Russian Covert Activities in Cyber Space

MARTIN POZDĚNA, Technische Universität Berlin, DAI-Labor

Aim of this paper is to investigate Russian state and non-state capabilities in cyberspace. Among other things it focuses on the ability to spread propaganda and disinformation and ability to wage a cyber war. Several present and past events that are in general perceived as Russian activity are described including Estonian cyber attacks in 2007, cyber attacks during Russo-Georgian war in 2008, paid pro-government comment trolling on Russian portals and the rise of international pro-Kremlin propaganda during the Ukrainian crisis.

CCS Concepts:•**Security and privacy** → **Social aspects of security and privacy;**

General Terms: Security, Human Factors, Legal Aspects

Additional Key Words and Phrases: Russia, Propaganda, Disinformation, Trolling, Cyber Warfare, Covert activity, Intelligence activity, Hacktivism, Cyber capability

Reference Format:
Martin Pozděna, 2015. Russian Covert Activities in Cyber Space. *TU Berlin* DAI-Labor, Autonomous Security, (September 2015), 12 pages.
URL: http://www.dai-labor.de/en/

1. INTRODUCTION

Information and communication technologies are playing ever increasing role in the everyday life of modern states and its citizens. Payments are executed online, large industrial installations are controlled through IT systems, contact with government is established online (including online voting in some countries) and public opinion is increasingly formed by information obtained online compared to offline sources like TV, radio or printed newspaper. Policy makers, including those in the Russian Federation, are slowly noticing those changes and try to set up mechanisms that would protect their respective countries against cyber threats as well as utilise its cyber capabilities in order to push their interests through both domestically and internationally.

Use of government sponsored cyber activities is a new and progressively evolving topic, which has a potential to reshape the governmental policies as we know them today. The most determining features of cyber activities are easy deniability, easy accessibility and the fact that each country is connected to each other thanks to the Internet. Therefore, any country can spy or attack any other in cyberspace and can subsequently easily deny that it was originator of such action. As cyber espionage and warfare phenomenon are relatively new, there is no international agreement defining what it actually is and how countries can protect themselves against cyber assault in place.[Carr 2009]

To complicate things even further, cyber capabilities of each state does not come solely from assets under its government direct control. Thanks to easy accessibility of cyber warfare and espionage tools and due to the fact that their proliferation is close

This paper was writen as a part of Autonomous Secuirity Seminar at DAI-Labor department of Technische Universität Berlin. LaTeX template used is modified Small Standard Format template of Association for Computing Machinery (ACM). It was obtained from http://www.acm.org/publications/article-templates/acm-latex-style-guide on 19th June 2015 and full credit for it goes to ACM organization and not to the author of this paper.

URL: http://www.dai-labor.de/en/

to impossible to regulate, any individual or company can perform cyberspace actions with or without consent of local government. This is unheard of in classical warfare or espionage actions. It is unacceptable for regular citizens of well-functioning state who are not affiliated with army or intelligence agency to possess military technique or intelligence tools.[Carr 2009]

It can be only guessed how sophisticated are Russian state cyber capabilities as any information concerning the topic are highly restricted. Nevertheless, it is known that Russian Federation inherited advanced classical intelligence capabilities from the former intelligence agency of Soviet Union known as Komitet gosudarstvennoy bezopasnosti (Committee for State Security (KGB)). KGB was established in 1954 and had reached major influence as intelligence agency of former Cold War superpower. It has never been dissolved as a such, but it splitted into domestic intelligence agency Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii (Federal Security Service of the Russian Federation (FSB)) and foreign intelligence agency Sluzhba vneshney razvedki (Foreign Intelligence Service of the Russian Federation (SVR RF)) in 1991. Both agencies are still believed to have major influence in international and domestic affairs of Russian Federation. According to Olga Kryshtanovskaya, a sociologist at the Russian Academy of Sciences, quarter of senior officials in Russian politics are members of FSB or other armed forces and if counting people that are in any way affiliated with security agencies this number grows to 75 percent.[Economist 2007] Amount of people affiliated with security agencies involved in Russia politics grew significanly during Vladimir Putin presidency, who himself served as KGB officer for 16 years. Although no proof of state cyber capabilities can be obtained, the prominent position FSB and SVR RF enjoys within Russian state suggests that they are both likely to be well-equipped.

When it comes to Russian non-state cyber capabilities it is widely known that Russia and Eastern Europe in general is home to some of the most advanced independent hackers in the world. Trend Micro report researching this phenomenon explains that emergence of highly-skilled hacking communities in the region was caused by two major influences. Firstly, it is the tradition of superb natural science education within the region, producing many people who are well-educated in mathematics and physics. Secondly, it was the chaos that was caused by shift from planned economy to market economy in most of the former Eastern Bloc countries. Hacking simply became one of the few viable options how to secure decent living for people talented in natural sciences.[Kellermann 2012] Those established hacking communities can be now utilised by Russian government as non-state cyber weapon in pursuing their goals in cyber space. Although, obtaining proofs that anything like that is happening is close to impossible there are some leads showing that Russian government is well-aware of this potential. For instance Russian authorities are unwilling to prosecute any Russian-based hackers unless they hit domestic targets. Moreover, they are reluctant to come to any agreement with international community that would allow international prosecution of cross-border hacking crimes.[Carr 2009]

This paper aims to investigate actions that are believed to originate in Russia, either at state agency or non-state independent hacker communities. First two sections aim to investigate Russian propaganda in cyberspace in form of paid pro-government comment trolling of domestic resources and rise of propaganda abroad during Ukrainian crisis. Last two sections aim to cover actions of cyber warfare that are believed to originate in Russia; Estonian cyber attacks in 2007 and cyber attacks that happened during Russo-Georgian war in 2008.

2. PAID PRO-GOVERNMENT COMMENT TROLLING

Freedom house report from 2013 mentioned that Russia have been at the forefront of paid pro-government commentating for several years trying to manipulate online discussions on Russian portals. Moreover, rating of freedom of Russian internet is constantly decreasing since the first report was published in 2009.[House 2013]

Although Russian government is trying to keep the existence of so called "web brigades" secret some information concerning its existence and the way they are spreading pro-Kremlin propaganda in cyber space has already leaked over the time. Anna Polyanskaya, Andrej Krivov and Ivan Lonko expressed their suspicion of existence of web brigades in the article "The Virtual Eye of Big Brother" back in 2003. They based their claims on analysis of the content of Russian online forums. They found out that in 1998 between 70 to 80 percent of comments in Russian speaking online forums followed liberal and democratic convictions which were in line with real-life convictions of Russian middle class and emigrants. However, the most prevalent ideas to be found on Russian online forums shifted considerably in just 4 years, with majority of comments following totalitarian values since then. Coincidently, Vladimir Putin rose to power in Russia just in this period, assuming Russian presidency in early 2000. It was discovered that most of the comments are posted by handful of distinguishable and very active individuals who in general support Kremlin policies. Among the most prevalent topics that were spreaded back in 2003 was aggressive and uniform criticism of USA and support of Putin administration campaigns during Second Chechen War. Another well-established pattern was to pretend to live in another country (mostly Western) and complain about the worst aspects of life in the Western countries compared to the advantages of life in Putin's Russia. When tracking the locations of originators of those comments, it turned out that they were submitted through various proxy servers around the world.[Polyanskaya et al. 2003]

First proofs that pro-Kremlin cyber propaganda is paid by state authorities or organizations affiliated with them began to emerge in early 2012. Hacking group named Russian arm of Anonymous managed to steal email communication between Vasily Yakemenko (founder of pro-Kremlin youth organization Nashi), Kristina Potupchik (Nashi spokesperson) and other youth activists. Email communication reveals that bloggers and commentators were paid (or received other benefits like iPads) for their articles and forum comments supporting Putin and his politics. It also revealed that the financial remuneration for each comment was 85 Russian roubles (approx. €2 back then).[Karimova 2012]

Subsequently, activists Lyudmila Savchuk and Marat Burkhard managed to infiltrate Saint Petersburg based company Internet Research, which is believed to be the main base of Russian web brigades. Marat Bukhard was used to work for department spreading propaganda on discussion forums of Russian provinces. He claims that there was a quota of 135 pro-Kremlin comments per shift allowing him to make gross salary of 45,000 RUB (average Russian salary being 32,611 RUB[Service 2015]) He identified Ukrainian crisis as one of the hotest topics of web brigades. They were supposed to spread information about how cruel Kiev junta (current Ukrainian government – described as fascist by Russia) is, shelling innocent civilians and shooting mothers and children. One of the objectives was also to suggest that NATO is to blame for those atrocities. Another topic was depicting Syrian president Bashar al-Assad as a friend of Russia or propagating domestic products like YotaPhone (domestic competition to established smartphones).[Parfitt 2015][Bidder 2015]

Lyudmila Savchuk is freelance journalist who decided to investigate rumours about Internet Research agency by getting employed there. When she joined the agency on the first day she was told that: "We were working for the good of the motherland and

that we were supporting the authorities." She had been working for Internet Research for 2 months before she was sacked for intentionally leaking information about internal workings of the agency to the news. She testified that people there work under security measures like CCTV surveillance or regular email checks. She personally encountered departments spreading propaganda on the following platforms: Facebook, Twitter, YouTube, Livejournal, VK (vkontante – social network similar to Facebook particularly popular among Russian speaking audience) and online forums which belongs to online newspapers or Russian provinces. Each 12 hour long shift started with enabling proxy in order to hide real IP of the author. Subsequently, they were given "technical assignments" which described what ideas and positions they are supposed to spread on the platform they are assigned to. As Lyudmila was in Livejournal group she was writing blog articles mostly targeting Ukrainian government, US president Barack Obama, European Union, prominent Russian opposition representative Alexei Navalny or punk band Pussy Riot.[Parfitt 2015][Bidder 2015] As an example, one of her articles posted under fabricated identity (which is still online by the time of this writing) suggests that Germany and the whole EU is facing harsh economical downturn due to the Russian sanctions imposed on imports of selected EU food products. It blames United States which according to the post forced EU to impose sanctions to Russia over Ukrainian crises and therefore caused the extensive damage to EU economy because of reciprocal Russian sanctions. It also suggests that unless EU gets rid of US dominance and starts to cooperate with Russia it would end up in devastation and ruins.[cantadora_1st 2015]

It is estimated that Internet Research agency employs around 400 people and that there are several more web brigades in different parts of Russian Federation. Nevertheless, no suitable proof can be found backing up either of those estimates. Lyudmila Savchuk only mentioned that she remembers some of her co-workers speaking about business trip to another location in Moscow. It was also mentioned by her that there are departments which are focusing on non-Russian speaking audience creating propaganda in other languages.[Chen 2015]

