DE GRUYTER OPEN
International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXIII No 1 2017

CYBERWARFARE

Petr HRUZA, Jiri CERNY

University of Defence, Brno, The Czech Republic
petr.hruza@unob.cz, jiri.cerny@unob.cz

Abstract: *The internet has to be considered a very dangerous battlefield. Nobody is secure. It is a paradox that those countries which do not feel vulnerable may be the most threatened by cyber war. This applies primarily to western powers and fast developing countries. Cyberattack may easily be ordered through the internet. Such an attack is cheaper than an attack by conventional weapons and at the same time it causes bigger economic losses. It is obvious from the military standpoint that cyberattacks and defence against them have to be an indispensable part of military activities. The reason is that the military consider the internet and virtual space to be the fifth area of employment of their forces, besides land, air, water and space. It is stated in the hypotheses that cyber activities will be an inseparable part of future military operations. The key objective will be to achieve information supremacy or information dominance on the battlefield. Thus developed countries develop and introduce new cyber weapons with the aim of striking the enemy´s command and control structures, its logistics, transport, early warning systems and other vitally important military functions at any time upon receiving an order.*

Keywords: Cyberwarfare, NATO, Cyberattacks, Cyberspace

1. Introduction

Cyberwarfare is a hot topic. Armed forces, intelligence, and law enforcement agencies have made computer security a top priority for investment and recruitment. In fact, current efforts to take the higher ground in cyberspace are so intense that many governments will overreach, with unfortunate ramifications for democracy and human rights around the world.

Cyberwarfare involves the use and targeting of computers and networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyberattacks, espionage and sabotage. There has been controversy over whether such operations can duly be called "war". **Cyberwarfare** has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"[1], but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations. [2]

Some governments have made it an integral part of their overall military strategy, with some having invested heavily in cyberwarfare capability. [3] Cyberwarfare is essentially a formalized version of penetration testing in which a government entity has established it as a warfighting capability. [4]

This capability uses the same set of penetration testing methodologies but applies them in a strategic way to:

- Prevent cyberattacks against critical infrastructure;
- Reduce national vulnerability to cyberattacks;
- Minimize damage and recovery time from cyberattacks [4]

Offensive operations are also part of these national level strategies for officially declared wars as well as undeclared

DOI: 10.1515/kbo-2017-0024

secretive operations. [5]
Despite these factors, there are still many sceptics over cyber war, and more questions than answers. Although malicious code has served criminals and spies very well, can cyberattacks offer soldiers more than a temporary, tactical edge on the battlefield? Can it have a strategic effect?

2. NATO Standpoint on Cyberspace

NATO countries legal standpoint on cyberspace is quite clear. NATO countries, including the Czech Republic, acknowledged within the NATO cyber defence policy, that international law, including the international humanitarian law, may be applied in cyberspace. This standpoint was acknowledged by the Allies also in the NATO Wales Summit Declaration (4-5 Sept. 2014).
Cyberspace is recognized as another sphere for the conduct of combat. Its importance is on the increase as it is the space in which attacks may be aimed at military, industrial and political cyber espionage, damage of state critical infrastructure, own enrichment, collection of information otherwise inaccessible, intentional dissemination of disinformation within the conduct of information operations in cyberspace (Warsaw Summit, 8–9 July 2016).
All NATO armies activities are increasingly dependent on the elements of civil critical information infrastructure. Mainly in the initial phases of conflicts cyberattacks will target information systems, communication systems and the systems of critical infrastructure (e.g. power industry, finance, transport, telecommunication, health system …). These systems will be targeted with the aim to disrupt command and control system, reduce conventional military capability and combat readiness of a state.
It is obvious from the military standpoint that cyberattacks and defence against them have to be inseparable parts of armed operations. It is stated in the hypotheses that cyber activities will be an inseparable part of future military operations. The key objective will be to achieve information supremacy or information dominance on the battlefield. Thus developed countries develop and introduce new cyber weapons with the aim of striking the enemy´s command and control structures, its logistics, transport, early warning systems and other vitally important military functions at any time upon receiving an order. [7]
For cyber operations, the Army will need to build trust and operate with NATO partners. The Army must be able to employ cyber capabilities at all echelons, including tactical echelons. The Army must be able to operate with existing authorities and be prepared to operate with increased authorities it might gain in the future.

