Pulaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warsaw, 17.07.2015

Author: Andrzej Kozłowski

The new strategy of the Department of Defense in cyberspace

At the end of April 2015, the newly-elected Secretary of Defense Ashton Carter announced the second strategy in cyberspace in the history of the Pentagon. The strategy presentation was held in Silicon Valley, the heart of the American IT sector. The published document replaced the strategy from 2011.

Pentagon strategy from 2011

In 2011, the Department of Defense published its 13-page "Strategy for Operating in Cyberspace" (partly declassified). The strategy marked five initiatives. The first involved treating the virtual environment as another area of military operations alongside land, sea, air and space. This involved the construction of the relevant units and structures to operate in cyberspace, which led to the creation of the United States Cyber Command (US CYBERCOM), under the U.S. Strategic Command. The second initiative consisted in agreeing on a new concept of defence, which emphasized the 'cyber-hygiene', understood as a reasonable use of software and improving ways to combat internal threats. An active cyber defence concept was also implemented, which consists in catching an attacker in a trap, and conducting a counterattack. The third point involved the cooperation with government agencies, primarily with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security and the private sector to exchange information. The fourth point included actions in the international arena, especially with regard to improving

> *Two elements distinguish the new Pentagon document against previous strategies. For the first time, it has directly indicated the possibility of conducting offensive operations in cyberspace, and has identified potential targets. Attacks would be directed at enemies' military command systems and critical infrastructure, in order to paralyse the enemy's communications. US CYBERCOM would command the operation not, as previously, the National Security Agency (NSA).*

NATO's ability to operate in a virtual environment. The last initiative was to increase the capacity of the United States in cyberspace through investment in technology and human capital.

The strategy of the Pentagon from 2011 did not mention anything about the offensive abilities; it was a summary of doctrines and strategy papers for each military unit that had earlier been developed. According to Professor Thomas M. Chen, the author of publications for the United States Army War College, it was too general, did not have clearly defined priorities and a strategic vision, and did not present plans to implement the outlined solutions.

Pentagon strategy from 2015

The new strategy meets the expectations of critics of the previous document. It is more detailed and clearly articulates the main tasks of the Pentagon in cyberspace which would consist of:

- defence of networks, systems and information of the Department of Defense;

- defence of the United States and American interests against the most malicious cyber attacks;

- readiness to assist in cyberspace in military operations.

In addition to clearly described objectives, the strategy has identified the main threats to cyber security of the United States, moving away from the extremely popular concept of an apocalyptic attack in a virtual environment, often compared to the Japanese raid on Pearl Harbour. The theft of intellectual property (blamed on China) has been indicated as the main risks, as well as attacks of low intensity, directed against single individuals and businesses. It has also highlighted the problem of proliferation of cyber arms due to the dynamic development of the black market in weapons of this type.

The strategy, like its predecessor, has determined five main strategic initiatives. The document envisages the construction of strength and ability to carry out operations in cyberspace, and provides for measures to employ young and talented experts in the field, training, construction of technical infrastructure and support for the National Initiative for Cyberspace Education. The second strategic objective takes into account defending the

network of the Department of Defense, securing Pentagon's data, and reducing the risk coming from a virtual environment in military operations. Under this initiative, the main tasks relate to improving the efficiency of military networks, information exchange about malware, and preventing internal threats. The third point has raised the problem of the defence of the United States and its interests against the most dangerous cyber attacks, capable of causing a serious damage. This is to be achieved by improving the system of predicting attacks, cooperation with other federal institutions, as well as the development of innovative defence capabilities. The fourth initiative involves providing the Pentagon with the capacity to control the escalation of conflicts in cyberspace. This is to be done by integrating the operations carried out in a virtual environment with those that take place in a classic battle. The last point concerns the strengthening of international organizations and partnerships with selected allies in the Middle East, Asia and NATO member states. A separate dialogue with China is also significant.

The strategy identifies entities responsible for these tasks. Cyber Mission Force, which is still under development, is divided into four groups, each of which carries different tasks:

- National Mission Teams - protecting the United States against attacks in cyberspace;
- Cyber Protection Teams - focuses on protecting Pentagon's network;
- Combat Mission Teams - provides support for regional commands;
- Support Teams - provides information and analysis.