3. RISE OF INTERNATIONAL PRO-KREMLIN PROPAGANDA DURING UKRAINIAN CRISIS

Efficiency of dissemination of domestic pro-regime propaganda in Russia seems to be quite high with majority of TV channels, radio stations or newspapers being controlled by pro-Kremlin forces and Russian speaking cyberspace flooded by propaganda of web brigades. Therefore, spreading the opinion among average Russian population that legitimate Ukrainian government was overthrown by fascist forces and that those forces pose a threat to Russian people living in eastern Ukraine and Crimea was not at all complicated. Fueling the atmosphere of fear and Western threat to Russian interests and sovereignty was masterly utilised by Putin administration to win overwhelming support among domestic audience (which is still largely influenced by Soviet era education) for annexation of Crimea and other actions of his administration.[Minina 2014][Dougherty 2014]

Despite Putin administration's clear success with spreading pro-Kremlin viewpoints domestically, its impact was very limited outside of Russian Federation before the outset of Ukrainian crisis. Although official government-owned international news channel "Russia Today" has been successfully operational since 2005 it was mostly Western viewpoint what was heard internationally. Fall of communism and breakup of Soviet Union greatly reduced Russian sphere of influence with Ukraine being one of a few Russian strategic partners left. Therefore, potential desire of Ukraine to associate with EU structures and NATO following the Euromaidan were perceived as major setback by Russian policy makers. Author believes that this was a main cause for Russian propaganda to go international and focus on spreading pro-Kremlin ideas among former

Eastern Bloc countries and major Western countries.[Elliott 2014] Main motivation for the publication of this paper was the boom of pro-Russian propaganda flooding Czech cyberspace (which is author's home country) after the start of Ukrainian crisis. Following two subsections will focus on the influence and distribution of pro-Kremlin propaganda in Ukraine and the Czech Republic.

3.1. Focus Ukraine

Research done by Shorenstein Center on Media, Politics and Public Policy states that intensity of propaganda related to the Ukrainian crisis reached similar levels to that of a Cold War. It describes that some parts of it remain the same like disinformation, half-truths and labeling, but it also incorporates some new aspects including heavy use of electronic communication, blogs and social networks.[Dougherty 2014] Although, both parties are using propaganda in this conflict, Russian one seems to have the upper hand.

For instance, Putin and its administration managed to circumvent the initial international outcry concerning the fact that Russia sent its troops to back up the annexation of Crimea. Pro-Kremlin propaganda was tirelessly denying that armed men in unmarked green uniforms who suddenly appeared in Crimea are Russian security units. Fact that Putin finally confessed after the successful incorporation of Crimea into the Russian Federation. Russian propaganda still justifies this move as necessary in order to save Russians living there against fascism that emerged in Ukraine after Euromaidan.[Dougherty 2014]

One of the strategically important aspects of Ukrainian crisis was for Russia to spread their own propaganda concerning all events happening in Ukraine. Portal StopFake.org was therefore set up on 2nd March 2014 with the main objective of disproving fake information about Ukrainian crisis, mostly focusing on information spreaded in Ukraine itself. Nowadays, it is available in Russian, English, Romanian and Spanish language. Since its inception in spring 2014 it managed to localise and disprove more than 500 fake or misleading information about Ukrainian crisis.[StopFake.org 2014]

I would like to provide one example of prominent fake new that originally appeared on Podrobnosti.ua (Ukrainian-based Russian language news portal) on 22nd May 2015 in article named "Carpatho-Rusyns are asking Poroshenko for the same status as DNR". Carpatho-Rusyns are ethnic group living predominantly in Zakarpattia Oblast (south-western district of Ukraine) who have distinct language from Ukrainian. DNR is abbreviation for Donetsk People's Republic, eastern district of Ukraine predominantly inhabited by Russians where clashes between rebels and Ukrainian government for region's autonomy takes place. Article claims that Carpatho-Rusyn representatives gathered in Kiev to call for autonomy of Zakarpattia Oblast from Ukrainian government and mentions Andrey Yurik as representative of Carpatho-Rusyns. Moreover, it also provides a link to the article from 14th March where they claim that Kremlin backs up idea of Carpatho-Rusyn autonomy in Ukraine.[Shevchuk 2015] Fake information spreaded to multiple Russian and Ukrainian news portal, among others First Channel, RIA Novosti or RBC-Ukraine.[StopFake.org 2015]

In response to this article Territorial Carpatho-Rusyns' Society, World Rada (legislative body) of Rusyns, Regional Society of A. Duchnovich, and the People's Council of Carpathian Rus released a statement saying that none of their representatives took part in alleged meeting in Kiev. They informed that Andrey Yurik has no mandate to speak in the name of Rusyn people. Moreover, they stated that this disinformation was spread in order to destabilise their region and the only party which could benefit out of it is Russia gaining pretext to stop fabricated discrimination by military means.[StopFake.org 2015][Prodan and Starosta 2015]

3.2. Focus Czech Republic

Majority of Czech area was liberated by Soviet army by the end of Second World War. Independence of newly reestablished Czechoslovakia was increasingly undermined by Soviets, leading first to the forced refusal of Marshall Plan and subsequently to the Soviet-backed coup d'état in 1948 establishing communist dictatorship in the country. Czechoslovakia under communist rule later became founding member of Comecon (Council for Mutual Economic Assistance – organization for economic cooperation of former Eastern Bloc countries) in 1949 and Warsaw Pact (military alliance of former Eastern Bloc countries) in 1955 making it de facto satellite state of Soviet Union with limited sovereignty. Communist rule in the country tried to reform itself by loosening restrictions on travel, speech and media in 1968, actions that were seen as a threat to the integrity of Eastern Bloc by Soviet policy makers. As a consequence, Czechoslovakia was invaded by Warsaw Pact armies (excluding Romania), replacing reformist government with conservative communist figures. Communist regime remained in power until the popular revolution overthrew it on 17th November 1989 with last occupation troops leaving the country on 27th June 1991. Czechoslovakia later dissolved into Czech Republic and Slovakia and both countries pursued re-integration with Western structures, joining NATO (Czech in 1999 and Slovakia in 2004) and European Union (both in 2004).

