Cyber-attacks and attack protection

Petr HRUZA
Department of Military Management and Tactics, University of Defence
Brno, 662 10, Czech Republic

and

Radovan SOUSEK
Jan Perner Transport Faculty, University of Pardubice
Pardubice, 53333, Czech Republic

and

Stanislav SZABO
Faculty of Transport science, Czech Technical University in Prague
Prague, 128 00, Czech Republic

ABSTRACT

Dependence on cyber space is not a frequent topic of discussion; the reason might be that people fear possible abuse of cyber space or they just do not understand the center of the problem. Cyber space is used more and more – which increases the dependence. The dependence can be abused in case of a terrorist or cyber-attack. Now, this is the space where future wars can take place. Together with the increase of using the IT we can mark an increased risk of misusing these technologies. Attacks aimed against the IT assets and networks are becoming a worldwide phenomenon and their impact result to extensive economic damage throughout both public as well we private sectors. What is the cyber-attack and what are anticipated targets of such attacks? How we can protect the cyber-space? Answers to all these questions are subject elaborated in our article.

Keywords: Cyber Attack, Cyber Security, Scenario and Target of Cyber Attack, Warfare, Cyberspace.

1. INTRODUCTION

Nowadays, more than ever before, we have to consider the slogan "information is worth of gold", no organization exist that does not pose some important information (no matter if commercial entity or state administration). Remarkable increase of utilization of both IT assets and software in current world leads, on one hand, to establishing the information community, acceleration of communication and extensive development of services. However, the dependency of the community on IT grows up because of this as well. With this growing dependency on IT a risk of misusing these technologies also increases, what can result to considerable damages.

A general trend in this area worldwide is to develop a quality protection of the IT systems against the attack that could result to their malfunctions. Attacks targeted against IT installations are a worldwide phenomenon and their impact result to extensive economic damages in both public and private sectors, in the national as well as global scale. In the case when the attack is aimed against the elements of critical infrastructure the security even the very existence of a particular country might be endangered.

Attacks against IT are gradually becoming more sophisticated and more complex. Assuring the cyber security in the individual countries is one of the key challenges of contemporary era. The infinity and ubiquity of cyber threats require the extensive international co-operation but also common effort when assuring the cyber security of the individual countries. The area of cyber security has been and will be one from decisive aspects of the security environment in advanced countries. Growing part of the economic activities is being shifted to the area of internet – the cyberspace. By establishing the social networks the most known cyberspace – the internet – becomes a substantial societal phenomenon, by what the community can be influenced significantly both positive as well as negative way.

Robert Mueller, the FBI Director (September 4, 2001 – September 4, 2013), stated at the conference on security in San Francisco in the spring 2012 the following: „*We are losing data, money, ideas and innovations. Together we have to find the way how to stop it… I am convinced that only two kinds of companies exist in this respect: those the hackers have already attacked and other that will be attacked. And these two groups are merging together very fast. I am worried that in a near future only such companies will exist whose systems have been attacked by hackers already and others whose systems will be attacked by hackers again.*"

When talking about cyber warfare we have to think hard and decide if we talk about a virtual battlefield within the Internet or about a real physical battlefield. Recently the cyber space has been militarized. Does that mean that developed countries are afraid of cyber warfare? Cyber warfare would happen without soldiers, weapons, tanks or rockets. Instead, attacks would be conducted by groups of computer warriors (or hackers). Is cyber warfare a real threat? Can cyber warfare paralyze the world or just a particular country? In these days nobody can imagine cyber warfare of a world scale. Probably it would be a world war of unforeseeable consequences. The risk of cyber warfare is and will be one of the most important topics in the field of information security in the following years.

