WISI OPINION No. 2/2018

Author: Karol Cheda

WARSAW INSTITUTE
FOR STRATEGIC INITIATIVES

RUSSIAN WAVE OF CYBERATTACKS

On 16th of April, U.S and British governments have warned of a “wide campaign targeting routers and firewalls” in cyberspace. More than million machines around the globe were targeted, affecting governmental institutions, private sector entities, critical infrastructure organisations and internet providers ensuring assistance for both of the sectors. The aim of the operation was to gain access to intelligence data, intellectual property and to create a ‘back door’ in software for further penetration. Although there is no direct evidence, specialists form the U.S State Department indicate that Russia is involved in these incidents.

The following attacks can be a part of a wide cyberspace campaign conducted by the Russian Federation since the May 2007 cyberattacks in Estonia. In recent years, the intensity of the attacks hit new highs after the development of cyberspace capabilities was recognised as a new priority (this fact was also mentioned in NATO’s Newport Declaration). One of the examples is the usage of NotPetya software during the Ukrainian conflict, which encrypted data crucial for public as well as private infrastructure. In result, the data was damaged and couldn’t be used later. Such activities could be perceived as a form of test how to paralyse a state by using cyberspace capabilities.

This case also displays a structural change of the character of cyberspace activities – the importance of organised hacker groups financed by the state, which also provides the necessary infrastructure and new technology, is constantly growing. Due to the ongoing professionalisation in cyberspace and the continuity of informal rivalry between states in this field, intensification of the activities aiming for the perception change concerning the evolution of military operations (cyberwarfare became an important element of it) shall be recognised as new priority.

POLISH POINT OF VIEW:

Poland shares a border with Russia and remains within its closest operational area. Due to Russian policy, which concentrates on the reconstruction of the Cold-War order through the extension of spheres of influence, **Poland is at the risk of cyberattacks. In this context, special attention should be paid during the next local elections this autumn**.

Development of cyberspace capabilities **shall be considered as one of the priorities**. Creation of the cyber defence system for the Republic of Poland requires:

setting-up of a consistent operational strategy;

construction of CSiRT (Computer Security Incident Response Team) system;

trainings for specialists;

good practices, importance of which is often overestimated.

Wave of Russian attacks targeted basic ICT network equipment like routers and consequently infected those that were not adequately secured. **The robustness of the cybersecurity system depends on its least protected element. That is why even the most advanced technological and institutional solutions will remain ineffective if the human factor fails**.

Based on:

- B. Jansen, E. Weise, *Russia is sponsoring cyberattacks in U.S. homes and businesses, U.S. and U.K. officials warn*, USA Today, https://www.usatoday.com/story/news/2018/04/16/russia-sponsoring-cyberattacks-u-s-homes-and-businesses-u-s-and-u-k-officials-warn/520981002/
- N. Lomas, *UK accuses Russia of 2017's NotPetya ransomware attacks*, Tech Crunch https://techcrunch.com/2018/02/15/uk-accuses-russia-of-2017s-notpetya-ransomware-attacks/
- U.S. Department of Homeland Security, https://www.dhs.gov/
- Edict of the Russian Federation President on the Russian Federation's National Security Strategy, http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf