*Information & Security: An International Journal*

Potii, Korneyko, Gorbenko, vol.32, 2015 http://dx.doi.org/10.11610/isij.3201

# CYBERSECURITY IN UKRAINE: PROBLEMS AND PERSPECTIVES

Oleksandr V. POTII, Oleksandr V. KORNEYKO, and Yrii I. GORBENKO

**Abstract:** The paper outlines the challenges and the main cyber threats (such as cybercrime, cyber terrorism, cyber war, vulnerability of the state's information infrastructure, unsatisfactory level of information security) in the Ukrainian cyberspace. Further, a classification of the negative impact of cyberattacks on critical information infrastructure is offered. The authors present Ukraine's cybersecurity strategy and policy, and describe the country's cybersecurity system, legal and regulatory aspects, and related specifics of Ukraine's educational system.

**Keywords:** Cybersecurity strategy, cybersecurity policy, cybersecurity threats, educational system.

## Introduction

A key issue in the context of globalisation of information exchange and the widespread use of information technologies is the protection of information processed by information and telecommunications systems. The characteristics of the cyberspace, the development and implementation of new information and communication technologies provide unlimited opportunities for the accumulation and use of information, and create a fundamental dependence on their proper functioning in all spheres of society and the state. This dependence represents a vulnerable element in the operation of certain facilities and of national critical infrastructure. It enables criminals to undertake unlawful actions in cyberspace by destroying the integrity, availability and confidentiality of information and/or by damaging information resources and telecommunications systems. Of particular concern is the opportunity for benefitting from the advantages of cyberspace in the interest of rogue political and military actors and for organising terrorist and hacker attacks.

In these circumstances, main task of the state is to take measures that to resist unlawful actions in cyberspace, to avoid or mitigate the negative consequences of the materialisation of cyber threats. Thus, cybersecurity has become an important element of the national security construct of any country that may need to defend against inter-

national criminal groups of hackers, IT-proficient criminals, foreign government agencies, terrorist and extremist groups, multinational corporations and financial-industrial groups, and others.

## Challenges and basic cyber threats in the Ukrainian cyberspace

The problem of ensuring cybersecurity in Ukraine has become urgent, in particular due to Russia's aggressive policy. Russia was conducting cyber warfare operations against Ukraine as part of its military incursion into Crimea, the Navy admiral designated to be the next commander of U.S. Cyber Command told Congress on 12 March 2014. Vice Adm. Michael Rogers, then nominee to head Cybercom and the National Security Agency, also said his biggest challenge if he was confirmed for the posts would be dealing with the threat of cyberattacks and penetrations of U.S. computer networks. "We clearly see that there's an ongoing cyber element to the challenges in the Ukraine at the moment," stated the three-star admiral.[1]

A lot of computers of the Ukrainian government, and at least 10 Ukrainian embassies abroad were subjected to dangerous cyberattacks associated with Russia, according to Financial Times.[2] By way of background, embassies of at least nine countries, among those Belgium, China, Germany and Poland, based in Eastern European countries, were also targeted by Russian hackers, who allegedly succeeded in gaining access to secret diplomatic information.

However, it was not only Ukrainian state agencies who suffered from cyberattacks, but also the country's private sector. About a third of all cyberattacks conducted in Ukraine were directed against business websites (30 %), according to Kaspersky Lab. Online media (20 %) and e-commerce (19 %) often become victims of DDoS. For their part, attacks on media portals are a convenient way to get more targeted traffic, which can then be monetised.

The average duration of attacks on .ua domains in the first half of 2012 was 11 hours, the longest being 13 days, 4 hours and 23 minutes, which was directed at the web site of a marketing agency.

Problems in the cybersecurity field in Ukraine are not a secret. Still, it is useful to outline the biggest challenges in the country's cyberspace. According to experts from the Institute for Strategic Research under the President of Ukraine, which in 2011 published an analytical report called "Cybersecurity: Global Trends and Challenges for Ukraine," the government is faced with five major problems with respect to the protection of the Ukrainian cyberspace:[3]

1. There are no Ukrainian governmental documents describing cyber threats to Ukraine, meaning that no state policy in the cybersecurity field exists. An-

other gap is related to the lack of terminological base in cybersecurity, resulting in underperformance of the special police and service units, which are not supported by respective legislation. Only recently the legal framework received proper attention and solutions to the problem are being sought.

2. There are no structures in Ukraine that coordinate the activity of different agencies during investigation of cybercrimes. Thus, cooperation is more at interpersonal level than on system level. Unfortunately, in Ukraine there is no large-scale training on cybersecurity with the involvement of all responsible departments (as, for example, "Cyberstorm" exercise in the USA).
3. Agencies are staffed with unskilled specialists, which is deemed problematic by many heads of relevant structures. The reasons for this are prosaic and include unsatisfactory level of training, the lack of tangible and intangible incentives to remain in the public service. In addition, there are no interdisciplinary research institutes that are engaged in a comprehensive study of the issues of information security.
4. The division of liability on cybersecurity matters among government agencies is not clearly defined.
5. The information and telecommunication network in Ukraine is vulnerable as it vastly uses foreign software products, which are not explored for potential vulnerabilities and holes.

More recently, the draft Ukrainian strategy on cybersecurity already identified the main threats for Ukraine in cyberspace.[4]

*Cybercrime.* Crimes using modern information and communication technologies are becoming more commonplace in the lives of Ukrainian citizens. The new technologies are used not only for committing traditional crimes, but also to commit crimes that are characteristic for an advanced information society. The greatest attention is focused on criminals' attempted violation or unauthorised use of the information and telecommunication systems of government, credit and banking, utilities, defence, industrial sectors. Classified information, circulating in the information and telecommunication systems, is traditionally of interest of other countries, organisations and individuals.

*Cyber terrorism.* Domestic enterprises, institutions and organisations, the malfunction of which constitutes a threat to life and health of citizens, can be potential targets of terrorist acts involving the use of modern information and communication technologies. No smaller threat is committing illegal acts to the detriment of third countries carried out using the information infrastructure of Ukraine.