This shift was generally unfavorable to Russian (as successor state of Soviet Union) geopolitical interests reducing its sphere of influence. Ever since Czech Republic is of a moderate interest to the Russian intelligence services. Every annual report of Security Information Service (Bezpečnostní informační služba – domestic intelligence agency of the Czech Republic) since 1996 warned that Russian intelligence activities in Czech Republic are extremely high and that the amount of Russian intelligence officers based in Czech are very high in comparison to the other foreign countries.[BIS 2015c][BIS 2015b] The rise of intensity of pro-Kremlin propaganda in the Czech Republic during Ukrainian crisis was personally experienced by the author of this paper and is also mentioned in 2014 anual report of Security Information Service stating the following:

"In relation to the Ukraine crisis Russia and its sympathizers engaged in white, grey and black propaganda. Russian methods of exerting influence and spreading propaganda were based on time-tested Soviet practices, i.e. concealing or covering up own (Russian/Soviet) steps and highlighting or demonizing Western reactions. Russia has been creating influence and propaganda structures in the Czech Republic over a long period of time. The role of these structures is to promote and protect Russian economic and political interest to the detriment of the interests of the Czech Republic, the NATO and the EU. Russia could draw on these structures after the situation in Ukraine deteriorated and did not need to start creating influence structures from scratch. Russian propaganda in the Czech Republic makes use of a number of tools: from ideologically manipulated citizens supporting Russian propaganda unknowingly, to professionals intentionally working with the Russians. Unveiling the memorial commemorating Internationalists (March 2014) demonstrated that the Czech public is highly perceptive to direct Russian (or other foreign) involvement in the Czech Republic. Russia is well aware of this fact; therefore, Russian-language propaganda related to the Ukraine crisis spread by Russian (state and non-state) actors did not play a major role in the Czech Republic. However, the Czech public was and is greatly influenced by Czech pro-Russian organizations and individuals using websites to present their interpretations of Russian stances. The arguments are put forward in a way leading Czech citizens to believe they are recipients of opinions held by fellow citizens not of Russian propaganda. On the one hand, a part of the Czech public is willing to protest a memorial commemorating Soviet occupants – internationalists from 1968, but on the other

hand it defends the Russian occupation of Crimea and the presence of Russian forces in Eastern Ukraine."[BIS 2015a]

Several non-state parties also warned about the rise of pro-Kremlin propaganda being spread in the Czech cyberspace. Discussion further intesified after Slovak activist Juraj Smetana published a list of 42 web portals that supposedly publish Russian propaganda in Czech and Slovak cyberspace. Sputnik news (formerly Voice of Russia – Russian government owned news agency) started to provide pro-Kremlin news in Czech language on 6th March 2015 with other unofficial websites also emerging or becoming more vocal throughout the Ukrainian crisis.[Kennedy and Kralova 2015][Sputnik 2015] Prague Security Studies Institute conducted a research into pro-Kremlin news portals (both officially linked to Russian government like Sputnik News and several others unofficial sources pretending to be independent) and published its results in June 2015 in the paper "The pro-Russian Disinformation Campaing in the Czech Republic and Slovakia". It concludes that all of the portals are spreading the same ideas although the one officially linked to Russian government has more informative and descriptive journalistic style with less use of conspiracy theories or emotionally charged words and pictures. The main ideas spread by those outlets according to the paper and author's own research are:[Smoleňová 2015]

— Presenting Russia as a stronghold of traditional 'unspoilt' values comparing it to the decadent Western societies.
— Depicting US and NATO as aggressor and threat which want to dominate the world.
— Suggesting that EU and NATO are about to collapse (reinforcing disputes among the EU member states).
— Promoting ostalgia in former communist states (feeling that life back in communist times was better than what people have now)
— Presenting current Ukrainian government as fascist and aggressive.

Prominent example of pro-Kremlin propaganda website rising suspicion in the Czech cyberspace is portal AE News (aeronet.cz). Aeronet presents itself as an independent news portal that is run by Czechs and Slovaks living in the Netherlands, Russia and USA. It claims to "provide information from alternative sources, decipher politics, disinformation and media propaganda and to write about consequences." Nevertheless, first glance on the website reveals that it is full of hard to verify information and conspiracy theories that are hugely in favour of Kremlin politics and in line with aforementioned main propaganda ideas. Some of the article headlines on AE News translates from English to Czech as follows:

— "Russian Federation is the stronghold of democracy facing Ukrainian and European Fascism."[Cvalín 2015c]
— "Secretary General of NATO warns again about Russia, citizens of EU are already tired of it."[Cvalín 2015a]
— "NATO counts with the attack on Russian armed forces"[Cvalín 2015b]
— "Fight between Germany and Greece for bilions of euros: Germans still haunted by its Nazi history. Future of EU is now endangered because of it."[Blahuš 2015]
— "Reality 25 years after the Velvet Revolution: 1.5 million people below poverty line, 2 million jobless people, 100 thousand homeless people, 2 million Czechs in execution, rents up to 30 times more expensive than before... but it does not matter, important is that bananas are cheap today!"[anonymous 2014]

