# Online Appendix B:
# Interviews on Cyber and Information Warfare in Ukraine

## "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?"

*Journal of Conflict Resolution*

Nadiya Kostyuk & Yuri M. Zhukov
University of Michigan

September 21, 2017

## Contents

# 1 Interview 1

## 1.1 Email: July 6, 2015

- **Q:** *Would you view the actions of the Ukrainian Cyber Forces (and any other non-state actors) as sending signals?*
- **A:** Sending what kind of signals? Do they provoke additional Russian aggression - no, I don't think so. Because Russia is crazy and inadequate, so they will be showing and even increasing aggression regardless of any actions by me (Ukrainian Cyber Forces) or other non-state actors. But, I considered all of the Ukrainian Cyber Forces' actions as resistance to aggression and more resistance by state and non-state actors (Ukrainian Cyber Forces) will force Russia to decrease aggression.
- **Q:** *Would you view them as war actions?*
- **A:** No, not war actions, since we do not "attack." We "protect" (even with attacking). I choose all actions wisely. I considered all the Ukrainian Cyber Forces' actions as resistance to Russia's aggression.
- **Q:** *Do these actions in cyberspace overlap with kinetic operations on the ground?*
- **A:** Sometimes, but a large part of all our actions is separate from ground operation and only supports them. Some of our operations prevent ground operations (particularly terrorists' actions). For example, when I block terrorist accounts in different electronic payment systems and banks, it prevents their further actions.
- **Q:** *Are they complementary?*
- **A:** Many of them are complementary to the ground operations. In some cases, like fighting against information warfare, our operations are the only possible option. Russia's cyber-attacks are also complementary to their ground operations.
- **Q:** *How effective are they? Please speak about both, Russian and Ukrainian, sides.*
- **A:** Different operations have various levels of effectiveness. Russia's information and cyber warfare (which I fighting against) is very effective. It is more effective compared with the actions of Ukrainian state-actors (More than a year have passed, and 100 percent of their work is offline (not using the internet). The Ministry of Defense, the Ministry of Internal Affairs, and the Security Service of Ukraine and other special services have a budget of about 100 billion *hryvnias* [local currency]. However, mostly the Ukrainian Cyber Forces and I do all the work online, and we do it for free). To compare state and non-state Russian programs with the Ukrainian ones, they work at their maximum capacity, spending billions of dollars cash for online actions and more for offline actions.

## 1.2 Email: July 10, 2015

- **Q:** *Is there cooperation between non-state actors and law enforcement agencies in fighting Russia's cyber-attacks?*

- **A:** Not very much. Starting with June 2014, I've sent all important information [refers to his intelligence collection] to Security Service of Ukraine and they just say "Thank you." This includes hacked data from sites, servers and e-mails (for that year we hacked 250 gigabytes of data http://on.fb.me/1JKFbj6), also audio, video, geo reconnaissance data, and URLs of separatists and terrorists sites. (So they can block them, but since last year, they have just blocked few sites – in comparison to our work - for 13 months we blocked and closed more than 110 sites of terrorists).

- **Q:** *Are there any efforts tailored towards fighting Russia's information warfare? How effective are these efforts?*

- **A:** Since the beginning of 014, all my actions [...] are done with the purpose of fighting Russia's information warfare and cyber warfare. About effectiveness of my efforts, you can see from what I did during this time at http://on.fb.me/1lFs0Av. Concerning government (and Security Service of Ukraine/law enforcements) efforts, there was a small amount of them and I almost did not see the effects of them. For instance, by the end of 2014, they created the Ministry of Information policy for these purposes. Still I haven't see any real efforts and results of their actions (except of empty words and spending budget money). I even gave my own information (photo and video of our reconnaissance) to help them in their work to fight Russian propaganda and show the truth.

- **Q:** *Is there any cooperation between Russian and Ukrainian cyber forces?*

- **A:** There is no such cooperation. I am talking about my Ukrainian Cyber Forces and other Russian hacking groups (pro-Ukraine and against Ukraine). But *Shaltay-Boltay*, for example, regularly disclose information, sometimes I found information there which is valuable for me. Information such as this helps me to get into accounts (e-mails and social networks) of different Russian people.

- **Q:** *Was there cooperation in the past?*

- **A:** No, there was not this type of cooperation.

- **Q:** *Are there any plans to develop cooperation in the future?*

- **A:** For now I have no such plans except using public information, as I mentioned above.

### 1.3 Email: August 15, 2015

- **Q:** *How would you feel that some IT specialists call the Ukrainian Cyber Forces actions as hooliganism (khylihanstvo) and not "cyber war"?*

- **A:** I don't respect these people and don't care about their position. So my only reaction will be to ignore such people. If necessary, I can also send these people to [uses inappropriate language]. Ukrainian Cyber Forces only do real work.

- **Q:** *Do you think it would be better to use offense rather than defense in an information war?*

- **A:** Yes I do. I think so and I do so - since the first day of work of Ukrainian Cyber Forces (and all my work against Russian information war before creation of Ukrainian Cyber Forces) I prefer offense. I also conduct teaching for the government and all Ukrainians through my publications (as all people in the world through my publications on English). But, the main goal against propaganda is to destroy it.
- **Q:** *For instance, instead of regulating everything, would it be better to spread this patriotic content?*
- **A:** Only spreading patriotic content is not enough. It would be unhelpful to de-zombie those, who fall under Russian propaganda. It will not protect everyone against this propaganda, so destroying it is required.
- **Q:** *"Russia lead cyber and kinetic warfare in Ukraine." Is there any overlap between these two?*
- **A:** Yes, there is overlap between them. All types of warfare intersect.
- **Q:** *Is it necessarily cyber warfare or, is it more so a cyber espionage campaigns?*
- **A:** Cyber espionage is appropriate during peace. When there is a war, then you need cyber warfare. There can be some cyber espionage campaigns, but mostly it is cyber warfare activities against the information war of Russia toward Ukraine.

### 1.4 Email: August 23, 2015

- **Q:** *What do you mean when you mention "Non-public actions against separatists" ("Nepublichini dii proty separatystiv")?*
- **A:** When I use a phrase "non-public actions against separatists" in my weekly report, I imply a "hacker" job that was done covertly.

### 1.5 Email: August 25, 2015

- **Q:** *What do you mean by "blocking"?*
- **A:** By "blocking," I mean using direct denial of service attacks http://on.fb.me/1Nu4ysQ. Every week I publish a list of all blocked websites achieved via submitting complaints to hosting providers. I've been publishing that list starting with the beginning of July. An attack can last for an hour, a day, or for a few days (for a few months), depending how strong protection for a specific website is. We have instances when we were able to make the website administrators close the website within one day. However, these administrators were able to operate this website again shortly. As a result, we had to start attacking it again. When I publish a list of blocked websites, I only include those websites that are blocked at that time. Additionally, even though some of the websites are blocked, I continue monitoring them to make sure that they do not become active again.

## 2 Interview 2, Email: July 12, 2015

- **Q:** *Is there any cooperation between the Russian and Ukrainian cyber forces? Was there cooperation in the past? Are there any plans to develop cooperation in the future?*
- **A:** Considering that Russia and Ukraine are *de facto* at war, I can hardly see any likelihood of their cooperating in the future, until there are major changes in their relationship.
- **Q:** *How would you characterize the information war in Ukraine? How effective is it?*
- **A:** Here is a definitional challenge. If by "information war" you mean cyberwar, I have no idea. However, this could as easily be about media and soft power, and if so, then I'd say that the Russians have been quite effective at using their information war to confuse the issues around the conflict in Ukraine, especially in Europe.

## 3 Interview 3, Email: July 10, 2015

- **Q:** *The Computer Emergency Response Team of Ukraine, how effective is it?*
- **A:** I used to work there. I am not active there now. However, they continue inviting me to give talks and to share my experience. For instance, a few weeks ago, they invited me to their office where we discussed their future development. They remember me very well as I was the one who helped to create the Computer Emergency Response Team of Ukraine when no one had any clue what it even meant. Now, they are trying to develop it further. First, they were established with the purpose of defending governmental information resources. At the beginning, they declared that they are open to any cooperation with anyone. But they are continued to use governmental resources. At the same time, they declared that they are willing to work with anyone and protect all information resources, not only the governmental ones [controversy]. Now they are trying to follow this trend. Their reputation was created during my time with this organization. This is when the team was created, the structure was created; we received needed equipment. We passed an international audit required for all organizations, *first.org*. Their inspector visited us and checked everything. He spoke to the team and to me, a team leader at that time. He had lots of questions. He spent almost the whole day. Then he created a report. And after that the Computer Emergency Response Team of Ukraine was accepted to the international community. There is a European Union fee; I think it is around $2000 dollars per year, if I am correct. And since they are still a member of this international community (*spilnoty*), no one will kick them out, and it means that everything is ok and the Computer Emergency Response Team of Ukraine continues its development. During my time there, international cooperation was well developed. There were teams from many countries in the world, Thailand, Brazil, Turkey, from Europe, Japan, and Korea. So even five years ago, there was a very active informational exchange between those teams, and the Computer Emergency Response Team of Ukraine had a very good reputation. As I understand, the reputation as a strong foundation is even better now. Their future development was created at a time when I was a part of this organization. Therefore, everything is good at the organization now. Now, as I understand they are trying to integrate within the society and information security specialists, because their salaries are funny (*smishni*) as they cannot earn money illegally and legally (*ofitsijno ta ne ofitsijno*).

So they recruit young specialists who receive 2000-3000 *hryvnias* [local currency] per month. These specialists stay for a year or two and then quit their jobs and move to a private sector to earn real money (*normalni groshi*). This is a huge problem for them. Thus, they need help from the community and specialists that work in a private sector and in the IT security branch of the private sector (*IT security businesi*), or help from free outsourcing. They can neither pay specialists for outsourcing nor can they pay appropriate salaries as they have a budget limit (*budzhetni obmezhennia*). Therefore, they are interested in exchange of experience, information, services with the sector and those specialists. This is how they are trying to solve this issue. At least, this is the way I understand this.

- **Q:** *Are they working with any governmental organizations that deal with cyber issues?*

- **A:** They have the closest cooperation with the Security Service of Ukraine. The head of their department confirmed that they are working with the cyber department of the Security Service of Ukraine at the conference last week. The way their cooperation works is that when they receive any information related to crime either from abroad, from inside of the country, or from their private contacts, they are required to share this information. I am not too sure if they have to share it with MVD [Ministry of Internal Affairs]. During my time, we signed an agreement/law (*nakaz*) according to which the Computer Emergency Response Team of Ukraine, as part of the government services of information protection, had to share such information with the Security Service, as the Computer Emergency Response Team of Ukraine is not a law-enforcement agency and cannot investigate this crime, document it, arrest people.

- **Q:** *Is the Security Service of Ukraine working with the hacker community officially or not? Do they have resources and capabilities to fight cybercrime alone/without any outside help?*

- **A:** Again, I do no have any precise information on this topic. You should understand that this is quite a close organization. However, the effectiveness of this organization is quite doubtful because they lack money, and the effectiveness of any organization depends on finances, after all. Again, there exist a problem of paying appropriate salaries to technical specialists. At the Security Service of Ukraine, operational specialists (*opertuvni spetsialistu*) are better than those at the Ministry of Internal Affairs, probably. But, good technical specialists are required for cybercrime investigation. This requires good technical possibilities, channels, servers, telecommunication equipment, which is quite expensive. I do not know and I cannot not comment on the effectiveness of the Security Service of Ukraine, but as a former employee and one of the people in charge of this department, and from talking to those who continue working in this department, I can say that very little has changed. The effectiveness is not zero but it is very low. Especially right now when all resources of law enforcement agencies are concentrated on fighting terrorism, occupation of Ukraine, and Russia aggression, etc. Therefore, their main tasks are to fight terrorism, cyberterrorism, and information war, deal with social networks, defacements, cyber-attacks on the governmental websites, including the websites of the President, National Bank, Verkhovna Rada [Parliament], etc. As long as war with Russia continues, these problems are their "0" "1," "2," and "3" priorities. And eventually, they might deal with hackers who rob a company. For instance, they will probably investigate crimes as attacks on the National Bank, or a systematic attack on PrivatBank, for instance, or any other huge bank, not necessarily a public but private bank, which has a

huge influence on the financial system of Ukraine. As there are critical infrastructure objects, attacks on which can influence overall security of the country. Other example of these can include: a fake presidential address is posted on his website; the work of important banks is being blocked. All this can cause real damage. Another example include the attacks that are committed against the SCADA systems, or nuclear power plants, hydroelectric stations, if they are internet-controlled. Such actions are example of cyberterrorism and the Security Service of Ukraine should investigate those attacks, at least to what extent their abilities allow them to do that.

