CYBER SECURITY *in* UKRAINE

International threats compel Kiev to establish a national *cyber security* system

By **Valentyn Petrov**, Secretariat of National Security and Defense Council of Ukraine

Analysis of Ukraine's national security confirms a high threat level related to transnational cyber crime and attempts by foreign governments, organizations and individuals to use modern information technologies against the state. Therefore, the development of a national cyber security system is vital to guarantee Ukrainian national security.

The number of computer attacks worldwide on national infrastructures is increasing. This results in the modification and leakage of data and the obstruction of critical infrastructure processes. Such consequences have caused a modification in foreign policy and defense doctrines in many countries, making a cyber attack equal to a military attack.

The NATO Strategic Concept 2010, adopted during the Lisbon Summit, focuses on possible cyber attack threats. In fact, it discusses categorizing a cyber attack as being equal to a traditional military threat. Informational security is a high priority for the Alliance. NATO cyber defense policy considers international partnership in cyber security to be one of the key elements of NATO's strategy in this domain.

This statement was confirmed by the Chicago NATO Summit Declaration, issued by the heads of state and governments at the May 2012 meeting of the North Atlantic Council. In particular, Article 49 confirms readiness to cooperate with foreign partners and international organizations on issues of cyber protection and

> The information revolution abolishes state borders in the classic sense, making the distinction between the actions of state and nonstate actors nonevident. This forms a new security environment where the "network" displaces traditional society.

Ukraine's President Petro Poroshenko chairs the National Security and Defense Council meeting in Kiev in February 2015. The council affirmed establishment of a national system to counter cyber crime.
EPA

underlines the necessity of strengthening Alliance capabilities in cyber defense.

Cyber attacks are often aimed at the information systems of state bodies and the health care, energy, financial and transportation sectors, causing dangerous and unpredictable consequences. Moreover, the conflict in Eastern Ukraine confirms the thesis that hybrid warfare is, in many aspects, supported by a wide range of cyber warfare instruments. One interesting aspect is that governmental informational resources and data bases are often targeted by terrorists, who consider such assets a means for establishing and enforcing their own capabilities to control certain territory and populations and to sustain economies and pseudo-governance.

Ukraine's National Security Strategy, adopted this year by the National Security and Defense Council and approved by presidential decree, declares that a key threat to national security is "vulnerability of critical informational infrastructure and governmental informational resources to cyberattacks." From our point of view, this threat requires adequate counteraction. Unfortunately, Ukraine is still in the process of deploying its National Cyber Security System (NCSS) that was foreseen by a previous version of the National Security Strategy dated 2012. The idea to organize the NCSS first emerged in 2010. The decision by the National Security and Defense Council of Ukraine mentioned "challenges and threats to national security of Ukraine in 2011" and the need for a "joint national system to counteract cyber crime."

While executing this task, it became clear that the issue of national security in the informational sphere requires a complex approach that takes into account not only criminal threats, but a full range of threats that vary depending on their origin, the tools used, the targets and, of course, their final purpose. As a result, the idea of a national cyber security system appeared. The NCSS combines sets of administrative, legal and technical measures related to informational security, and data protection of potential vulnerabilities in the defense, law enforcement and intelligence sectors.

This includes the following groups of cyber threats: cyber war, cyber terrorism, cyber espionage and cyber crime. These classifications demand that the NCSS include several subsystems: the defense cyber security system, the law enforcement system and the national security system (focused on cyber terrorism and espionage).

Nevertheless, we must take into account the in-depth transformation of social ties and relations caused by the penetration of modern information technologies into all spheres of life. The information revolution abolishes state

borders in the classic sense, making the distinction between the actions of state and nonstate actors nonevident. This forms a new security environment where the "network" displaces traditional society.

For example, an individual hacker can work for himself, a transnational organized crime group, an extremist group of politically motivated "hacktivists" or one, or even several, governments. Or, a single virus can be used for intercepting credit card numbers, accessing restricted information (state or commercial) or gaining control over sophisticated defense systems. The same synopsis applies to botnets.