2. CYBER-ATTACKS

A cyber-attack takes place in cyberspace. Cyberspace can be understood as a metaphor describing virtual (non-physical) environment created by interconnecting computer systems in the network. In cyberspace there is the same interaction between subjects as there is in the real world – but without necessity of physical activity. Information is shared either in a real time or it can be delayed, people can buy things, share experience, search contents, conduct research, work, or play. [6]

A cyber-attack is an activity carried out by an attacker, aim of whom is to get, modify, or destroy data (information, influence in a negative way or take over the control of some elements of cyberspace infrastructure). Cyber-attacks happen more and more frequently and are better organized. Dealing with their consequences is more and more expensive. This damage can reach a level that can endanger prosperity, security and stability of a country or an organization (possibly an individual). The fundamentals of cyber system security are supervision of cyberspace system infrastructure elements, security incidents management, regular audits, cyberspace systems vulnerability assessment, or carrying out penetration tests. [7]

Cyber-attack affects key features of a technology. This can endanger lives of people, or seriously endanger a process of production, technology, or services. That is why a cyber-attack can be defined as an attack on the structure of information technologies. The aim of such attack is either damaging or gaining sensitive or strategically important information. It is very often connected with politically or militarily motivated attacks. [8]

In these days organized crime in cyberspace provides more profit but lowers the risk for a hacker to be traced and tried. Ministries and government agencies all over the world face hundreds or thousands of attacks every day. Their security is threatened by hackers sponsored by money coming from foreign countries and organizations. They also focus on international companies which very often are not, in case of a cyber-attack, willing to cooperate with the police or FBI. The reason is they are afraid of long and demanding investigation. [4]

An effort to limit the attacked subject's activities (making their web sites unavailable, so called "hacktivism") or political activism (changing information, disinformation, scaremongering) which is connected with, so called, "perception management" (influencing public opinion using manipulative information chosen for target subjects) can be found among the cyber-attacks targets. These targets are different from common targets of hackers, crackers, or electronic sprayers who usually attack web sites in order to demonstrate their abilities. In cyber warfare we talk about coordinated activities purposely targeting other countries or a group of people.

Probably the most famous cyber-attacks are the ones on SCADA systems using the Stuxnet worm. The most famous published attack delayed start-up of Iranian Bushehr nuclear plant. The attack was focused on uranium enrichment factory in Natanz where fuel for this power plant was being prepared. The Stuxnet worm spread all over the world; apart from sixty thousand cases in Iran we know about a million cases in China. [5]

3. CYBER-ATTACK SCENARIO

If we start to talk about the cyber-attack targets, most people think that they are not concerned by it, rather, that it is a government administration issue, respectively, an issue for institutions involved in the national defence or national security. Such way of thinking, however, pose a serious security risk in the area of the cyber threats.

Cyber-attack, in general, has to be hidden, or kept under cover until the last moment at least. The real target must not become apparent until the sufficient conditions to attack it effectively are not created. Here we can obviously see a parallel to common military tactics, and a hacker, even he/she is to conduct the attack by other weapons, is the same fighter as the soldiers in the field in this sense. Fighting principles are then similar to those of conventional war. Therefore, for future conflicts we have to be prepared to situations like beyond the classical war conflict we will also have to face the attacks against critical communication and information elements of a given country. As an example we can name the attacks of the Anonymous hackers group that attacked hundreds of the Chinese official websites early in April 2012. They achieved to change contents of these sites. Hackers attacked them as a protest against the censorship of internet enforced by Beijing officials.

Within the cyber combat we will encounter attacks aimed to e-government, i.e. against applications linking the government ministries with the population of a given country. These attacks will be masked and will come via home PCs of common private users in a particular country attacked. It is expected that all the applications of ministries will be attacked and put inoperative; also penetration to the steering information systems of ministries will also occur. Other group of professional hackers is to conduct attacks using tactic of parallel attack aimed to all banks in the country, including the national bank. This will result to the total collapse of trading and blocking the nationwide banking systems; another stage is expected to encompass the continuing extensive cyber-attack against crucial ministries and medical care systems aimed to the effort to eliminate their information systems completely (police database systems, tactical and information systems, medical care, etc.). Partial elimination of the information role of the state cyberspace is also expected to occur as well as the energy sources shutdowns (e.g. by imitation of nuclear power station accident, remote takeover of administration, etc.). Disruption the integrated rescue system will result to general panic together with elimination of the general mass media.

