"Dimitrie Cantemir" Christian University
Knowledge Horizons - Economics
Volume 7, No. 2, pp. 115–118
P-ISSN: 2069-0932, E-ISSN: 2066-1061

www.orizonturi.ucdc.ro

CYBER TERRORISM THREATS TO CRITICAL INFRASTRUCTURES NATO'S ROLE IN CYBER DEFENSE

Constantin GEORGESCU[1], Monica TUDOR[2]

[1,2]Dimitrie Cantemir Christian University Department of Economics and International Affairs, Bucharest, Romania,
[1]E-mail: cgeorgescu93@yahoo.com, [2]E-mail: mkgeorgescu@gmail.com

Abstract *We live in a world that got hooked on Internet and computer use to ensure correct operation aa our countries of all critical infrastructure or systems that make up the social and economic life, and our safety in all areas, depends on the ability of information systems. From this belief originates planners and military analysts and intelligence that these systems will be the major target, or unique in some cases of attacks aimed at paralyzing large information structures, annihilating or destroying networks, databases and central servers.*

Keywords
Cyberterrorism, NATO, cyber-space, autonomous aircraft, critical infrastructure

1. Introduction

Over the past 20 years, information technology has developed greatly. From an administrative tool to optimize office processes, it is now a strategic instrument of industry, government or military. Before September 11, the risks and threats in cyberspace were discussed only small groups of technical experts. But since that day, it became clear that the cyber world entails serious vulnerabilities for various companies, which are increasingly interdependent.

Size cyber world, is a dimension of contemporary war, from the classic place on land, sea, air, space and now in addition cibernetic.Pe space facilities, the Internet has its vulnerable parts, which are run by criminals spies or simply people who want to do harm.

Cyber terrorism (cyberterrorism) is defined as the deliberate and politically motivated action by the attack on computer communication networks, computer software, computer systems and databases. These attacks can cause harm and thus violence against noncombatant targets. Such terrorist acts are declared illegal if produced by individual agents or affiliates in many national and sub national groups.

The term "cyber-terrorism" refers to the use of information warfare tactics and techniques by terrorist organizations, affecting cyber-space. Cyber-terrorism that operate exclusively in cyberspace and will not destroy dizic infrastructure that supports the existence of cyberspace. While cyber terrorists pursuing an impact on the actions of individuals "real" in the "real" world, they operate within the virtual world of cyber-space to manipulate these participants.

Cyber-terrorism objectives are: taking control of networks that regulate critical infrastructure such as water supply networks, air traffic, the energy, military networks, traffic signs system, financial systems, telecommunications etc.; taking control of industrial systems and energy; theft technology, business plans, projects and insider trading information or secrets.

We can talk about cyber terrorism when "terrorists" use of ICT tools to affect different targets. Examples:

• In 1994 hacker Merc (unidentified) took control of a company's network called Salt River Project can thus control the irrigation channels.

• 1997 airport control tower Worcester, Massachusetts was attacked by a hacker. The risk of air accidents and deaths were grown for 6 hours.

• Also in '97, in Sweden, a hacker blocked hotline (911) creating panic.

• In 2004 Sven Jaschan, a student of 18 years, has affected the computer network of Delta Air Lines and British coastguard causing damage of 500 million dollars.

• Terrorist 007 (Younis Tsouli) helped two other associates of al-Qaeda network help to plan terrorist attacks using the Internet. In 2005 he pleaded guilty and was sentenced to 16 years in prison.

Terrorism and cyber warfare are the two most important threats to humanity, and NATO and the European Union must take steps to create defense systems. The possibility of starting a cyber-war is analyzed with seriousness and professionalism, given that such a conflict would throw the world into chaos unimaginable.

Until today, 90% of attacks that could be considered legal, terrorist-informational, did not reach any legal discussion because "victims" have been thousands of miles of "attackers" positioned in different countries or continents and in most of them as "attackers" were working in the service of states.

The first reported cases of terrorism informational caused by terrorist groups "established" occurred in 1998 in Sri Lanka by "Tamil Tigers" in Serbia in 1999 by one of Serbian policeman who attacked NATO information systems, and of course in the conflict between Hamas and Israel-Hizbulah since 2006.

There are many cases that do not reach the press because of restrictive legislation on terrorism, for example, several attempts to derail fast trains in Japan (Shinkansen), which are fully computerized or in some cases criminal penetration of air traffic control networks.

For the first time in the history of aviation in 2013, a passenger plane without pilot flew over the UK. The experiment took place in April, and depending on the aircraft building industry, in a maximum period of five to twenty years, at the latest, free commercial planes will be manned airports.

The test flight is part of Astraea, worth £ 62 million and is funded by both the aviation industry and the UK Government, according to the Daily Mail. During flight, the aircraft is monitored by a satellite operator. It can control computers and aircraft flight controls can achieve. If the contact is lost, the plane is scheduled to land safely.