- **Q:** *How effective are non-state actors in leading the information warfare and committing cyber attacks? How much damage is being done by those attacks? Do they have any influence on the population? Do any governmental organizations or non-state actors try to counter this information warfare?*

- **A:** Except the Federal Security Service's 18th center in Olgino, many other non-state sponsored groups commit attacks because of their ideological ideas or because of their personal benefits. If we speak about the people of Ukraine, we speak of the state-sponsored information warfare, massive *fakes* etc, that we all can witness every day. This is what any citizen observes online. For instance, if the website of the President or Verkhovna Rada [Parliament] is blocked, it is not a big deal for any citizen. He will not be able to read a draft law or law today, but he can tomorrow. If there is a difficulty in exchange of correspondence, this is not a critical situation, no one dies, no one is hungry, no one loses his home. Therefore, if we evaluate the influence of these cyber-attacks on public, it is minimal. As far as I know, before this war in Ukraine, there was a very low level of online control in the service sector or power stations, or hydroelectric stations. There is no point attacking those stations, as they are completely independent. Even if they have the SCADA systems, those systems are used for collecting information online. For instance, an employee of such stations uses the internet to collect information on the market of electro-energy tariffs. The network that he uses to connect to the internet is not connected to the system that is used to control the station. This was the trend for a long time and I am afraid nothing will change for a while. If we speak of our side, we have Eugene Dokukin, who is the most prominent fighter against Russia's cyber aggression. However, his methods are not all legal. He publishes his daily updates on what he has done, which include how he prevents the financing of terrorism, which accounts he has blocked, etc. He uses many legal as well as illegal methods. For instance, defacements are actually against the criminal code of Ukraine. If we speak of work of the Ministry of Information, I cannot say that their work on information war prevention is obvious. Maybe they are doing work sometimes, but for us, as specialists, it is not obvious. We are not even speaking of the influence of their work, but just a demonstration of their skills in some way – I cannot speak of this, as I do not have such information.

- **Q:** *Can we call the Ukrainian Cyber Forces' actions "propaganda"? How effective are they?*

- **A:** I stopped following him and his actions a year ago or so. He has no connection to propaganda at all. He is interested in concrete operations, for instance, in blocking terrorists' accounts and websites, blocking domains, and Facebook accounts by filing complaints to the administration. These are examples of legal actions. Or, for instance, another not too legal approach is to find a website vulnerability and block this site. Or another illegal technique is

to use a direct denial of service attacks. For instance to find a website vulnerability and to change the website content – a so-called *defacement*. This is also illegal.

- **Q:** *Can we view his actions as war operations?*
- **A:** His personality type is... he does not like talking to people too much. We all knew him before the war started. He likes to find problems/vulnerabilities. For instance, he scanned the Ministry of Defense website and found many vulnerabilities. He wrote about this to the ministry. The ministry did not respond to him for a long time, and the vulnerabilities were not fixed. He complained for a long time because of this situation. He talked about this for a long time to many people. Despite the fact that this website had vulnerabilities, these vulnerabilities were minor and it was almost impossible to exploit them for criminal purposes. For instance, an HT programmer left out a piece of a code. Of course, it is a vulnerability or sloppiness, but it is not a huge problem. Even a few years ago, Dokukin used to love scanning governmental website resources and to send those agencies letters with a long list of vulnerabilities. He would say, "this is what I have done and you are not making any changes. Six months have passed since I told you about those vulnerabilities and you are not implementing any changes. You are paying lots of money to huge companies, but you have many issues (*a u vas tak kin i ne valiavsia*)." This is how we know Dokukin. It is difficult to talk to him. He attended our conference a few times. He is a bit scandalous. He has some physical limitations (in terms of his health), so he leaves his home very rarely. Maybe these limitations influenced his character. He lives more in a virtual world than in real one. Nevertheless, what he is doing, I venture to say that it is more good than bad. Of course, he uses those methods [meaning illegal]...but what he is doing is effective. At least, he is doing something. I do not think that our government spends anything on fighting cyberwar. At some point ten years ago, there existed a secret department on special information operations and cyber war within the Security Service of Ukraine. It was a high secret department but everyone knew of it. It existed for a year or two and then it was shut down, around 2007 or 2008. Maybe it was reopened after the Estonia attacks. I do not know as I left the Security Service of Ukraine in 2005 and was not interested in what was happening there.
- **Q:** *If we try to sum it up, can we say that we witness mostly propaganda from the Russian side and cyber-attacks (war actions) from the Ukrainian side? Have I understood you correctly?*
- **A:** From the Ukrainian side? Our people understand that everything is upside down (*vse z nig na golovu vystavleno*). Their disbelief in Russia's propaganda motivates counter-propaganda in Ukraine. This is how counter-propaganda, not sponsored by anyone, works in Ukraine. Let me explain what counter-propaganda means – explaining that this is true, that it is fake, and that people are being lied to on both sides, Ukrainian and Russian. There is no concrete strategy by the Ukrainian side. I do not see it. Ideally, it should have been done via coordination by the National Security and Defense Council, the Security Service of Ukraine, Ministry of Internal Affairs, or by civil society groups. They should have provided clear instructions on the ways we should achieve a specific result. There is no Ukrainian broadcasting in Europe, but there is a Russian one, and this is one of the components of the information war. If we speak of cyber war, we use offense much more than defense, and volunteers and independent groups are doing all this.
- **Q:** *Is the state doing anything in this vein?*

- **A:** It is trying, or at least it pretends that it is doing something. But to pay people... The system should be built similar to the one in Olhino. They should gather people in one place and put them in front of computers. They should take a huge task, break it down into smaller pieces, and divide those small pieces among specialists. Each team leader should be aware of his team's tasks and responsibilities on each level of the team. Each next person in charge should know more, and etc. They should have a strategy and tactic. We do not have such approach in Ukraine. I do not [know about this]... as you know, what two know, everyone knows (*shcho znayut dvoie, znaie svuni*). If we had at least 100 of those paid specialists working by using this scheme, it would have been known. Since the information is not out there, it means that we do not have such a scheme. And how can we have such a scheme? Russia sells oil and gas and earns billions. And they have money even until now while Ukraine has nothing but loans. Only a very rich government can allow itself to finance these projects, which do not bring any profit but is only ideological work. Only a very rich country can spend money on ideology.

- **Q:** *Do they have independent hackers in Russia? Are all of them working for the Kremlin?*

- **A:** Definitely working for the Kremlin. In Russia under the current regime, nothing can be independent. The definition of being independent is a philosophical term, as no one in any country in the world can be completely independent. However, considering the responsibility of police and special forces, and the police state that was built under the total control of police and special forces over the citizens, they [citizens] are not independent. In Russia, they practice such control especially over the internet and business. No one rentable business works in Russia without the Federal Security Service of Russia, the Ministry of Internal Affairs, or the Kremlin administration protection. Therefore, it is hard to speak of being independent... of course, some organizations say that they are independent. One day they become prominent, especially in the West. The next day the Federal Security Service of the Russian Federation workers come to their office and tell them what they are allowed to say, what they are not allowed to say, and what will happen if they do not listen to the former's instructions. This is a complete lie [referring to being independent in Russia]. Nothing in Russia is done without the Federal Security Service's control.

# 4 Interview 4

## 4.1 Email: July 8, 2015

- **Q:** *How would you characterize the work of non-state actors (e.g., Ukrainian Cyber Forces, Cyber Berkut, and Anonymous Ukraine) in leading attacks against Russia? How effective are their means in achieving their goals?*

- **A:** I'm confused. I thought Cyber Berkut was pro-Russian. What I understand is that most of their cyber-attacks were little more than publicity-focused pranks.

- **Q:** *Would you view the actions of the Ukrainian Cyber Forces (and any other non-state actors) as propaganda? Would you view them as war actions?*

- **A:** Mostly propaganda. I am not quite sure what a war action is, but at least in the American context, no speech and limited speech acts can qualify as acts of war.

### 4.2 Email: July 20, 2015

- **Q:** *You mentioned that "Super-patriotic hackers on both sides have conducted harassing, but small cyberattacks on each other." The footnote that you refer to mentions Cyber Berkut. Do you think that they are super-patriotic hackers or, simply the Kremlin-recruits that were given a task to run the information war and commit cyber-attacks in a particular way? In addition, how would you characterize the Green Dragon? Are they a part of the cyber group unofficially or sponsored by the Kremlin?*

- **A:** Many super-patriot hackers may as well be recruits (many are not, however). The term implies that they are not on the government payroll (at least not as civil servants – could be wrong in this particular case). I am unfamiliar with Green Dragon.

- **Q:** *You mentioned that there were no attacks on critical infrastructure in Ukraine and Russia? Can we conclude that such attacks did not take place because one, the Ukrainian side does not have capabilities to execute this type of attack; two, there is no critical infrastructure in Ukraine that has internet-connected control (in addition to the reasons you already mentioned in your chapter)?*

- **A:** Capabilities always have to be measured with respect to the other side's vulnerabilities (there are perfectly serious people who assume that any system can be broken into, but they are many systems which have not been broken into either). I doubt that the first is true because there are very talented hackers in Ukraine. #2 may be true, but many systems that are unconnected today could become connected tomorrow – bad for security, but not everyone worries as much about cybersecurity as they could.

- **Q:** *Would you please elaborate on your statement: "some of its best (or at least best criminal) [implying Ukrainian] hackers are of Russian descent, hence unlikely to work for or on behalf of Kiyv." How do you know that they are of Russian descent? Is there any published study that talks about this?*

- **A:** None that I recall. That was just my impression.

## 5 Interview 5, Skype call: July 10, 2015

- **Q:** *Can we speak of cyberwarfare and information warfare in Ukraine separately? Or are they interconnected? How effective is one or the other in Ukraine? Please speak on both sides, Ukrainian and Russian.*

- **A:** I think it is a mix between Russia, Ukraine, and the West. Russia is waging information warfare against Ukraine, it is also waging it against the West, and, to some extent, it is waging it against Ukraine in the West. So when Russia says this: "Ukraine is run by the Nazis or there was a putsch, or Ukraine is the failed state, that is an attack on Ukraine in the West." The message in Ukraine is different in a way, a bit less important, I think. The biggest damage Russia can do in Ukraine is in the West because Ukraine cannot win this without Western support. Ukraine has done a pretty good job in trying to deal with Russia's information warfare, but it is up against a multi-billion dollar propaganda machine, and they are pretty effective.

- **Q:** *Is there any separate cyberwarfare taking place?*
- **A:** Cyber was very important for the Russians at the beginning, and they were able to get all over Ukrainian government networks and they probably had better picture of what was happening in the military, defense, security world than the Ukrainian authorities did. So that was a very, very big deal for them and they were very successful in that. And if you google it, you've got the name of it [...] something like Ouroboros...
- **Q:** *Yes, Snake.*
- **A:** Snake. They were pretty good at that and I am sure they are still are. Maintaining a secure network is very difficult, and the Americans are not very good at it. Moreover, you have to pretty much assume that Russians have a full access to most things inside Ukraine still. It is very hard to clean a network once it has been affected.
- **Q:** *Do you think they have such an easy access to the Ukrainian network because of its former Soviet connections (e.g. former Soviet employees are still employed in some agencies; lots of Ukrainian agencies were built using former Soviet Union standards)? Or because Ukraine does not have an adequate protection?*
- **A:** I think it is both. In order to keep networks secure, you need to design it properly, and the other is to prevent a breach. If you have a properly-designed network then the breach is less serious. The information is compartmentalized. You've got this idea of defense and debt, and it is very hard to get what they call "route" or "route care," which is the ability to change routes on network. I think Ukraine was weak on both – the networks were not well-designed; and on the human side, [not clear what he says] easily penetrable. You need only one bad guy to put a USB stick in one port or one computer, and on a badly designed network, and you've got the whole thing.
- **Q:** *How involved are non-state actors in this conflict (both sides)? And what is Russia's relationship with its hacker community?*
- **A:** I do think that there is a clear dividing line, as far as there has been lots of Russian hackers who are working for both, cybercrime organizations and for the Russian state. That is a bit different from China where you have, basically, military units that do this. In Russia, my impression is this, and I recommend you to look at FireEye's report about Russia's hacking which was very good. What I know basically comes from that. We do see a clear overlap between military intelligence and criminal, and particularly between intelligence and criminal. And also the use of these [not clear what he says] disruptive tactics as well as botnets and denials of service attacks which again are a good choice for criminal networks because they are engaged in extortions, but they also useless in [not clear what he says] mechanism.
- **Q:** *To what extent can we associate recent cyber-attacks in Ukraine (and elsewhere) with the war? Or propaganda? Did they influence the course of the conflict?*
- **A:** I think you have to separate what you mean here by cyber-attacks, distributed denial of service attacks over political weapon, or getting onto a government network and reading emails. This is something all countries do to other countries. All big countries have capabilities to do this. Also, trying to read the negotiation partners' emails and documents is standard

espionage. But it seems to me the main dimension of the conflict is number one – military, number two – information, which is not quite the same as cyber; and number three – financial or strictly economic. So I do not think that one could say that the Russians are [not clear what he says] cyber as in terms of penetrating and disrupting networks is the main thing that Russians are doing to Ukraine, as there are easier things that they can do.