On the top of that, it is close to impossible to find out who is behind AE News portal. Overwhelming majority of articles is published by anonymous authors. Website claims that company behind the website is American European News, B.V. with residence in office building near to the Eindhoven airport in the Netherlands. However, fast check

with Dutch company register (http://www.kvk.nl/zoeken/) reveals that no company under this name is registered in the Netherlands (as of 13th Sep 2015).Additionaly, Czech journalists from magazine Respekt called manager of the office building where this company supposedly reside just to find out that its manager has never heard anything about company named American European News.[Kundra 2015] If one try to contact the company he/she can only do it through email or UK or US phone number (suspicious enough for supposedly Dutch entreprise targeting Czech audience). Website also states that any communication with the subject needs to be conducted in English, Russian or Dutch as there is no Czech/Slovak speaking administrative personnel yet. Moreover, aeronet.cz domain is registered using Domains By Proxy service, hiding its real owner. When I first investigated the website in June 2015 it was hosted in Bratislava, Slovakia, but it moved to CloudFlare hosting since then. AE News claims to operate out of donations provided by its supporters in order to "stay as independent as possible."

4. ESTONIAN CYBERATTACKS

Estonia was forcibly incorporated into Soviet Union during Second World War and stayed as one of its republics until the dissolution of Soviet Union in 1991. This period is perceived by Estonian government and international players including European Union as unlawful occupation. After the collapse of the communist empire, Estonia pursued the change of its geopolitical orientation similar to that of Czech Republic joining NATO and European Union in 2004. There is a sizable Russian minority (approximately quarter of Estonian population) living in Estonia as an inheritance from the Soviet Union times. On 26th April 2007 domestic and international tension arose as Estonian government decided to move bronze statue of a Soviet soldier commemorating those of them killed during Second World War from Tallinn city center to its outskirts. Several Russian officials protested, called for the dismissal of Estonian government and riots among Estonian Russians broke out. Those actions were accompanied by cyber attacks targeting critical Estonian IT infrastructure that were unheard of at the time and managed to paralyse some parts of state services.[Lesk 2007]

DDoS attack targeted government institutions and key businesses including banking systems. Although attack was not so overwhelmingly strong (some reports claim the loads to be around 90 Mbps), Estonia (as a small country where such a loads were unexpected) was unable to counter the attack at the time. In spite of relatively weak attack several key state institutions were affected including disruption of operation of some governmental organizations and loss of connectivity to emergency line.[Economist 2008] Estonia finally had to cut off Internet connectivity to the outside world causing substantial troubles for Estonian users both domestically and abroad. The strength of DDoS attack gradually decreased on 10th May 2006.[Lesk 2007]

Despite some of the initial claims that initiator of the attack can be traced back to Russia, there was no hard evidence that Russian government was involved in the attack. Mikko Hypponen, Finnish security researcher, claimed that attack would have been more effective if Russian state cyber capabilities had been utilised.[Lesk 2007] On 3rd Mar 2009, Sergei Markov (state duma deputy) surprisingly announced during conference about information warfare in 21st century that it was his assistant who started the cyber assault against Estonia back in 2007.[Carr 2009] He supposedly stated: "About the cyberattack on Estonia... don't worry, that attack was carried out by my assistant. I won't tell you his name, because then he might not be able to get visas."[Coalson 2009] However, it is unsure whether this claim was reality or just attempt to gain publicity.

Impact of Estonian cyberattacks lead the country and also NATO to reconsider its capabilities to counter rising threat of cyber attacks. As a consequence, NATO Coop-

erative Cyber Defense Center of Excellence was established in 2008 in Tallinn, capital of Estonia, conducting research in cyber conflicts and preparing international cyber network defense exercises “Locked Shields”.

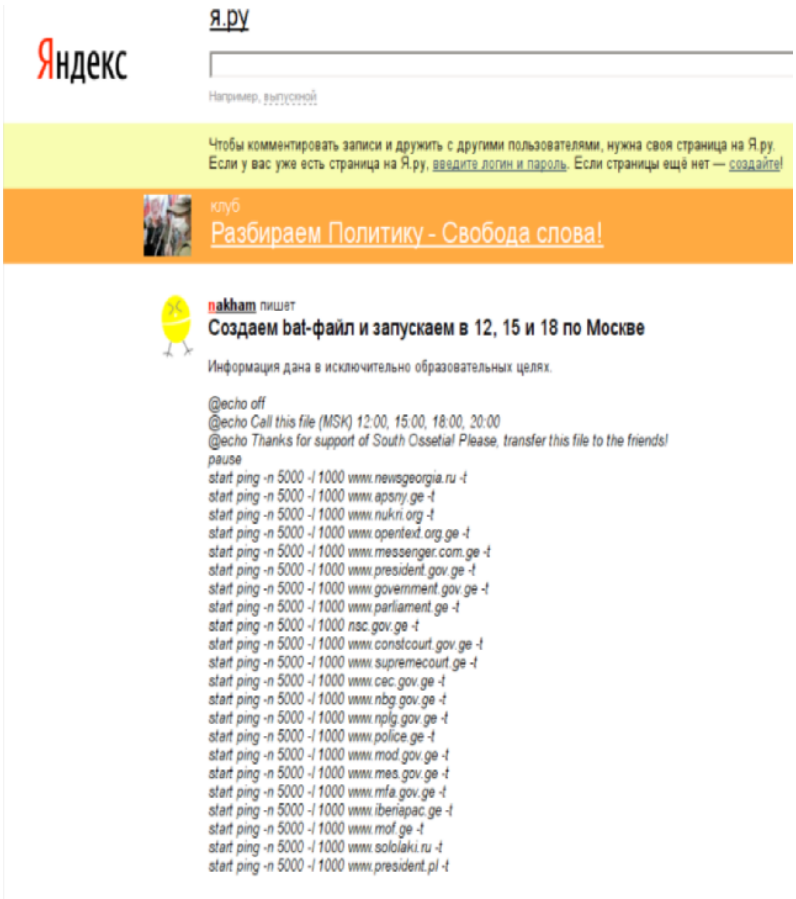
5. CYBER WARFARE AS PART OF RUSSO-GEORGIAN WAR