Supporters of "autonomous aircraft" said this during the industry to ensure all safety measures. They argue that most aviation accidents are caused by human error and eliminate human personnel should handle this situation.

While opponents' unmanned commercial aircraft deemed accidents could be more frequent due to computer errors, human errors only. However, they added that there is a greater risk that the planes would be diverted from cyber-terrorists, and the passengers will not agree to travel with such aircraft.

Software "Stuxnet" became public in June 2010, when something like a "digital penetration bomb armored targets' attack Iranian nuclear program. By this early warnings sent by experts since 2001 have become reality, suggesting that the cyber dimension might be used sooner or later to execute attacks will have serious consequences in the real world lethal.

Stuxnet showed the potential risk of malicious software affecting the computer systems of crucial importance in the management of supply.

During the crisis generated by Kosovo, NATO faced its first serious incidents caused by cyber-attacks. This has led, among others, NATO e-mail account is blocked for several days for external visitors and the operation Alliance website to be interrupted repeatedly.

In a manner typical of the period, it was felt, however, that the cyber dimension of the conflict has done nothing to limit actions under NATO information campaign. Cyber-attacks were seen as a risk, but as one limited in scope and potentially destructive, requiring only limited technical responses accompanied by efforts to inform the public on a small scale.

In 2010, in Lisbon, was established Strategic Concept that qualifies as cyber threats directly targeting vital national security infrastructure, which can reach levels likely to endanger "prosperity, security and national stability and Euro-Atlantic". This concept has also emphasized the need for accelerated efforts in cyber defense and mandated the North Atlantic Council to develop a new policy of NATO cyber defense, which was adopted June 8, 2011 and an action plan. Summit in Chicago in 2012, reaffirmed this policy by creating the department responsible for protecting against cyber-attacks nCircle NATO (NATO Computer Incident Response Capability). In Chicago in 2012 on the idea to bring all NATO networks under centralized protection and implementation of critical elements of full operational capability nCircle, finally, creating the NATO Communications and Information Agency (NCIA).

The report "Origin of Hacks" hacking attempts identified 981 million worldwide in the third quarter of 2012, up 23 million from the number identified in the second quarter, the top four countries in the top origins of the US attacks, Russia China and Ukraine or that the SPAM messages are between 80 and 98% of all messages in circulation - they spread a multitude of viruses and malicious software.

In Moldova, according to statistics by the Centre for Cyber Security, only the period 17 May to 21 November 2012, the total electronic messages addressed to central public administration authorities about 986,500 messages were legitimate, while more than ca. 8.5 million were SPAM, which contained 874 viruses detected. A massive wave of cyber-attacks three weeks showed last year that NATO countries heavily dependent on electronic communications were extremely vulnerable on the cyber front.

During Georgia-Russia conflict occurred massive attacks against government websites and servers in Georgia, offering cyber war period more shape. These actions have not produced, in fact, no physical damage. However, they have weakened the Georgian government during a crucial phase of the conflict. They also had an impact on its ability to communicate with a national and global public opinion very shocked.

It was observed clear that Russia started the war in Georgia cyber some items that were used in the Crimea which shows that site will be cyberattack battlefield of

the future, while Russia is the second state as potential behind the US in this field. The complexity of this type of war makes it very dangerous for anyone, including Romania opponents can attack by our own computer systems that manage electric grid, transportation system, and water and nutrition financial institutions.

SRI Director George Maior said in 2013 only 14% of requirements, from the perspective of the threats, are covered by the budget in 2014, he was mentioning also that attacks the previous years, to address some important ministries of Romania. SRI is the authority on terrorism and in terms of counterintelligence and counter-phenomenon. The attacks came from abroad but it is difficult to prove whether they came from state entities.

Regarding the vulnerability of Romania in front of a terrorist threat, George Maior said that "every state is vulnerable, no matter how powerful." Romania has signed a protocol agreement with the NSA and or to let NSA wiretaps operate on the national territory or to receive data from our own massive interceptions.

The last major cyber-attack was reported in 2013 and covered several government organizations in Europe, including Romania and could be initiated by a State. The statement was SRI spokesman Sorin Sava.

The higher technological level, software attacks signaled the end of February, has a greater impact than "Red October". So powerful that could affect national security of Romania. The attack, which was manifested by malware applications, targeted several government organizations in Europe, including Romania, in order to spy and gather information geopolitical confidential.

Even worse is that behind this attack could find no mere hackers. A cyber-attack of this complexity requires extremely expensive engagement resources worth million, money that not everyone has them available. That led to believe that SRI behind the attack could find a state that could best to beat such amounts.

According to estimates SRI attack could affect Romania's national security compromised entities profile. For this reason, SRI by specialized teams to react to cyber-attacks, took steps to identify all organizations that have been targeted Romanian hackers. Currently, in Romania the system well prepared to meet the threats, the financial and banking system. An example of Cyber Terrorism that our country is not proud was when a group of Romania had access to compute systems that controlled life from a research station in Antarctica, risking the lives of 58 scientists involved. Luckily, the culprits were stopped before irreparable damage occurs.