*Cyber war.* The military sector is undergoing profound changes as a result of the developments in the cyberspace. Most countries in the world are actively transforming their defence potential, and strengthening their capabilities for warfare in the cyberspace and for protection against similar actions of the enemy. Due to the various ways in which information security impacts Ukraine's defence sector, its capabilities are considered as more susceptible to cyber threats. The implementation of modern information technologies forms a separate, cyber sphere of warfare, along with the traditional *land*, *air*, and *maritime* components. An appropriate level of defence capabilities means that there are units able to provide cyber defence.

*Vulnerability of the information infrastructure of the state.* Recently, information resources of financial institutions, transport and utilities companies, state agencies that provide security, defence and respond to emergencies, official websites and email servers have become frequent victims of cyberattacks and cybercrime. The sharp increase in the number of recorded cases of cyberattacks against government information resources reveals a change-of-victim pattern in hackers' operations. In addition to that, the spread of politically motivated activity of cybercrime groups that carry out attacks on government and private websites leads to violation of information resources, as well as the reputation and financial losses.

*The unsatisfactory level of information security in the event of state control.* This may affect the sustainable functioning of critical information infrastructure, lower the defence capacity of the state, inject economic, financial and political instability, weaken the image and attractiveness of investment, etc.

The results of the risk analysis above are taken into account in the process of drawing government regulations. One example is taking into consideration potential negative impact of cyberattacks on critical information infrastructure[5] in the following fields and/or systems:

- environmental safety (technogenic emergencies);
- energy security;
- economic security;
- national defence, national security, and the public order;
- system of governance;
- socio-political situation in the country;
- image of the state;
- financial system;
- operation of transport infrastructure;

- operation of information and communications infrastructure of the state, including its interaction with the infrastructure of other countries.

## Framework of Ukrainian's cybersecurity policy and strategy

Evolving challenges and threats made it necessary to develop a public policy in the field of cybersecurity. Towards that effect, in 2012-2013 the Parliament proposed amendments to some laws of Ukraine. However, the new political and economic reality demanded more comprehensive solutions from the country's leadership. At the end of 2013 and in the beginning of 2014, a number of draft documents were elaborated that are currently under discussion. These include: Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine,"[6] Presidential Decree "Strategy for ensuring cybersecurity of Ukraine," Resolution of the Cabinet of Ministers of Ukraine "On approval of the agenda for protection of state information resources from unlawful interference in their activities."[7]

The main objectives of the cybersecurity strategy of Ukraine are:[8]

- to identify the main approaches for designing and executing public policy in the field of cybersecurity;
- to build the basis for a legal framework in the field of cybersecurity that is consistent with international standards;
- to create a modern national system of cybersecurity;
- to create conditions for cooperation among the public and private sector, citizens, society and the state in countering cyber threats, as well as for effective international cooperation in the area of cybersecurity;
- to ensure cybersecurity of critical information infrastructure facilities;
- to create an environment for the development of education and training in the field of cybersecurity.

Cybersecurity is to be pursued in line with the following principles:[9]

- rule of law, legality and respect for human rights and freedoms;
- integrated approach to the implementation of legal, institutional, technical and informational measures;
- priority of prevention;
- inevitability of responsibility for committing cybercrimes and offenses;
- ensuring the restoration of violated rights and legitimate interests, and damages caused by cybercrime;
- cooperation between the state and the private sector with the participation of civil society in ensuring cybersecurity;

- ensuring cybersecurity for protecting critical information infrastructure;
- effective, comprehensive and consistent measures to protect information and information resources in cyberspace;
- uninterrupted state control on information security at critical information infrastructure sites;
- cooperation at international level for effective mutual assistance in countering cyber threats.

The draft Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine" defines the basic directions of state policy in the field of cybersecurity,[10] as presented in Figure 1.

Creating a secure national segment of cyberspace will help maintain an open society and ensure safe use of the cyberspace by the community. An important measure in this regard is to define mandatory requirements for critical information infrastructure facilities, protection of personal data, control for the protection of information circulating at such sites. It is necessary to develop a list of assets of critical information infrastructure, which include elements that are essential to the national security and defence of Ukraine. These objects urgently need to be protected against cyberattacks. Further, the efficient operations of cybersecurity and information security units must be ensured. In addition to that, effective measures to reduce the risk of threats to information and ensure security and protection of state information resources in information, telecommunication, and information and telecommunication systems must be taken.


**Figure 1: Basic directions of Ukraine's state policy in the field of cybersecurity.**

Public administration-related improvements in the field of cybersecurity are considered as a basis for effective prevention of interference in the internal affairs of Ukraine and neutralising attacks on its information resources from other states. Strengthening cybersecurity will also promote the development of Ukrainian innovative products and create conditions for a faster economic development.

Improving the state's defence capabilities in the cyberspace might result in greater effectiveness of the Armed Forces of Ukraine, allowing them to provide an adequate response to real and potential cyber threats to Ukraine. To this purpose, the Armed Forces of Ukraine must be prepared to counter acts of aggression in the cyberspace, to protect military information infrastructure against real and potential cyber threats. It is important to support the existing multilateral training on defending against cyberattacks on public and private infrastructure, and to initiate new types of exercises. This will develop a network of teams responding to computer emergencies (CERTs). Another objective is to strengthen the coordination within the defence and security sector of Ukraine to combat cyber threats, strengthen the technical and technological capabilities of the state, and increase scientific and human potential of public bodies that perform the functions related to ensuring the safety of cyberspace in Ukraine. A system for training in the field of cybersecurity for the Armed Forces of Ukraine and other structures from the defence and security sector of Ukraine is also needed.