Another task of cyber warriors is anticipated to be to inflict the last crushing attack to the national communication system (mobile phone operators, internet services providers, etc.) and against the crucial points of the existing networks. This will result to interruption of communication, security and support role of the national administration cyberspace. Possible variant of the cyber-attack will be just the simple disruption of the national monetary and financial system together with disinformation campaign.

4. CYBER WARFARE

When we start talking about cyber warfare targets, most people assume this has nothing to do with them. They believe this is their government's issue, or better said, an issue for an institution related to a country's defense or security. However, this way of thinking can be very risky under the terms of cyber threats.

Cyber warfare can be perceived as an effort of a country to penetrate into computers or computer network of another country in order to damage or violate its integrity. Cyber security glossary defines cyber warfare as "*Use of computers and the Internet to wage a war in cyberspace. System of extensive, often politically motivated, related and mutually provoked organized cyber-attack and counterattacks*". [2, p.58]

Cyber warfare can be perceived as a use of computers and information technologies to carry out acts of war at governments and large organizations levels. Cyber warfare starter can be an individual, organization, or a state institution. There are a lot of different kinds of cyber warfare – from specialized hacker attacks to generally aimed attacks aim of which is to eliminate a particular service or paralyze critical infrastructure of the attacked country. An attack that completely cuts off the connection to the Internet is the highest level of cyber warfare.

Today's cyber-attacks are primarily carried out in order to achieve information concerning diplomatic, economic, and military programs. Paralyzing critical infrastructure of a particular state can represent a secondary target. Naturally, a cyber-attack must be hidden all the time, or, at least, until the last moment. The real target must not be revealed until sufficient forefront allowing an efficient impact is created. Parallel with common war tactics can be seen here. Although hackers use different weapons, in this sense they are the same warriors as common soldiers in the field. The principles of a combat are similar to a classical conventional war. That is why in future conflicts we can expect that beside a standard war conflict there will also happen attacks on significant communication and information points of a given country. [8]

5. CYBERSPACE PROTECTION TASKS

To provide the cyber security and to assure the respective rights for information self-determination via access to working services of the information community, it is necessary to process the information on the occurrence of the cyber security issues from as big number of resources as possible. For the same reason it is necessary to coordinate the protective measures. Services of the information community are characterized by their networking capabilities and even a very small element of the network can influence remarkably its elements, no matter if being close or on the geographical distance.

According to Veselý [7] these are the following tasks:

- Coordination of countermeasures for IT security incidents in the critical infrastructure.
- Gathering the information on serious security incidents.
- Coordination of filling the security gaps in the critical computer systems.
- National critical infrastructure must not be internet-dependant fully, but has to be capable of operation in case when a cyber security crisis occurs.
- Have an emergency plan of actions to be taken in case of becoming a victim of a cyber-attack.
- Resolutions of information-security incidents in cooperation with owners and operators of impacted parts, telecommunication operators, internet services providers and government administration components.
- Generation and distribution of skills on selected areas of information and cyber security among public.
- Generation of capabilities to defend against cyber-attacks.
- Achieving international consensus on the standards of behaviour in the cyberspace.
- Reduction of vulnerability of government systems and critical infrastructure elements.
- Cooperation with foreign organizations and presentation of the Czech Republic in the field of information security at international level.
- Support of education of professionals in the area of the cyber security.
- Increasing the enforceability of law in the area of cyber security.
- Improving prevention and build-up of general awareness.
- Improving the awareness in private sector.
- Generate the administration professionals in the area of IT security systems.
- Understanding the tactics of attackers, their techniques and procedures enabling conversion the protective measures to suitable forms.
- Be ready to prevent the attack or to respond as fast as possible in case of being compromised.
- Prioritize the prevention, but maintain focus also to detection and suitable response to attack.
- Keep assured that the suppliers in the area of critical infrastructures are not compromised and pose sufficient backup measures in case if their systems are disrupted.

