Information & Security: An International Journal

Volodymyr Bik, vol.31, 2014, 69-72 http://dx.doi.org/10.11610/isij.3103

PROTECTING THE NATIONAL INTERESTS IN THE DOMAIN OF INFORMATION SECURITY AS A FUNCTIONAL TASK OF THE SBU

Volodymyr BIK

Abstract: The development of modern information technologies and innovations in all areas of life resulted in new threats to national and international security. Over the past decade, such threats as transnational cybercrime, cyber terrorism, the use of cyber weapons transformed from potential and hypothetical into real ones. Combating those threats has become a priority of the national security and defence sector. The article focuses on how the profound changes in the global security system, in combination with the evolution of the cyber threats, influenced the activities of the Security Service of Ukraine (SBU), turning the Service in a key element of the future national cybersecurity system. The author reasons for enhanced international cooperation and systematises practical examples of effective international efforts to counter cyber threats.

Keywords: information security, cyber threats, cybersecurity, intelligence, SBU, international cooperation.

Introduction

The development of modern information technologies and innovations in all areas of life resulted in the upsurge of new threats to national and international security. Over the past decade, once vague challenges such as transnational cybercrime, cyber terrorism, and the use of cyber weapons have become more apparent. Thus, combating those threats has turned into a priority task of the national security and defence sector.

The information revolution has also added new quality to traditional national security threats such as espionage, terrorism, organised crime, illicit arms trafficking, drug smuggling and human trafficking. Finally, information technology has led to the transformation of social relations, demanding that special services employ radically new approaches in the intelligence gathering process.

International criminal and terrorist groups, radical organisations, foreign intelligence agencies, multinational corporations, organised crime groups of hackers, as well as criminals with high skills in IT could all be source of the abovementioned threats.

Meanwhile, even the neutral status of a certain state may not prevent its information resources and information infrastructure from being used to the detriment of its interests or to the detriment of third countries' interests. In today's globalised world, where modern technologies face no boundaries in virtual space, the issue of Ukraine's information sovereignty becomes particularly important.

Inevitably, the profound changes in the global security system, in combination with the evolution of the cyber threats, influenced the activities of the Security Service of Ukraine (SBU), which is turning into a key element of the future national cybersecurity system.

First steps towards enhancing Ukraine's information security

The updated National Security Strategy of Ukraine (revised in 2012) stipulated as one of its strategic priorities the development of a national cyber security system. The plan for the systems' development was introduced in the Annual National Program (ANP) for NATO-Ukraine cooperation in 2013, and was detailed by the SBU in the draft version of the ANP for 2014.

Prior to that, in 2012 a new department within the SBU was established to provide counterintelligence protection of the state interests in the field of information security. The Department was formed on the basis of a relevant unit which had functioned as part of the SBU for over 10 years.

The main tasks of the Department are:

1. Countering internal and external threats aimed at:
    a. governmental telecommunications systems, information resources, e-government systems;
    b. critical information infrastructure (including communications systems in the energy and financial sector, life support systems, transportation facilities, elements of the national security and defence system);
    c. the national systems of technical and cryptographic protection of information.
2. Combating cyber terrorism, counteracting the use of Internet for propaganda of terrorism.
3. Combating cybercrime that threatens national security.
4. Controlling the circulation of special technical devices aimed at covert gathering of information; protecting the citizens' rights from unlawful use of the abovementioned special equipment.

Ukraine's International Cooperation in the Field of Information Security

There is no doubt that more often than not finding solutions to such problems is impossible without an adequate level of international cooperation.

In the framework of cooperation with European partners, representatives of the SBU permanently participate in meetings of the Cybercrime Convention Committee, an OSCE informal working group to develop confidence-building measures in the field of cyber security, as well as in the UN intergovernmental expert group on cybercrime.

Currently the SBU together with the OSCE implements a project called "Support to Effective Cyber Security Policy in Ukraine," aimed at improving the effectiveness of countering modern challenges to the information security of Ukraine.

In addition to that, the annual expert staff talks NATO-Ukraine on cyber defence have become one of the most useful tools of the bilateral relations, particularly in terms of information exchange on current problems in the sphere.

The SBU also maintains effective bilateral cooperation with a number of national intelligence and law enforcement agencies, namely from Azerbaijan, Belarus, Belgium, UK, Armenia, Cyprus, Lithuania, Netherlands, Poland, the Russian Federation, Romania, USA, France, Sweden, etc.

An important aspect of the international cooperation is the SBU's taking part in two of the six biggest international operations in 2010 and 2011: "Trident Breach", which took place in October 2010, and "Trident Tribunal" of June 2011. During the latter, the SBU, together with law enforcement agencies from 10 countries, was involved in a coordinated effort targeting illegal activities of an international criminal hacker group which functioned under an existing commercial entity. The criminals used the sale of fraudulent computer security software, which, once installed, provided them with full access to all personal data (including account numbers, passwords, etc.). As a result of the group's activity losses amounting to more than 72 million USD were caused.

Furthermore, in collaboration with partner intelligence agencies from several European countries, the SBU identified administrators and users of online resources of a terrorist nature.

At the end of 2012, the SBU prevented an attempt by an organised crime group of hackers, which operated in Ukraine, to steal 500 million USD from the international payment system Visa through malware. According to the information obtained while working on the case, the vast amount of the stolen money would fund terrorist activities. The organiser of the scheme was deported from Ukraine.

In 2013, the SBU, in cooperation with the foreign security service FSB of the Russian Federation, detained on the territory of Ukraine a group of hackers, including developers and distributors of the "Carberp" malware, which provided criminals with illegal access to bank data, passwords and electronic keys of numerous entities, causing losses estimated at around 260 million USD.

All examples of cooperation mentioned above clearly demonstrate that modern cyber threats often go beyond the purely criminal sphere and enter the domain of national security. Moreover, they confirm the thesis that fighting against them is impossible without appropriate information exchange between partner intelligence services and law enforcement agencies.

At present the main areas of cooperation include:

1. Establishment of a mechanism for urgent exchange of information about:
   a. new forms and methods of cyber threats realisation;
   b. features of malicious software installation;
   c. persons involved in hacking activities;
   d. cyberattacks, specifically on critical information infrastructure facilities;
   e. persons involved in the implementation of those cyberattacks.
2. Sharing experience on the current problems and latest technologies in the field of cyber security, as well as on the monitoring of cyber threats.
3. Trainings in the field of modern information technologies; joint trainings in cyber defence.
4. Joint research in the field of cyber security, development of systems for monitoring and protection.

Major General Volodymyr BIK is Head of the Department for Counterintelligence Protection of the Informational Security of the State in SBU – the security service of Ukraine.