- **Q:** *In your article, you mentioned that Russia aims to achieve the following three goals: to recreate a Russian empire, to stop the European Union's ability to control energy pipelines, and to weaken and divide the West. How effective are cyber-attacks and information warfare from the Ukrainian side (state or non-state actors) in preventing Russia from achieving these goals?*

- **A:** Among other things about cyber espionage is that you do not really know how effective the other side has been. So we can well assume that Russia is well-informed about Western divisions and maybe they have some targets there. And Germany, they know what Russia [not clear what he says]. Assessing the effect of cyberespionage is really a "guess what." But we can say that Russia has been really effective on the information warfare as they are trying to get across this idea that Ukraine is an author of its own misfortune, that Ukraine is run by extremists and the European Union is aggressive and pushed into Ukraine. There are all these things, which are basically nonsense. And Russia is just responding to North Atlantic Treaty Organization's expansion entirely, there is so much nonsense that you hardly know where to start. It has had an effect. Did I answer your question?

- **Q:** *Not quite.*

- **A:** I could not hear your question. I forgot your question.

- **Q:** *Edward Lucas mentioned that Russia aims to achieve the following three goals: to recreate a Russian empire, to stop the European Union's ability to control energy pipelines, and to weaken and divide the West. How effective are cyber-attacks and information warfare from the Ukrainian side (state or non-state actors) in preventing Russia from achieving these goals?*

- **A:** Oh yes. The main aim at this moment is to demoralize Ukraine, to make the Ukrainians feel that the European values were just "baloney." The whole idea of Maidan was just a mistake. The West is not really going to help. You face decades of war, poverty, and division. And if they can really make Ukrainians feel that, then maybe Ukrainians have already had this, not very good governments and [not clear what he says] deal with Moscow. So if they can exhaust and demoralize Ukraine, I think this is the number one goal. And for that, they just need to keep on doing what they do really, because the West is not [...], the economy is bleeding at the moment, and the West is not really helping you, not helping nearly enough. So the pro-Western sentiment is gaining, that is really sad. However, I think it is still possible what Ukraine will turn around and reform its work and people will say, "Yes, this is going ok." But, I think at the moment Ukrainians can quite reasonably feel abandoned by the West. And that is a very good combination of despair in Ukraine and passivity in the West; that is a perfect mix in the Russian point of view.

- **Q:** *Can we witness propaganda coming from the Ukrainian side?*

- **A:** Ukrainians are probably the world's experts in dealing with Russian information warfare. I have a huge respect for StopFake, for example. So I think you [implying the Ukrainians] are doing the right thing but I just wished that Western media paid more attention to analysis and reporting, like the expertise that you have on this. And one thing that the Ukrainians forget or sometimes I would say overlook is that the West is so busy with, and this is not for quotations but I wrote this for the Economist, but you've got the Greece Crisis, the Islamic State, and migration – all piling up on the one's desk. And people think, "Ukraine, yea, there was a ceasefire, do we have to worry about that right now?" And this is good for Russia. I am not saying that Russia creates these sorts of crises but it helps the Kremlin. They can just carry on, slowly destroying Ukraine psychologically, while the West is busy with other stuff.

- **Q:** *Is there any overlap between information warfare, cyberwarfare, and kinetic operations in Ukraine? Please speak of both sides.*

- **A:** I did not know enough about military side to have a view on that. But I could imagine that there is a "cyber" battlefield that is so separate. So that is all about. Try to work where the troops are by looking [not clear what he says], and trying to read their communication. My thing is that Russia's greatest weapon, Russia's greatest advantage, is the ability to break the other side's moral. And if you destroy, confuse the command and control, and demoralize the soldiers in a front line, then you can win without having to do too much on the military side. And the Crimea was the best example of that, where you had large numbers of well-armed Ukrainian soldiers in the Crimea who could have been led, could have resistant, could have made the cost of operation far higher for Russia. Perhaps, even impossibly high [cannot hear what he says] in their orders. I think I exemplified the way Russia sees these things.

- **Q:** *Can we label such warfare as psychological?*

- **A:** If you read the Gerasymov Doctrine [...] analyzed very brilliantly in Latvia: If you get non-military stuff right, the military end of operation is just a detail. I think the Russians did not expect such strong military resistance in the Ukrainians. [not clear] to the cyber and also volunteer battalions. Ukrainians have placed much stiffer military resistance than the Russians were expecting. And the Ukrainians did not fall in places like Odesa, they do not want to be part of Novorosiia. Putin had to do on the military side more than he thought he was going to. I think that the fundamental part of Russia['s plan] is that Ukraine must not look a success story. If possible, Ukraine must look like a failure. And if they can succeed, which in part is a matter of economic pressure and also propaganda information warfare, then the Ukrainians will give up on the West [not clear].

- **Q:** *Is Russia using patriotic hackers for this information warfare? Are those hackers state-controlled?*

- **A:** You are using these terms that have broad meanings, "cyber" and "hackers," and so on... I think Russia has an ability to look inside of all sorts of decision-making processes, using cyber espionage means. They can also disrupt or degrade the other sides' capabilities [not clear] if they want to. I have not seen much of that. I think every now and then we see the direct denial of service attacks on the Ukrainian websites. To me honest, I have not seen any of these that makes me think that is a particularly big deal for the Russians.

- **Q:** *Why has Russia not used "visible" cyber warfare tactics in Ukraine, like those used in Estonia and Georgia? Why does Russia not use the command and control cyber operations as it was seen during the Georgia invasion?*
- **A:** That is a good question. Estonia was one of direct denial of service attacks and in Georgia there was massive penetration of Georgian networks. They are quite separate things. There was a little bit of defacement attacks and things like that. I will be cautious of marking Georgia and Estonia together as similar things. One of the equivalent of an artillery attack while the other one was sort of special forces. Categories and precise language are really important in this. But I do not know, it is a good question why the Russians are not doing more in cyber [work] in Ukraine. Maybe they are already on their network and they do not want more. If you disrupt things then people start changing everything. So if you just sit there quietly and observe what it is going on, I strongly doubt that even the Security Service of Ukraine has got their networks clean at this moment and that is a very good thing from the Russian point of view to just sit there. They probably know more what is going on in the Ukrainian army than Yatsenyuk or Poroshenko do. That is a sort of invisible cyberespionage rather than cyber-attacks, and it has not completed attacks on Ukrainian critical infrastructure. If they wanted to they truly could. They could have made on power stations stop producing power [not clear]. They probably see that as escalation, and that it would probably attract a lot of unpleasant attention from the European Union if they had done that.
- **Q:** *I've actually talked to one computer scientist in Ukraine about critical infrastructure protection and he mentioned that, in fact, the attacks are not possible as these objects are not connected to the internet. Would you agree with such an assessment?*
- **A:** It is an advantage of being a backward country. You reduce your own vulnerability. I would imagine it could be true for some objects. But I still think that if he wanted he could probably bring down the entire Ukrainian telephone system, if he wanted to. I am not a huge expert on sort of destructive cyber-attacks. There are other people that you could probably talk to. I am more interested in the propaganda side.
- **Q:** *How would you characterize work of the Ukrainian non-state actors (the Ukrainian Cyber Forces, or Anonymous Ukraine) in information warfare?*
- **A:** I think Ukraine has done really well on the information front. I think there are, and I do not know too much of it, but there are very good Ukrainian hackers who put their efforts on the government's side. I will get back to what I said earlier, StopFake and its information warfare efforts have been really admirable. The Ukrainian government's propaganda is pretty old in fashion and the strategic location [not clear] is pretty lame. And a lot of Ukrainian embassies do not seem to know that there is a war going on, are intimidated or have low capability. When people deal with information, how much value in making mistakes rather than getting information correct? But I think that behavior of non-state actors are exemplary and everyone involved in the business is sort of...
- **Q:** *When you mention non-state actors, do you mean civil society or non-governmental organizations?*
- **A:** Yes, this is what I meant.

# 6 Interview 6

## 6.1 Meeting: July 1, 2015

- **Q:** *How would you characterize information war in Ukraine? How effective is it?*
- **A:** Russia started information war on the region of Ukraine. The evidence for such victory is a social question. However, Russia did not win information war outside of this territory. If it had won, then no country would have supported Ukraine. Russia is winning information war in some countries, using illegal means, and usually such victory is temporary. For instance, it is winning in Greece now, a country, which announced default and is hoping to get some support from Russia. In Donbas, Russia is winning. In the unoccupied territory of Ukraine, Ukraine is winning information war.
- **Q:** *Do you think Ukraine is leading information war as well? Is there any evidence of the Ukrainian propaganda?*
- **A:** There is no Ukrainian propaganda. Yes, Ukraine forbade to broadcast TV shows that have war themes. Yes, we forbade, with some delay, the Soviet symbols. This was not an act of propaganda; rather we did what we were supposed to do a long time ago, following the tradition of other Soviet countries, such as Estonia, etc. Propaganda could be defined as sending the same message using various channels. Usually, the state sends the same message. We can witness this happening in Russia. Everything that was independent in Russia crashed. In Ukraine, on the contrary, we have not witnessed any changes; therefore, there is no propaganda. If the state had created some propagandistic messages, then it should have started blocking all channels, as every channel has a different message. Moreover, every channel makes a decision which political message to send. For instance, Kolomuiivskii is following his own goals – he would like to go back to politics — and he needs a channel to achieve such goals. He sees that most people have a patriotic mood and uses this. Such approach could be called as editorial politics of the channel not state propaganda. In Russia, on the other hand, editors of all [media] channels are being gathered and are told which message they should send and which main themes should be broadcasted. For instance, last year, we witnessed this when all Russian channels talked about Novorosiia and the Donetsk People's Republic and Luhansk People's Republic. Then, when the topic changes, language and expressions that the channels use change. The Moldovans are very scared now as they say that a similar information war is happening there. The main message states that the rights of the Russian minorities are being discriminated; the Russian language is being discriminated and forbidden in use. Moreover, Russians have been placing lots of weapons and military technology in Transnistria. Thus, the Moldavians are very scared of becoming Russia's new target. The Moldavians are interesting in working with us [StopFake] to create a similar entity to our project. StopFake started on March 2, 2014. It is composed of the Ukrainian journalists. In the beginning, it was oriented towards the Crimea and East Ukraine. Now, we have audience in Russia. Our organization follows the European standards – we understand the need to provide two opposing views and the truth will lie in the middle. In the case of Ukraine, there is only black and white, and there is a desire to find the truth. Once we saw this, we decided to take information that goes from the Russian sources and provide compromises to it, using videos and photos. The main principle is not to disprove everything by words

only (as both sides are the interested parties in this conflict) but to use evidence to achieve this. Often we take the North Atlantic Treaty Organization's speeches that demonstrate misinformation by facts, photos taken from surveillance, etc. Fighting propaganda should be achieved by providing facts.

- **Q:** *How effective are non-state groups (e.g. Ukrainian Cyber Forces) in leading information war in Ukraine?*

- **A:** They are effective in influencing youth, however the internet (online environment) is not the only element. Russian propaganda became successful because it consists of many elements: TV, newspapers, and social media sources, where many young people remain active. Earlier the youth was resistant to propaganda because they were able to use the internet in order to find an accurate description of the events. Now, the situation is quite opposite because the internet is full of propaganda. A few news channels in Russia that tried to send the opposition's message were closed (e.g., *NTV, Dozhd'*). Even business channels decided to follow the official message in order to not be shut down. Now the Russian media is using a new technique – they provide 10 different versions of the same event; all those versions are often not true. And when the Ukrainian channel provides the 11th version, which is actually correct, people do not believe it because they are tired of lies. The goal of the Russian channels is to show that "Nothing is true, everything is possible" (from the book by Pomarantsev). StopFake, Ukraine Today, UkrKryz-tsentr, and InterNewsUkraine compose UkrWorld. We meet once a month and create similar messages (not propaganda). At the same time, we also share our experiences from traveling abroad and what we heard of the Ukrainian image abroad. We discuss how other countries perceive us, why they perceive us in such a way, and what can be done to improve our image abroad.

- **Q:** *How has the Ukrainian identity been shaped by this information war? Has the meaning of being Ukrainian changed? What does it mean to be Ukrainian now?*

- **A:** All people are showing their protest by wearing T-shirts, for instance, and in such a way one can see what it means to be Ukrainian. By their protests, people demonstrate that they are Ukrainian.

- **Q:** *How can we fight Russia's propaganda?*

- **A:** Civil society started being active after the EuroMaidan. Once the war started, people understood that the state does not have money and realize the importance of creating civil society. The Ukrainian state is not helping in the creation of this civil society; there is no "inner censorship" (*vnytrishnia tsenzura*). Civil society has been neither supported not blocked by the state.