Georgia was one of the Soviet Socialist Republics from 1922 until the Soviet Union breakup in 1991. Move for independence of Georgia was in general opposed by minority ethnic groups living in South Ossetia (Ossetians) and Abkhazia (Abkhaz). Ethnic tensions after Georgia gained independence lead to the war in both regions which subsequently declared independence from Georgia. Russian Federation provided support to both breakaway republics and conflict was initially settled by means of combined Russian, Georgian and Ossetian peacekeeping forces. Nevertheless, diplomatic relations between Georgia and Russia deteriorated greatly when Georgia pursued NATO Membership Action Plan and Russia started to support the independence of both regions. Tensions were rising starting with occasional skirmishes and finally lead to the Georgian army enter into South Ossetia on 7th August 2008. Russian troops promptly joined the conflict in order to back up South Ossetia and Abkhazia. Conflict was swiftly settled with the support of international community and it is believed to be the first military conflict in which physical war was accompanied by cyber war.

Shadowserver, non-profit group of security specialist monitoring illegal online activity observed first DDoS attack towards the website of Georgian president Mikheil Saakashvili already on 18th July. Some of the requests that were flooding Saakashvili’s website contained strings like “win+love+in+Rusia” and website remained down or unresponsive for several days. Nevertheless, the real warfare in cyberspace only started along with the physical conflict between Russian and Georgian troops on 8th August 2008.[Nazario and DiMino 2008] StopGeorgia.ru website emerged advising about which high-profile websites can be attacked from Russian and Lithuanian IP addresses. Moreover, it provided tutorials on how to launch DDoS attacks and forums where more experienced hackers were advising those with limited technical background on other vulnerabilities like SQL Injection and which websites are prone to them.[Carr 2009] Other Russian forums also provided scripts and advises on how to target important Georgian websites. Figure 1 shows forum post from Yandex.ru (popular Russian search engine and internet services provider) with Windows batch script meant for ICMP flooding of important Georgian website. Post advices to execute the script on 12pm, 3pm and 6pm Moscow time along with thankful message for the support of South Ossetia.[Nazario and DiMino 2008]

There were also occasions of BGP instability which caused the Georgian traffic to be rerouted through Russia or gave rise to other infrastructure issues. There is nevertheless no hard evidence whether this was intentionally caused by Russian actions or other issue related to infrastructure or physical war campaign.[Nazario and DiMino 2008] On the other hand counter attacks against Russian websites were also spotted and website stopgeorgia.ru was taken down for sevaral days by cyber attack.[Carr 2009]

There is no hard evidence available that would prove that Russian Secret Services were in any way directly involved in cyber attacks during Russo-Georgian war. However, there are claims that cyber attacks were organized so swiftly that the preparations needed to commence already before the actual physical conflict broke out on 8th August (which would indicate state involvement).[Carr 2009] On the other hand, proved attacks mostly consisted of DDoS (either supported by individuals or botnet to hire), quite unsophisticated SQL injections and defacements which would rather indicate that attack was carried out by non-state hackers of moderate technical skills.[Nazario and DiMino 2008]


Яндекс

Я.ру

Например, выпускной

Чтобы комментировать записи и дружить с другими пользователями, нужна своя страница на Я.ру.
Если у вас уже есть страница на Я.ру, введите логин и пароль. Если страницы ещё нет — создайте!

клуб
Разбираем Политику - Свобода слова!

nakham пишет
Создаем bat-файл и запускаем в 12, 15 и 18 по Москве

Информация дана в исключительно образовательных целях.

```
@echo off
@echo Call this file (MSK) 12:00, 15:00, 18:00, 20:00
@echo Thanks for support of South Ossetia! Please, transfer this file to the friends!
pause
start ping -n 5000 -l 1000 www.newsgeorgia.ru -t
start ping -n 5000 -l 1000 www.apsny.ge -t
start ping -n 5000 -l 1000 www.nukri.org -t
start ping -n 5000 -l 1000 www.opentext.org.ge -t
start ping -n 5000 -l 1000 www.messenger.com.ge -t
start ping -n 5000 -l 1000 www.president.gov.ge -t
start ping -n 5000 -l 1000 www.government.gov.ge -t
start ping -n 5000 -l 1000 www.parliament.ge -t
start ping -n 5000 -l 1000 nsc.gov.ge -t
start ping -n 5000 -l 1000 www.constcourt.gov.ge -t
start ping -n 5000 -l 1000 www.supremecourt.ge -t
start ping -n 5000 -l 1000 www.cec.gov.ge -t
start ping -n 5000 -l 1000 www.nbg.gov.ge -t
start ping -n 5000 -l 1000 www.nplg.gov.ge -t
start ping -n 5000 -l 1000 www.police.ge -t
start ping -n 5000 -l 1000 www.mod.gov.ge -t
start ping -n 5000 -l 1000 www.mes.gov.ge -t
start ping -n 5000 -l 1000 www.mfa.gov.ge -t
start ping -n 5000 -l 1000 www.iberiapac.ge -t
start ping -n 5000 -l 1000 www.mof.ge -t
start ping -n 5000 -l 1000 www.sololaki.ru -t
start ping -n 5000 -l 1000 www.president.pl -t
```