3. Targets of Cyberattacks

Most people believe that the targets of cyberattacks do not concern them. They believe that it is a problem of a state, or the institutions having relations to the state defence and security. Such a way of thinking is a serious risk in the area of cyber threats.
Cyberattack has to be concealed, or at least kept in secret till the very last moment. The real target must not be revealed before sufficient preconditions are created for its efficient strike. There is obviously an analogy with a common combat tactics and although hackers attack with other weapons, they are the same combatants as soldiers in the field. The combat principles are similar to those of a typical conventional war. Therefore, we have to be prepared that typical future war conflicts will be accompanied by attacks against important communication and information nodes of a state. [8]
Each computer network is as secure as its weakest part. Computer connection into the computer network represents the biggest risk. The risk of a developed information society is in its dependence on information and communication systems. A state, the governance of which has a high degree of

informatization, is much more vulnerable than a state with a low degree of informatization. Thus, the cybewar is a real phenomenon for such developed states. It is conducted in close proximity and anybody of us may be its participant, as well as its victim. On the one hand, modern technologies make our lives easier, but on the other hand there is an increased risk they will be abused. It is significantly easier to paralyze modern states on the level of digital processing and exchange of information. Thus, the most developed states and their modern armies cannot ignore their cyber security. [8]

Cyberattack is usually carried out on the technology control elements which may seriously threaten people´s lives, production, technology, or service. Cyberattack may thus be defined as an attack against the infrastructure of information technologies with the aim to cause damage or get sensitive or strategically important information. It is most often connected with politically and military motivated attacks. Cyberattacks will soon become a bigger threat than terrorism. [9]

4. Cyberwarfare Methods

The increasing number of internet users resulted in the fact that propaganda is spread more efficiently in cyber space than e.g. through leaflets airdropping. The spreading of malware is easier, more available and faster with the increasing number of users. Therefore the threats of cyber attacks are also more likely.

There are various methods of cyber attacks in cyber space ranging from the moderate to the merciless ones, such as follows: [10]

- **Vandalism**: common attacks on government web sites. Such attacks are usually fast and do not cause serious damage;
- **Propaganda**: dissemination of political news mainly through internet;
- **Collection of data**: collection of classified information which is not sufficiently protected;
- **Access denial**: attacks against e.g. armed forces which use computers and satellites for communication. Orders and reports may be intercepted and altered, which may result in dangerous situations for the army;
- **Network attacks against infrastructure**: attacks on transmission systems of the companies in power engineering, gas industry, heating industry, oil industry and communication infrastructure, which are sensitive to cyber attacks;
- **Non-network based attacks against infrastructure**: abuse (or rather utilization) of common computer hardware and hardware used in internet operation and security. Virus is hidden in hardware, software, or maybe even in microprocessors.

Cyber war may further be classified in the same way as a conventional war into defensive and offensive cyber war. [11]

4.1 Defensive Cyberwarfare

In case of defensive cyber war it will be important to determine strategically important installations. At present such installations are buildings and the decisive criteria are their geographical locations, equipment, etc. These installations may also be virtual in case of cyber war. In order to prevent an attack or reduce loses and damage it is necessary, prior the attack itself, to minimize the number of input access spots, introduce multiple software security, hardware security and properly screen and train the personnel with network access permits.

