Cyber-conflict between the United States of America and Russia

CSS CYBER DEFENCE HOTSPOT ANALYSIS

Cyber-conflict between the United States of America and Russia

Zürich, June 2017

Version 1

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Author: Marie Baezner, Patrice Robin

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Oliver Thränert, Head of Think Tank

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: Cyber-conflict between the United States of America and Russia, June 2017, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Targets:	US State institutions and a political party.
Tools:	*Remote Administration Tools*[1] delivered by *spear phishing* emails.
Effects:	Heightened tensions between the USA and Russia in cyberspace and in physical world.
Timeframe:	Tensions evident since 2011 and still ongoing, with a hot phase during the 2016 US presidential elections.

Cybersecurity and cyber-defense are domains that grew in importance during the last ten years, especially after the cyberattacks in Estonia in 2007 and the use of cyber capabilities in combination with conventional military means during the conflict between Russia and Georgia in 2008. These events demonstrated that state actors were willing and able use cyber capabilities in their military operations.

This analysis examines the particular hotspot of the cyber-conflict between the USA and Russia in relations to cyber-defense. In this report, a hotspot is defined as the cyber aspect of the relations between states in the context of tensions or conflict. This relates to series of actions taken by states and non-state actors in cyberspace.

The main objective of this hotspot analysis is to bring a better understanding of the incidents that occurred during the presidential elections in the USA and their effects. The goal is also to see how the situation was managed by the USA and how it reacted, in order to learn from it and be able to prepare for similar situations.

Description

Since 2015, several US institutions and the US Democratic National Committee (DNC)[2] have been the victims of a series of intrusions in their networks. The perpetrators, believed to be the Russian hacker groups "APT28" and "APT29", used *spear phishing* emails to deliver *Remote Administration Tools malware*. These techniques enabled the hacker groups to remotely access their victims' computer networks and gain access to sensitive data. The stolen data from the DNC was later published at strategic times during the US presidential elections, interfering in the democratic process and potentially helped the Republican candidate, Donald Trump, win the elections. In October 2016, The US government officially accused the Russian government of having ordered the network intrusions.

Effects

The analysis found that the tensions between the USA and Russia over activities in cyberspace had a variety of effects on the US domestic level and on the international level. The social and internal political effects were marked by a loss of trust in the legitimacy and integrity of the democratic process, as well as a loss of credibility for the Democratic candidate Hillary Clinton. The USA also took time to respond politically to the cyberattacks, which made it look indecisive. The economic effects were limited to costs in cybersecurity and forensics. The technological effects were restricted to a possible increase in expenditure in cyber-defense, and the possible classification of voting systems as critical infrastructures.

The international effects of the tensions between the USA and Russia over cyber-activities were the possible escalation of the situation and its spilling into a conventional war, the situation remaining the same, or deescalating. The tensions could also lead to an increase in cooperation in regard to state behavior in cyberspace. Several European states also expressed fears of seeing a similar scenario developing during their national elections in 2017.

Consequences

Several consequences can be derived from the intrusions in US networks, the disclosure of information during the elections and their effects. States could try to prevent similar situations from happening by improving their cybersecurity measures and education. They could start an integrative program involving the whole society aimed at revealing propaganda and misinformation campaigns. They should closely monitor the evolution of the relations between the USA and Russia as well as the US support to NATO to adapt their own strategies. They should try to promote international cooperation regarding state's behavior in cyberspace to reduce mistrust and the risks of misinterpretations.

[1] Technical words written in italics are explained in a glossary in section 7 at the end of the document.

[2] Abbreviations are listed in section 8 at the end of the document.

1 Introduction

The importance of cybersecurity and cyber-defense increased significantly during the last ten years. The cyberattacks that targeted Estonian institutions in 2007 and the cyber-operations conducted alongside the military ground operations during the conflict between Georgia and Russia in 2008 demonstrate the increasing relevance of the issue. The study and evaluation of hotspots brings concrete examples to support the theoretical and abstract concepts of cybersecurity. Their objective is to detail how victims of cyberattacks were affected and how they reacted to them. This report also serves as a basis for a broader study that will compare the various hotspots, and provide advice on how states can improve their actions if faced with similar situations.

This document will be updated when new elements are discovered or when significant changes in hotspots occur. The aim is to keep the document up to date with current issues to stay as accurate as possible.

This hotspot analysis examines the particular case of the tensions between the USA and Russia in relation to activities in cyberspace. Since the international intervention in Libya and through the various peace talks over the civil war in Syria, the tensions between the two states steadily increased. They reached a new level with the cyberattacks on the US Democratic National Committee's (DNC)[3] networks during the US presidential elections. It reached the point that former Soviet leader, Mikhail Gorbatchev, stated that the relations between the USA and Russia are at their lowest point since the end of the Cold War (Gaouette and Labott, 2016).

This hotspot is relevant because it is an ongoing and fast-developing issue, which also has repercussions on other conflicts and events in the world like the wars in Syria and Ukraine (e.g. in Syrian peace negotiations or in the development of sanctions imposed on Russia after the annexation of Crimea).

The report will proceed as follows. In section 2, the report describes the historical background and chronology of events before and during the cyberattacks on the US presidential elections. It lists and summarizes events that have shaped the tensions between USA and Russia to give the context in which the cyberattacks unfold.