There are three main reasons for the failure of the fight against cybercrime and cyber terrorism in Ukraine. Firstly, there are no established definitions of key terms and concepts ("cyberspace," "cybersecurity," "cyber attack," "cyber war," "cyber terrorism") that can be effectively applied in practice by the law enforcement agencies. Secondly, the current legal framework in the field of cybersecurity is either underdeveloped or needs to be updated. Thirdly, there is no unified national system for protection against cybercrime with appropriate legal backing.

To solve these problems it is necessary to improve the regulatory and legal framework in the field of cybersecurity, in particular to ensure the implementation of the Convention on Cybercrime, ratified by Ukraine on 7 September 2005, by incorporating it into national legislation, to improve criminal law to include separate clauses, where the object of unlawful behaviour are elements of critical information infrastructure. In operational terms, it is also important to carry out constant monitoring of the cyberspace in provide for timely detection, prevention and neutralisation of cyber threats, as well as to increase the level of international cooperation on issues related to cybercrime and cyber terrorism.

An important activity is to reduce the vulnerability of objects of critical information infrastructure. One of the main tasks in this area is to ensure the protection of critical

information infrastructure against incidents and unlawful acts in the cyber domain. Strict compliance should be ensured with the legal requirements for the protection of state information resources, using cryptographic and technical means of protection of information, including personal data protection.

As regards international cooperation, it is important to ensure full and active participation of Ukraine in the European and regional cybersecurity systems. This will increase the role of Ukraine in the formation of global policies on cyberspace protection and in supporting international initiatives in the field of cybersecurity, taking into account the national interests of Ukraine. Government activities should be in line with assumed international obligations in the field of cybersecurity, and aim to promote prevention of the militarisation of cyberspace, facilitating the creation of international rules of conduct of States in cyberspace and improving the international legal framework in accordance with challenges to national and international security.

## Cybersecurity system of Ukraine (organisational arrangements at national level)

The cybersecurity system of Ukraine includes the following military and law enforcement agencies (Figure 2): State Service of Special Communication and Information Protection of Ukraine (SSSCIP), Security Service of Ukraine, Ministry of Internal Affairs of Ukraine, Ministry of Defence of Ukraine (more specifically, the Defence Intelligence), and Foreign Intelligence Service.

*The State Service of Special Communication and Information Protection of Ukraine (SSSCIP)* is the only institution in Ukraine, which specifically deals with issues of cybersecurity. It participates in the formulation and implementation of the state policy in the sphere of protection of state information resources, cryptographic and technical protection of information.


**Figure 2: Organisation of the cybersecurity system of Ukraine**

SSSCIP's activity is legally framed by:[11]

- Law of Ukraine "On State Service of Special Communication and Information Protection of Ukraine";
- Decree of the President of Ukraine № 717 of 30 June 2011 "On the Administration of State Service of Special Communication and Information Protection of Ukraine";
- Decree of the Cabinet of Ministers of Ukraine № 1772 of 16 November 2002 "On approval of an order of cooperation of the Executive Authorities on how to protect information of state information resources in information and telecommunication systems";
- Decree of the Cabinet of Ministers of Ukraine № 688 of 03 August 2005 "On approval of the Registry information, telecommunication and information and telecommunication systems of executive, and enterprises, institutions and organisations that belong to their jurisdiction";
- Decree of the Cabinet of Ministers of Ukraine № 373 of 29 March 2006 "On approval of the Rules of providing information protection in information, telecommunication and information telecommunication systems";
- Orders of the Administration of State service of special communication and information protection of Ukraine.

The main domains of the SSSCIP include:

- determining the level of protection of information and telecommunication authorities' systems;
- unified antivirus protection system;
- international cooperation in the protection of information resources;
- interaction with state authorities;
- protection of state information resources;
- interaction with the administration domain .UA.

With respect to cybersecurity the SSSCIP includes the following bodies: the Department of Special Information Telecommunication Systems, the State Centre of Protection of Information-Telecommunication Systems, and the State Enterprise "Ukrainian Special Systems." The following units are also part of the Service: Cybernetic Protection System, Registry of Information and Telecommunication Authorities' Systems, Centre of Antivirus Information Protection (CAIP), Assessment of Protection of State Information Resources, Computer Emergency Response Team of Ukraine (CERT-UA).

The State Enterprise "Ukrainian Special Systems" acts as the National Confidential Communication System operator. The National Confidential Communication System (NCCS) was established in 2006 to secure communication among governmental authorities of Ukraine. The NCCS supports the following basic services: videoconference, e-document, web portal for state authorities, antivirus information protection, key certification, secure telephone communication.

Service units such as CERT-UA and CAIP deserve special attention.

CAIP addresses the viruses that threaten the state information resources. One of the basic tasks of CAIP is the introduction of a unified system for antivirus protection of state information resources in ITS. Modern system for information security cannot function without reliable antivirus software. Thus, CAIP examines antivirus program facilities with the aim of determining the possibility for their application in Ukraine, and carries out express examination of antivirus updates. As of today, 450 security administrators of ITS of state authorities are connected to CAIP's web server for receiving antivirus updates. However, in Ukraine the lack of a national project to implement a common antivirus programme is considered a serious gap.

For its part, CERT-UA is responsible for the international cooperation in addressing the cyber threats. The main tasks of CERT-UA are:

- prevention, detection and elimination of the consequences of unauthorised actions against the state's information resources and information and telecommunication systems;
- study and analysis of computer incidents;
- investigation and elimination of cyber threats;
- consulting and methodological assistance in the protection of state information resources;
- cooperation with international organisations to respond to unauthorised actions (for example, with the Forum for Incident Response Team Security – FIRST).

The main types of cyber threats, addressed by CERT-UA are:

- malware (lock information output system failure, cyber espionage, unauthorised transfer of funds);
- botnets;
- Internet fraud (fishing, wishing, etc.);
- DDoS-attacks;
- exploitation of vulnerabilities in software and hardware;
- unauthorised access to information systems, web resources and violation of the irregular mode of operation.

