# Ukraine's Top Cyber Cop on Defending Against Disinformation and Russian Hackers

November 17, 2020

Dmitry Smilyanets

November 17, 2020

*Editor's Note: In recent years, Ukraine has become an involuntary testing ground for some of the most dangerous cyberweapons in the world. When the U.S. Justice Department unsealed charges last month against six Russian intelligence officers, prosecutors detailed how Russia used malware to damage Ukraine's power grid in 2015 and 2016, and targeted the country in 2017 with the NotPetya attack that quickly spiraled out of control and is considered the most costly cyberattack in history.*

*Throughout that time, Serhii Demediuk perhaps played the most prominent role in defending Ukraine against digital intrusions, investigating cyberattacks and the groups behind them, and strengthening the country's capabilities in cyberspace. In 2015, Demediuk was tasked with building out Ukraine's CyberPolice force, which prosecutes cybercriminals and thwarts state-sponsored attacks. Last year, the president of Ukraine appointed Demediuk as the Deputy Secretary of the country's National Security and Defense Council.*

*Demediuk talked to Recorded Future expert threat intelligence analyst Dmitry Smilyanets about the most dangerous attacks he's dealt with, as well as new threats that he's bracing for. The interview was conducted in Russian and translated to English with the help of a* *professional translator, and has been lightly edited for clarity.*

**Dmitry Smilyanets: You said recently that the Russian special services collect information about Ukrainians through social media mobile applications, and also uses social networks to spread disinformation to influence and manipulate public opinion. Can you share examples of what you've seen?**

**Serhii Demediuk:** First of all, it should be said that social networks are still the most accessible platforms for the dissemination and exchange of various information and are the most suitable space for manipulating the opinions of users. The data that users themselves leave there allows others to determine their personalities with very high accuracy, calculate their preferences and hobbies, as well as political beliefs at the time of the analysis. Existing artificial intelligence technologies very quickly identify and filter out specially-crafted bots, fictional accounts, and other unnecessary accounts. This information makes it possible to classify users of social networks into social groups necessary for the massive use of social engineering in order to gain psychological control over the most active users of a particular group. And then, as they say, it's a matter of technology—to whom and in what quantity to provide the necessary information to obtain the expected result. The result can be anything, including an aggressive attitude towards anything or anyone, support for radical movements, groups, etc.

*Serhii Demediuk*

Controlled media are used in order to get the result obtained from the internet and bring it to life. The appearance of critical information from the social network in the media is an indicator of its veracity and the embodiment of emotions accumulated online, which can be anything. And given the fact that social networks have long ceased to be an exclusive consumer service for the communication between friends, and have become a mouthpiece for politics and an advertising platform for business, their use has become attractive to everyone, without exception, including the special services of different countries, including Russia.

The issue of fakes and misinformation about the COVID-19 pandemic has appeared in almost every country. Today, the international community is actively looking for ways to prevent the spread of false content on social platforms, as well as to increase the responsibility of social networks for inadequate measures related to the identification and removal of specially-created fake accounts. But the corresponding measures taken by different countries have almost no effect. I believe this is due to the fact that the governments, including Ukraine, communicate very poorly with their citizens. They provide officially only that information which, in their opinion, should be of interest to citizens, and incomplete or hidden information about facts always arouses curiosity and breeds distrust. In addition, psychologically most people do not trust authorities by default, which in itself reinforces this distrust. Moreover, the majority of people don’t trust their governments by default, which only heightens this distrust. Therefore, any misinformation that criticizes or exposes the actions of state bodies will always be in demand. There are many and very different examples of this manipulation. Just think of the case of Cambridge Analytica.

As for Ukraine, I can give just a few examples that demonstrate the power of social influence. To do this, I want to mention the events of this past February that took place in the Ukrainian village of Novi Sanzhary (in the Poltava region), when the dissemination of inaccurate information on social networks and the media about a possible unprecedented coronavirus infection caused riots during a meeting of Ukrainian and other citizens evacuated from Wuhan. The situation in Novi Sanzhary was caused by the lack of reliable and complete information from the government and inconsistency in the information policy of the authorities that took part in the evacuation. This situation, associated with the evacuation of Ukrainian citizens from Wuhan, was used by Russia as part of the information war against Ukraine, using the topic of coronavirus to destabilize the situation throughout Ukraine.

