

**MODERN CYBER
WEAPONRY AND THE
“WEAPONIZATION” OF
IDEAS: HOW ELECTIONS
ARE TRANSFORMED INTO
CYBER OPERATIONS**

Barandiy Marta

Rozendaal Viktoria

Shutyak Yuliya



Conference proceeding

Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks

Brussels - 25/06/2019

DOI 10.34054/bdc000

The history of Russian hacking. The Gerasimov doctrine and the aggressive foreign policy of the Russian government

Despite the technological disadvantage Russia has in comparison to the west, Russia's ability to conduct cyber operations and information wars nowadays should not be taken lightly. In the last 10 years most political campaigns in countries, that are situated within the orbit Russian political interests, suffered some sort of Russian meddling. This includes cyber attacks, information and propaganda operations, attacks on infrastructure, political bribery and intimidation of opponents - all of which have been repeatedly called to atten-

tion by various civic organizations. "It is important to note that the methods used by Russia nowadays do not differ much from those used during the Cold War. The current regime simply learned on the experience of the KGB, which this isn't strange given that the regime is built on the legacy of the KGB. For example, when looking at the disinformation campaign in Lithuania, it is possible to notice that the campaign is no different than the campaigns conducted by the Soviet government" - reveals Marius Laurinavicius, the author of "A Guide to the Russian Tool Box of Election Meddling", in an interview to Promote Ukraine.

In nowadays Russia it is correct to assume that the Kremlin is controlled by the Gerasimov

doctrine when it comes to confrontation with those the Kremlin considers as its enemies. The doctrine emphasises the increased use of non-armed methods in carrying out warfare, which in proportion to the army forces should be 4 to 1.

Some experts say that this new doctrine does not really stress anything new. The only new thing that separates modern Russian warfare from the time of the Cold war are the new methods developed as a result of the progress made in the field of IT, more specifically - cyber weapons. Hence, current Russian aggression against sovereign nations could be referred to as a hybrid war. Consequently, an important role is played by cyber soldiers on

all fronts of this new type of warfare - such soldiers were not present during the time of the Soviet Union. Accordingly, cyber soldiers are employed in almost every field when carrying out a hybrid war.

How did the tradition of Russian hacking develop?

With the invention of the internet in 1983 and its rapid development, Russia faced hard times as it became increasingly difficult to control information flows. Accordingly, Russian special forces had to find solutions that address the problems of modern times. If you can not win at something, you have to be at the head of it - such a tactic was employed by the Russian political elite which made it a priority to invest into the development of IT professionals. Fortunately, preconditions to such development were available, as the Soviet Union had a sufficiently decent lev-

el of growth in the field of sciences at that time. In fact, little may know but it was a Soviet researcher, Alexey Pajitnov, who developed the world renowned game of "Tetris".

The rapid development of Russian hacking activity began in 1998, during a period of crisis when a lot of programmers were left jobless. These programmers were then employed by the government with the intention of transforming them into hackers working for the regime, commonly known as hacktivists.

"Hacktivists are everywhere. And there is a whole variety of them. Some have state sponsors. Some do their work simply for the idea" - reveals a well known Russian hacker, arkanoid, during an interview with Promote Ukraine.

The most famous hacker groups and their attacks

Hacktivists are everywhere. And there is a whole variety of them. Some have state sponsors. Some do their work simply for the idea

The first big hacker groups started appearing in the early 2000s. These groups are currently known as APT29 and APT28, abbreviated from Advanced Persistent Threat. APT28 is a group of Russian origin, when from the mid 2000s, they have been active in attacking the media, space and defense sectors of countries in Western Europe. German special operations have even accused the group of hacking into the Bundestag. The same hackers were also responsible for the attack on French newschannel TV5Monde, as a result of which the channel had to suspend broadcasting and on the website of the channel a symbol of ISIS was displayed.

APT29 became active in 2015, and were responsible for hacking into the network of the White House, the US State Department and the Joint Chiefs of Staff. The hackers also attacked the energy, financial and pharmaceutical sectors as well as American universities and research institutes. These attacks, however, were not only limited to the United States. Organizations located in Europe, Brasil, China, Turkey and central Asia also fell victim to such attacks. Experts have thus concluded that APT29 is a Russian group of hackers. This is evidenced by Russian words in the code, the hours of operations which coincided with Moscow time and the peculiarities of the viruses - reports the Russian site Агентства.Py.