Cyber attackers have got a clear goal with an easy plan. The key to success is the moment of surprise during attack. The earlier the defender responds to the attack, the easier it may be to stop or repulse it. If such an attack with the moment of surprise is conducted, it is first necessary to stabilize the whole system and thus deal with the surprise. Second, it is necessary to detect the attack and try to understand the

attacker´s plans and intentions. Then the attack may be repulsed. It must not be forgotten that the attack analysis always has to follow. Based on acquired information, the protection of critical infrastructure (hardware and software) has to be increased in order to prevent possible subsequent cyber attacks. [12]

4.2 Offensive Cyberwarfare

Firstly, we have to be aware of the aspects of offensive cyberwarfare and compare them with traditional aspects (conventional war, diplomacy, etc.). Such a type of war may be more acceptable for public than employing the means of conventional war. Although a cyberwarfare may avoid direct casualties, there are still indirect dangers. Critical infrastructure is somewhere between state and private sectors. It includes e.g. water distribution network, electric energy network, air traffic control, and other systems critical for the functioning of a particular country. Enemy may take advantage of our dependence on cyber space and gain strategic advantage in a possible conflict. It is assumed that a cyber war would precede a conventional war. [12]

Future possible cyberwarfare are reasons for our serious concerns. Unlike traditional wars requiring a vast amount of sources, such as weapons, personnel and equipment, cyber wars require somebody who has got appropriate know-how, computers, and willingness to create chaos. Enemy may be everywhere, even inside the country or organization. An intense attack may be carried out by only a few hackers with the help of standard computers. [12]

Another terrifying aspect of cyber war is the fact that cyber attack may be either part of a coordinated attack, or it may only be an idea of a malicious hacker, e.g. with a funny idea. No matter what the attacker motive is, cyber attacks may cause big financial losses. And many countries are pitifully unprepared to manage such unexpected cyber attacks. [12]

5. May Forces Ratio Be Calculated In Cyber Space?

Various tactical calculations may be part of combat planning. One of such calculations is the ratio of forces and resources. The ratio of forces and resources is prepared as a supplementary document, mainly to the decisive phases of task (combat order) fulfilment. Such a ratio may be elaborated either quantitatively, or qualitatively. Authors present the numbers (assumed) of forces and resources employed by enemy and friendly forces in individual required categories in quantitative forces ratio, while in case of qualitative forces ratio the quality of employed forces and resources is considered. Such quality is considered in the final ratio of forces and resources of a given category through so called combat potential. The fact is that enemy forces and resources are considered on the basis of probability assumptions. It is a summary of qualitative and quantitative data about the forces and resources of fighting parties with the help of which a better idea of combat capabilities and the likely outcome of combat can be obtained. [13]

How is it possible to **calculate the ratios of forces of cyber armies** being against each other in a war cyber conflict? Is it feasible to carry out such a calculation? In fact, it is almost impossible. In case of war in cyber space it is quality, not quantity, which counts. A hundred of specially trained soldiers of cyber units may fail face to face with one talented enemy (a cyber attacker). Quantitative supremacy need not be decisive in cyber space. Thus, is it enough or not to have 100 or 1.000 specially trained soldiers? [13]

I think that military cyber units may be compared at least according to the following three criteria:

- Capability of **carrying out** attack in cyber space (offensive potential);
- Capability of **preventing attack** (defensive potential);
- **Dependence** on cyber environment (dependency).

Other aspects considered for more detailed comparison may be the capability of restoring key systems, existence of supplementary or contingency systems, crisis plans, etc. In case of cyber combat we deal with rather potential possibilities for calculating the forces ratio of cyber units, because more detailed information is never available. The reason is the fact that any statement of future attacker may help the opponent to be better prepared for potential weaknesses, provoke testing operations, and breach public confidence. The future attacker´s statement about perfect protection of his own network may provoke testing operations carried out not only by potential attackers, but also by haphazard non-state actors (e.g. hackers) with the aim to reveal possible weaknesses. [13]
I have been dealing with the calculation of forces ratio in cyber space since 2013. More detailed description of the outcomes in qualitative and quantitative calculation of forces ratio is beyond the scope of this contribution.