An important aspect of the information and propaganda operations of the Russian special services was an active internal and external information policy regarding the maximum coverage of events in Ukraine from a perspective favorable to the Russian Federation—numerous talk shows, the creation and promotion of the relevant communities in social networks. All this is then scaled through other communications (related communications, Internet resources, satellite TV). The activities of the Russian special services are manifested in the intensification of work to attract expertise (institutes of civil society created by them) to information operations, which produces an additional targeted negative impact on the public opinion of our citizens.

In addition to intensive anti-Ukrainian information campaigns inside Ukraine, the Russian Federation systematically intensifies them abroad. One of the priority tasks of the Kremlin’s information and propaganda activities with regard to Ukraine is to provoke tension between our state and neighboring countries (Poland, Hungary, Turkey, other neighboring and allied countries). For example, the Russian special services have been directing active anti-Ukrainian information and propaganda activities towards Poland. Among Polish users of social networks, the most popular of which are Facebook and Twitter, content which allegedly indisputably proves the facts of cooperation between the Organization of Ukrainian Nationalists (OUN) and the Ukrainian Insurgent Army (UPA) with the Hitlerite regime during World War II and the UPA’s implementation of massive war crimes against the peaceful Polish population is widely disseminated [*Editor’s Note: The OUN and UPA were nationalist* *political organizations active during World War II that fought extensively against the Polish communist army. In recent years, the Parliament of Poland officially accused the groups of genocide, which has been disputed by historians outside of the country*]. The reason the Russian Federation does this is the total flooding of the information space of our neighbor with false, primitive disinformation that is accessible to ordinary citizens.

A similar example of an information operation aimed at undermining the relations between Ukraine and its neighbors, using social networks, is the dissemination at the end of 2019 through Telegram channels controlled by the special services of the Russian Federation ("Mole of the SBU", "Joker DNR") of information about the alleged murder on the border with Hungary, of four SBU officers. At the same time, it was noted in news reports that the group "performed tasks of documenting smuggling traffic" through the "private section of the border" of Ukraine with Hungary and Romania. This provocation, with reference to anonymous sources in the SBU, was further amplified by a number of Russian media outlets. In turn, the SBU exposed this fake a week before the mass dissemination, which nonetheless did not affect the organization and holding of anti-government rallies on this issue.

Today we can already assert that the organizers of these information attacks and the spread of disinformation against Ukraine are the employees of the military unit of the Russian Federation 54777.

I believe that in order to prevent potential threats that may be caused by the use of social networks and messaging apps, it is necessary to develop media literacy of society at the state level. In our country, we managed to include that priority in the National Security Strategy of Ukraine, recently approved by the President of Ukraine. In particular, raising the level of media culture in society should become a tool to counter the spread of disinformation. I also urge everyone to train themselves to, by default, not trust information from unverified sources, primarily those that appear on social networks or with a link/reference to them.

> Of course, the law enforcement agencies of our country know that the listed hacker groups of the Russian special services have a spy network in the hacker environment of Ukraine. Most of these participants have been identified and are being monitored."

**DS: Do you think attacks such as the ones targeting Ukraine's critical infrastructure should be regarded as military aggression? How can they be countered?**

**SD:** All attacks on critical infrastructure should be judged according to their classification. Attacks aimed at damaging network infrastructure and interference in the operation of information systems—the performance of which can negatively affect the life of society—should be regarded as terrorist, irrespective of whether these attacks were internal or external.

Such attacks can be classified as military aggression only if they come from another state and are aimed at changing the sovereignty, territorial integrity, or political independence of our state. But it is hard for me to imagine what these attacks could be without the use of classical armed forces.

It has been necessary to prepare for counteracting such attacks since the very beginning of the development and use of information systems and technologies. First of all, this is the selection and training of personnel for their maintenance, administration, and implementation of security, both external and cybernetic. The human factor (insider knowledge) is still key in this area.

It is advisable to use software with available source code that can be checked for vulnerabilities. In addition, you need to connect to existing systems to exchange information on cyber incidents, both public and private, in real-time. Never use software and hardware from one vendor when building information systems.

And the most time-consuming and boring factor for the employer is systematic training in cyber hygiene. As my experience in the field of cyber defense and combating cybercrime shows, the majority of successful attacks resulted mainly from the negligent or careless attitude of employees of the victim institution, organization, or company.