### 6.2 Email: July 11, 2015

- **Q:** *You mentioned that the UkrWorld meets in order to discuss similar messages that should be shared on media sources (besides other activities that are being discussed during those meetings). You also mentioned that those messages are not propaganda. How does the UkrWorld make sure that those similar messages transmitted by various channels in Ukraine are not taken as Ukrainian propaganda?*

- **A:** Not quite. We do not discuss messages that should be spread in Ukraine. Each edition has its own editorial policy and its objectives. The group is called UkraineWorld, and we all meet at the conferences abroad, round tables, and give interviews abroad to foreign media. So we can spread information about Ukraine abroad. That is what we are discussing at the meeting. The information we distribute is not propaganda, because it is true, even if it is negative. We recognize that Ukraine has still corruption, that some soldiers in Ukrainian battalions break the law and are wanted under the law, etc. These messages can hardly be called propaganda here or elsewhere. Our goal is to communicate and share information that we have on topics that are important to us. For example, if someone is planning to speak at a conference in Europe on the theme "The presence of Russian troops in Ukraine" he turns to the other members groups who did not attend that conferences, asks to share all the facts and evidence that they have on the topic. All members share their information and this person is super prepared to present. This is the main reason why we have this group. We do not spread misinformation; we recognize mistakes and faults of our government; our group is independent from the government.

- **Q:** *To what extent can we associate information warfare in Ukraine (and elsewhere) with the war? Did they influence the course of the conflict?*

- **A:** In Ukraine it all began and continues with Russian media misinformation campaigns. They misinformed people in the Crimea about mythical "fascists" in Kiyv. As a result, the Crimeans supported the Russian troops when the Ukrainian troops entered the Crimea. Russia media continued to lie about the Nazis, as if they existed and came to power in Kiyv and were planning to kill the Russian-speaking population in the Donbas. As a result, population in the Donbas picked up weapons (and some are still holding it and continue to fight) - and went to fight with Ukrainians supporting Russians. Therefore, information warfare in Ukraine is an indivisible part of kinetic war and is one of the main reasons why physical violence has started. If we did not have information warfare, the kinetic, physical war would not have started, and even if it had, it would have lasted in a completely different manner.

- **Q:** *Edward Lucas mentioned that Russia aims to achieve the following three goals: to recreate a Russian empire, to stop the European Union's ability to control energy pipelines, and to weaken and divide the West. How effective are cyber-attacks and information warfare from the Ukrainian side (state or non-state actors) in preventing Russia from achieving these goals?*

- **A:** From the Ukrainian side, there are only defensive operations. We try to defend against their information warfare by refuting their lies. However, we do not attack Russia using our own lies. In Ukraine and Europe, the Ukrainian side is currently winning information war since most of the European countries has adopted sanctions against Russia. However, Ukraine alone cannot win this war. Europe should help Ukraine to fight this information warfare (some of the European countries, such as the Baltic states, are doing this already in an effective way).

- **Q:** *Would you evaluate Russia's and Ukraine's information warfare as psychological warfare (using such tactics as playing on positive emotions by personifying soldiers and demonizing the West)? How effective is it?*

- **A:** Yes, definitely. Psychology is being used for creating propaganda. This is the most effective method. If propaganda have not played on emotions (so-called or even killed children, cruel soldiers, crucified boys), it would never be effective. I'd advise you to talk to psychologists on this topics as they can share some valuable information on how using emotions helps to persuade people.

## 7 Interview 7, Email: August 9, 2015

- **Q:** *How would you characterize the work of non-state actors (e.g. the Ukrainian Cyber Forces, Cyber Berkut, and Anonymous Ukraine) in leading information warfare and executing cyber attacks against Russia? How effective are their means in achieving their goals?*

- **A:** Well, typically, these groups have skilled hackers in their ranks, but not skilled enough to pull off a major take-down of governments. They can hack social media and email accounts, and government websites that aren't very well secured. But they cannot do little more than that. In terms of "information warfare," they've played a minimal role at most. There have been instances where they've allegedly hacked and stolen emails from government accounts, but the information obtained from them has not pertinent to the war, and therefore has made very little splash in the press.

- **Q:** *Would you view the actions of the Ukrainian Cyber Forces (and any other non-state actors) as propaganda? Would you view them as war actions?*

- **A:** As propaganda, yes. They have an agenda. As war actions (and I'm not exactly sure what you mean), I'd say no.

- **Q:** *Do these actions in cyberspace overlap with kinetic operations on the ground? Are they complementary? How effective are they? Please speak about both, Russian and Ukrainian, sides.*

- **A:** I can't say they do. I don't have enough info on this.

- **Q:** *Is there cooperation between non-state actors and law enforcement agencies in fighting Russia's cyber-attacks? Are there any efforts tailored towards stopping Russia's information warfare? How effective are these efforts?*

- **A:** There have been joint efforts, but they are few and far between, as far as I understand, and they have been tailored to combatting Russia's information warfare. However, the Security Service of Ukraine likes to keep a tight lid on its operations, and so I don't have much in the way of specific information regarding those joint efforts.

- **Q:** *Does the Ukrainian government have a cyber unit? How would you evaluate its capabilities compared to non-state actors (e.g. the Ukrainian Cyber Forces) in Ukraine, or Russia's cyber state or non-state actors? Are there any plans to develop stronger capabilities of such forces? Do those units execute cyber-attacks? Do they take part in information warfare? Why? Please speak about both sides.*

- **A:** Yes, the Security Service of Ukraine does have a cyber unit that is subordinate to the counter intelligence department. As I understand, they have some skilled people on staff, but finding highly talented people to work for very little pay (government jobs typically pay poor, meager salaries) is difficult. Many of those people skilled in the IT sector in Ukraine prefer to work for private companies who pay larger salaries or hacking for criminal enterprises.

- **Q:** *To what extent can we associate recent cyber-attacks in Ukraine (and elsewhere) with the war? Did they influence the course of the conflict? What network security lessons can we learn? What national security lessons can we learn? Is the concept of cyber war still more hype than reality?*

- **A:** I wouldn't say that cyber-attacks have played a large role in the conflict.

- **Q:** *How would you evaluate Russia's cyber tactics in Ukraine? How successful are they? How do the tactics used by state and non-state actors compare?*

- **A:** Honestly, it's difficult to know who is behind each attack. That being said, because I can't think of any cyber-related event in particular that has changed the course of the conflict, I would say that whoever is behind the cyber-attacks we've seen has not been largely successful.

- **Q:** *Edward Lucas mentioned that Russia aims to achieve the following three goals: to recreate a Russian empire, to stop the European Union's ability to control energy pipelines, and to weaken and divide the West. How effective are cyber-attacks and information warfare from the Ukrainian side (state or non-state actors) in preventing Russia from achieving these goals?*

- **A:** I would say the Ukrainians, in this case, have not been very successful. I think Russia has a huge advantage in the information game, and Ukraine is just playing catch-up.

- **Q:** *Would you evaluate Russia's and Ukraine's information warfare as psychological warfare (using such tactics as playing on positive emotions by personifying soldiers and demonizing the West)? How effective is it? Does it overlap/map out with the kinetic operations on the ground?*

- **A:** Well, Russia is a master manipulator in terms of information warfare. Through state media and propaganda, the Kremlin has, with great success, been able to influence the Russian population, but also the Russian-speaking population in eastern Ukraine. We know this because people on the ground repeat the stories they hear from Russian state media and propaganda. They use the say terminology in describing certain people, groups and events. For example, the words "junta" and "fascist" come to mind. They weren't in most people's daily lexicon prior to April 2014. Now we hear them used all the time. And in supporting their use of them, they recite fictitious stories told by Russian state media, such as the famous incident of the "crucified boy" in Sloviansk.

- **Q:** *Do you think the Ukrainian information war exists? Does Ukrainian propaganda exist? How effective is it? If it does not exist, why not?*

- **A:** Of course Ukrainian propaganda exists. Kiyv itself pumps out plenty of its own propaganda. The president owns one of the largest TV channels in the country. You can count everything reported by it as propaganda. The government has also created the Ministry

of Information, which is the clearest example of propaganda tool. There is also plenty of non-state sponsored propaganda, which is, unfortunately, what much of Ukraine's media has become. I think some of it has been successful within Ukraine, but certainly, it has little effect internationally.

- **Q:** *Why is Russia using cyber criminals to attack Ukraine? Wouldn't it be better to hire cyber professionals? What is the goal and reason for such tactics?*
- **A:** I didn't know that Russia is using cyber criminals. However, one thing to keep in mind is that few governments pay cyber professionals more money than they would make in the private sector.

## 8 Interview 8, Skype call: July 15, 2015

- **Q:** *Can we speak of a separate cyberwarfare (attacks that leave to disruption) and information warfare (propaganda and its psychological aspect) in Ukraine? Or are they interconnected? How effective is one or the other in Ukraine? Please speak of both sides, Ukraine and Russia*
- **A:** I would actually separate these two things, as cyber war is rather technical. It is a question more for technical experts. Kenneth [Geers] probably can tell you more about it. Information war that takes place in cyberspace is very different; its methods and results are completely different from those used for cyberwar. Information war is propaganda. It is just a type of propaganda. And the war between Ukraine and Russia has demonstrated - maybe some people did not even expect this – that information that moves freely in cyberspace with no borders can be used as propaganda. It demonstrated that it [information war] exists for a specific layer of population not only in Ukraine but also in Europe. There are many people who easily believe in what they hear. I think such an easy exposure to propaganda depends on what kind of people they [these people] are. The majority of them are those dissatisfied with their positions in the society, economic and political positions – the protecting layer of population (*protestnyi prosharok lyudei*). By believing in what is presented to them via information messages, they try to find some alternative ways, explanations of what is happening in Europe and in global and socio-economic developments.
- **Q:** *Do you think the language can influence this development? For instance, some people do not speak English and do not have an access to the alternative sources of information.*
- **A:** No, I do not think so. We can observe this phenomenon in Europe. There are many people in Europe who believe in what Russian media produces in English. Language does not play a key role here. Propaganda happened to be quite effective as there are people who want to believe in it. This is the main reason. It does not matter what language is used to deliver it.
- **Q:** *Can we say that there is the Ukrainian propaganda as well?*
- **A:** You should understand that when a country is in a state of war, a lack of propaganda implies for a country just to easily give up. The situation is quite different [did not finish his sentence]. Let's take any Western country that is or was in a state of war, quite different laws become effective then; more military-oriented rules become a priority; freedom of speech

becomes limited; there are many dangers; a free flow of information can put many human lives in danger. Therefore, the Ukrainian propaganda exists to some extent. The representatives of the public sector see their main so-called destination in assisting in fighting this information war. They are not journalists who have to take into consideration various points of view. These people, on the contrary, see what the good and evil is and they take that side that they consider the good is.

- **Q:** *Is there any overlap between kinetic and military operations in East Ukraine? Are they complementary?*

- **A:** These events that take place in Ukraine are connected in such a way that if any issue, which occurs in Ukraine, could be initiated by Russia. Often Russia does it with the purpose of spreading its propaganda. At the same time, you need to understand how huge is Russia's budget to achieve these goals. Unfortunately, we cannot say the same about Ukraine. Everything is done by volunteers and civil society in Ukraine. If they see any problem, they start make noise about it and spreading information about it. Thus, it is quite hard to compare Russia's and Ukraine's propaganda as the former has lots of money and skilled specialists whereas only enthusiasm of its people is the moving force in Ukraine. I wish I were wrong about this. However, this is how it looks like.

- **Q:** *Thus, can we say that non-state actors and civil society are more active in Ukraine, and in Russia...*

- **A:** It is not quite correct. Having an active society is excellent but it would have been much better if these actions [referring to tactics of the Ukrainian side] were built on some type of a strategy, were done according to some plan. It is great that something is done spontaneously (it is better than nothing at all). However, it would have been much better if a state would provide some attention to actions by non-state actors.

- **Q:** *The state does not pay much attention to the actions by non-state actors due to the lack of funds, or...*

- **A:** Because there was no strategy related to information warfare in the past. No one was aware of such possibility [to use information as weapon]. At the same time, budget is also a reason. Secondly, the propaganda part was always quite important in Russia – a creation of information channels and internet firms. A lot of money was given to these initiatives as Russia's policies were oriented towards the outside world, towards conquering the global political and business influence. Unfortunately, Ukraine has never had such goals. Thus, there is no foundation right now that could be used to fight information warfare. Only now, some departments and policies are being created; some of them are related to information security. However, these initiatives are far from being ideal.

- **Q:** *Do you think Russia has similar volunteers that act independently from the government?*

- **A:** It is quite hard for Russia's volunteers not to cooperate with the government, as Russia is a totalitarian state that follows its active citizens' every step. It is quite dangerous for a group to exist independently from the government, even if this group follows the official governmental policies. Thus, these groups [refers to volunteers] should be under the government control.

At the same time, I think that there are certain groups of people who act according to their beliefs, but those beliefs are not based on human values and democratic values. In any society, there are such types of groups.

- **Q:** *How would you characterize the actions of such non-state actors as the Ukrainian Cyber Troops, Cyber Berkut, and the Anonymous Ukraine? How effective are they?*

- **A:** It is quite good that these groups exist and started working in this direction. Unfortunately, I do not see any actual numbers/statistics based on which we can evaluate their effectiveness. Ok, it is quite good that everyone knows of their existence. However, in order for someone to be able to evaluate their effectiveness, we need to know what their audience is, what their actions are, and what their official results are. Unfortunately, I did not come across such information.