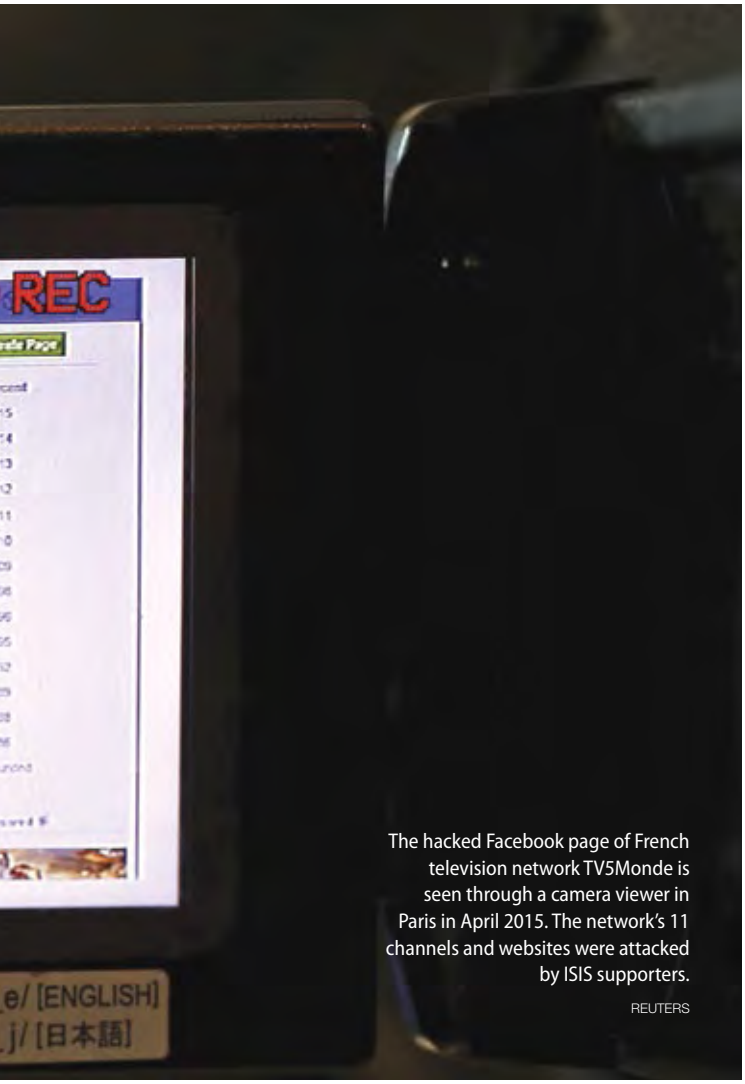
The situation is not so clear if we discuss targets of cyber attacks. For example, banking systems can be attacked for the ordinary purpose of theft, to destabilize the financial system as a whole — as happened several times in South Korea — or to apply political pressure, as was the case with the cyber attacks on PayPal, MasterCard and Visa, all in retaliation for these companies' decisions to block the accounts of WikiLeaks founder Julian Assange in 2010.

We are facing a complex, innovative threat that requires fresh approaches to find solutions. The NCSS is primarily a system of interaction among the main cyber security players, combining intelligence, law enforcement and government agencies that regulate telecommunications and information security. It aims to detect, prevent and suppress cyber threats; reduce the likelihood of their occurrence; and minimize the harm caused by their implementation. This system requires close cooperation with the private sector — telecommunications and Internet service providers, owners and operators of critical information infrastructure objects, and private companies specializing in information security.

The NCSS should be organized not only by classical threat definitions, but also by functionality and should include the following subsystems: an advisory system, responsible for general management, strategic decisions supporting the state's cyber security leadership and coordination of different authorities; and a cyber threat monitoring system, which should combine technical means, computer emergency readiness teams (CERTs),

information from Internet service providers, banking institutions, law enforcement and antivirus companies, and include intelligence data obtained by special services, intelligence agencies and financial monitoring. This information from different sources should be concentrated and processed in a single place, in real-time, for immediate decision-making. Cyber protection of critical information infrastructure facilities should include a set of technical protection measures, personnel security clearances, and counterintelligence protection relating to terrorism and other illegal actions.

Efficiency assessment and decision-making should be considered essential conditions for the NCSS to properly perform. The absence of a single institution responsible for the general coordination of cyber security measures complicates, slows, and in some cases, makes it impossible to take the necessary steps to respond to cyber attacks, especially given their high degree of latency. The main public sector actors in the field of cyber security are the Ministry of Defense, the Ministry of Interior, the State Service for Special Communication and Information Protection, and the Security Service of Ukraine (SSU). Deployment of the NCSS must be accompanied by appropriate adjustments in the process of defense and security sector reform.



The hacked Facebook page of French television network TV5Monde is seen through a camera viewer in Paris in April 2015. The network's 11 channels and websites were attacked by ISIS supporters.

REUTERS

In 2015, Ukraine's Cabinet of Ministers created a draft cyber security law, which will enter the term "cybersecurity" and other terminology that uses the prefix "cyber" into national legislation. It is expected that upon adoption of these amendments, the new law on cyber crime will be developed by the Ministry of Internal Affairs. The new law should significantly improve the institutional capacity of national law enforcement agencies, and the ministry will ensure its final implementation of the Budapest convention. The Ministry of Defense also developed amendments to Ukrainian law on defense that include the issue of cyber security in the military sphere.

There is no doubt that the State Service of Special Communication and Information Protection should be a key element of the NCSS. However, its present functions, determined by law, should be deeply revised to give it cyber defense supervision and control authority over critical facilities infrastructure. Unfortunately, the agency has no authority in this area and is responsible only for government informational resources. However, on a positive note, the Computer Incident Response Team CERT-UA is housed within this unit.

Finally, the (SSU) has recently established a new functional counterintelligence unit to protect state interests in information security. Today, the law gives the SSU sufficient power not only to participate in the NCSS, but to act as its forming element. Thus, the SSU is a law enforcement agency. As the leading agency fighting terrorism, it protects not only national sovereignty, constitutional order and territorial integrity, but also the state's economic, scientific and technical capabilities and citizens' rights. In addition, it is responsible for protecting national information capabilities and the national communication system.

As the state authority, and a specially authorized body in the field of counterintelligence activities, the SSU's objectives include the development and implementation of measures to prevent, eliminate and neutralize any threats to the interests of the state, society and the rights of citizens. This legislative framework already allows the SSU to take comprehensive measures in the area of cyber security.

Ukraine is in the process of developing and institutionalizing a national cyber security system. Adoption of a cyber security strategy is an important step in this process. At the same time, Ukraine is reviewing and revising its cyber security capabilities for national security and defense. In this context, the Ministry of Defense's already-completed defense review might be useful, together with the expertise of international cyber security experts. □