The main clients of CERT-UA's services are: state authorities, local authorities, military units, state enterprises, institutions and organisations, concerning state information resources. CERT-UA provides alerts and warnings, incident handling, incident analysis, incident response support, incident response coordination, announcements, and security consulting.

CERT-UA cooperates with partners from more than 30 countries in the world and is full member of FIRST (Forum of Incidents Response Security Teams, www.first.org). CERT-UA is registered as a "listed" team in TI (Trusted Introducer, www.trusted-introducer.nl). For example, in 2013 CERT-UA has cooperated with foreign teams from Australia, Austria, Belgium, Canada, China, Denmark, Estonia, Finland, France, Germany, Holland, Hungary, India, Israel, Italy, Japan, Korea, Lithuania, Malaysia, Norway, Pakistan, Poland, Portugal, Romania, Russia, Saudi Arabia, Spain, Taiwan, Turkey, the USA, and others within the CERT framework, processed 232 reports for incidents from foreign CERTs and sent 140 messages to Ukrainian and 92 notifications to foreign Internet service providers to stop the spread of malicious software.

Among the units of the *Ministry of Defence of Ukraine* with responsibilities in ensuring cybersecurity are the Electronic Warfare Troops, specialists from the Main Intelligence Directorate (MID) and the Central Office of Information Security and Cryptology of the Joint Staff. The Electronic Warfare Troops are responsible for the C2 systems' security, for carrying out deliberate electronic jamming of enemy communications, as well as for disrupting the management of enemy information systems. MID experts are involved in the implementation of special measures to ensure the national interests in the information sphere. These may include intelligence activities, information espionage, and investigative measures. The tasks of the General Intelligence and the Foreign Intelligence Service in the field of cybersecurity of the country are classified.

Operative and search work is the responsibility of law enforcement agencies such as the *Ministry of the Interior and the Security Service of Ukraine*.[12] In the structure of the Ministry of Interior of Ukraine there is a special unit – the *Office for the Fight against Cybercrime*. The main task of the Office is "organisational and practical support for the implementation of the state policy on the prevention of and countering crimes and offenses committed with the use of information technology and telecommunications networks." The unit directs the fight against fiscal fraud on the web (e.g. fraud with bank cards and accounts), and the struggle against various forms of xenophobia.

The Security Service of Ukraine has a department for counterintelligence protection of the interests of the state in the field of information security (www.sbu.gov.ua). The legal basis for the unit's establishment is Decree № 34 of the President of Ukraine of

25 January 2012 "to promote the concentration of forces and resources, optimisation of administrative activity in the task of protecting the legitimate interests of the state and the rights of citizens in the information field of intelligence and subversive activities of foreign intelligence services, illegal encroachments by organised groups and individuals." The department's work is kept secret, but one can indirectly measure its success by the number of news pieces on the neutralisation of hacker groups and "telephone terrorists."

Despite gaps in the legislative and administrative spheres, the structures to protect Ukraine's cyberspace have been established. The initiative for adopting a special law on cybersecurity demonstrates the will of the state to form a strong basis to protect its systems from cyberattacks. The next step is to create a unified system of cyber defence, bringing together the work of the various agencies and departments, spearheading the state policy in the field of cybersecurity.

The draft Ukrainian strategy for cybersecurity is aimed at establishing a national cybersecurity system (see Figure 3). The main objectives of the system would be: formulation and implementation of the state policy in the field of cybersecurity; monitoring of cyberspace in order to identify, prevent and neutralise cyber threats; identification, prevention and stopping of cybercrime; and provision of cyber defence of critical information infrastructure.

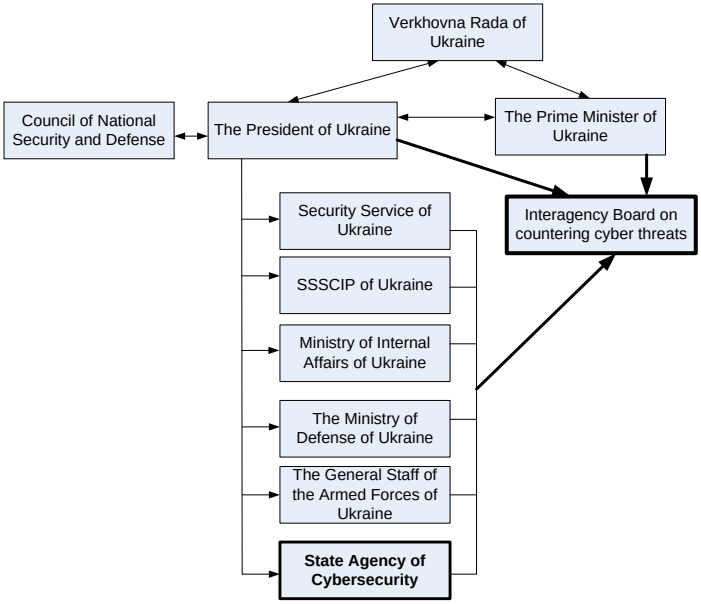


**Figure 3: Proposed organisation of Ukraine's system for cybersecurity**

The figure visualises the structure of the prospective national system for cybersecurity. Notably, the establishment of an Interagency Board to develop proposals for correcting the internal and external policies of cybersecurity has been proposed. The President would lead the college, while the Prime Minister and the heads of other departments would sit on the board as members.

A State Agency for Cybersecurity would further be created to coordinate the actions of the relevant actors in Ukraine. It is planned that the agency would carry out the following tasks: organise the interaction of relevant actors; keep a register of assets of critical information infrastructure; analyse the international cybersecurity landscape and external threats to cybersecurity; conduct exercises and training in the field of cybersecurity; international cooperation, and so on.

Some practical steps have already been taken for the establishment of a unified system for the fight against cybercrime. In principle, such a system may include the following functional elements: a national system for monitoring and responding to threats in cyberspace (rapid identification of an attacker and localisation); a system to prevent threats and vulnerabilities in cyberspace; a system for investigating cybercrime; and a national system for protection of critical information infrastructure.