With time, Crowdstrike, a company operating in the field of cyber security headed by Dmitri Alperovitch, an American of Russian descent, gave these hacker groups their new names. APT29 became Cozy Bear and APT28 became Fancy Bear. Another well known hacker group is Turla, the core of which, according to data provided by experts, is composed of Rus-

sian-speaking hackers and is also known by names such as Snake or Uroburos. Close to 45 different countries have suffered as a result of this group's activities in the past 8 years.

Russian special forces are considered to be at the head of these large hacker groups. Determining the location of these groups is close to impossible, so figuring out their location comes down to comparing the methodological approach they employ when hacking.

The first of the more impactful cyber attacks carried out by these groups could be traced back to the attack on the Estonian network after the moving of the monument to the Unknown Soldier in 2007. The hackers blocked the Estonian banking system, hijacked the government correspondence system and blocked the media.

A more notable attack, after which the whole world began recognizing the danger posed by hackers, was the break-in into the servers of the Democratic party in the USA a day before the elections and the subsequent leakage

of valuable information to resources such as Wikileaks

As a result of this, Russia was openly accused of conducting cyber attacks, whereby Russian special forces were called the directors of such operations. In the past 10 years, thousands of cyber attacks took place all over the world. Below, we shed light to 10 of the biggest and most striking attacks, in our opinion:

1. April - May 2007. Attack on Estonian servers after the moving of the monument to the Unknown Soldier in 2007. The DDoS attack was concentrated on state-owned enterprises and financial establishments. As a result of the attack communication and connection was cut off.
2. August 2008. After the pro-Western government in Georgia unleashed its army against the seperatist republic that was supported by Moscow, Russian land, air and naval subdivisions invaded the country. The invasion was carried out with the help of hackers attacking the Georgian internet. This is the



first time Russia coordinated its physical army with cyber activity. As a result, Georgian internal communications were blocked.

3. March 2014. For the second time, Russian was coordinating its army and cyber activity. The DDoD attack was 32 times the size of the previous attack during the invasion of Georgia, as it blocked the internet throughout the peninsula. In the meantime Russian “little green men” took control of Crimea.

4. May 2015. Hackers got inside the computer networks of the German Bundstag, which is now considered as the biggest cyber attack in German history. German intelligence later revealed that Russia was behind this attack, carrying it out as a means of looking for information in regard to German deputies and cooperation with NATO.

5. December 2015. Russia hackers attacked the central management system

of the Ukrainian electrostation, which 235,000 buildings without energy.

6. June 2015 - November 2016. Hackers got into the computers of the Democratic party in the US and got access to private information on the officials, which was then spread throughout the media and Wikileaks. Both the CIA and the FBI believe that the intrusion had at its core the objective of disrupting the elections, damage the reputation of Hillary Clinton and help Donald Trump win.

7. October 2015. Security experts believe that the Russian government attempted to hack into the computers of the Dutch government in order to obtain the Dutch account of the MH17 flight over Ukraine.

8. May 2017. Macron leaks - hackers took hold of 20,000 emails associated with president Macron’s campaign during the French presidential elections in 2017 two days before the final vote was cast.

9. Summer 2016. Attack on World Anti-Doping Agency (WADA). Russian spies connected to the computers of various agency functionaries to figure out how the organization functions.

10. June 2017. Massive global cyber attack with a focus on Ukrainian companies, including the National Bank of Ukraine via the virus NotPetya. The virus also infected personal computers in France, Germany, Italy, Poland, the UK and the US.

How the Kremlin recruits the hackers

By spreading its ideology of “spiritual moral values” combined with “patriotism” Moscow gains volunteers who wish to enforce these values both online and offline.

Recent footage of the Russian channel “Rain TV” (Dozhd) about cyber-vigilantes shows the depth of incorporation of the

message of the Kremlin in the society, that “moral values is a matter of national security”.

These “volunteering cyber-militants” cooperate with the Russian state institutions to point to “extremists” in the web. There is even a draft law of the ruling party “Yedinaya Rossiya” about the legitimization of their status and the “hacking actions” they undertake.

This measure is actually a further step to control the information space inside the country and to timely reveal the protest mood of the population.