- **Q:** *They have social media pages in Facebook and twitter. They also keep their audience updated on their actions. Therefore, such information could be found there. However, I am not sure how effective it is because it is quite hard to check the effectiveness of their actions. Are Cyber Berkut and Cyber Riot Novorosiia composed of the Ukrainian citizens that are dissatisfied with the current government or Federal Security Service of the Russian Federation's representatives? Cyber Riot Novorosiia is quite a new group and it was created in May of 2014.*

- **A:** I think it is the latter [refers to them as the Federal Security Service representatives or a group that cooperates with the Federal Security Service of the Russian Federation obviously]. You should understand that the Ukrainian citizens who are dissatisfied with the current government are not standing with their weapons in East Ukraine. We [refers to the Ukrainian citizens] have been able to elect officials, create parties, and suggest our proposals quite freely in Ukraine. And the situation that we have in the East, it is *apriori*. It sounds quite strange. Moreover, you are aware of the origins of the project "Novorosiia." No one in Ukraine has heard of this word until Putin announced it [refers to the project]. Therefore, it sounds quite strange to say that the citizens of Ukraine created such word all of a sudden.

- **Q:** *To what extent can we associate recent cyber-attacks in Ukraine with the war? Did they influence the course of the conflict? What network security lessons can we learn?*

- **A:** It is quite hard to say anything before we know true reasons for Russia's actions. You are probably aware that some think that Russia is trying to destabilize Ukraine using all possible means. At the same time, we should be quite careful of this point of view and should not label any view that does not correspond with the Ukrainian official view as Russian. It is quite doubtful that any Ukrainian organizations can execute cyber-attacks. These attacks are most likely of the Russian origin as their main goal is to destabilize Ukraine. Everything that takes place in the Ukrainian cyberspace is not as massive as it was in Estonia when the North Atlantic Treaty Organization was forced to reevaluate its cyber security strategy. I hope that the Ukrainian society will be able to prepare itself for the future threats, using single [cyber] incidents that already occurred.

- **Q:** *Actually my next question was going to be why has Russia not used "visible" cyber warfare tactics in Ukraine, like those used in Estonia and Georgia?*

- **A:** The main reason is that Ukraine is not viewed as a well-connected [to the internet] country. It is quite dangerous for the North Atlantic Treaty Organization to face a cyber-attack as the latter can affect all possible spheres of life starting with communal services and ends with public services. Unfortunately, it took quite a long time for Ukraine to be connected online. Some of such initiatives are still ongoing. Therefore, even if Ukraine faces any cyber attacks, damage caused by them could be fixed quite quickly. Secondly, Ukraine is a larger country than Georgia is and it has more capabilities to resist cyber-attacks. For instance, the Ukrainian civil society has been quite actively fighting Russia's information pressure with no funding, using its own initiative.

- **Q:** *Would you agree with the following answer to this question: "After the Soviet Union's collapse, Ukraine has been using Russia's equipment in its information sphere. Therefore, Russia does not need to hack anything as it already has the access to what it needs."*

- **A:** Cyber-attacks are not the same as espionage; they play a more destructive role; they are more like a terrorist act with the goal of showing population that not everything is stable in their country. This is my view on this. Russia has huge capabilities for collecting secret information. Estonia is not far ahead from Ukraine in terms of those capabilities. Thus, I would disagree with such answer. I think the main reason [why cyber attacks took place in Estonia and Georgia but not in Ukraine] are that number one - the role of cyberspace is more important in those countries [refers to Estonia and Georgia]; number two - Estonia became a testing ground where cyber weapon was massively used. Thus, the main goal of the Estonian attacks was not their results but rather how this experiment would take place and the effect.

- **Q:** *Is there cooperation between Russian and Ukrainian cyber forces? Was there cooperation in the past? Are there any plans to develop cooperation in the future?*

- **A:** I have not heard that we have any special cyber units until Russia's propaganda started taking place. It is quite hard for me to say anything about cooperation. Maybe some specialists in this area would be able to tell you more about cyber units in our government's structures. My view is that if those units even existed, their main areas of work would have included economic espionage, and something related to that, but nothing close to what is happening now.

- **Q:** *Is there cooperation/joint efforts between non-state actors and law enforcement agencies in fighting Russia's cyber attacks? Are there any efforts tailored towards fighting/stopping Russia's information warfare? How effective are these efforts?*

- **A:** Unfortunately, I do no know too much information about this. From what I've heard, I can say that all these initiatives [refers to those by non-state actors] are independent from the government structures. There is no coordination from the government side. On the one side, it is quite a positive trend [refers to having non-state actors acting independently] that shows that our society is democratic – non-state actors can create their own initiatives and there is no need for a totalitarian control over them. On the other side, if something similar happens in any other country [did not finish his sentence]. The advantage of a totalitarian country is that it can accumulate lots of resources by using force during the war; all [not clear what he says] become military and belong to the state. Every citizen belongs to its state. In a democratic state, Germany or Switzerland for instance, the organizations will act

independently and bring benefits to its state in a specific situation [refers to war]. I doubt that the German secret services will be controlling their civil society organizations [that act in the information sphere] and start cooperating with them. Civil society and some governmental structures can be working on information security. These organizations can cooperate with each other but they cannot be part of one mechanism as it is in Russia. Therefore, during the war, they [refers to non-state actors and their initiatives] are more vulnerable in a democratic country than they are in a totalitarian one.

# 9 Interview 8

## 9.1 Meeting: June 29, 2015

- **Q:** *How would you characterize the work of non-state actors (e.g. the Ukrainian Cyber Forces, Cyber Berkut, and Anonymous Ukraine) in leading information warfare and executing cyber-attacks against Russia? How effective are their means in achieving their goals?*

- **A:** Anonymous is mostly composed of researchers who do research for various governments. Cyber Berkut usually provides fake information. They mostly set up the facts. For instance, they mention that they hacked an email and provided evidence. When one examines their evidence, he can see that, in fact, they either use information about the people with the same last name (*odnofamil'tsi*) or fake the signature.

- **Q:** *How effective is the cooperation between the Ukrainian Cyber Forces and the Security Service of Ukraine?*

- **A:** Dokunin is not adequate. Yes, he is sending his information to the Security of Service of Ukraine but they are not doing anything with it. They are not taking him seriously.

- **Q:** *Does the Ukrainian government have a cyber unit? How would you evaluate its capabilities compared to non-state actors (e.g. the Ukrainian Cyber Forces) in Ukraine, or Russia's cyber state or non-state actors? Are there any plans to develop stronger capabilities of such forces?*

- **A:** Yes, they do have such unit, a unit that collects money. People who have any moral values left the unit a long time ago.

- **Q:** *Is there cooperation between Russian and Ukrainian cyber forces? Was there cooperation in the past? Are there any plans to develop cooperation in the future?*

- **A:** Yes, they used to cooperate. Officially, there is no cooperation between these two forces now. However, many former Committee for State Security of the Soviet Union officers (people of the former apparatus) continue working as part of the Security Service of Ukraine.

- **Q:** *Why has Russia not used "visible" cyber warfare tactics in Ukraine, like those used in Estonia and Georgia?*

- **A:** They understood that the main thing in a cyber conflict is that no one should understand that something is happening. Thus, it is impossible to catch someone by his hand (*piimatu kohos' za ruku*).

- **Q:** *Is there cooperation between Russian and Ukrainian cyber forces? Was there cooperation in the past? How would you evaluate Russia's cyber tactics in Ukraine? How successful are they? How do the tactics used by state and non-state actors compare?*

- **A:** Ukraine does not have any methods. Russia uses a "reverse engineer" method. For instance, about 6 years ago, they started using contests to recruit talented people. They offer high salaries (around $5000 dollars), and use patriotism and terrorism as two appealing recruiting themes. Once they are able to hire a person and a person is part of a system, they start asking him to accomplish other tasks. When I was a student and the Security Service of Ukraine came to recruit us (it was 10 years ago), they offered us salaries of 700 hryvnias [local currency]. Whereas in Russia the government understood that hiring hackers is important, in Ukraine we still have insurgent groups (*partizanshchyna*). It is important that we have professionals in our cyber units who will receive professional-level salaries. When our government understands this, then we will have the desired and needed changes.

- **Q:** *Which cyber-attacks were used during Maidan? Are there any attacks that are different from those used during the war in the East?*

- **A:** No. When the North Atlantic Treaty Organization meets with various cyber forces in Ukraine, they only observe how these forces fight with each other and keep blaming each other for failures.

### 9.2 Email: July 5, 2015

- **Q:** *Would you please clarify your following quote: "A hacker is characterized not by his technical skills, rather by his ability to launder money illegally. One possible distinction between white-hat and black-hat hackers is those who participate in various contests are white-hat hackers; and those who work with law-enforcement are black-hat hackers." Specifically, I am interested in the part related to "black-hat hackers are those who work with law-enforcement agencies." If I misunderstood your statement, please specify it. Thank you.*

- **A:** Black-hats usually do not work with law-enforcement. But if they're caught, they will collaborate, as hackers do not want go to jail. White-hats work for enterprises, usually the use similar tools as black-hats and present their research on security conferences. And guys which work for government they have much more advanced tools that white-hats and black-hats, and they try to be as much hidden as possible, not showing themselves on hackers forums and not showing off in research conferences.

- **Q:** *"Many cyber criminals moved to the Donetsk People's Republic and Luhansk People's Republic and we should distinguish between the occupied and unoccupied Ukraine." What are the trends in the occupied territories? Are those hackers cooperating with Russian hackers? Are they leading information warfare? How effective are their cyber attacks/cyber war? How much do those attacks overlap with the kinetic operations on the ground? Do hackers in the occupied Ukraine have prevalence in terms of capabilities over the hackers in the unoccupied Ukraine?*

- **A:** Many criminals moved to Donetsk People's Republic or Luhansk People's Republic, some of them perhaps related to carding. I'm really not sure how many hackers moved, as they're

just trying to do business and live in comfortable conditions. Luhansk People's Republic and the Donetsk People's Republic have very bad quality of life. Cyber-criminals are not trying to be in politics, even they do not use direct denial of service tactics on government sites, to not attract attention. They just do business and earn their money. There is no borders in cyber-crime. If hackers/carders want then can go to every country for a while to make money (e.g. process stolen credit cards). So I'd rather not distinguish between Ukrainian and Russian cyber-criminals, or Polish, or Romanian, etc. They do not support any national ideas. Now I do not see much overlapping, e.g. have no evidence for cyber-support of big battles (*Debaltsevo, Illovaisk*). But it was just after the revolution and during Maidan, during elections. Now this is just a continuous intelligence gathering. I will think more about the overlap.

- **Q:** *Do you think the Ukrainian information war exists? Does Ukrainian propaganda exist? How effective is it? If it does not exist, why not?*

- **A:** Actually government tries to affect public opinion in Ukraine but they're not very effective, people do not trust. Good example - PR about mobilization to army, or that we have to trust new police. But I think many people are pessimistic about it. In Russia or occupied territories government does nothing. Look, they're just going to create a new information security concept for Ministry of Information (related to public relations, not data security). I've got the document for review and it is really poor and bad quality. It will just not work.

- **Q:** *Could you please send me any additional information about the reverse engineers method? How Russia recruits its hackers?*

- **A:** Russia has two pipelines of hackers:

  1. caught by police/Federal Security Service/etc. Not to go to prison hackers for law-enforcement
  2. working with students. HR from military/Federal Security Service/etc. come to universities and recruit talented students. Then they work for simple projects, and then more and more secret and politically related. For students Russia do a lot of hackers' competitions, their student teams one of the world leaders. More about CTF: https://ctftime.org/ http://aciso.ru/events/3475/ http://ctfnews.ru/competition/2/news
  3. work with independent researchers, I think more rare, and they usually do not trust them.

- **Q:** *Why is Russia using cyber criminals for attacking Ukraine? Wouldn't it be better to hire cyber professionals? What is the goal and reason for such tactics?*

- **A:** In 2008 Georgia and Estonia, Russia did not have professionals, so they actively used hackers. Now they use a lot of professionals. But! Not every unit or agency has access to this capacity. Still they would like to have their own intelligence. I'm pretty sure that Russian police does not have access to professional resources. But they have a lot of hackers, so they use them to support their operations, get independent source of intelligence. Not every unit in the Federal Security Service of Russia has access to professionals, so they use hackers as cheap and available resource as well.

