarming statement - or scare tactics, call it what you will - came from a report released by the UK Home Affairs Select Committee, which claimed that the UK is losing the fight to protect people from cyber criminals, or "e-crime"."We are not winning the war on online criminal activity. We are being too complacent about these e-wars because the victims are hidden in cyberspace," said committee chair Keith Vaz in the report on e-crime, which arrived after a 10-month inquiry.[8]

On the evidence available, it is clear that the number, sophistication and impact of cybercrimes continues to grow and poses a serious and evolving threat to Australian individuals, businesses and governments. Although it is difficult to quantify the total costs, evidence from operational agencies suggests that economic costs of cybercrime in Australia are substantial. As many instances of cybercrime go unreported, it is difficult to give an accurate figure. However, non-government estimates put the cost of cybercrime in Australia as high as $2 billion annually.[9]

COMPONENTS OF THE SECURITY OF INFORMATION

A successful organization should have the following multiple layers of security in place to protect its operations: physical security, personnel security, operations security communications security, network security and information security. Physical security, to protect physical items, objects, or areas from unauthorized access and misuse. Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations. Operations security, to protect the details of a particular operation or series of activities. Communications security, to protect communications media, technology, and content.

[6] http://www.the 41st.com/sites/default/files/41st-Parameter-Cyber-Crime-Whitepaper.pdf, accessed date 09.04.2015.

[7] Denis Caleta, Paul Shemella, Intelligence and Combating Terrorism New Paradigm and Future Challenges, 2014.

[8]http://www.theinquirer.net/inquirer/news/2285740/cyber-crime-is-a-bigger-threat-than-nuclear-war-uk-government-warns, accessed date12.04.2015.

[9] National Plan to Combat Cybercrime, Australia/ Norton Cybercrime Report 2012.

Network security, to protect networking components, connections, and contents.
Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.[10]

An information system is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output and stored. Information system is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output, and stored. Each of these information system components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.[11]

The software component of the information system comprises applications, operating systems, and assorted command utilities. Software is perhaps the most difficult information system component to secure because software programs become an easy target of accidental or intentional attacks.

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information.

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. Systems developed in recent years are likely to make use of database implemented in ways that are less secure than traditional file systems.
The people can be the weakest link in an organization's information security program. In this regard process of security clearance is very important to higher the right people in organization. Education and training are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link.

Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information. The Information System component that created much of the need for increased computer and information security is networking. When information systems are connected to each other to form local area networks, and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge. The physical technology that enables network functions is becoming more and more accessible to organizations of every size.

[10] Michael E. Whitman, Herbert J. Mattord, "Principles of Information Secyrity"; Fourth edition, 2011, pg.8.
[11] Ibid, pg.16.

Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough. Steps to provide network.[12]

THE NATIONAL INFORMATION INFRASTRUCTURE

The term National Information Infrastructure had been popularized by Al Gore in the 1990s. This use of the term "cyber infrastructure" evolved from the same thinking that produced Presidential Decision Directive on Protecting America's Critical Infrastructures (PDD-63).[13] Presidential Decision Directive focuses on the security and vulnerability of the nation's "cyber-based information systems" as well as the critical infrastructures on which America's military strength and economic well-being depend, such as the electric power grid, transportation networks, potable water and wastewater infrastructures.

The term "cyber infrastructure" was used in a press briefing on PDD-63 on May 22, 1998[14] with Richard A. Clarke, then national coordinator for security, infrastructure protection, and counter-terrorism, and Jeffrey Hunker, who had just been named director of the critical infrastructure assurance office. Hunker stated:

> *"One of the key conclusions of the President's commission that laid the intellectual framework for the President's announcement today was that while we certainly have a history of some real attacks, some very serious, to our cyber-infrastructure, the real threat lay in the future. And we can't say whether that's tomorrow or years hence. But we've been very successful as a country and as an economy in wiring together our critical infrastructures. This is a development that's taken place really over the last 10 or 15 years — the Internet, most obviously, but electric power, transportation systems, our banking and financial systems."*[15]

The widespread integration has brought about three major information infrastructures. The first is the National Information Infrastructure, which is the key network element within a country that enables its information society to function and determines the efficiency of its functionality. The second is the Defense Information Infrastructure which serves a country's defense organization, both military and civilian, and the third is the global Information Infrastructure, which provides the international connectivity to the National Information Infrastructure. In defense terms, these infrastructures largely determine the functional efficiency of a country's warfare capability, and in both defense and broader national security terms, they provide a pathway to cyber war and information operations.[16]

The National Information Infrastructure is the nationwide interconnection of communications networks, computers, databases and consumer electronics that make vast amounts of information available to users It encompasses a wide range of equipment, including cameras,

[12]I Michael E. Whitman, Herbert J. Mattord, "Principles of Information Secyrity"; Fourth edition, 2011, pg.18.