Internationally, one of the motivation elements of the hacking groups working with the Kremlin is national pride, like in the case of “Fancy Bear” (known as APT28) who hacked the World Anti-Doping Agency and revealed US and UK athletes’ (so far legal) drug use. It was done with the purpose of revenge for banning Russian athletes from the Olympic and Paralympic Games for drug use.

Using patriotism is not the only method of the Kremlin to gain support from the activists, including cyber-activists. Another way to build government’s “cyber-strength” is to encourage those having particular skills and talents. By placing ads on social media sites government backed recruiters offer jobs to college

students and professional coders.

One of the most efficient approaches is to find those hackers who “have problems with the law” and blackmail them. Thus, back in 2013 Russian deputy minister of defense, Gen. Oleg Ostapenko, said that they were forming units called science squadrons and that they might include hackers with criminal histories. The same year a cyber-criminal Alexey Belan was arrested in Greece on the request of the USA but he avoided extradition and fled to Russia. There he was trapped: he was forced to work for the FSB in order to avoid further criminal charges. On the order of Russian intelligence and together with another “hacker for hire” who was from Canada he conducted cyber-attacks against Yahoo.

Not only criminals are blackmailed but also those who act in good faith. The 2015-story of Mr. Vyarya - the coder who was put in the situation where he had to reject to work for the Russian government, proves how mean the methods of Russians can be.

Mr. Vyarya who helped to secure the websites of opposition leaders and media channels was “forced” to witness a DDOS attack done with the help of the Bulgarian software which Russian military contracting company Rostec

planned to buy. Following this cyberattack against Ukraine’s Defence Ministry he was proposed to “run” and to improve this software. After he declined the job offer, he was forced to flee the country.

One more type of recruiting is to give tasks to the programmers without telling them what the purpose is, like in the case of a Ukrainian coder who had been paid to write customized malware without knowing its purpose, only later learning it was used in Russian hacking against Ukraine and other Western states.

How Russia transforms elections into cyber operations

Ukraine

The internal affairs of Ukraine have always been an area of special interest for Russia. The previous presidential elections were not an exception to this rule. For these elections, the Kremlin designated 350 million dollars, but how was this money be used? After all, no major cyber attacks happened during the elections? “If we don’t hear about cyber attacks, that doesn’t mean that they did not happen. If in a usual week we identify 10,000 cyber inci-



dents, then during the first round, there were 10 times more of such incidents and in the second round, 20 times more during the recent election” - says Roman Boyarchuk (PU), the ex-head of CERT-UA, a specialized subdivision of the state center for cyber protection and counteraction of cyber threats of the Special Communications and Information Protection of Ukraine, who held the position until June 2019.

According to Boyarchuk, the main types of attacks during the Ukrainian presidential elections were scanning attacks. These attacks scan the system in an attempt to find vulnerabilities to exploit.

Who carries out these attacks? “We have to look at who needs them. Do hackers operating by themselves, need to commit to these attacks? After all, some of the attacks, including DDoS attacks, are rather expensive. Concludingly, it is possible to say that such attacks are sponsored by large corporations or states” - reveals Boyarchuk.

In the case of the presidential elections in Ukraine, Russia did not have an evident favourable. Therefore, Russia worked on discrediting the electoral process as whole - conclude many experts. What means were employed?

The difference is that during the elections in 2014 Ukraine was unprepared in terms of cyber security, however this time Ukrainian officials knew what to expect, constantly emphasising on the importance of having complex sessions on the protection of national cyberspace. Hence, Russian hackers were unsuccessful in influencing the electoral process as efficiently as they did last time.

“Before every election, special action is taken on the preparation of reliable software used in the election, which is approved by the National Security and Defense Council. Thus, major issues with or consequences of cyber attacks during the elections were not witnessable” - comments Roman Proskurovskyi (PU), the head of the department of the maintenance and implementation of key management sys-

tems of the National Bank of Ukraine.

However, traditional methods of hacking were still used.

Phishing

Traditionally, Russian hackers applied pressure on the members of the Central Election Commission (CEC), stated Sergey Demedyuk, the head of the department of cyber policy, a day before the elections.

