Information & Security: An International Journal

Valentyn Petrov, vol.31, 2014, 73-77 http://dx.doi.org/10.11610/isij.3104

ESTABLISHING A NATIONAL CYBERSECURITY SYSTEM IN THE CONTEXT OF NATIONAL SECURITY AND DEFENCE SECTOR REFORM

Valentyn PETROV

Abstract: Experience of recent years indicates that cyberattacks are often aimed at informational systems of state bodies, healthcare, energy, financial and transport sector, etc. with increasing, unpredictable consequences. The 2012 National Security Strategy of Ukraine includes a provision on establishing a national cybersecurity system. Its effective implementation requires to take into account not only threats of a criminal nature, but a full range of threats with varying origin, tools used, targets and purpose. This paper presents an analysis of the current state of threats, related to transnational cybercrime and attempts to use modern informational technologies by foreign governments, organisations and individuals. The national cybersecurity system—the set of administrative, legal, technical measures related to informational security and data protection—continues to be one of the key elements to guarantee national security. This article is focused on the cyber dimension of the national security, in particular its legal aspect in context of an ongoing defence and security sector reform.

Keywords: cyber threats, cybercrime, cybersecurity system, legal framework, security and defence reform.

Introduction

In an international context there has been a stable trend for increasing the number of cyberattacks on national critical infrastructure. Examples of recent years show that attacks are often aimed at information systems of public and private bodies in the healthcare, energy, financial and transport sector, causing unpredictable consequences. Those could include leakage of data, or interrupt the functioning of critical infrastructures.

This has been taken into account and lead to the update of foreign policy and defence doctrines of many countries, levelling cyber to military attacks and treating them as *casus belli*.

NATO's Strategic Concept of 2010, adopted at the Lisbon Summit, also focuses on cyber threats, with information and cybersecurity taking a place among the priorities of the Alliance. Notably, one of the key elements in NATO's cyber defence concept involves international partnership to increase cybersecurity.

This has been confirmed by the Chicago Summit declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council on 20 May 2012, where article 49 expresses readiness to cooperate with foreign partners and international organisations on the issues of cyber protection and underlines the necessity of strengthening the Alliance cyber defence capabilities.

Conceptual Aspects of the Ukrainian Cybersecurity Policy

Ukraine faces similar challenges and threats. The National Security Strategy, which was amended in 2012, lists among the state's priorities in the security domain the establishment of a National Cyber Security System (NCSS).

The idea to organise a NCSS first appeared in 2010. Then, a decision of the National Security and Defence Council of Ukraine "On challenges and threats to national security of Ukraine in 2011" declared the necessity for the establishment of a joint national system to counter cybercrime.

While executing this task, it has become apparent that the protection of the national security in the information field requires a comprehensive approach, taking into account not only threats of criminal nature, but the full range of threats that vary in terms of their origin, tools that are used, targets at which they are aimed at and, of course, their final purpose. As a result, the concept for the establishment of a NCSS started to take shape. The system was supposed to employ a set of administrative, legal, and technical measures related to information security and data protection, combining the capabilities of defence, law enforcement and intelligence sectors.

In this respect the following groups of cyber threats were considered:

- cyber war;
- cyber terrorism;
- cyber espionage;
- cybercrime.

Such a classification demanded from the NCSS to include three sub-systems:

- cyber defence security system;
- law enforcement system;
- national security system (targeted on cyber terrorism and espionage).

It was recognised that it was not possible for the NCSS to cover all spheres of life, transformed by the penetration of modern information technologies.

The information revolution has abolished state borders in their classical meaning, blurring the difference between the actions of state and non-state actors. It has shaped a new security environment where "network" has become the opposite of traditional society. For example, a single hacker could work for himself, for a transnational organised crime group, for an extremist group of politically motivated "hacktivists" and, finally, for one or even several governments. In terms of tools – the same virus can be used for interception of credit card numbers, for gaining access to classified information, no matter whether of governmental or of commercial origin, and for taking over sophisticated defence systems. The same logic could be used to discuss the issue of botnets.

A cyberattack could also pursue multiple purposes. For example, bank information systems could be attacked with the aim to destabilise a particular country's financial system, as experienced several times by South Korea, or to exert political pressure, as was the case with the cyberattacks on PayPal, Mastercard and Visa, which blocked the accounts of Julian Assange in 2010.

Thus, new approaches are required to cope with this multifaceted threat.