**DS: Which “bear” is the most active in Ukrainian networks—APT28, also known as Fancy Bear, or APT29, known as Cozy Bear? Do you expect these groups to coordinate with people on the ground in Ukraine? Do you see an overlap between cybercriminals and those engaged by government special services?**

**SD:** According to the information I know, Turla, APT28, and Sandworm are still active. The latter even tried to launch a supply chain attack like NotPetya again.

Of course, the law enforcement agencies of our country know that the listed hacker groups of the Russian special services have a spy network in the hacker environment of Ukraine. Most of these participants have been identified and are being monitored. Some of them agreed to cooperate with law enforcement agencies and special services of Ukraine. This is laborious and fruitful work with our international partners.

Observing the hacking activities of the Russian special services showed that, in addition to their regular employees they also employ cybercriminals.

The confirmation was that on days free from special operations, they were engaged in common criminal activities, from the distribution of ransomware to the theft of cryptocurrency. It was these crimes that gave us the opportunity to identify almost all members of these groups, both intelligence officers and cybercriminals.

In addition, for all their crimes, these groups used the same methods of renting servers, registering accounts, legalizing and using stolen cryptocurrency (both for the needs of criminal activity and for personal purposes), as well as creating botnets. They didn’t worry much about the malware they used for almost all of their operations with minimal changes to the code. Their “bearish habits” also led to other mistakes, which I cannot yet talk about, except for the ones above, which made it possible to identify all participants and their accomplices in Ukraine and the European Union, as well as to determine the belonging of each to a particular group.

**DS: Recently, the U.S. Department of Justice officially accused six officers of the Russian GRU of military unit 74455 for attacks on, among other things, critical infrastructure in Ukraine. Perhaps you can comment on this in more detail?**

**SD:** I can only say that the CyberPolice of Ukraine has done a tremendous job on this case. In the early days of the attack, police officers were recording and establishing the digital traces from all servers that were used in the attack both in Ukraine and abroad around the clock. Of course, not all countries contributed to this. Precisely until the moment when they themselves began to feel the consequences of this attack, and this was the first two or three hours after the active phase of the attack. At the same time, these couple of hours were enough for the criminals to clean up some of their servers.

It was the information collected at that time that made it possible to restore in detail all the events and track all the participants, all the way up to their organizers, who were announced by the U.S. State Department.

It should be noted that all affected countries were involved in the investigation of this case. But active investigative actions, according to the information that we received, were carried out only in Britain, the U.S., Ukraine, and France. During the first months of the investigation, it was possible to quickly establish the involvement of the Russian special services and their Sandworm group in organizing the attack. But it took three years to identify all of the involved GRU officers and their accomplices, as well as to collect evidence regarding each of their roles. The duration of the investigation was associated with the differences in the criminal procedural legislation of each country, which took some time to resolve within the framework of international norms. So, when we established the involvement of a suspected group of hackers in other crimes (for example, interference in the French elections, attacks on critical infrastructure in Estonia), these facts were immediately classified by the British and American sides and were independently investigated by each side separately.

But this did not prevent us, along with the French side, to identify and decrypt the TOR server, which hosted Sandworm’s command and control panels and stored almost all the malicious programs that were used for attacks. The data obtained became the key evidence of the criminal activities of the GRU of the Russian Federation.

At the same time, in addition to the GRU officers indicted by the U.S. Department of Justice, many Russian-speaking accomplices living in the European Union and Ukrainian citizens were identified, who agreed to cooperate and provided supporting evidence of the guilt of the accused.

**DS: For several years now, official cooperation between the special services of the Russian Federation and Ukraine has been degrading, and in some areas is completely absent. But as far as I know, in the post-Soviet space, talented hackers maintain relations with specialists in information. How can you explain the lack of politics in the cyberspace domain? How do you deal with information leaks?**

**SD:** Fortunately, not all residents of the Russian Federation support the policies of their president and his government. At this stage, there can be no official cooperation, except for diplomatic work and other activities related to saving human life. Many citizens of Ukraine and Russia still have contacts, acquaintances, friends, relatives from both sides. These connections are mainly maintained at the household and commercial level, which allow them not only to maintain relationships but also to carry out good projects, although, unfortunately, there are facts to the opposite as well. In such relationships, you need to understand one thing: If one person does not recognize the political views or other beliefs of the other, then there will be no relationship between such people.