On 12 October 2014, SSSCIP established a task force for responding to computer incidents in order to prevent information security breaches. The coordinating centre includes representatives of the SSSCIP, the Security Service of Ukraine, the Ministry of Interior, the Foreign Intelligence Service, the Ministry of Defence, the General Staff of the Armed Forces of Ukraine, the Prosecutor General's Office and the National Commission of state regulation in the field of communication and information. In addition, the task force will be joined by representatives of the leading telecommunications operators and service providers, as well as non-governmental organisations such as ISACA. The objectives of the task force are to speed-test computer incidents; to report the information to CERT-UA; to coordinate forces and means to prevent violations of information security in information and telecommunication systems; to discuss and develop effective mechanisms for cybersecurity expert advice for companies and organisations. The task force has also to inform the public about hacker attacks and eliminate them. The creation of this task force is the first step towards the creation of a national centre for cyber defence and for countering cyber threats.

## Features of national organisation, regulatory framework, and terminology in the field of cybersecurity

The Ukrainian legal framework for counteracting crime in cyberspace only partially meets the needs of the moment, as it does not always cover key elements needed to achieve effectiveness. Today in Ukraine there is a number of laws and other acts at

different levels, covering the problem of cybersecurity, in particular the Laws of Ukraine "On State Service for Special Communication and Information Protection of Ukraine," "On Information," "On State Secrets," "On Data Protection in Information and Telecommunication Systems," "On the National Security of Ukraine." In addition to that, there are two strategic documents relevant to the cybersecurity domain: the National Security Strategy of Ukraine and the Information Security Doctrine of Ukraine. Furthermore, the Parliament of Ukraine ratified the Convention on Cybercrime. Accordingly, the current Criminal Code of Ukraine stipulates responsibilities for crimes using "computers (PCs), systems and computer networks and telecommunications" (Section XVI, articles 361-363).

Urged by internal and external aggression, the strengthening of the legal framework for cybersecurity has become even more important. As noted earlier in the text, in the last months, Presidential decrees "Strategy for ensuring cybersecurity of Ukraine" and "On some measures for the protection of state information resources in information and telecommunication systems," draft Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine" and Resolution of the Cabinet of Ministers of Ukraine "On approval of the agenda for protection of state information resources from unlawful interference in their activities" have been developed. Certain provisions of these documents have been discussed previously in this paper.

Overall, the national legislation must include:[13]

- concepts and categories of cybersecurity;
- threats to cybersecurity;
- decision-making and separation of powers in cybersecurity;
- criteria for classification of objects of critical information infrastructure, and a list of the above mentioned objects;
- authority of government agencies to take measures to counter cyber threats against such objects;
- mechanisms for public-private partnership in ensuring cybersecurity.

At the level of law, it is necessary to provide a system to prevent cybercrime and increase public awareness of specific forms of cybercrime. The legislation should be the basis for the establishment of a unified national system against cybercrime.

Currently a common view on the concept of cybersecurity begins to take shape in Ukraine. It considers services and systems provided over the Internet that should also be properly secured. The focus has shifted to the socio-economic sphere and has gone beyond the traditional sphere of information security. Today, it has also become important to provide reliable services to the user at the household level, small and medium-sized businesses, and to secure the national critical infrastructure and public

administration against cyberattacks. This, in the authors' opinion, is the main goal of cybersecurity.

Cybersecurity is ultimately the task of ensuring the confidentiality, availability, and integrity in a separate area of interest – in the space of information systems integrated via Internet. The cyber domain is highly vulnerable to attack and thus needs uninterrupted protection. This means that along with the classical means for information protection, more attention should be given to active elements for protection, such as intrusion detection systems, security incident management systems, security restore systems, intelligent control systems, and others.

Cybersecurity is considered from two points of view. First, from the perspective of the state, it represents the capability to protect important interests (rights) of the citizen, society and the nation in the cyberspace. Another perspective sees cybersecurity or cyber protection as a set of organisational, legal, military and technical controls (actions), aimed at guaranteeing cybersecurity.

Cyberspace is an environment formed as a result of the interface of information and telecommunication systems and networks. The critical information infrastructure is an element of the cyberspace and includes critical information and telecommunication systems, automated C2 system and other systems. If the functioning of these systems is violated, the national security and capability to defend may be threatened. A set of threats exists for the critical infrastructure and, consequently, for cyberspace. Broadly taken, cyber threats are events and factors that threaten cybersecurity.

Cybercrime is an unsafe action into cyberspace. For its part, cyber terrorism is a terrorist activity, which takes place in cyberspace or uses cyberspace (for example, information systems or Internet).

Cybercrime and cyber terrorism are put into practice by cyberattacks. A cyber attack is an unauthorised action that is realised with the help of information technology and aimed at the confidentially, integrity and accessibility of information, the functioning of critical information infrastructure, or information systems. A cyber incident is considered to be an extraordinary event which represents an attempt to realise or the realisation of a cyber attack.

Countries have different interests in the national segment of the cyberspace. To defend their interests, countries will implement their policy in their respective national segment of cyberspace by realising various activities, which may involve the use of armed forces, paramilitary forces and/or special services. From a Ukrainian point of view, cyber war is an action of foreign armed forces, paramilitaries or special services in cyberspace directed against the national interest of Ukraine. To defend its national interests Ukraine is constructing a system of cyber defence. Cyber defence is a set of

political, economic, social, military, scientific, information, legal, and organisational measures directed towards defending the information sovereignty of Ukraine. This requires a comprehensive approach to be taken by government agencies, the private sector and the civil society. For examples, special structures and forces to ensure readiness in the national segment of cyberspace should be formed, and assets should be allocated to provide response to cyber threats and cyber incidents.