[13] Presidential decision directive/nsc-63, 1998.

[14] Press briefing by Richard Clarke, national coordinator for security, infrastructure protection, and counter-terrorism; and Jeffrey Hunker, director of the critical infrastructure assurance office, 1998.

[15] Press briefing by Richard Clarke, national coordinator for security, infrastructure protection, and counter-terrorism; and Jeffrey Hunker, director of the critical infrastructure assurance office, 1998.

[16] Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security", 2015, pg.36.

scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, television, monitors, printers and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of National Information Infrastructure. [17]

A NATIONAL STRATEGY FOR CYBERSPACE

National security is a concept that a government, along, should take all necessary measures to protect the state and its citizens against all kind of national threats. One of the threats are the computer crimes. Measures taken to ensure national security include: using diplomacy to rally allies and isolate threats, marshalling economic power to facilitate or compel cooperation, ensuring the resilience and redundancy of critical infrastructure, using intelligence services to detect and defeat or avoid threats and espionage, and to protect classified information and using counterintelligence services or secret police to protect the nation from internal threats.

The best solution to be successful to fight the cyber crimes is the National Strategy to secure cyberspace. This National Strategy to Secure Cyberspace is part of our overall effort to protect the states. The National Strategy to Secure Cyberspace outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cyber security. The Strategy highlights the role of public private engagement.[18]

The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all. Therefore, the National Strategy to Secure Cyberspace helps reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them.[19]

The Cyber strategy builds on a systematic and structured combination of ends (goals and objectives), means (resources and capabilities) and ways (how the means are used to accomplish the ends), tempered with due analysis and considerations of the risk and costs. To develop a national strategy for cyberspace, therefore is to simultaneously create cyber resources and procedures that can contribute to the achievement of specific national security objectives.[20] The most important part of cyber strategy concerns the ends for which cyber capabilities might be used. These ends are part of the larger military, political, economic, diplomatic and national security objectives being sought. The key contribution of a national strategy for cyberspace will be to explicitly and clearly demonstrate how it makes possible the attainment of all the other strategies, most especially the National Strategy.[21]

[17] Dictionary of Military and Associated Terms, US Department of Defense, 2005.

[18] The National Strategy to Secure Cyber Space, USA, 2003.

[19] Ibid.

[20] Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security", 2015, pg.18.

[21] Ibid.

CONCLUSIONS / RECOMMENDATIONS

During my analysis and research in this paper, in order to increase the efficiency in combating cybercrime we have reached to the conclusions and recommendations which first of all might be able to serve others as a reference point for research and scientific studies. Therefore, bellow we will present the conclusions and recommendations:

- Securing cyberspace is an extraordinarily difficult strategic challenge that requires a Coordinated and focused effort from entire society—the entire international community.
- The cornerstone of cyberspace security strategy is and will remain a Public-private partnership.
- To increase the number of experts in the security organs and specialized units dealing with cybercrime.
- The lack of international cooperation between states in field of the security of information, remain the main challenges in fighting cybercrimes
- Advancement of inter-institutional cooperation between different structures of information technology for sensibilization of groups of interest and preventing the risk of their occurrence. The co-operation should be advanced not only within national security agencies but also with international security agencies.

BIBLIOGRAPHY

- Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security", 2015.
- Economic and Social Council, ECOSOC/64444, 37 th &38 th Meetings, Council briefed on Cybersecurity, July 2010.
- N. K. Katyal, Criminal Law in Cyberspace në University of Pennsylvania Law Review, vol. 149, 1003 2001, R. M. Couch, A Suggested Legislative Approach to the Problem of Computer Crime, 38 Washington and Lee Law Review, 1194, 1981;
- Michael E. Whitman, Herbert J. Mattord, “Principles of Information Secyrity”; Fourth edition, 2011.
- Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley Sons: first edition, 2000.
- Computer Crime & Intellectual Property Section (CCIPS) at U.S. Department of Justice, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001.
- Willis Ware. “Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security.” Rand Online. 10 October 1979.
- National Plan to Combat Cybercrime, Australia/ Norton Cybercrime Report 2012.
- Dictionary of Military and Associated Terms, US Department of Defense, 2005.
- UN Security Council, Resolution 1113.
- The National Strategy to Secure Cyber Space, USA, 2003.
- The cost of cybercrime, Detica, February 2011.
- Message Labs Intelligence: 2010 Annual Security Report, Symantec.