A couple of months before the voting, he said that pro-Russian hackers often most target the servers of the Central Election Commission and the computers of the commission’s coworkers. By doing so, they attempt to get inside the system in order to manipulate the presidential election. Consequently, the hackers would use virus infected electronic gift cards, promotional newsletters, propositions to renew the software, and other harmful phishing materials in order to obtain passwords and personal information.

Attacks on objects of critical infrastructure

During the first round of presidential elections in Ukraine, the official website of the State Register of Voters of Ukraine failed for several hours - on this resource, voters can specify whether they are in the lists at a certain polling station, and find out exactly where they should vote. Experts said the alleged breakdown was the result of a Ddos attack.

It was also heard that the Security Service of Ukraine prevented a hacker attack on Ukrainian media and telecommunications objects (telecom operators and large telecommunication companies) by Russian special services. "The aim of the cyberattack was likely to create maximum social resonance and negative informational influence on the eve of the presidential elections in Ukraine," the SBU emphasized.

However, fortunately this time authorities managed to prevent large infrastructure disasters. "We cannot now state the causes of certain disasters happening in the world - with

planes and so on, but the safety of navigation systems is a very important issue. Also, the objects of critical infrastructure deserve special attention - we remember the situation with the Boryspil airport (2017 - author.) When the power supply was cut off for one and a half hours, and all this time planes circled around. Luckily there was enough fuel. To avoid this, it's important to build a security system" reveals Andrei Pazyuk, director of the Ukrainian Academy of the Cyber Security to Promote Ukraine.

The discreditation of the electoral process

One of the important directions of Russian hybrid aggression in Ukraine on the eve of the election was the discrediting of the electoral process as such. Pro-Russian journalists in the media and trolls in social networks spread information about the unlawfulness of the Ukrainian election.

So, the successful defense platform The Suc-

cessful Ward disseminated information about allegedly the presence of dead souls in the electoral list and the trampling of votes in favor of Poroshenko.

Social media and media activity

On the eve of the election, the Security Service of Ukraine issued a video of a Russian agent whose job was to buy or rent a page in social networks and use them in the interests of Russia.

"To my knowledge, these accounts were then used to publish political ads or fake articles" - he told the video.

How many pages have been distributed by Russia before the presidential election in Ukraine? We can say with certainty that there were more than 2000 of such a pages. As many accounts and groups were deleted by Facebook on the eve of the elections in Ukraine. All of them were related to Russia and distributed fakes and misinformation.

The experts of the Committee of Voters of Ukraine determined that the main purpose of propaganda was to destabilize the election process itself and to devalue it. So, the key messages of the last election campaign in Ukraine were as follows: “the president does not affect anything,” “the choice has already been made to us”, “your choice does not affect anything “.

EU

If there was no obvious candidate for Russia at the last elections in Ukraine, then there were too many Russian favorites during the European Parliament elections. Russia directly or indirectly supports almost all anti-European movements, and so the right and left radicals of Europe.

Thanks to this support, they were even close to forming a coalition - however, the European voter still figured out the situation and prevented radicals from coming to power. But their positions have increased considerably.

The traditional favorites of the Kremlin are the French National Front Marine Le Pen, the Italian “ League of the North ” Matteo Salvini, the Al-

ternative to Germany and other Eurosceptics. Therefore, according to experts, the main messages of Russia in the elections to the European Parliament were as follows: Europe collapses, power loses control (over the invasion of migrants), European values are in jeopardy.

“I saw how Russia intervened in the American elections in 2016. And I can say that its intervention was successful only when it was about real fears in the American society. And the same thing in Europe. Listening to the propaganda of the extreme right - the persecution of Christians against Muslims, Poles against the Germans. And this explains the real disparities in Europe with catastrophic consequences, “said William E. Echikson, head of the Digital Forum Center for European Policy Studies in an interview with Promote Ukraine.

Here hackers also used their traditional set of tools.

Phishing

Between September and December 2018, there were about 104 attacks targeting workers from organizations located in Belgium, France, Germany, Poland, Romania and Serbia. These attacks, aimed at obtaining data and

accessing computers, were directed at think tanks and institutes which often have direct links with politicians and state institutions. So Microsoft which reported the attacks, directly links them to the European elections.

Social Networking Activity

241 million, or half of Europeans may have faced misinformation in social networks related to Russia, said SafeGuard Cyber. 6.7 thousand automated bots published and distributed regional-oriented material, created for each individual country.