I think the relationship between hackers and IT and information security specialists is built at exactly the same level.

With regard to counteracting information leakage, in this regard, there have been many recommendations developed that cannot be disclosed. In the public sector, for this, in addition to technological traps, there is the use of the tactic of dividing sensitive and critical information into parts, which in a segmented form will not pose any threat if disclosed. Covertly identifying such information for each user and periodically using distorted information for rechecking remains an effective method.

**DS: Given the language and cultural and historical overlaps between Russia and Ukraine during Soviet times, is it possible to do effective counterintelligence in Ukraine? Does it exist?**

**SD:** Counterintelligence activities in Ukraine are carried out at a high level. Just look at the recent arrest of SBU General Shaitanov, who was recruited by the FSB of the Russian Federation.

Our counterintelligence officers are doing an excellent job, they are great. Not all circumstances can always be made public. Therefore, I cannot comment on counterintelligence operations in cyberspace.

*Serhii Demediuk*

**It is no secret that most of the most famous and talented hackers are Ukrainians. Why are there so many? Do you know them personally? Which Ukranian hacker do you respect the most?**

**SD:** To be honest, I do not know how to explain this phenomenon. I can only express my opinion and suggest that this may be related to the historical past and modern history of our country, in which our citizens have developed a desire to be free and independent. These are the qualities inherent in hackers.

Unfortunately, I cannot know all of the Ukrainian hackers. I only know those whom I've come across while working in law enforcement and with whom I work now. I know not only their names but a little more. There are an awful lot of them. Of course, not all of them are personally acquainted with me, because my previous activity did not always provide for this, but it obliged me to establish, search, and know them all personally.

We work with the community, there are different people who help out, depending on the tasks. Each specialist in their own direction, it is impossible to single out one brightest one, and I don't think that would be a good idea anyway. Because if they work as a group, they do incredible things.

While I was still the head of the CyberPolice, as a sign of our cooperation, I received a gift from these guys—the personal hashtag #cyberdemediuk, which they use to designate me to this day.

I can only say that there is a woman hacker I know who I like, who during my period of becoming a CyberPolice officer taught me a lot, made me think like them, accept them as they are. A very good person.

**DS: What was the most interesting investigation during your service in the CyberPolice of Ukraine? How did you manage to uncover it?**

**SD:** Here you need to consider that I happened to be the one who created the CyberPolice in Ukraine. Which means that, over the course of a very short period of time, it was necessary to develop a methodology, new ways of detecting and solving cyber crimes that were not inherent in the police. Therefore, almost all the investigations in the period of 2014 and 2015 were interesting. Over the course of time when I was the head of the Ukrainian CyberPolice, we had quite a few excellent cases, which we often recall with our colleagues. I think these stories may turn into a decent book in the future. But most of all, I remember investigating the case of the activities of a hacker group, which at the end of 2017 was engaged in compromising cryptocurrency wallets on blockchain.com. The crime was committed for more than three years right under everyone's noses and no one paid attention to it.

We were able to establish that members of this group, systematically through Google Adwords, advertised their phishing resources (for example, xn--blockchan-d5a.com, blokchreain.info, blokchreain.info, blokcheains.info, some using Punycode) to users who searched for the phrase blockchain. The attackers deliberately relied on the widespread practice of Internet users getting to sites using search resources, mainly Google, so as not to manually enter the URL in the browser line.

The phishing they used was different at that time in that it essentially proxied the blockchain.com resource using servers based on Nginx + LuaJIT that redirected requests to the original site. The change of these headers themselves was carried out using a module written in the Lua programming language (in the Nginx web server). After the user logged into the site, the modified Javascript (modified my-wallet.js) would steal the private and public keys, sending them to the attackers' servers via a POST request with the following data: sharedkey, password, secondPassword, isDoubleEncrypted, pbkdf2_iterations, accounts.

The whole process of stealing the money was fully automated. The criminals had only to keep track of advertising updates, purchase similar domains, and also administer and regularly hide the servers that hosted phishing resources and control panels. The Ukrainian hackers were responsible for the final actions, which lead us to the entire group since it was through them that we managed to gain access to their encrypted communication channels and find out that the group had up to eight members, six of whom were in the British Isles.