## 10 Interview 10, Skype call: September 2, 2015

- **A:** So where should we start?
- **Q:** *I sent you a list of questions.*
- **A:** We can start at the beginning, I guess. So okay, the first question: can we speak separate cyber warfare and information warfare? I wouldn't... in the case of Ukraine... there's a really, there's a very difficult to make them separate, I think, because they are very interconnected. In my view, most of the stuff that's going on is information warfare-oriented. Either it's uh... you know, let's take the example of [Adidas?] attack against prominent websites. For example, the North Atlantic Treaty Organization's Cooperative Cyber Defense Centre of Excellence had an attack when the Ukraine crisis started and the North Atlantic Treaty Organization's Cooperative Cyber Defense Centre of Excellence's website was off, I don't know, for a few hours during the weekend. And essentially, if you look at the facts, it's [Adidas?] attack, disruption and denial of service. But, if you look at the effects of how it was used, it's... the main objective is to gain... you know, does information warfare have any value in it? It was reported by the international media the cyber group that did those attacks came to prominence they showed us as being weak, although the technical facts of it was that it was a really [simple] attack. Yes it denied access to our website, but it was just an under data's attack. Since these data attack, and also if you have information, you can just, for example, we really assume that this is cyber-attack. Then also, it's not really destruction, it's more or less generating some information and this also I think applies to the... which are regarded as the most sophisticated cyber-attacks that may have link with state organizations. I mean, those cyber espionage campaigns, so that's also information oriented. We haven't seen any information even really manipulated. There's no data integrity questions, or really disruptions. Even those data attacks which... you know, for me, it seems like the actual effects of it aren't really substantial – they're more or less about gaining publicity and creating this general thought of war or... putting fuel to the crisis. Even if a national news outlet is taken off line for a few hours, nothing really changes. It just a nuisance, I guess. (pause)
- **Q:** *Okay so but do you... so my question is, as I said, information or cyber warfare attacks in the case of Ukraine, they are not as effective as they could have been. So do you have any reason why they have not been as effective as they could have been? Why they not have been used, you know –*
- **A:** Do you mean why, for example why Russia hasn't blown up anything or has non-information warfare effects, do you mean that? (pause) Right, for instance they are using but we don't know. The used at the beginning there was a cyber espionage campaign, Armageddon, according to the report, they claim it was Russia state-sponsored. And it was huge and I think it was described in March or April 2014 and every single time that something like this was discovered they basically figure out a new way and continue doing this way in Russia. But I haven't seen any new reports saying "oh yeah, they actually continued doing this"... think the cyber espionage from all of the sides the major cyber wars that are going on, that's like a norm. Yeah, but this is espionage, you know. This is eavesdropping. But it doesn't have you know... I think a lot of people assume that for example Russia has packets. Its capabilities which could actually you know have a real life kinetic effect. You know manipulating with

the SCADA system or you know having a real effect just listening in is a different matter and I think espionage is very active. And allegedly Russian and all the main powers in the world are engaged in it. But in terms of... so are you asking me why aren't there those attacks which would lead to more real life consequences?...I think, in the book, where you are also writing, by the way thanks for that, I enjoyed your chapter.

- **Q:** *Oh, thank you!*
- **A:** I think it's a good contribution. I think it's cool that you understand the Ukrainian problems. Because a lot of authors have this big strategic view and they may not be aware of what actually is taking place in Ukraine since most of them don't speak Ukrainian nor Russian.
- **Q:** *But you have a few people, I think you have three or four people?*
- **A:** We have the ex-chief of the Ukrainian Certified Emergency Response Team. Kenneth actually translated his text from Russian to English, which was cool.
- **Q:** *Oh really, it was in Russian? Yeah Kenneth's Russian is really good, I saw him back in July and we went for lunch, and he switched all of a sudden to Russian and I mean I knew he spoke some Russian, and his wife learned something but I wasn't sure how what level he had and yeah. He switched to Russian to talk to the waitress and we talked a little bit and like 'wow, he's really... his Russian's really good.' Plus, he lives there so (pause), he loves it.*
- **A:** Seems to be enjoying it. But regarding the book, Martin Libicki is writing for the book and his main question is why didn't anything real happen? So, my answer here is a mix of Libicki's opinion and my opinion because I know I'm very influenced by that because I read it and so on. The first thing is that if you look at Ukraine there might be the question of targets – whether there are targets that are worth attacking and whether there are targets that are actually very cyber dependent. The assumption that the Ukrainian infrastructure may not be up to date in those terms, you know what I mean. There's nothing to attack maybe. And also, when you think of it, I think it's difficult to see the reason why Russian would attack because it has achieved all of his objectives without doing it. If you look at the Crimea or Eastern Ukraine, what still matters are the little green men or actual tanks and bombs. So there's this question if there was need and if there are targets? And also, one might assume that, this is just an assumption that may be a reason, that Russia may not be willing to show what it's actually capable of because it achieves its objectives otherwise so there's no really practical or strategic nature to use very sophisticated cyberattacks resulting in destroying something. And the thing that Libicki claims and also others, I think James Healey and others, there's no need because Russia already has access to Ukrainian systems. I don't know the technical specifics, hypothesis here is that it can already eavesdrop in or manipulate with the system because it has so many still today so many historical connections so many technical links already with the Ukrainian infrastructure, if you know what I mean. That's another point why people assume Russia hasn't used anything. It already has the power to... they listen in, yet there's no need. My personal view is that there's no need to do it. If you look at global developments, I think states are restraining themselves from attacking critical infrastructure, I think that's a general norm of developing. And also the UNGGE, the latest group of the United Nations' governmental experts, just adopted those

norms, recommended actually that states shouldn't attack critical infrastructure. So in that sense the Ukrainian case represents, also in the book, that in fact cyber powers, or states who allegedly have those capabilities are exercising restraint because they... because cyber hasn't really changed things. Russia doesn't want to attack Ukrainian infrastructure just because it doesn't want to attack Ukrainian infrastructure. And those assumptions that that attribution doesn't matter and it's really easy to mask the identity of the attack. Really it hasn't changed this general view on how states view or think about more serious attacks against each other. That's my kind of idea or understanding. And also, another reason might be that if Russia would do this attack especially in the case of the Crimea, now it is not so relevant maybe that this assumption but I remember someone saying that it would be against Russia's discourse and saying that it was not involved and if you would see a really sophisticated cyber attack. Although 10 percent attribution is impossible you could see that it's really was Russia. Although I don't think this is real motivation now, but somebody said that. That it doesn't want to act against its discourse, where he says that he is not involved in the conflict.

- **Q:** *So, if we can move to the second question, I am interested very much in non-state actors and their involvement in cyber attacks. You can choose any other question if you prefer... like for instance, all of the stuff that... let's even start with basic – Cyber [unclear] and Anonymous Ukraine and Ukrainian Cyber Forces. First of all, what do you think those groups are? Are they truly what they claim, are they not? Do they have any connections to the government? Or are they completely independent? And then maybe we can talk about their actions, if there's any effect, any use or it's more just the publicity. And do their actions actually influence somehow what is happening in Ukraine? I'm not speaking necessarily in terms of them but maybe minds and hearts of the people, they can actually influence the citizens of the country.*

- **A:** Okay, let's start with some questions. We can close the door. (pause) So, first of all, maybe in terms of attribution or connections with the state or state funding or whatever I think it's really difficult to tell... The thing that really struck me... let's take the example of, I would think that there might be signs of the links to the government. And one example is Cyber Berkut, it was Cyber Berkut who released this phone call between the Foreign Minister and the European Union Higher Representative. There was this sniper thing where our minister briefed the European representative that they were not sure who was behind the sniper attacks in [...] and so on. So I think I may be mistaken, but I think that the Cyber Berkut released this, so if you look at the sophistication when you need to gain access to a minister's phone, it means you either have links with the Russian telephone agencies or you yourself have some sophisticated capabilities to listen in to those phone calls. So to me, that was a sign that for example, Cyber Berkut may have links with the government. But of course you cannot really tell. Another sign which has been highlighted was when the peace talks... all the attacks stopped. And so that's also a sign that there might be the links. But of course you cannot really tell and there has been no evidence and nobody has actually looked into that. I would personally assume that there has to be some kind of a link, but I don't know how substantial is it. What do you think?

- **Q:** *Yeah, I'll tell you what I think but one question – so, when interview people I introduce this dimension... so you think the Cyber Berkut, that they have this link to the Russian government, right?*

- **A:** They might have, but I do not know.
- **Q:** *Yeah, yeah, but it might have. Some people were saying that they might have something, some kind of a dig at all to the government, they were saying that maybe it's former officers... former like the Security Service of Ukraine officers who were unhappy with the new government. Ukrainian, actually, government. Do you think this can also be a possibility or it's very unlikely?*
- **A:** Without really knowing what's the situation with the former officers, I would just based on logic, assume why not? (pause) I mean it might be that they receive some kind of a funding through some kind of a link, or it might be that they're really actually operating in Russian in a room in a governmental space. Nobody really knows. Part of it is that the Security Service of Ukraine can leak stuff.
- **Q:** *But also like if [IBN] make their attacks and whatever they were saying, you can see an exact trend where if something really important happens then you can see a lot of posts by them. I think now, I haven't checked in the last month, but recently they've been way less active than what they've been doing –*
- **A:** You mean Cyber Berkut?
- **Q:** *Yeah. So even if they do that stuff... and also even if they know actually because they claim a lot of things, they post a lot of links. Like we just logged forty websites today and they post some websites, but again you don't know if they did or some of these sites are actually working. I feel like –*
- **A:** But as I understood, they're constantly leaking emails and stuff.
- **Q:** *Yeah*
- **A:** So of course you ask how can they do it? And it's not really, it's not every... it's not that you download a script and start leaking stuff, it has to be some capability behind it.
- **Q:** *True, but some of the websites that they're leaking... some of it might –*
- **A:** I think fake, as well.
- **Q:** *Right, some of the stuff is really fake and a lot of the things that you actually read – like for instance, sometimes some of the things... do you speak Russian or anything like that?*
- **A:** Only a little bit.
- **Q:** *Yeah so some of the stuff is obviously in Ukrainian or Russian, but also if you actually read the content of the email, it feels like they translated or created... like the language is very... and I would say people who don't have a very good grasp of the appropriate norm of normal writing. The language that they use is very like two guys are talking on a street to each other, you know? So, I doubt that the Ministry of Education would ever say something like this. But then they sign, and this and this, and again people don't know if again some random person reads this stuff they of course are going to believe it.*
- **A:** And I think that's the point.

- **Q:** *That's the point, and so I think their stuff is also just a part of machine and propaganda...*
- **A:** Yeah I think that's the full name of it, it's information warfare and propaganda. I don't think they're an actor we should be afraid of in terms of destruction or damage. It's fully... you can see that it's a tool for Russian information warfare and it's another small actor in it. And in terms of efficiency, I don't really know, it's hard for me to say I think... do you claim that an average person wouldn't understand that it's fake or...?
- **Q:** *No, I'm not saying that the average person would not understand. I think now they actually started paying more attention and they actually people... but at the beginning, when everything started and it was so much of everything and you were like under the influence and I think in the beginning, more people believed in that stuff. Now, of course, the war has been for a while and people like 'oh let me actually take some time and read' but I feel like at the beginning –*
- **A:** Yeah, I think their aim was to create this general crisis environment and feed it somehow. And of course, generating progression is tough and you can see it was part of the larger Russian information warfare campaign. That's how I see it, and that's how actually most of the cyber activities... as part of a larger information campaign.
- **Q:** *Only Russian, or you see this –*
- **A:** I think it's both sides. But I have to see more examples of [unclear] and more examples of Russian espionage and so on. But it's just such a subjective feeling that it's more active from the Russian side. But I can talk about this distinction – Ukraine and Russia distinction – afterwards, do you have any questions on the activist side?
- **Q:** *No, you can talk about that. I would like to cover also Ukrainian Cyber Forces, if that is possible.*
- **A:** To be honest, I really don't know what they have done, I guess direct denial of service attacks are seeming tactics, right?
- **Q:** *Yeah, they do like direct denial of service attacks and blocking websites and... they block a lot of social media –*
- **A:** Yeah, the usual stuff.
- **Q:** *The usual stuff, to stop Russia from spreading propaganda and also they block the bank account. Like they contact the bank and try to ask them to block specific accounts because this account [unclear] in Ukraine, something like that. And they also hack closed-circuit television cameras trying to collect... um...*
- **A:** Yeah, I know there was this guy hacking Russian printers and printing pictures out or something.
- **Q:** *Right, so this exactly what they do.*
- **A:** I think in general, you can view this as a normal part of conflict, I mean it's hacked into... I think that's a modern conflict right there. You have people who fight for their opinions, and

views, and objectives online and I guess that's the case for Ukraine and cyber troops as well. I think maybe there are activists centrally, but this is a normal phenomenon you can see and I think you will see this stuff happening in every future conflict. You have some active groups doing some inner stuff on direct denial of service defacements, blocking social media or whatever. So you could claim that this is just how things work now and how political view is expressed. And I think in the case of Cyber Berkut, there's a lot of volunteers as well, as I understand, they recruit people and are paid, if I'm not mistaken.