Distribution of propaganda and misinformation

Thousands of trolls and bots produced and distributed misinformation and propaganda. Mostly, they adhered to extreme right ideology, propagating anti-European and Islamophobic ideas.

However, in the opinion of most experts, the worst behind. Both Ukraine and EU countries have learned to resist Russian cyber threats. After all, the elections in Ukraine were held

honestly and transparently. And in Europe, as if someone would not want, the revenge of the right forces did not happen yet.

Attribution of cyber-operations: how do we know it was the state?

Governments and private companies are increasingly likely to discover and attribute cyber operations. For good assessment of a cyber-attack it has to be considered who benefits from the attack and whether it could be a false flag operation. To properly attribute the attack, one has to consider the intelligence and the technical components of the operation.

Credible attribution implies that the society trusts the attributors. In many cases the attributors are the intelligence services that do not tend to declassify their sources. Besides the “international cooperation is needed to discover every element in the chain of cyber attack”. Example of such cooperation is the Five Eyes intelligence grouping, made up of the UK, the USA, Canada, Australia and New Zealand, that attributed devastating NotPetya attack to Russia and WannaCry to China.

In 2018 the intelligence services of the US, the UK and the Netherlands attributed cyber-attack against World Anti-Doping Agency and the Organisation for the Prohibition of Chemical Weapons to Russia’s GRU-backed hacker group Fancy Bear (APT28), the group that became bolder after hacking France’s TV5 in 2015. Dutch intelligence was able to track the Russian hacking group “Cozy Bear”. This group is blamed for the attack against Democratic National Committee. In these cases, concerned states were able to attribute and to share the findings with their societies, and it made the attribution credible. The evidence may not always be presented. But it does not mean that it does not exist.

Not only public services monitor the attacks but private companies report on Russia’s cyber-interference too. Thus, the above-mentioned “Cozy Bear” was first identified by the Russian-born Dmitry Alperovitch, co-founder of the US-firm “CrowdStrike”. Dutch company “Fox-IT” identified the Russia-backed group “Turla” that used malware rootkit Snake to hack German Bundestag end of 2018 and Belgian Ministry of Foreign Affairs in 2014. The company “CrowdStrike” helped investigate cyberattacks Gameover ZeuS of the criminal with the nickname “lucky12345”. Gameover

ZeuS aimed at stealing bank account data of the victims. After more than 10 years of tracking the guy, thanks to common efforts of public institutions and private firms the mastermind was identified. It was Evgeniy Bogachev, who was residing in the Russian resort city Anapa. The investigators established that the network of Bogachev was involved in collecting information on Ukraine right before Russian invasion in the country. Connecting many dots helped assume that he worked for the Kremlin.

The American IT-company “FireEye” and the Finnish “F-Secure” each published papers revealing Russian government-backed cyber operations. The first one - “APT28: A Window Into Russia’s Cyber Espionage Operations?” (2014, complemented with new evidences in 2016) and the second - “The Dukes: 7 Years of Russian Cyber-Espionage” (2015).

Ukrainian cyber-security experts Viktor Zhora and Nikolay Koval were able to identify the malware that was used to load onto a Ukrainian election commission server a graphic faking the results of the elections. This fake image was then used by the Russian TV channels to spread lies that the “ultra-rights won Ukrainian parliamentary elections” in 2014.

The EU takes the position that “attribution to a state or a non-state actor remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of state responsibility”.

Outsourced Kremlin’s cyber-operations: what risks?

There are plenty of risks for the Kremlin and any other state that plans cyber-attacks using the money of its tax payers. Firstly, cyber operations embroil such countries in real world scandals that undermine rather than advance their own policy goals as well as weakens international cooperation on the issues of global importance. Secondly, cross-border operations are hard to control, and the mistakes done by hackers can escalate quickly. And thirdly, cyber-criminals may “hit back” - they may reveal the names of those for whom they work or leak any other information.

Risks for the companies

IT firms who willingly accept the job offer originated in the Kremlin, compromise their over-

all commercial and reputational gains. Thus, in 2014 Italian company “Hacking Team” lost its export license because it sold iPhone hacking software to the “Advanced Monitoring”, Russian firm working with FSB. Also, misleading information about who is behind certain public information campaigns can lead to removal of the social media pages with millions of followers like in the case of Maffick Media.