Then, for a comprehensive investigation, we began collaborating with the threat intelligence division of Talos, Cisco, and British colleagues (SW RCCU), as a result of which the entire group was arrested. According to the investigation, the group controlled tens of millions of U.S. dollars.

Another good story is about the black notaries. A group of Ukrainian hackers hacked into the computers of our notaries and re-registered expensive real estate on their behalf to third parties. But that is a very long story since a lot of atypical methods were used here to gain access to the necessary devices and unprecedented conspiracy methods.

**DS: How did you manage to achieve such effectiveness with your CyberPolice and crime detection? Is it because white hat hackers work in the CyberPolice? How frequently are people with a questionable past accepted to the civil service—namely**

**the hackers whom you managed to identify?**

**SD:** Of course, the key element in the work of the CyberPolice, I believe, were those very white hat hackers—special agents, as we called them—whom we managed to convince with great difficulty to work for us in 2015. This was an innovation for our country and it was the first time this was done. But now, after some time has passed, I can safely say that this was one of the best initiatives that I managed to implement. High-class specialists came to serve in the police. It was these guys who introduced new and non-traditional approaches to our work. Of course, when the work of a white hacker is strengthened by the capabilities and authority of law enforcement agencies, such as conducting operational and technical activities, this achieves an excellent result.

It was not easy to recruit white hat hackers. This was due to the fact that the public sector could not then offer decent compensation to such specialists. Provide them with proper hardware and software. But the most difficult factor in this was psychologically convincing these people to share their knowledge and best practices with the state. But everything worked out and the CyberPolice was born.

As for the official cooperation with the citizens of Ukraine, who are suspected by the law enforcement agencies of other countries of hacking their information systems or committing other cybercrimes, but who at the same time did not commit anything similar on the territory of Ukraine, this is another initiative of mine. It is motivated by the fact that, according to Ukrainian legislation, citizens of Ukraine cannot be extruded to other countries. Secondly, most of the cybercrimes in which such persons are suspected were mainly committed unintentionally or under the duress of third parties. Thirdly, they have colossal non-typical knowledge that could be useful both to our state and to the state to which they caused damage. And most importantly, they are aware of their responsibility and are ready to redeem their guilt by working for the state. But so far this initiative remains unrealized. There are an awful lot of disagreements in our own and in international legislation that need to be resolved. Therefore, interaction with them remains at the level of tacit cooperation in accordance with our legislation.

**DS: In early 2020, hacker attacks on the servers of the Ukrainian gas company Burisma circulated widely, which fed into the "Ukrainian scandal" in the U.S. and the impeachment of President Donald Trump. What's your expert opinion on this situation?**

**SD:** Publicly, this scandal began with an article in The New York Times in January of this year, where journalists of the publication, referring to the report and words of Oren Falkowitz, co-founder of the cybersecurity company Area 1 and a former employee of the National Security Agency, announced a phishing attack that was carried out in relation to the subsidiaries of Burisma Holdings, such as KUB-Gas, Aldea, Esko-Pivnich, Nadragas, Tehnocom-Service, Pari and the Ukrainian television company Kvartal 95, on New Year's Eve.

It should be noted that these attacks were identified by one of the cybersecurity subjects of Ukraine. During the analysis of this phishing, it was found out that it was the handiwork of the hacker group of the Russian GRU—APT28. We suspect that their main goal was to gain access to the company email and intranet. At the same time, it is still not known whether this attack was successful, since no victim showed any desire to make an official statement. Ukrainian legislation provides for the investigation of such incidents in the private sector only on the basis of a written request from the victim.

This attack was not assessed as critical, since similar actions are carried out quite often on their part, everyone is aware of them and prepared to repel them. And the fact that the publication of this information resonated in the American media is due, in my opinion, exclusively to the impeachment process against President Trump.

**DS: What currently keeps you up at night?**

**SD:** Fortunately, I rarely have sleepless nights. This is probably due to the fact that 26 years of service in the police have taught me to take everything calmly and not get worked up. But the situation with COVID-19 certainly concerns me and makes me worry about my relatives and friends.

**DS: Most experts consider ransomware and ransomware groups to be the most serious threat in 2020. What do you think about ransomware? How do you fight it?**

**SD:** I believe that this phenomenon will remain relevant until such time as people start to treat cyber hygiene as normal hygiene of their health, until they learn to regularly back up critical information as a matter of fact and store it appropriately, and until they stop paying criminals.