## Ukrainian educational system in the cybersecurity

Cybersecurity is an integral part of the national security, which is dependent on many factors, including the human factor. The human is the main carrier and user of information, becoming the subject and object of information warfare. Therefore, the security of information resources depends on:

- the public awareness of the cybersecurity issues of individuals, society and the state;
- the level of specialised training of state and military leadership, of armed forces and special services personnel;
- the level of training of civilian and military experts.

The inadequate training, the lack of information about new threats in cyberspace, and the misunderstanding of the use of new technologies represent threats to cybersecurity in Ukraine. Another threat is the low level of security culture of the population. Ukraine is also part of the trend for an increasing use of electronic devices and services by households, but there is little knowledge about threats in cyberspace.

Thus, the issue of forming a new system for training is topical and timely for Ukraine. According to the authors, one of the possible answers to the cybersecurity challenges is the transformation of the education system in the field of information security and cybersecurity.

Accordingly, the main goals of the transformation should be to provide training of highly qualified specialists and to build cybersecurity culture among Ukrainians, understanding the threats of cybersecurity and the consequences of their occurrence. Achieving these objectives will allow Ukraine to modernise its education system in the field of cybersecurity to meet new challenges. Hence, the role of educational and scientific research in the field of information security is very important.

The education system in the field of cybersecurity should be tasked to:

- develop and coordinate research work in the field of cybersecurity;
- create favourable conditions for young professionals in the field of information technology and facilitate their employment in Ukraine;

- amend the curriculum and programmes of secondary and higher education, training of scientific and pedagogical staff;
- strengthen state support for major areas of science and technology as the basis for the creation of advanced information technologies;
- develop national programmes to improve public awareness of cyber threats;
- support the efforts of civil society and business to increase public awareness on pressing cyber threats;
- provide continuous training of civil servants and employees involved in key critical infrastructures.

In addition, the education system should be transformed in the context of the Bologna process and the requirements of the new Law on Higher Education.

In the USSR training of specialists on information security was carried out by military and special educational institutions. Programmers, radio engineers, mathematicians who graduated from these institutions were engaged in security of government communication, technical and cryptographic information security, counteraction to foreign intelligence technical services. After Ukraine achieved independence, a national system for training specialists in the field of information security was organised and powerful research teams were created. High-quality training centres were set up in Kyyiv, Kharkiv and Lviv.

The authors suggest that the future structure for training in cybersecurity in Ukraine involve:

- training of civilian experts in the field of information security and cybersecurity (IT-sector, banking, critical infrastructure);
- training of military experts and experts for special services (cyber war, fight against cybercrime and cyber terrorism);
- special training and advanced training staff of public administration and the government;
- training Ukrainian citizens and their adaptation for life in the modern information space.

Training should be carried by experts from three areas of expertise:

- technical experts in security and military science (information security, cybersecurity and so on);
- technical experts in engineering (computer science, software engineering, computer engineering and so on);
- experts in the social sciences, business and law.

Three groups of standards of higher education have been under development for training.

The first group are standards of higher education 1701 "Information Security."[14] This knowledge sphere includes three areas of training and five specialties (see Table 1). Training is carried out at the level of bachelor and masters' degrees.

The second group are standards of higher education related to the 1701 "Information Security" standard. Some of these standards include:

- 0501 "Informatics and Computer Science (Computer Science, Computer engineering, software engineering);"
- 0502 "Automation and Control (Systems Engineering);"
- 0509 "Radio, Radio and Communication Devices (Radio, Telecommunications);" and
- 0403 "System Sciences and Cybernetics (Computer Science, Applied Mathematics, Cryptology)."

The third group are standards of higher education in areas of social sciences, business and law:

- 0302 "International Relations (International Relations, International Information);"
- 0303 "Journalism and Information (Journalism, Advertising, Public relations);"
- 0304 "Law;"

**Table 1: Standards of higher education 1701 "Information Security."**

| ***Bachelor*** | ***Master*** |
|---|---|
| 6.170101 Security of information and communication systems | 7.17010101 Security of information and communication systems<br>7.17010102 Security of the state information resources |
| 6.170102 Systems of technical information security | 7.17010201 Systems of technical information security and Automation of its processing |
| 6.170103 Information Security Management | 7.17010301 Information Security Management<br>7.17010302 Administrative management in the sphere of information security |

- 0301 “Social and Political Sciences (Sociology, Practical Psychology, Political Science);”
- 0201 “Culture (Documentation and Information);” and
- 1601 “Military Science, National Security” and others;

The eighteen Ukrainian universities carry out training of specialists in the field of information security.[15] The number of universities which train experts in different specialties and at different levels is given in Table 2.

**Table 2: Training of specialists in the field of information security in Ukraine.**

| *Specialties* | *Bachelor* | *Master* |
|---|---|---|
| 170101 Security of information and communication systems | 18 | 12 |
| 170102 Systems of technical information security | 17 | 12 |
| 170103 Information Security Management | 12 | 4 |
| 17010302 Administrative management in the sphere of information security | - | 4 |
| 17010102 Security of the state information resources | - | 1 |

The subjects taught in the Information Security in Computer Systems training programme are given in Table 3.

**Table 3: Subjects taught in the Information Security in Computer Systems training programme.**

| *Subject* | *ECTS* |
|---|---|
| Higher Mathematics | 19 |
| Physics | 10 |
| Information Technology | 4 |
| Operating Systems | 4,5 |
| Architecture of Computer Systems | 3 |
| Applied Cryptology | 8,5 |
| Technical information security systems | 4,5 |
| Fundamentals of circuit theory, signals and processes in electronics | 4 |
| Information Security Management | 3,5 |
| Data protection in information-communication systems | 12,5 |
| Programming Technologies | 13 |
| Integrated security solutions: design, implementation and maintenance | 11 |
| Design of information security | 5 |

The analysis of the training programs and the learning outcomes allows the authors to make the following conclusions:

1. Education in Ukraine is primarily aimed at creating technical specialists in the fields of information security and cryptography.
2. Basic special educational disciplines provide technical skills and do not consider such skills as leadership, resource management, human resources, business processes, risks, etc.
3. The attention given to information security management skills is not sufficient.