Fig. 1. DDoS batch script posted on Yandex.ru [Nazario and DiMino 2008]

6. CONCLUSIONS

As described throughout the paper there are several acts of cyber propaganda and cyber warfare that are likely to originate from Russia. Universally, it is extremely simple to deny and mask involvement in cyber activities for any government, including the Russian one. Therefore, there should be no surprise that Kremlin officially rejected all accusations and that there are no conclusive proofs that Russian government was actually involved in any of those actions.

The most conclusive evidence is present for the acts of dissemination of pro-Kremlin cyber propaganda. As in this case it is continuous activity it is more likely to be exposed over the time (unlike Estonian or Georgian cyber attacks which lasted just few days). Testimonies about institutions employing armies of people producing cyber propaganda exist along with exfiltrated email communication of people close to Kremlin who supposedly paid others for such activities. Any potential claims that such an activity is expression of civic society and act of non-state patriotic Russian hackers are unlikely to hold. Mainly because free civic society never represents itself as 100 percent pro-government and anti-opposition at the same time. Russian state cyber capabilities seems to be advanced enough in this area thanks to the experience gained over the time (first allegation of governmental sponsored cyber propaganda appeared in 2003)

and reasonable support provided by the government. There is generous state funding for such activities. Evidence confirms above average paychecks for people involved in cyber propaganda activities as well as significant investments in official international news outlets like Russia Today or Sputnik. Therefore, it seems that Russia possess one of the most advanced cyber propaganda and disinformation campaign capabilities and realizes its importance for promoting their political goals at the same time. Rise of international pro-Kremlin propaganda in cyberspace during Ukrainian crisis only supports this claim.

On the other hand, evidence present in both Estonian and Georgian cyber attacks is insufficient in order to draw any conclusions about direct Kremlin involvement. Facts like low technical complexity and the way attacks were coordinated through online forums rather indicate that non-state hackers of moderate experience were mostly involved in those attack. State with the third highest military budget in the world is likely to be able to carry out more than DDoS and simple SQL Injection attacks in the cyber space. Possible explanation might be that both Estonia and Georgia were rather too weak opponents to fully utilise (and reveal to the whole international community) state cyber warfare potential. In any case it was important wake up call for everybody that cyber war techniques can and will be utilised in the future and that all countries should set up adequate protection mechanisms for their critical infrastructure.

REFERENCES

anonymous. 14th Nov 2014. Zapáchající realita 25 let po Sametu: Půl druhého miliónu Čechů pod hranicí chudoby, 2 milióny lidí bez práce, 100 tisíc Čechů bez domova, 2 milióny Čechů v exekuci, nájemné až 30x vyšší než tehdy... ale to nevadí, hlavně že jsou dnes levné banány! goo.gl/mf0AV9. (14th Nov 2014). Accessed: 13th Sep 2015.

Benjamin Bidder. 1st Jun 2015. Paid as a Pro-Kremlin Troll: 'The Hatred Spills over into the Real World'. http://www.spiegel.de/international/world/interview-with-ex-russian-internet-troll-lyudmila-savchuk-a-1036539.html. (1st Jun 2015). Accessed: 4th Sep 2015.

Security Information Service BIS. 2015b. Annual reports in Czech. http://www.bis.cz/vyrocni-zpravy-historie.html. (2015). Accessed: 13th Sep 2015.

Security Information Service BIS. 2015c. Annual reports in English. http://www.bis.cz/vyrocni-zpravyEN.html. (2015). Accessed: 13th Sep 2015.

Security Information Service BIS. 4th Sep 2015a. Annual Report of the Security Information Service for 2014. http://www.bis.cz/vyrocni-zpravaEN6c8d.html. (4th Sep 2015). Accessed: 13th Sep 2015.

Petr Blahuš. 19th Mar 2015. Souboj Řecko vs. Německo o miliardy EUR: Nacistická minulost Němce stále dohání. V ohrožení je proto nyní osud celé Evropské unie. goo.gl/bMzbY7. (19th Mar 2015). Accessed: 13th Sep 2015.

cantadora_1st. 3rd Mar 2015. Plokhiye Predchuvstviya: Pochemu YA Perezhivayu Za Sestru, Zhivushchuyu V Yevrope. http://cantadora-1st.livejournal.com/249714.html. (3rd Mar 2015). Accessed: 4th Sep 2015.

Jeffrey Carr. 2009. *Inside Cyber Warfare*. "O'Reilly Media, Inc.".

Adrian Chen. 2nd Jun 2015. The Agency. http://www.nytimes.com/2015/06/07/magazine/the-agency.html. (2nd Jun 2015). Accessed: 4th Sep 2015.

Robert Coalson. 6th Mar 2009. Behind The Estonia Cyberattacks. http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html. (6th Mar 2009). Accessed: 13th Sep 2015.