The US Congress House of Representatives approved an Act on cyber security in April 2012 that enables the government and private sectors to cooperate when resolving the protection against hackers. By this new Act the US security components are empowered to share the confidential information on internet threats to private companies that can then better protect their networks against the attacks of hackers. This cooperation should work vice versa as well, what causes worries of those who struggle for protection of personal data. They anticipate that the security components will be enabled to gather large volumes of sensitive date on non-government entities what is otherwise restricted by the US law.

6. POSSIBLE CYBER WARS OF THE FUTURE

Possible cyber wars of the future are the reason for all of us to feel discomposed. In spite of traditional warfare, which requires a huge amount of sources (weapons, personnel, equipment), cyber warfare just needs somebody with the right knowledge, computer technology; somebody who wants to cause confusion. The enemy can be anywhere; even outside the nation or an organization. A strong attack can be carried out just by a group of hackers using standard computers.

Another horrifying aspect of cyber warfare is that a cyber-attack can come as a part of a coordinated attack, or it can be just a sick idea of a wicked hacker who just wants to have a good time. Regardless what the attacker's motive is, cyber-attacks can cause huge financial losses. Many countries are desperately unprepared to face these unexpected cyber-attacks.

First of all it is necessary to realize the aspects of cyber warfare and their comparison with traditional aspects (conventional warfare, diplomacy, etc.). This kind of warfare can be more acceptable for public than the use of conventional warfare means. Although it is possible to avoid losing lives and damaging property by the use of cyber warfare, yet there is still risk of indirect danger. On the border between state and private sectors, there is a critical infrastructure. Here we talk about distributive water conduit, electric energy, air traffic control and other systems that are crucial for all countries. It is just the attack on critical infrastructure that can lead to paralyzing the network used by health service, water management and other vitally important elements of the country. During a conflict the enemy can make use of our dependence on cyber space and get a strategic advantage. It is supposed that cyber warfare will precede conventional warfare. That is why it is necessary to define critical communication and information structures in order to set priorities for cyber defense of the country. [9]

7. CALCULATING THE PROPORTION OF FORCES AND MEANS IN CYBER WARFARE

Calculating the proportion of forces and means in cyber warfare Various tactical calculations can be a part of combat planning. On of such calculations is proportion of forces and means. Proportion of forces and means is processed as an auxiliary document especially in decisive phases of task (combat task) accomplishment. Proportion of forces and means can be processed in quantitative or qualitative ways. When talking about quantitative proportion of forces and means the processors quote number of deployed (anticipated) enemy and own forces and means divided into required categories. When talking about qualitative proportion of forces and means quality of deployed forces and means is taken into consideration. The quality is included into final proportion of forces and means in a given category via so called "combat potential". The fact is that considered enemy forces and means (as for especially quantity but also quality) are stochastically assessed. When expressed mathematically, we talk about a sum of qualitative and quantitative data concerning forces and means of both belligerents, which, when compared, can provide us with a concept of combat possibilities of both belligerents and of a possible combat result.

Looking for a mathematical formula that would be able to calculate proportion of forces and means in the field of cyber warfare has become a new trend in the last few months. How can proportion of forces and means of cyber armies involved in a cyber war conflict be calculated? Is it realistic to carry out this calculation at all? In fact, it is nearly impossible. In case of a cyber space war it is not quantity that counts but quality. A hundred trained soldiers from special cyber units can fail facing one gifted adversary. We can talk about numerical superiority; however, it does not have to be crucial in cyber spaces. Is a hundred or a thousand specially trained soldiers too many or not enough? [9]

I think that cyber military units can be compared using following three criteria:

- Ability to carry out an attack in cyber space (offensive potential).
- Ability to avert an attack (defensive potential).
- Dependence on cyber environment (dependence).