- **Q:** *In Russia or—*
- **A:** I think in both cases, I would assume. So you can join them, or I might be wrong.
- **Q:** *No, I mean they provide a bunch of recruitment information and this and that... so I guess if you can compare both of the countries, Ukraine's whatever information and attacks and Russia – which one do you think is more effective, if we can compare them?*
- **A:** Difficult to compare, my own personal opinion is that the Russian campaign is more effective because it's more coordinated. But now we'll talk about the general campaign. It seems to me that they're more coordinated and they're not really restrained by this Western normative framework. You know, if Ukraine blocks some channels, it gets criticism from the West or if it just creates blunt lies, Russian media tells all the time, it's a little bit blocked by this normative framework. That's the general problem with the European Union – how to combat a machine that has no rules to it – you know, Russian propaganda works really well because it's just ruthless. That's kind of the feeling I had, but you know that Ukraine has also countered this to a certain extent with similar means. Blocked some TV stations and so on. And if you look at actions, it's the same actions – DDoS, and so on. It feels to me this question – Russian information operation or information campaign, however you call it, propaganda, is more effective. It's more coordinated and it's more thought-through. And of course, they have more resources. I always have this... I know the Strategic Communications people – that's the main question, how to counter it? And the usual line is that we have to do good journalism and produce believable stuff. There's this whole ideology behind it. But I think people see that it doesn't work against Russia that is ruthless in generating propaganda. I think this western liberal, I don't know how to put it, mindset is a little bit restrictive in that sense. But, I don't have the solution for it. We shouldn't apply the same tactics as Russia does. But in terms of Ukraine, I don't really know how it has done so in the context of information warfare. Maybe you know better, I'm sure you know better.
- **Q:** *So with the case of Russia, just to follow up on one question, so you're saying they have a more organized approach. Do you think – Estonia, Georgia – they always claimed that patriotic hackers were those doing the most work, right? Do you think the patriotic people are involved in this, or is it more like as we saw, they have a factory of trolls? People they hire and pay money for, you know, people who –*
- **A:** I think people actually take part in this as well, as I said with the activist thing, I think that's how things are now. But, Putin has the highest support rates now so there are lots of people I'm sure that actually do it voluntarily. But it seems like it is somehow organized, not from the top but it's organized and either they provide the tools or they provide opportunities

for volunteers to take part in this. I think in the Georgian case as well, if I'm not mistaken, there were some forums where they distributed those tools and I'm sure [unclear].

- **Q:** *You mentioned this but just to make sure – can we say that the recent cyberattacks are an act of war, or a new tool of war, like how did they change, if they change the course of countries, like Ukraine or maybe we can say like in Ukraine it's not but in some other country it is, I don't know.*

- **A:** It depends on how you define war. It's easy to say that there's a war happening in cyberspace because there is. But if I have to take this cyber aspect out of the conflict, I think nothing really would be different. You know what I mean? The same objectives would be achieved. But, having said that, it's definitely a part of it and it's utilized to a large extent by these actors, and especially, I've said it several times, for information warfare purposes. But, in terms of war in the conventional sense, I don't think it has influenced it substantially. You were at the [unclear] right? The conference that we organized?...In that panel as well, they agreed that for example, if the little green men when they entered the Crimea, they went to the [...] into town and just cut it down. So that is telling what really matters. So, that's my view. So, I think you've got my point.

# 11 Interview 11

## 11.1 Email: August 23, 2015

- **Q:** *Is there any general (weekly or monthly) statistics on cyber-attacks that provides information which sector suffers the most and who/what country/what group is the villain? I am looking for something that is available for the public.*

- **A:** We do not have such statistics because we have not enough time to do it. It's like a photo from war - no time to make selfie because we need to shoot/kill/defend our lives. All public available information about attacks and their types is shown on our website. For example 2014 year - http://cert.gov.ua/?p=2019 (sorry but it's in Ukrainian only).

- **Q:** *How effective is the work of the Computer Emergency Response Team of Ukraine? What is needed to increase its effectiveness even further? What challenges does it face now?*

- **A:** Quite effective but we wish to do more. We need more co-operation with other organizations in cybersecurity. We face all types of cybernetic threats (DDoS/APT/fishing/hack attempts/information leaks and so on).

- **Q:** *How closely does it cooperate with Europe, the United States or Russia, if at all? How would you evaluate this cooperation? What could be done to make this cooperation more advantageous for both parties?*

- **A:** We cooperate with different organizations from more than 100 countries. Most of them are FIRST accredited, from the Computer Emergency Response Team of Ukraine, or cybersecurity specialized parties/people.

- **Q:** *What are the main areas of focus that the Computer Emergency Response Team of Ukraine is now considering the war in the East? Are you investigating any cyber-attacks that relate to this war?*

- **A:** It's a political question and I don't want to answer on it. We're investigating different attacks and from East too.

- **Q:** *How closely does the Computer Emergency Response Team of Ukraine cooperate with other governmental and private organizations that focus on cybersecurity in Ukraine? Do you cooperate, officially or not, with any non-state actors (e.g. the Ukrainian Cyber Troops)?*

- **A:** Yes, we cooperate closely if necessary. We do our job and all other organisations and people - are our partners in this process. We cooperate both officially and not, no matter for us. Main point - effectiveness of this cooperation.

### 11.2 Email: August 25, 2015

- **Q:** *Earlier, you mentioned that you need more cooperation from organizations and people. Would you please specify what kind of organizations and people (especially since you mentioned that you have been already cooperating with many volunteers from 100 countries)?*

- **A:** We cooperate with different types of commercial, governmental, and corporate response teams in a restricted mode [...]. Also we interact with different external parties outside our constituency. Antivirus laboratories, law enforcement agencies of foreign countries, white/gray/black-hatted cybersecurity community are welcome too. All who can help us to react better are our partners and informants.

- **Q:** *Also, you mentioned that you cooperate with non-state actors in Ukraine. Would you please mention who are you working with and what type of assistance do you get from those actors?*

- **A:** If You can do something useful for us in cybersecurity - say it and I hope we can cooperate. The community understands, very sensitive information about individual constituents may be disclosed in the process. For example, if the Computer Emergency Response Team of Ukraine discloses who helps us to solve some problem with X that X can harm to that disclosed individual or organization. Information disclosure policy is described in RFC-2350 section 3.4.2 of "Cooperation, Interaction and Disclosure of Information."

## 12 Interview 13, Skype call: July 6, 2015

- **Q:** *How various companies protect against cyber-attacks and how much these measures are effective??*

- **A:** During the last 10-12 years, I have experience working on providing protection to various companies: telecommunication companies, financial institutions, trust funds, and oil industry. They appear in this order in terms of their effectiveness and level of cybersecurity. Telecommunication companies take the first place in their level of protection since they spent lots of money on it. They have client-fraud protection measures as part of their business

arrangement with their clients. Additionally, the size of their client body is another reason for such good cybersecurity. Any telecommunication operator has at least 10-12 million of clients (even though it is not even a large size) of different technical background and moral values. Information on such differences could be used for malicious purposes. For instance, one of the subscribers has found out that the telecommunication operation offers a bonus (few minutes, etc) due to the New Year, for instance. A person start using these minutes but stops paying attention to how much minutes in total he had used. After the holidays [holidays in Ukraine last from January 1 to January 14th], while sobering up, a person realizes that his bill is huge. Since there is no Sim-card registration in Ukraine, a person throws away his card. Such examples are not unique. During the holiday season, telecommunication operators can loose million of dollars. As a rule, the subscriber who finds out about bonus calls all his relatives in Russia, Poland and shares information about the bonus. A few years ago, such tendency would not spread too fast (*lavinoobrazno*), but because of Twitter and Facebook, such a phenomenon happens rather quickly since people find out about this from Twitter and Facebook within only a few minutes. Once employees of telecommunication companies return to work after the holidays [refers to the Ukrainian holiday season mentioned above], some of them are either being fired or do not receive their salary bonuses since someone needs to take responsibility for such actions. Banks are next in their level of cybersecurity since they suffer more from cyber crime and they do operate with large money but not their own money. Last year [refers to 2014], we witnessed the first example when banks were the targets of cyber criminals. A few years before, the targets were those institutions against which a theft was fairly easy, such as limited liability companies and private enterprises. They would often hire accountants from the outsourcing companies who owe so-called *keys* to 20-30 private enterprise owners and perform for them operations in the client bank. Banking entrepreneurs work in a simple fashion. Once they got an access to the workplace of the automated accountant (in fact, there is a person who sits the entire day in her house and does some wiring), this accountant receives a company plan via email and she processes money to their certain identified account. She has an electronic email, internet access, and access toward the client bank and all the *keys* on her hard drive. Through a remote access connection to her computer, the criminals wire money to the places they want. Obviously once this accountant decides to go to back and sleep, it is not possible to do. But during the business day, cyber criminals are able to wire money to their accounts, especially if they use different banks, small amounts of money. In such cases, it is hard to stop from doing this. Insurance companies and collection agencies are next on the list. They have good cybersecurity measures not because they have an urgent threat of cyber crimes but because they either want to support their external image/reputation or are a public international company that has to follow certain regulations in Europe and the United States. And the rest of companies only establish their cybersecurity measures after the incident. For instance,a recruiting or judicial firm has a staff of 3-5 people who keep all their emails on Google Drive. Its staff does not care about their cybersecurity protection measures until it is too late. But once they suffer an incident, they try to find free consultation by asking their acquaintances for help and save them money in such a way.

- **Q:** *Where these cyber-attacks are coming from? Are the Ukrainians stealing from their own people?*

- **A:** Are they stupid or what? No one steals in the country he operates in because they could be

eventually caught. The first hacker's rule is – "do not steal where you live" (*tam, de zhyvesh, tam ne kradesh*). Criminal groups that operated from Russia were stealing from Ukrainians. Now, the climate in the country has changed and members of these groups immigrated to Ukraine. That is not good either since now these groups are Europol's jurisdiction. In Russia, there are only a few cases that involve prosecution of cyber criminals. One of them took place because Zrubliovskiy was using a direct denial of service attack against Aeroflot that belonged either to Putin's son-in-law or his nephew. If that was not the case, these criminals would have been still free. As I mentioned earlier, criminal groups are moving to Ukraine since the country has a more liberal political climate and they can move small amounts of money anywhere. These groups who operate from Ukraine do not steal from Ukraine. Criminals that reside in the following countries – Ukraine, Romania, Belarus, and Turkey – steal from the West...[removed questions that deal only with cybercrime in Ukraine]

- **Q:** *You mentioned that many hackers moved to Ukraine, has this influence cyber and information warfare in the country in any way?*

- **A:** No, since these immigrants are not politically active. We can define so-called *hackers* into three groups:

  - opportunists – those who break everything they can
  - economically motivated
  - politically motivated

  Economically motivated hackers are distinct from politically motivated ones. They do not overlap in their goals. Maybe China is an exception where hackers break into Western systems and provide this information to their own companies. In the West, such an arrangement is strictly forbidden. Even if they had received schemes of a Chinese submarine, they would have taken lots of time to decide what agency should deal with it because of United States' unique jurisdiction. Ukraine does not have such an arrangement as China does since we do not have budget for it, as a result we cannot say that someone is state-sponsored. There are some individual hacktivists and we can observe their actions. These hacktivists are all Ukrainians (no immigrants). They are similar to the Anonymous but these groups do not even hide their identities as no one prosecutes them since they only attack Western targets. They have some kind of a nucleus, similar to the Anonymous, and a bunch of people who are willing to do these kind of activities. They use direct denial of service attacks against specific websites, hack into closed-circuit cameras, etc. These group do not present a serious threat. On the other hand, there are state-sponsored groups that mask if they are Cyber Berkut. Only a narrow group of people know who these groups, for instance me, in fact are. This narrow group of people work against such state-sponsored groups but they cannot speak of their operations freely/openly.

- **Q:** *Which state-sponsored? I do not think it is Ukrainian. Also, I've looked at their website and it looks to me as simple propaganda. Do you think it is effective?*

- **A:** Not effective. They just did some activity online and you are right in calling these actions as "propaganda." They saw that these actions are not effective (*efectyvnosti nul*) and they decided to buy trolls for themselves and that it will be more effective to post comments on

ru.net. They have chosen such strategy. This is what we can witness now. There are research papers related to this topic. Those trolls sit in St. Petersburg. Such tactic is more effective than to investigate zero-days. From the operational point of view, it is easier for them to troll the internet and to remain as an officially separate organization. They apply the same approach to the internet as they use in military.