The industrial base for the production of national information security tools has been developed. There have been good results in the development of technical and cryptographic protection in Ukraine. National cryptographic standards have been developed.

Ukraine has significant achievements in postgraduate education: philosophy doctor and doctor of science theses (see Table 4). The main scientific schools preparing information security staff are in Kyiv, Kharkiv and Lviv.

The students' competitions in the field of information security are carried out every year to support advanced training of students. High level is demonstrated by students from the Kharkiv National University of Radio Electronics, the National Technical University of Ukraine "KPI," the Institute of Special Communication and Security Information, the Karazin Kharkiv National University. After leaving university graduates are ready to work at various positions (see Table 5).

**Table 4: Achievements in Ukraine in developing postgraduate education.**

| *Code* | *Science area, group of specialties, specialty* | *Science area* |
|---|---|---|
| 05.13.21 | System of Information Security. The theoretical, scientific, technical and technological issues related to organisation, creation of methods and tools to protect information during its storage, processing and transmission using modern mathematical methods, information technology and facilities.[16] | Technical sciences |
| 21.05.01 | Information security of the state. Information security state – the branch of science that studies the problem of information security of national interests of Ukraine, studying and justifying forms and methods of protection of the individual, society and the state from external and internal threats in the information sphere, as well as ways to improve the efficiency of information systems in modern conditions.[17] | Technical sciences |

**Table 5: First employment of information security graduates.**

| *Bachelor* | *Qualification* | *First positions* |
|---|---|---|
| 6.170101 Security of information and communication systems | Specialist in information security in information and telecommunication systems | Inspector<br>Specialist of public service |
| 6.170102 Systems of technical information security | Specialist in technical information security. | Engineer<br>Specialist of public service<br>Specialist of technical expertise<br>Operator of radio engineering control<br>Inspector of telecommunication |
| 6.170103 Information Security Management | Expert in the organisation of information security | Expert in the information security organisation with limited access<br>Specialist in a privacy mode<br>Specialist in supervision and protection<br>Specialist on the organisation of information security |

Finally, some problems in the cybersecurity education in Ukraine should be noted, namely:

- insufficient and delayed training of teaching staff, supporting the educational process;
- insufficient level of modernisation of teaching and laboratory facilities in universities;
- insufficient involvement in the course of training (re-training) on information security of civil servants;
- insufficient level of cooperation among ministries and agencies for training specialists in information security; and
- excessive commercialisation of the courses in information security.

## Conclusion

The priorities in the field of cybersecurity in Ukraine could be summarised as follows:

1. Raising public awareness and improving the culture of cybersecurity of Ukrainian citizens. Building a culture of human security is a very important task. Citizens

should be aware of the risks of using e-services. They need to know the minimum security requirements. They must be able to act in emergency situations. Public awareness of cyber threats is an important element of cybersecurity.

2. Development and implementation in the national industrial base of national cryptographic standards. Powerful industrial base systems and information protection are important elements of national security. Another important area is the development of national standardisation of encryption. Ukraine has already developed a national standard for block encryption and digital signature. Standards for stream encryption and hashing functions were also developed. National cryptographic standards are an element of assurance of cryptographic security systems. National production of cryptographic protection reduces security risks.

3. Ensuring cloud technologies' security. Cloud technologies are widely used in business and public life. But they are also sources of new threats to confidentiality and privacy. Cloud technologies' security is one of the priorities in protecting the cyberspace.

4. Harmonisation with international and European standards in the field of information security. Ukraine has clearly defined the motion vector of integration with the European Union. It is necessary to analyse the state of standardisation of the EU in the field of cybersecurity. Harmonisation with European standards is an important task. It will help integrate the Ukrainian market of e-services with the EU and eliminate technical barriers in trade.

5. The development of a national public key infrastructure (PKI) and the creation of a national infrastructure for trusted e-services face a number of challenges. Some of those are related to the practical use of PKI – unification, standardisation, interoperability, scalability, guaranteed cryptographic strength. The task of creating infrastructure for trusted e-services is interrelated with the PKI and aims to provide digital signature, digital stamp, authentication websites, and electronic document delivery. For its part, the PKI would provide integrity, non-repudiation and confidentiality of electronic documents. It is necessary to clarify the concept of electronic identification, analyse the state of standardisation and experience from implementing electronic identification in the EU.

6. The main issues related to the accessibility of national critical information infrastructure are: 1) to protect it against unauthorised access; 2) to ensure availability for authorised users. This service is particularly important in terms of cybersecurity. The information disseminated by Snowden and recent developments in Ukraine show that the protection against unauthorised access and unauthorised data entry deserve extraordinary attention. Technologically developed countries allocate considerable re-

sources to solving such problems. Privacy is also ensured by the protection against unauthorised access to information and resources.

## Notes:

[1] Bill Gertz, "Inside the Ring: Cybercom's Michael Rogers confirms Russia conducted cyberattacks against Ukraine," *The Washington Times*, 12 March 2014, www.washingtontimes.com/news/2014/mar/12/inside-the-ring-cybercoms-michael-rogers-confirms-/?page=all.

[2] Sam Jones, "Ukraine PM's office hit by cyber attack linked to Russia," *Financial Times*, 7 August 2014, www.ft.com/intl/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0. html

[3] Dmytro V. Dubov and Mykola A. Ozgevan, "Cybersecurity: the World Tendencies and Challenge for Ukraine," (NISR, 2011); Dmytro V. Dubov, "Strategic Aspects of Ukrainian Cybersecurity," *The Strategy Priorities* 29, no. 4 (2013): 119-126.

[4] "Cybersecurity strategy of Ukraine," draft, accessed on 15 October 2014, available at: www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf, and "Cybersecurity strategy of Ukraine," draft, accessed on 15 October 2014, available at: http://cst.org.ua/docs/lipen-OUT/strategiya_kiberbezpeku.pdf.