Operationalisation of the Ukrainian Cybersecurity System

From Ukrainian point of view, the national cybersecurity system should represent a system of systems, including intelligence, law enforcement, and government agencies regulating telecommunications and information security, cooperating with the aim to detect, prevent and suppress cyber threats, to reduce the possibilities of their occurrence and to mitigate the negative consequences thereof. The functioning of such a complex system is impossible without close cooperation with the private sector – telecommunications and internet service providers, owners and operators of critical information infrastructure sites, as well as with private companies specialised in information security.

Thus, the NCSS is seen as organised not only in line with the classical threat-oriented manner, but also taking into account functional aspects, and so including the following sub-systems:

- advisory system – responsible for general management, strategic decision support to the top state leadership on cybersecurity issues, and for the coordination of relevant authorities;
- system for monitoring cyber threats – such a system should combine technical means, CERTs, information from internet service providers (ISPs), banking institutions, law enforcement, anti-virus companies, etc., including intelligence data obtained by special services, intelligence agencies, and financial monitoring. The information coming from different sources should be concentrated and processed in a single place in real time for immediate decision-making;

- system for cyber protection of critical information infrastructure facilities of the state – this system should employ a set of measures for technical protection, personnel security clearance, and counterintelligence protection of these facilities from foreign intelligence, acts of terrorism and other illegal activities.

The capability for urgent assessment and decision making should be considered an essential condition for the proper performance of the NCSS. Furthermore, the absence of a single institution responsible for the general management of cybersecurity measures might complicate, slow down and, in some cases, make impossible to undertake the necessary steps to respond to cyberattacks, especially given their high degree of latency.

For these reasons, the deployment of the NCSS must be accompanied by appropriate adjustments in the process of defence and security sector reform. The main public sector actors in the field of cybersecurity today are the following institutions: Ministry of Defence, Ministry of Interior (MoI), the State Service for Special Communication and Information Protection, the Security Service of Ukraine.

The Cabinet of Ministers of Ukraine has drafted a bill "On Amendments to the Law of Ukraine on National Security," tackling cybersecurity. The bill is expected to finally introduce into the national legislation the term "cybersecurity" and related terminology. It is also expected that, following the adoption of the amendments, a law on cybercrime will be developed by the MoI of Ukraine, which has to improve significantly the institutional capacity of national law enforcement agencies and to ensure the final implementation of the Budapest Convention. In the meantime, the Ministry of Defence of Ukraine has developed amendments to the law "On Defence" which deal with the issue of cybersecurity in the military sphere.

Without any doubt, a central element of a national cybersecurity system should be the State Service of Special Communication and Information Protection. However, its functions, determined by a specific law, should be revised, so that this Service can turn into a national authority for cyber defence of critical infrastructure. Unfortunately, as of today, the agency has neither authority nor the instruments and leverage in this area, being responsible only for the government's information resources. A positive fact is that a specialised unit – Computer Incident Response Team (CERT-UA) already functions within the agency.

Furthermore, the Security Service of Ukraine (SBU) has recently established a new functional unit of counterintelligence protection of state interests in the field of information security.

The law gives SBU sufficient powers not only to be part of the NCSS, but also to act as its founding element. The SBU is a counterintelligence agency, responsible for fighting terrorism, and for performing the task of protecting not only national sovereignty, constitutional order, territorial integrity, but also economic, scientific and technical capabilities and interests of the state and citizens' rights. In addition, the

SBU is responsible for protecting the national communication system. All above-mentioned confirms that the legislative framework already allows the SBU to take comprehensive measures in the area of cybersecurity.

Conclusion

To conclude, Ukraine has made significant progress in the development and institutionalisation of a national cybersecurity system. An important step in this direction should be the adoption of a cybersecurity strategy, presented during this year's NATO-Ukraine cyber defence staff talks. At the same time, a review of Ukraine's capabilities in the area of cybersecurity is expected to assess their contribution to the sector of national security and defence. In this context, the experience of the defence review already conducted by the Ministry of Defence of Ukraine might be useful along with the expertise of the international expert community.

Valentyn PETROV is a Major in the Security Service of Ukraine (SBU) and Head of a Unit within the SBU Department for Counterintelligence Protection of the Informational Security of the State. Major Petrov is an expert of the in the area of information security. He holds a PhD and conducts research in the broad field of cybersecurity. He can be reached at icd_info@ssu.gov.ua.