- **Q:** *Why has Russia not used "visible" cyber warfare tactics in Ukraine, like those used in Estonia and Georgia?*
- **A:** In Estonia, we did not witness ( *priamykh*) cyber-attacks, as attribution remains a problem. Most of the traffic occurred inside of the country and was controlled by pro-Russian "elements" in Estonia.
- **Q:** *Why don't we observe massive cyber-attacks in Ukraine?*
- **A:** Because we do not have massive support. The percentage of support is much lower than the one we had in Estonia.
- **Q:** *How can you characterize the relationship between the hacker community in Ukraine and the state?*
- **A:** There is no such notion in Ukraine as a deal with law enforcement agencies (*zdelka iz pravosydiiem*). Such approach is not used here. When a person is caught, no one hires him; he is being recruited. After that, some cooperation is possible because we do not have the base of informants. This relationship in Ukraine is informal; they are not being paid; they are not being protected. Thus, the relationship exists on the detective-criminal level. This interaction/cooperation occurs on the level of such personal relations. Not more than that, unfortunately, as the effectiveness of such cooperation fails. Then, there are those politically motivated people, such as the Ukrainian Cyber Forces and others, who are just doing their own business. Their cooperation with law enforcement agencies occurs in such a way that the later do not touch the former. Their interests are not in conflict and in such a way they coexist. However, there is no signal from the government level about that the government cooperates, depends on, or in the partnership with these non-state actors. As for the former ones, such cooperation would mean to lose one's face (*vtratutu oblucchia*). They sometimes receive information from them asymmetrically. For instance, they broke into something and sent it to the Security Service of Ukraine, but I do not think that the Security Service of Ukraine thanks them for such help. The Security Service of Ukraine might be using this information in their work. However, I do not think that they are able to recognize that they are working with non-state actors. Not now...[removed questions related only to cyber crime in Ukraine]
- **Q:** *You spoke about trolls. Do you think we have them in Ukraine, state-sponsored or not? If we compare the information war in Ukraine and Russia, which side is more successful? Is there a winning side?*
- **A:** I never asked myself such questions (smiling). Of course, I cannot evaluate this objectively as I am not a consumer of such information. Thus, I cannot evaluate its effectiveness. I am isolated from it. I am aware of volunteer initiatives that were realized as a list of accounts of

maximum amount, maybe it was a list of those trolls – a base – so they have/lead the bot base. Specifically, every worker of a company has 10-20 bots, depending on his programming skills and effectiveness, and talents. And they enumerate those bots and collect them in one base and now this list is composed of 200-300 bullet points when I saw it the last time. There is also an interesting work by the Western author (do not remember his name, unfortunately), who dis-activates this scheme. Specifically, he has a model of social network of bots of Twitter. He deals with Twitter mostly. With the help of APIs of a social network, he found one bot, then he looks what this bots writes, then he looks for these phases, and then he looks who else writes the same or similar phrases, and so on. And then he looks for the connections between those accounts, checks who they follow and who follows them. And then he presented a huge automatic network and automatically demonstrated that this network was the Kremlin bots, at least. Therefore, the system is not complete but correct. There are no humans there.

- **Q:** *Do we have any system similar to the one you described in Ukraine?*
- **A:** But for what purposes? We do not have any need for this now as people are very actively involved in this kind of work and doing it for free. And there is no reason for it.
- **Q:** *And how effective is their work?*
- **A:** Very effective, as we can see. We have plurality of thoughts, bots are being stopped/prevented (*botiv baniat'*) – all is working very effectively. I think public initiative in this way will be more effective because it is more difficult to make people work than to initiate patriotic moods online and to observe some kind of positive sense in this work. Plus, people are doing it for free based on their own principles (*vuxodiachu iz svoiix vlasnux idealiv*). And it will more expensive to use bots.
- **Q:** *If we compare capabilities of Russia and Ukraine, do we have more capabilities in this sphere?*
- **A:** We cannot use their methods as we will become like them. So we cannot compare capabilities. It is good as long as we have the required sentiments as they are more effective. Once the sentiments are over, we will be able to see a picture more clearly. I hope it will not happen. I think it will not be too good to create a troll bureau. If this becomes known to the public, it will not be good.
- **Q:** *How effective is the work of non-state actors (Ukrainian Cyber Forces , Anonymous Ukraine)? How is it perceived by the youth and Ukrainians in general? Do they have lots of support? Are they in fact doing important work? Or is it more propaganda? Are they trying to make a name for themselves?*
- **A:** This is not a massive movement (speaks of Anonymous Ukraine). The generation that composed Anonymous in the West is absent in Ukraine. It is similar to check books that jump over this stage of evolution. When the generation that is active now was growing , we did not have Myspace, Tumblr, and other systems of the thought consolidation and possibility of ruling huge masses in the internet in Ukraine. So I call this movement as a miniature of Anonymous as a movement now. There is the same model but the foundation is not effective for these things, for these tasks and we can see what is happening. So there

is some activity, we cannot say that it is very effective, but it is slightly effective. In a majority, people sympathize. I personally know some people in this movement and cannot be sympathetic to this movement (smiling). I think their motives are different from what they actually demonstrate.

- **Q:** *Follow-up on your answer about "bots," are they computers?*
- **A:** I didn't say exactly that, maybe I was not clear at this point. They are still humans, but they are bot herders rather than single account owners. Each operator has a number of fake personas controlled either manually (if the operator is not tech savvy) or by the means of automation. Many if not all social networks provide APIs these days, also there are event managers like Mention and [...]. All this allows for action automation across the accounts and social networks using some programming language, usually it's Python. Anyone with basic coding skills can do that, I'd compare the level of bot herding sophistication to the one of Search Engine Optimization.

## 13 Interview 14, Email: July 21, 2015

- **Q:** *Why has Russia not used "visible" cyber warfare tactics in Ukraine, like those used in Estonia and Georgia?*
- **A:** The Russian Federation is trying to use a new tactic of the "hybrid war," one characteristic of which is a complete denial of using one's military and propaganda operations against the other side. The same approach is being used during the latent war – Cyber Berkut that became famous because of its fake and real cyber-attacks against Ukrainian government information infrastructure, financial and other institutions has declared that it is fighting against the illegal Ukrainian government. At the same time, Cyber Berkut does not associate itself with the Russian Federation. But there are some suspicions that, in fact, it is a part of the Federal Security Services of the Russian Federation.
- **Q:** *To what extent can we associate recent cyber attacks in Ukraine (and elsewhere) with the war? Did they influence the course of the conflict? What network security lessons can we learn? What national security lessons can we learn? Is the concept of cyber war still more hype than reality?*
- **A:** In fact, we are talking about individual instances that either have a propagandistic nature or attempt to attack various defense systems. At this point, the aggressor carries out intelligence activities and analyzes the security of information infrastructures and the state's ability to counteract modern challenges in cyberspace. Because of the efforts of teams' of national cybersecurity experts, we manage to avoid serious consequences as a result of cyber-attacks that were carried out against Ukrainian information infrastructure. All this should be reflected in the National Security Doctrine and legal framework in this area, including the Law of Ukraine "On cyber security." Any changes to the legal code of Ukraine, coupled with reforms of an information security sector should provide a basis for the formation of powerful forces in combating cyber threats during peace and wartime.
- **Q:** *Would you view the actions of the Ukrainian Cyber Forces (and any other non-state actors) as propaganda? Would you view them as war actions?*

- **A:** We can hardly call actions by Ukrainian hacktivists in cyberspace as military actions. First of all, the Ukrainian law does not have definitions of cyber warfare, cyber weapon, cyber-attacks, cyber security, etc. Second, these actions are neither controlled nor coordinated by security forces (unlike the aggressor's actions) and most likely these actions are at the edge of a legality-illegality line or might be even completely illegal. A main goal of most of the actions is counter-propaganda, blocking web resources and financial and social media accounts of terrorists, and intelligence collection.

- **Q:** *How would you characterize the work of the Ukrainian Cyber Forces and Anonymous Ukraine? How effective are their means in achieving their goals?*

- **A:** The activities of these groups can be viewed only through the prism of their own initiatives, legal assessment of their actions have yet to give in accordance with the law. Obviously, "white" hackers volunteers intended to help the state oppose the aggressor in cyberspace. Such help is effective in resisting cyber-attacks and propaganda coming from the aggressor side. However, participation of these volunteers in state cyber defense operations are minimal.

- **Q:** *How effective is the cooperation between the Ukrainian Cyber Forces (UCF) and Security Service of Ukraine?*

- **A:** There is no doubt that the Security Service of Ukraine follows the Ukrainian Cyber Forces' actions. Additionally, the Security Service of Ukraine receives intelligence information from them. However, it is hard for me to speak whether there is any kind of coordination between these two groups or whether the Security Services of Ukraine manages the Ukrainian Cyber Forces' actions.

- **Q:** *How would you evaluate its capabilities compared to non-state actors (e.g., the Ukrainian Cyber Forces) in Ukraine, or Russia's cyber state or non-state actors?*

- **A:** One can assume that the Security Service of Ukraine does not have a sufficient number of officials with adequate technical skills compare to the volunteer group of these "white" hackers. It is also clear that the Security Service of Ukraine possesses financial, organizational and legal instruments that far exceed the cumulative potential of volunteers. This allows, if necessary, to engage qualified technical specialists to work with the Security Service of Ukraine to address any issues that might arise. Compared to the aggressor's organizations, the Security Service of Ukraine has been greatly weakened organizationally and intellectually during the times of the presidency of Viktor Yanukovych and because of the direct participation by the Federal Security Service experts in these operations. Technical and financial capabilities of Russia's government agencies in cyberspace are much broader compared to the Ukrainian ones. Participation by non-state groups of cyber criminals in Russia's cyber actions aimed at harming Ukraine should be considered exclusively in the context of overall Russia's government policy.

- **Q:** *Is there any cooperation between Russian and Ukrainian cyber forces? Was there cooperation in the past? Are there any plans to develop cooperation in the future?*

- **A:** There is some evidence of cooperation and information exchange of between their Computer Emergency Response teams. Such cooperation is in fact required by FIRST regulations.

A few years ago, cooperation between cyber forces was better since many experts from both countries either studied or worked together during the Soviet Union times. Regarding the expansion of this cooperation in the future, it is unlikely in the short term, at least until the Eastern Ukrainian territories and the Crimea are returned under the Ukrainian state control.

- **Q:** *What are the main tactics developed by hackers that are used in the war in Eastern Ukraine?*
- **A:** You can find out more information about their tactics from a Facebook page of Ukrainian Cyber Forces leader Eugene Dokukin. He posts information about his own activities online.
- **Q:** *How would you evaluate Russia's cyber tactics in Ukraine? How successful are they? How do the tactics used by state and non-state actors compare?*
- **A:** ... Tactics are primarily tailored towards supporting propaganda information operations, collection intelligence and security analysis of information infrastructure systems. In terms of state and non-state actors, many believe that most of them that participate in cyber operations against Ukraine are control by Russia's government.
- **Q:** *How would you characterize information war in Ukraine? How effective is it?*
- **A:** The main aggressor's strategy at the moment is to wait and to try to shake the political situation in Ukraine. Information warfare is used to generate, support and escalate the kinetic conflict. While at the national level, it is possible to resist such tactic, it is not the case for the territories that are not controlled by the Ukrainian government.
- **Q:** *Do these actions in cyberspace overlap with kinetic operations on the ground? Are they complementary? How effective are they? Please speak about both, Russian and Ukrainian, sides.*
- **A:** All ground military operations that may be carried out by both sides, would go against the agreements reached in Minsk. Of course, Ukrainian and Russian mass media sources report cases of using weapons on the front line.
- **Q:** *Does the Ukrainian government have a cyber unit? How would you evaluate its capabilities compared to non-state actors (e.g. the Ukrainian Cyber Forces) in Ukraine, or Russia's cyber state or non-state actors? Are there any plans to develop stronger capabilities of such forces? Do those units execute cyber attacks? Do they take part in information warfare? Why? Please speak about both sides.*
- **A:** According to the Security Service of Ukraine's structure, information about which is available on their website, it has a department that is responsible for counterintelligence protection of state interests in the field of information security... Some plans to strengthen this department might exist but they are not public as most information about the activities of this department.
- **Q:** *Edward Lucas mentioned that Russia aims to achieve the following three goals: to recreate a Russian empire, to stop the European Union's ability to control energy pipelines, and to weaken and divide the West. How effective are cyber attacks and information warfare from the Ukrainian side (state or non-state actors) in preventing Russia from achieving these goals?*

- **A:** The effectiveness of any actions by Ukraine aimed at protecting its information space depends on Ukraine's coordination of its actions with the international community, specifically with the experts from developed countries. The tasks that Ukraine is facing now have a global character and can be only solved by joint efforts of international organizations.

- **Q:** *How active are patriotic hackers in committing cyber-attacks or information warfare? Is there a massive mobilization of hackers (as it was in Estonia or Georgia) to participate in these actions? How independent/connected to the Kremlin are they?*

- **A:** There is a partial mobilization of the armed force in Ukraine; this mobilization includes cybersecurity specialists as well. However, there is no evidence demonstrating that such specialists are used specifically for defending Ukraine's cyberspace. Also, there is no evidence that Ukraine's government organizations are using white-hat hackers for information or cyber warfare. Even if there is a cooperation between a Ukrainian citizen and the aggressor, it falls under Ukraine's law enforcement agencies jurisdiction.

- **Q:** *Do cyber professionals or amateurs participate in the current conflict? Please speak of the Russian and Ukrainian sides.*

- **A:** Volunteer groups of white-hat hackers are vocal about their cybersecurity activities; they potentially involve amateurs to work with them. We also cannot exclude a possibility of cooperation between cybersecurity experts and government agencies.