Cyberterrorism type attacks are mostly non-political sabotage is causing financial damage, as if disgruntled employee who released an amount of untreated wastewater in Maroochy Shire, Australia. Computer viruses have degraded or closed in other cases some non-essential systems in nuclear power plants, but this is not believed to have been a deliberate attack.

Cyber security is a sensitive topic in the relationship between China and the US and was one of the main topics on the agenda of meetings between presidents Barack Obama and Xi Jinping.

China has said it is deeply concerned Snowden's claims (accused of spying computer) according to which the United States illegally entered many internet networks in Hong Kong and China, including Tsinghua University, which houses one of the main centers of the internet country, and Chinese mobile networks. Beijing has said he discussed the matter with Washington.

Because cyber weapons are much cheaper than traditional weapons, terrorists and criminals migrate to this type of attack at a rapid trend alarming. Watching events of recent years, we can say that it is possible that cybersecurity to become the second largest concern at Overall, after classical terrorist actions involving a large number of human factors in achieving them.

For this new type of terrorist strikes using a very small number of members with specific training for three categories of "cyber warriors": a hacker (who is often specialized information systems entering computers or remote) a cracker (specialist in breaking security systems and codes of progression of the program) and a phreacker (specialist in telecommunications fraud).

Cyber security threats have become more serious in recent years. They are not limited by borders and an increase in frequency and sophistication. Membership universal cyber space, security risks involved cybernetic attacks and the global nature of the effects, impugn international cooperative efforts to ensure the security of information systems.

As a defense alliance, NATO has identified and recognized early in the last decade, cyber menace seriousness and importance of protecting networks.

Cyber defense appeared on the agenda of NATO Summit in Prague in 2012, and was later confirmed as a priority at the Summit in Riga in 2006. A policy in this area has been agreed for the first time, the Heads of State and Government at the Bucharest Summit in April 2008.

The rapid development of sophisticated attacks and character placement basis in center led NATO security agenda, documents Lisbon Summit (Strategic Concept and Summit Declaration) 2010 confirming this.

New Strategic Concept describes the threats directly targeting cyber security as vital national infrastructure, which can reach levels likely to endanger "prosperity, security and national stability and Euro-Atlantic". Consequently, this type of challenges impugn

the development of the Alliance's ability to prevent, detect and defend against their recovery after their occurrence and coordinating national cyber defense capabilities.

While NATO Strategic Concept art sets strategy for the next decade Summit Declaration provides in-depth review of the current political allies regarding its adoption a security environment dynamics.

Following the tasks set by the Lisbon Summit, NATO has developed a cyber-policy and action plan reflects the main changes and demands urgent matter. NATO defined in these documents, objectives, identified structures and allied organizations that will be involved in the defense of allied and mechanisms for coordinated action.

NATO provides a platform for coordination and consultation regarding cyber threat assessment and identifies solutions at both ally and in cooperation with the partner format. Starting from the global nature of Cyber State, cooperation with partners, government organizations and the private sector is an issue of critical importance to defense field.

In the process of maintaining and developing an effective approach on national security, Romania stability guidelines for cyber security in order to protect their own communications systems and information transfer and to reduce at the same time risks to the Alliance, through the implementation of specific tasks arising from the implementation of NATO policy in cyber.

2. Conclusions

The conclusion is that even today, a great challenge is the terrorist propaganda through thousands of existing websites, which are "educated" staff recruited or contact subversive current or aspiring members of these organizations.

Cyber Terrorism can have many consequences, such as the weakening economy of a country or more can have a serious impact on a large number of people. It can also affect businesses on the Internet. Thus, merchants and service providers that produce revenue through websites (via advertising, providing services) may lose money in the event of failure or downtime of the site following the intervention of cyber criminals.

The problem is primarily true fragility of the Internet architecture. The initial structure of the Internet "unregulated open-architecture" has been used for these elements to penetrate the great importance of servers and user countries to circumvent, modify and sabotage strategic database. The only possible defense existence today is the separation of these Internet networks, which would prejudice would increase the level of connectivity and IT costs at all levels.

References

1. Andrew M. Colarik - Political and Economic Implications, Idea Group Pub, Hershey Pennsylvania in 2006

2. James F. Dunnigan - The new global threat: cyber-terrorism, Financial Week Curtea Veche Publishing House, Bucharest 2010

3. Shakarian, Paulo - The 2008 Russian Cyber Campaign against Georgia, Military Review, Vol. 91, No. 6, November-December 2011

4.http://www.business24.ro/articole/terorism+cibernetic

5.http://jurnalul.ro/stiri/politica/mircea-dusa-terorism-cibernetic-650183.html

6.http://www.ziare.com/articole/terorism+cibernetic

7.http://www.hit.ro/articole/terorism+cibernetic/hāCH