[5] Order of the Cabinet of Ministers of Ukraine p. № 1135-r Kyiv, "On the Action Plan for the protection of state information resources," 5 November 2014, accessed 10 November 2014, available at: www.rada.gov.ua.

[6] Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine," draft, accessed 4 June 2013, available at: w1.c1.rada.gov.ua/pls/, and Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine," draft, accessed 17 September 2014, available at: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article.

[7] Order of the Cabinet of Ministers of Ukraine p. № 1135-r Kyiv, "On the Action Plan for the protection of state information resources," 5 November 2014, accessed 10 November 2014, available at: www.rada.gov.ua.

[8] "Cybersecurity strategy of Ukraine," draft, accessed on 15 October 2014, available at: www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf, and "Cybersecurity strategy of Ukraine," draft, accessed on 15 October 2014, available at: http://cst.org.ua/docs/lipen-OUT/strategiya_kiberbezpeku.pdf.

[9] Ibid.

[10] Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine," draft, accessed on 4 June 2013, available at: w1.c1.rada.gov.ua/pls/, and Law of Ukraine "On the basic principles to ensure cybersecurity of Ukraine," draft, accessed 17 September 2014, available at: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article.

[11] Oleksandr Korneyko, "State Service of Special Communication and Information Protection of Ukraine – a key factor in the protection of public electronic information resources in Ukrainian cyberspace," Presentation at international conference "Cybersecurty-2013," Yalta, Ukraine, e-mail message to author, 2 October 2014.

[12] Website of the Ministry of the Interior of Ukraine, accessed on 10 September 2014. http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754.

[13] Dubov and Ozgevan, "Cybersecurity: the World Tendencies and Challenge for Ukraine."

[14] List of public higher education institutions licensed in the areas of 1601, 1701 in the field of knowledge "Information Security," accessed on 15 November 2014, http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article.

[15] Standards of higher education 1701 "Information Security," accessed on 10 Nov. 2014, http://iszzi.kpi.ua/index.php/ua/biblioteka/normativno-pravova-baza/nmk-informatsijna-bezpeka.html.

[16] Passport of specialty 05.13.21 System of Information Security, accessed 15 November 2014, http://search.ligazakon.ua/l_doc2.nsf/link1/MUS969.html.

[17] Passport of specialty 21.05 Information security of the state, accessed 15 November 2014, http://search.ligazakon.ua/l_doc2.nsf/link1/MUS969.html.

Oleksandr V. POTII is colonel, Doctor of Technical Science, Professor of Department of information systems and technologies security of V. N. Karazin Kharkiv National University. He graduated from the Kharkov Higher Military School of Rocket Forces as an Engineer in Radioelectronics in 1993. In 1996, he received a PhD degree in Automatic Control Systems for Armed Forces. In 2008, he was awarded a doctoral degree in Information Security Systems. He has published more than 90 articles dealing with issues of information security, cryptography, PKI and e-services. He took part in the development of national standards and legal documents related to information security. He is a guest lecturer at the Kharkiv National Aerospace University and Kharkiv National University of Radioelectronics.

Oleksandr V. KORNEIKO, Major-general, Ph.D., Professor of Department of Cybersecurity of National Technical University of Ukraine "Kiev Polytechnic Institute" is First Deputy Chair of the State Service of Special Communication and Information Protection of Ukraine. In 1982 he graduated with honours from the Kyiv Military Institute for Communications Engineering and received a degree in the field of Electric Wire Connection. In 2000, he got his Ph.D. degree in Military Cybernetic, Control Systems and Telecommunications. He has authored over 130 scientific and educational works on the theory of telecommunications, special communications, cryptographic and technical protection of information. From January 2007 to May 2012 Oleksandr Korneiko worked as Deputy Head for Academic Affairs of the Institute of Special Communication and Information Protection of National Technical University of Ukraine "KPI," the educational institution of the State Service of Special Communication and Information Protection of Ukraine. On May 2012, by Presidential decree he was appointed Deputy Chair of the State Service of Special Communication and Information Protection of Ukraine.

Yurii GORBENKO received a master's degree at the Department of Information Technology Security of Kharkiv National University of Radio Electronics in 2003. He is technical director of the Private Enterprise Institute of Information Technology. Mr. Gorbenko is candidate of technical sciences in the field of information security systems. He has authored four books and over 40 articles. Mr. Gorbenko has experience as scientific director of 30 research projects.

## Bibliography

Cybersecurity strategy of Ukraine In draft., 2014.

Dubov, Dmytro V., and Mykola A. Ozgevan. Cybersecurity: the World Tendencies and Challenge for Ukraine. NISR, 2011.

Dubov, Dmytro V.. "Strategic Aspects of Ukrainian Cybersecurity." The Strategy Priorities 29, no. 4 (2013): 119-126.

Gertz, Bill. "Inside the Ring: Cybercom's Michael Rogers confirms Russia conducted cyber-attacks against Ukraine." The Washington Times (2014).

Jones, Sam. "Ukraine PM's office hit by cyber attack linked to Russia." Financial Times (2014).

Korneyko, Oleksandr. State Service of Special Communication and Information Protection of Ukraine – a key factor in the protection of public electronic information resources in Ukrainian cyberspace In Cybersecurty-2013. Yalta: Presentation at international conference, 2014.

List of public higher education institutions licensed in the areas of 1601, 1701 in the field of knowledge "Information Security"., 2014.

On the Action Plan for the protection of state information resources In Order of the Cabinet of Ministers of Ukraine. Kyiv, 2014.

On the basic principles to ensure cybersecurity of Ukraine In Law of Ukraine., 2013.

Passport of specialty 05.13.21 System of Information Security., 2014.

Passport of specialty 21.05 Information security of the state., 2014.

Standards of higher education 1701 "Information Security".

Website of the Ministry of the Interior of Ukraine., 2014.