Also, everyone should understand that most ransomware has already been decrypted. The sooner victims report ransomware to the appropriate authorities or companies that are engaged in countering it, the sooner new decryptors will be developed and measures taken to identify ransomware. Unfortunately, people prefer to pay the ransom instead of contacting law enforcement agencies through intrusive bureaucracy and the lack of an immediate response to such appeals.

Therefore, the most effective way to counter ransomware is to systematically inform citizens about the observance of cyber hygiene rules.

> Everyone should understand that most ransomware has already been decrypted. The sooner victims report ransomware to the appropriate authorities or companies that are engaged in countering it, the sooner new decryptors will be developed.”

**DS: What will be the most significant cyber threat in 2021? Are you ready to combat it?**

**SD:** I think there will be several such threats. The first is related to working remotely in connection with the pandemic. The low level of training of such users has led to the fact that criminals are trying to gain access to corporate resources to steal corporate data. In this regard, the amount of phishing developed specifically for these needs will grow. Already today, we are recording phishing campaigns that are reaching a qualitatively new level of phishing using neural networks. And your previous question about the rise of ransomware was related precisely to this.

The second is related to the military actions that are currently taking place around the world. They are increasingly accompanied by malevolent actions in cyberspace. All this leads to the danger of compromise and destruction of government data, as well as disruption of critical infrastructure facilities. At the same time, more and more often compromised popular application programs will be used for such attacks, as was the case with the NotPetya attack, when the M.E.Doc accounting program updates were used or other well-known industrial attacks using the CCleaner program.

All cybersecurity entities in our country are ready for these threats and are doing everything possible to prevent them at the preparatory stage.

**DS: You've made an incredible career in international relations and information security and have become an icon in modern Ukraine for your patriotism. How did you manage it and what challenges do you face at work?**

**SD:** It's nice to hear such words. But I can evaluate myself and my actions only for myself in order to analyze my goals versus what has been achieved, formulate new ones, and correct mistakes. A public assessment should be given by others, especially those who have been affected by my actions, regardless of their role and place. As for your question, in my opinion, the main thing is to always remain a patriot of your homeland, respect your profession, colleagues, and opponents, and strive to become a professional in your field. And also to admit your mistakes and never be ashamed to constantly learn. These are the basic principles that made me who I am.

In law enforcement, I went through all the career stages—from cadet to general, from an ordinary operative to the head of an independent unit—without bypassing a single one. And this, probably, also played an important role in my formation. In addition, my operational experience gained in the Ministry of Internal Affairs in the operational development units that were engaged in detecting crimes in the highest echelons of authority helped me a lot.

Regarding challenges, it should be noted that they are a necessity. After all, certain challenges are the engine of growth. I think that here it is necessary to emphasize only the most important elements that slow down the progressive development in the sphere of national cybersecurity—this is the lack of qualified specialists who are ready to work in government positions, the lack of understanding among senior officials of government goals and problems in the information and cyber spaces. And this applies not only to Ukraine. As a consequence, there is a lack of appropriate regulatory statutes that would regulate interaction and cooperation between the state and the private sector, especially with foreign specialists and companies. And most importantly the underestimating of cyber threats that can come from both hostile countries and our own citizens, especially from employees of companies, institutions, and organizations, through their ignorance or negligent approach to cyber hygiene.

**DS: It is obvious that your experience, connections, and knowledge will be very valuable in the western labor market in the field of threat intelligence. Tell me a secret—what are your post-retirement plans?**

**SD:** I plan to use my experience to help those guys who are confused and who cannot find a way out of bad situations themselves. After all, I know that many of them are left alone with the problems that arise with law enforcement agencies. There are very few, and in our country, there are no people or organizations at all that would provide professional assistance to such children. For this, I have already received a lawyer's license and now I am looking for like-minded people among my colleagues.

At the same time, I will pass on my knowledge to the younger generation through consultations, lectures, training. Perhaps I will try to leave something in the book. And of course, I will continue to learn everything new.

Mission-driven and Russian-speaking intelligence analyst with type A personality. Dmitry has twenty years of experience and expertise in cybercrime activity that includes being a former member of an elite Russian-based hacking organization.