Hacked emails of Russian company “Oday technologies” revealed that they have helped Russian secret services to conduct their activities in cyberspace. Such cooperation erodes trust in the company when revealed.

At the same, other Russian companies like Kaspersky Lab want to show that they “distance” themselves from the Kremlin after allegations of Kremlin spying.

Risks for the IT specialists

Hacking for the state does not deprive these actions of criminal nature. When the attacks are discovered, the state for which the hacker works, denies its involvement. Despite publicly campaigning for recruitment of hackers, Moscow never admits that they work for the

Russian government and abandons them when they get in trouble. The trouble can be of different sort. Thus, hackers and their families undergo the risk of financial or legal consequences, and when they are “trapped” in Russia, they cannot travel to Europe for education, vacation or work.

In 2014 for the first time a criminal case was open in the USA in regard to the Russia-backed high scale hacking operation. Two programmers Canadian of a Kazakh origin Karim Baratov and the above-mentioned Latvian Alexey Belan were paid by two Russian intelligence officers Dmitri Dokuchaev and Igor Sushchin for hacking six thousands and getting information about half a billion of Yahoo accounts. The key role in the attribution of this attack played the British intelligence MI-5. “Hacker for hire” Baratov was sentenced for five years in prison whereas Belan has been put on the “most wanted list” in the USA. Dmitri Dokuchaev was arrested in Moscow in suspicion of sharing information with the foreign intelligence.

When cyber-attacks get attributed, which happens often nowadays, the individuals undergo high risks to get “trapped” between criminal charges and blackmailing, and the companies

- to lose reputation and licenses. Cyber-operations taint those working for the Kremlin; they embroil Russia in scandals with other states undermining international cooperation regarding issues of real, global importance.

Legal aspect: Ukraine and the EU

Europe began to care about cyber security much earlier than in Ukraine. In 2004, the EU established ENISA - European Union Agency for Network and Information Security. Furthermore, they adopted a number of laws on the European and national levels to strengthen cooperation in the field of cyber security.

Unlike Europe, Ukraine has only recently begun to think seriously about its cyber security, even though many laws were adopted a long time ago.

“No country can counteract cyberattacks on its own. We need to unite our forces”, said the European Commissioner for the Digital Single Market and Vice President of the European Commission Andrus Ansip during a meeting with Ivanna Klampush-Tsintsadze, Vice-Prime-Minister for European and Euro-Atlantic Integration of Ukraine in Decem-

ber 2018. Andrus Ansip underlined the importance of deepening cooperation between Ukraine and the EU in the area of cyber security. In terms, Ivanna Klampush-Tsintsadze noted a significant progress achieved in this pillar within the Eastern Partnership Initiative and emphasised that “Strengthened cooperation between Ukraine and the EU would create a solid platform for confronting cyberattacks” that often targeted important infrastructural objects in the country.

Both parties have begun to prepare for this dialogue well before the meeting. The awareness of the reality of cyberattacks and the importance of cyber security by the governments of the member countries of the Council of Europe, of which Ukraine is also a member, was reflected in the Budapest Convention on Cybercrime in 2001, which, to some extent, served as the basis for the formation and development of both international cooperation and national legislation in the field.. This convention was ratified by Ukraine in 2006, and, together with the Constitution of Ukraine and a number of other normative legal acts, serves nowadays as the legal basis for ensuring the cyber security of Ukraine.

The Convention defines the principles of com-

bating computer crime, extradition, mutual assistance, voluntary reporting of information and other procedural issues related to the fight. As stated in the Convention itself, it serves as the main document for international co-operation in the area of cybercrime on the territory of the member-states of the Council of Europe in the absence of other international treaties in this area between individual signatory countries. Accordingly, within the framework of the Convention, Ukraine was able to cooperate with international organizations and law enforcement agencies of other countries on issues related to the detection and investigation of computer technology crime. The effectiveness of such cooperation is confirmed by many examples of detention and extradition of cybercriminals, including the arrest of the organizer of the international criminal platform “Avalanche” or the arrest of a German hacker who stole online stores.