Two elements distinguish the new Pentagon document against previous strategies. For the first time, it has directly indicated the possibility of conducting offensive operations in cyberspace, and has identified potential targets. Attacks would be directed at enemies' military command systems and critical infrastructure, in order to paralyse the enemy's communications. US CYBERCOM would command the operation not, as previously, the National Security Agency (NSA).

The second element is to return to the concept of deterrence. Initially the Pentagon rejected this option, considering it inadequate to a virtual environment. At present, however, close cooperation between intelligence and the private sector would make attribution of the attack as the most possible. In addition, there are plans to implement the concept of 'deterrence by denying benefits', which consists in creating immune computer systems frustrating an attacker.

Conclusions and recommendations

1. The new U.S. strategy has continued and expanded the assumptions and achievements of the previous one. But it is not limited to defining strategic objectives, but also provides detailed solutions to ensure their implementation, which was missing in the previous document.

2. The United States have returned to the concept of deterrence, which may suggest a belief in their own ability to track and identify an attacker. This belief seems to be wrong, the last major hacker attack, where attackers seized the data of persons employed in intelligence agencies and the armed forces, has showed that the attack attribution capacity is insufficient. The most famous case of identifying the attacker – the Chinese 61398 military unit, responsible for spying operations in cyberspace – took a private company Madiant several years to handle. This shows that the concept of deterrence in a virtual environment has a limited chance of success.

3. The fact that the U.S. officially admitted in a strategic document to conducting offensive operations in cyberspace is a breakthrough. However, problems may occur in the form of attacking objects of dual-use (civil and military) and the absence of rules of engaging forces in a virtual environment. The entries of the strategy confirm the thesis about the militarization of cyberspace.

4. The role of military forces in protecting key American institutions in cyberspace and the private sector has definitely increased. The Obama administration has reduced the importance of keeping relative balance between the civil and military sectors, which had been maintained by previous administrations.

5. Mentioning the need to establish a dialogue with China demonstrates the importance of this player in a virtual environment. It does not seem, however, possible in the near future. Both sides accuse each other of carrying out sophisticated espionage operations in a virtual environment, and it is unlikely that China or the United States would stop them. Although the parties conduct dialogue on cyber-security, it mainly concerns the less controversial issues, such as the fight against spam.

6. Pentagon's new strategy shows that conducting offensive operations in cyberspace has become the norm. Also, the Polish armed forces should take appropriate action to develop such capabilities, taking into account, among others: creating their own malicious software

or botnet. In particular, it must be remembered that NATO's security policy in the virtual world was and is heavily influenced by American solutions, therefore, possessing offensive capability in cyberspace will undoubtedly play to Poland's advantage within NATO.

7. Poland as a member of NATO should join the Multinational Cyber Defence Capability Development Project, which includes the Netherlands, Romania, Denmark, Norway and Canada. These are the countries with developed system of cyber defence. This initiative aims to improve sharing of sensitive information, increasing awareness about dangers and potential hacker activity and to develop joint work on improving the existing cyber defence systems.

Author: *Andrzej Kozłowski, Research Fellow at the Casimir Pulaski Foundation*

The Casimir Pulaski Foundation is an independent, non-partisan think-tank specializing in foreign policy and international security. The Pulaski Foundation provides analyses that describe and explain international developments, identify trends in international environment, and contain possible recommendations and solutions for government decision makers and private sector managers to implement.

The Foundation concentrates its research on two subjects: transatlantic relations and Russia and the post-Soviet sphere. It focuses primarily on security, both in traditional and non-military dimensions, as well as political changes and economic trends that may have consequences for Poland and the European Union. The Casimir Pulaski Foundation is composed of over 40 experts from various fields. It publishes the Pulaski Policy Papers, the Pulaski Report, and the Pulaski Viewpoint. The Foundation also publishes "Informator Pułaskiego," a summary of upcoming conferences and seminars on international policy. The Foundation experts cooperate with media on a regular basis.

Once a year, the Casimir Pulaski Foundation gives the Knight of Freedom Award to an outstanding person who has promoted the values represented by General Casimir Pulaski: freedom, justice, and democracy. Prizewinners include: Professor Władysław Bartoszewski, Professor Norman Davies, Alaksandar Milinkiewicz, President Lech Wałęsa, President Aleksander Kwaśniewski, President Valdas Adamkus, Bernard Kouchner, and Richard Lugar.

The Casimir Pulaski Foundation has a partnership status with the Council of Europe.

www.pulaski.pl