Petr Cvalín. 11th Apr 2015b. NATO počítá s útokem na ruské ozbrojené síly. http://aeronet.cz/news/nato-pocita-s-utokem-na-ruske-ozbrojene-sily/. (11th Apr 2015). Accessed: 13th Sep 2015.

Petr Cvalín. 29th May 2015a. Generální tajemník NATO opět varoval před Ruskem, občany EU to už unavuje. http://aeronet.cz/news/generalni-tajemnik-nato-opet-varoval-pred-ruskem-obcany-eu-to-uz-unavuje/. (29th May 2015). Accessed: 13th Sep 2015.

Petr Cvalín. 3rd Mar 2015c. Ruská federace je silnou demokratickou hrází proti ukrajinském a evropskému fašismu. http://aeronet.cz/news/ruska-federace-je-silnou-demokratickou-hrazi-proti-ukrajinskem-a-evropskemu-fasismu/. (3rd Mar 2015). Accessed: 13th Sep 2015.

Jill Dougherty. 2014. Everyone Lies: The Ukraine Conflict and Russia's Media Transformation. http://shorensteincenter.org/wp-content/uploads/2014/07/d88-dougherty.pdf. (2014). Accessed: 5th Sep 2015.

The Economist. 23rd Aug 2007. The making of a neo-KGB state. http://www.economist.com/node/9682621. (23rd Aug 2007). Accessed: 3rd Sep 2015.

The Economist. 4th Dec 2008. Marching off to cyberwar. http://www.economist.com/node/12673385. (4th Dec 2008). Accessed: 15th Sep 2015.

Chris Elliott. 4th May 2014. The readers' editor on... pro-Russia trolling below the line on Ukraine stories. http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online. (4th May 2014). Accessed: 5th Sep 2015.

Freedom House. 3rd Oct 2013. Freedom on the Net 2013. https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf. (3rd Oct 2013).

Anastasiya Karimova. 13rd Feb 2012. Kremlevskaya Blogodel'nya. http://www.kommersant.ru/doc/1868022. (13rd Feb 2012). Accessed: 4th Sep 2015.

Tom Kellermann. Sep 2012. Peter the Great Versus Sun Tzu. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/op_kellermann_peter-the-great-vs-sun-tzu.pdf. (Sep 2012). Accessed: 3rd Sep 2015.

Paula Kennedy and Simona Kralova. 2nd Apr 2015. Russian bid for Czech hearts and minds. http://www.bbc.com/news/world-europe-32070184. (2nd Apr 2015). Accessed: 13th Sep 2015.

Ondřej Kundra. 28th Feb 2015. Putinův hlas v Česku. http://www.respekt.cz/z-noveho-cisla/putinuv-hlas-v-cesku. (28th Feb 2015). Accessed: 13th Sep 2015.

Michael Lesk. 2007. The new front line: Estonia under cyberassault. *Security & Privacy, IEEE* 5, 4 (2007), 76–79.

Elena Minina. 29th Mar 2014. Why do Russians support intervention in Ukraine? http://www.aljazeera.com/indepth/opinion/2014/03/why-do-russians-support-interv-2014328174257483544.html. (29th Mar 2014). Accessed: 5th Sep 2015.

Jose Nazario and Andre M. DiMino. 2008. An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf. (2008). Accessed: 15th Sep 2015.

Tom Parfitt. 24th Jun 2015. My life as a pro-Putin propagandist in Russia's secret 'troll factory'. http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html. (24th Jun 2015). Accessed: 4th Sep 2015.

Anna Polyanskaya, Andrej Krivov, and Ivan Lonko. 30th Apr 2003. Virtual'noye Oko Starshego Brata. http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm. (30th Apr 2003). Accessed: 4th Sep 2015.

YU. Prodan and M. Starosta. 22nd May 2015. Vidkryta zayava rusyns'kykh orhanizatsiy Zakarpattya. http://www.transkarpatia.net/transkarpathia/actual/48909-vdkrita-zayava-rusinskih-organzacy-zakarpattya.html. (22nd May 2015). Accessed: 6th Sep 2015.

Russian Federal State Statistics Service. 2015. Uroven' Zhizni Naseleniya. http://www.gks.ru/bgd/free/B15_00/IssWWW.exe/Stg/dk03/6-0.doc. (2015). Accessed: 4th Sep 2015.

Igor' Shevchuk. 22nd May 2015. Rusiny Zakarpat'ya trebuyut ot Poroshenko statusa kak u DNR (foto). http://podrobnosti.ua/2035969-rusiny-zakarpatja-trebovali-spetsstatusa-pod-administratsiej-poroshenko-foto.html. (22nd May 2015). Accessed: 6th Sep 2015.

Ivana Smoleňová. Jun 2015. The pro-Russian Disinformation Campaing in the Czech Republic and Slovakia. http://www.pssi.cz/download/docs/253_is-pro-russian-campaign.pdf. (Jun 2015). Accessed: 13th Sep 2015.

Sputnik. 6th Mar 2015. Sputnik promluvil česky. http://cz.sputniknews.com/czech.ruvr.ru/2015_03_06/Sputnik-promluvil-cesky-4040/. (6th Mar 2015). Accessed: 13th Sep 2015.

StopFake.org. 2014. About us. http://www.stopfake.org/en/about-us/. (2014). Accessed: 6th Sep 2015.

StopFake.org. 27th May 2015. Fake: Russinians Demand Autonomy. http://www.stopfake.org/en/fake-russinians-demand-autonomy/. (27th May 2015). Accessed: 6th Sep 2015.