Ability to restore key systems, existence of spare or back-up systems, emergency plans, etc. can be considered to be other aspects to be used for more detailed comparison. In case of cyber warfare we rather talk about potential possibilities of proportion of cyber forces calculation because concrete information is not available. The reason is that any statement made by a future attacker can inform the adversary about his possible potential weaknesses and can provoke trial actions or can lead to losing public confidence. A future attacker issuing a declaration concerning his own network perfect security can provoke trial action carried out by both potential attackers and random nongovernmental people (e.g. hackers) aim of whom is to discover possible weaknesses. [9]

8. CONCLUSIONS

Cyber-attacks will soon become a bigger threat than terrorism. Both public and private sectors are trying hard to protect their critical information and communication infrastructures from one of the biggest threats of the 21st century – cyber-attacks. The main task of a national cyber defence is to protect national communication and information infrastructure and systems from cyber-attacks.

With the emergence of targeted attacks and advanced persistent threats, it is clear that a new approach to cyber security is required. Traditional techniques are simply no longer adequate to secure data against cyber-attacks. Advanced persistent threats and targeted attacks have proven their ability to penetrate standard security defenses and remain undetected for months while siphoning valuable data or carrying out destructive actions. It is obvious that even the most secure computer networks are susceptible to attack.

Cyber-criminals, as well as the advertising agencies are currently very capable to utilise the current trends and events. They know what is currently "in" and misuse this information to internet frauds. Very often they utilize the method of social engineering, a current phenomenon among the computer threats.

Finding a mathematical formula to calculate proportion of forces and means in the field of cyber warfare has become a new trend in all armies.

9. REFERENCES

[1] Richard A. CLARKE, Robert K. KNAKE. **Cyber War - The Next Threat to National Security and What to Do about It**. USA: Ecco Press, 2010, 290 s. ISBN 9780061962233

[2] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. **Cyber Security Glossary**. The second updated edition. Prague: The Police Academy of the Czech Republic in Prague, 2013, 200 s. ISBN 978-80-7251-397-0. [in Czech].

[3] **Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk**. The New York Times, USA, 2009. [online] [2014-01-28].

<http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?ref=cyberwar&_r=0l>.

[4] **Jak by mohl vypadat kybernetický útok na ČR**. [online] [2014-01-30]. <http://tm.m.idnes.cz/blog/clanek.248339.idn>. [in Czech].

[5] **Kybernetické útoky**. [online] [2014-02-10]. <http://www.ceskatelevize.cz/porady/10121359557-port/739-kyberneticke-utoky/>.[in Czech].

[6] McQUADE III., Samuel. **Encyclopedia of Cybercrime**. Westport: Greenwood. 2008.

[7] VESELÝ, Josef. **Cyber attacks**. In Cyber attacks to information systems. Prague: The Police Academy of the Czech Republic in Prague, 2012. ISBN 978-80-7251-371-0. [in Czech].

[8] HRŮZA, Petr. **Cyber Security**. The first edition. Brno: University of Defence. 2012, 90 p. ISBN 978-8-7231-914-5. [in Czech].

[9] HRŮZA, Petr. **Cyber Security II**. The first edition. Brno: University of Defence. 2013, 100 p. ISBN 978-80-7231-931-2. [in Czech].

[10] NĚMEC, V., VITTEK, P., KRULA, L. **Security management tools and UML standard at international airport**; In: 9th international scientific conference - New trends in aviation development; Gerlachov, Slovak Republic, 2010, ISBN 978–80–553 0475–5.

[11] NĚMEC, V. **Examinations of aircraft staff in Czech Republic**, New development trends in aeronautics, Košice, Slovak Republic, ISBN 80-8073-520-4

[12] KRAUS, J. - NEMEC, V., FAJČIK, P.: **The Use of Wireless Sensor Network for Increasing Airport Safety**; In: MAD – magazin of Aviation Development, Volume: 1, Issue: 5, September 2013, s.: 16-19; ISSN 1805-7578

[12] FUCHS, P., SOUSEK R., et all.: Dopravní infrastruktura jako prvek kritické infrastruktury státu, Košice 2011, ISBN 978-80-8928256-2