However, long before the adoption of the Convention, Ukraine had already adopted the Law of Ukraine “On Information” as of 1992, the Law of Ukraine “About copyright and related rights” as of 1993, Law of Ukraine “On the protection of information in information and telecommunication systems” as of 1994, and the Criminal Code of Ukraine in 2001 identified

criminal liability for crimes in the use of electronic computers (computers), systems and computer networks (Section XVI). In addition to the legislation already in force at that time, the new Civil Code of Ukraine of 2003 contained human rights, including the right to privacy, and defined key provisions on intellectual property.

Also, the development of the legislative field in Ukraine continued after the signing of the Convention. For example, the Law of Ukraine “On Protection of Personal Data” of 2010 regulated legal relations of the protection and processing of personal data in order to ensure the protection of the fundamental human right to non-interference in private life.

However, the biggest impetus to the development of the field of information and information systems protection was the aggression of the Russian Federation against Ukraine, which caused the need for additional measures and encouraged Ukraine to adopt two more important documents. First, this was the Order of the President of Ukraine “On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 “On Strategy of Cyber Security of Ukraine”. According to Article 1 of the Strategy of the Cybersecu-

rity of Ukraine (hereinafter - the Strategy) the creation of conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. This strategy delineated the functions of public authorities in the field of cyber security, where the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the National Bank of Ukraine and state intelligence agencies would form the basis of the national system of cyber security.

In 2017, Ukraine adopted the Law of Ukraine “About the basic principles of providing cyber security of Ukraine”. This law had defined a significant number of concepts that are new to the legal system of Ukraine such as cybersecurity, cyber-threat, cyber incident, cyberterrorism. In addition, this law defined objects and subjects of cyber defense in Ukraine, which outlines the range of enterprises and institutions subject to cyber defense. According to this law, the National Coordination Center for Cyber Security is the main body in the field of cybersecurity as the working body of the National Security and Defense Council of Ukraine. At the same time, none of the articles established responsibility for cybercrime,

and administrative or criminal liability is determined by the Administrative [xv] and the Criminal Code of Ukraine.

“The situation with cyber defense since 2017, after the appearance of the virus Petya, provided us with the first document on Cybersecurity that appeared in the industry which defined the functions of authoritative bodies. So, we can say that cybersecurity in Ukraine was born in the year 2016”, - tells us Roman Proskurovsky from the National bank of Ukraine.

In turn, in the EU, the European Agency for Network and Information Security ENISA is the competent body operating in the field of cybersecurity. ENISA was established in 2004 and is responsible for information security in the European Union as well as contributing to the development of a culture of networks and information security among citizens, Internet service users, enterprises and organizations of the European Union’s public sector.

In March 2019, the EU adopted the Cybersecurity Act, which corresponds to the current state of the development of the information sphere, and calls for and defines the legislative basis for the dissemination and enhancement of the cyber-hygiene culture in society.

On its way to eurointegration, Ukraine under-

stood that cooperation with ENISA becomes one of the most important directions of common work. Ukraine is preparing to sign an agreement on cooperation with ENISA, which will allow it to conduct a more effective, professional and powerful counteraction to cybercrime. However, it seems that despite the progress made in the development of national legislation, as well as relations with the EU, Ukraine has problems not only with the full harmonization of legislation in the field of cybersecurity with the European legislation, but also problems with the implementation of the provisions of the laws and control over their implementation, which gives great opportunities for criminal activity. At the same time, the EU does not stand still - it deepens and constantly improves its regulatory framework. This situation provides even more challenges for Ukraine in the field of cyber security, especially on the road to European integration.

Web: www.promoteukraine.org
Contact: info@promoteukraine.org

Promote Ukraine is a non-profit start-up. It is a politically and governmentally independent organization situated in Belgium. It consists of a thriving team of professionals who on a pro bono basis seek to give voice to Ukrainian civil society in Europe and, in particular, throughout Belgium. We believe in European values such as civil rights, good governance and equal opportunities. Through connecting EU businesses and politicians with Ukrainian stakeholders, we facilitate the sharing of best practices between EU and Ukrainian partners with the goal to bring Ukraine closer to EU norms and values from a bottom-up perspective.



 [promoteukraine](https://www.facebook.com/promoteukraine)

 [promoteukraine](https://twitter.com/promoteukraine)

 [promoteukraine](https://www.instagram.com/promoteukraine)