6. Cyber Defence in the Czech Republic

Gradual steps have been taken in building the cyber defence in the Czech Republic. At first, the Government tasked Military Intelligence to build a unit capable of conducting operations in cyber space. Why Military Intelligence? Army is responsible for the defence of the Czech Republic and the Military Intelligence is the military intelligence service and a constituent of the Czech Ministry of Defence. Moreover, cyber space is not a typical battlefield, it is rather information space, and intelligence service traditionally plays an important role in this area. Advantage is also the fact that Military Intelligence is the only Czech intelligence service both on our territory and abroad.
The Military Intelligence builds the National Centre of Cyber Forces, which will systematically monitor and report anomalies in cyber space. Cyber space monitoring is important and irreplaceable in cyber defence. The monitoring enables us to identify in time certain phenomena which may indicate the preparation of cyber attack. The systematic monitoring will be provided through technical means located in the networks of the Czech providers of electronic networks.

7. Conclusions

The seriousness of cyber threat is underestimated. Cyberattacks of any kind are very sophisticated offensive instruments against which there is not an easy defence. There is a common chacteristics of all such attacks – they are of low costs for attackers, but their consequences, elimination and possible prevention are more and more costly and the damages may reach billions of dollars. Those who suffer from such attacks are individuals, economic entities, government institutions and also armed forces. Damages of the largest degree range from the theft of secret or sensitive data to the destabilization of various infrastructures or even critical information infrastructure.
As the biggest problem remains the fact that hackers are difficult to be caught due to the anonymity of internet. Even a more serious problem will occur when states become participants.

Acknowledgements
This work was supported by the project no. VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems" supported by the Ministry of the Interior Security Research Programme of the Czech Republic in the years 2015-2020.

References

[1] CLARKE, Richard A. *Cyber War*, HarperCollins (2010) ISBN 9780061962233.

[2] COLLINS, Sean (April 2012). "Stuxnet: the emergence of a new cyber weapon and its implications". *Journal of Policing, Intelligence and Counter Terrorism*. **7** (1). Retrieved 6 June 2015.
[3] CLAPPER, James R. "Worldwide Threat Assessment of the US Intelligence Community", Senate Armed Services Committee, 26 February 2015 p. 1.
[4] USAF HQ, Annex 3–12 Cyberspace Ops, U.S. Air Force, 2011.
[5] FARWELL P. James and Rafael ROHOZINSKI, Stuxnet and the future of cyber war, Survival, 2011.
[6] HRŮZA, Petr; SOUŠEK, Radovan; CHLAN, Alexander. *Cyber attacks and cyber warfares*. In: Recent Researches in Telecommunications, Informatics, Electronics and Signal Processing. Baltimore, MD, USA: WSEAS Press, 2013, p. 100-107. ISSN 1790-5117. ISBN 978-960-474-330-8.
[7] HRŮZA, Petr; SOUŠEK, Radovan and SZABO, Stanislav. Cyber-attacks and attack protection. In: *WMSCI 2014 - 18th World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings*. Orlando, Florida, USA: International Institute of Informatics and Systemics, IIIS, 2014, p. 170-174. ISBN 978-1-941763-04-9.
[8] ISAAC R. Porche, PAUL Christopher, SERENA Chad C., CLARKE Colin P., JOHNSON Erin-Elizabeth and DREW Herrick. T*actical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Santa Monica, CA: RAND Corporation, 2017.
[9] HARAKAĽ, M. and M. OBERT, *Contemporary cybernetic threats analysis*. In: Science & Military. - ISSN 1336-8885. - Vol. 10, No. 1 (2015), pp. 5-12.
[10] PIKNER, Ivo and ŽILINČÍK, Samuel. Military concepts and hybrid war. *Forum Scientiae Oeconomia*, 2016, vol. 4, no. Spec Issue No 1, p. 25-33. ISSN 2300-5947.
[11] BARÁTH,J. and M. HARAKAĽ, *Test bed for cyber-attacks mitigation*. In: AFASES - 2011: scientific research and education in the air force: the 13th international conference of scientific papers : Brasov, 26-28 May 2011. - Brasov : Air Force Academy, 2011. ISSN 2247-3173. - pp. 587-592.
[12] HRŮZA, Petr. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012, p. 90. ISBN 978-80-7231-914-5.
[13] HRŮZA, Petr. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013, p. 100. ISBN 978-80-7231-931-2.