Section 3 explains the various tools and techniques used during the intrusions into US networks, as well as who were the targets and to whom the cyberattacks could be attributed. It shows that several US institutions and the DNC have been the victims of a series of intrusions in their networks. The perpetrators, believed to be the Russian hacker groups "APT28" and "APT29", used *spear phishing*[4] emails to deliver *Remote Administration Tools (RAT) malware* to remotely access their victims' computer networks and access data.

Section 4 analyses the various effects of these tensions on domestic and international levels. It demonstrates that the domestic effects of the cyberattacks were felt in social, political, economic and technologic fields. The social and internal political effects were characterized by a general loss of trust in the legitimacy and integrity of democratic processes. Also the Obama administration appeared indecisive in its political response to the cyberattacks on the account of the time it required. Economic effects were marked by the costs for the victims of such cyberattacks. Technological effects were limited to a possible increase in expenditure in cyber-defense and a possible classification of the voting infrastructures as critical infrastructures. International effects could be an escalation of the conflict in cyberspace spilling over to a conventional war, the situation remaining the same or a de-escalation with the promotion of international cooperation on cyberspace.

Finally, section 5 details some consequences that could be derived from this case and which state actors could implement. It sets out how state actors can decrease their risks of being the victims of similar intrusions by improving their cybersecurity measures, developing their education in regard to cyber, encouraging the whole of society to reveal propaganda and misinformation campaigns, monitoring the evolution of the relations between USA and Russia, and promoting *Confidence Building Measures (CBM)*.

[3] Abbreviations are listed in section 8 at the end of the document.

[4] Technical words written in italics are explained in a glossary in section 7 at the end of the document.

2 Background and chronology

The historical background and the chronology of the events in this hotspot are important for understanding how the tensions between the two states developed, provide the context in which the cyberattacks took place, and how the current dynamic was set in place.

Russia lost its power and pride after the fall of the Soviet Union and the USA was free to act without any counterbalance. When Putin became President, his goal is give back to Russia the glory of its past. After 11th of September 2001, Russia moved closer to the West than it had ever been, but the situation did not last and tensions started to develop after the US intervention in Iraq in 2003. The conflict in the Caucasus in 2008 demonstrated to the world that Russia was ready to use military actions as foreign policy tools. However the event that definitively cut Russia away from the West was the multi-state military intervention in Libya in 2011, to which the former Russian President, Dmitry Medvedev, agreed. However, Putin openly disagreed with the intervention (Ornos et al., 2017). Since then every move from each side was even more under scrutiny and was seen as a way to provoke the other.

Date	Event
08.2008	For several days, rebels from South Ossetia, supported by Russia, physically attack Georgian armed forces. In a retaliation raid, Georgian armed forces kill twelve peacekeepers from the Commonwealth of Independent States and injure many more. This raid serves as argument for Russia to invade the country. The conflict lasts a month, but during this period Russia shows that it was capable and willing to use its military force as an instrument of its foreign policy. It was also during this conflict that Russian forces test their tactic of combining cyberattacks (*Distributed Denial of Service (DDoS*) attacks and *website defacement*) in combination with kinetic forces (Giles, 2016, pp. 4–5).
03-10.2011	USA participates in the multi-state military intervention in Libya under a United Nations (UN) mandate (Klion, 2016).
12.2011	Putin wins the legislative elections, but the opposition organizes demonstrations to protest against the election results. During the protests, Russian armed forces used automated *DDoS* tools to disrupt media and social media pages in order to stop the discussions over the elections (Giles, 2012). Russian President Vladimir Putin hold the US Secretary of State at that time, Hillary Clinton, responsible for inciting protests on social media (Sanger, 2017).
07.2013	In a Cooperation Dialogue, the USA and Russia agree on measures concerning Information and Communications Technology (ICT) security (The White House, Office of the Press Secretary, 2013).
15.03.2013	A hacker named "Guccifer" hacks the email account of a former aide of Bill Clinton. The hack reveals that Hillary Clinton, during her time as US Secretary of State, used her unclassified private email account to exchange sensitive and classified information about foreign policy matters, which is not permitted by federal policies (Kessler, 2015).
03.2014	Russian troops invaded the peninsula of Crimea. In this conflict, Russia also conducted cyberattacks alongside its armed forces' operations on the ground in order to gain advantage and to cause confusion in the Western media (Giles, 2016, pp. 31–33). In a speech at the University of California, Clinton compares this Russian expansion to the annexation of Austria by Hitler in 1938 (Klion, 2016).
10.2014	Several servers of the White House and the US Department of State are hacked (Perez and Prokupecz, 2015).
12.2014	The new Russian military doctrine is published, which also detailed the concept of "Information warfare" (Giles, 2016, p. 27).
Early 2015	An unclassified network from the Pentagon is hacked (Crawford, 2015; Stewart, 2015).
07.2015	The email servers of the US military's Joint Chiefs of Staff are hacked (Martin, 2016; Starr, 2015). About the same time, the hacker group "APT29" manages to breach the DNC computer network (US Department of Homeland Security and Federal Bureau of investigation, 2016).
22.07.2015	The UN group of governmental experts (UN GGE), including representations of 20 states, along with the USA and Russia, publishes a report on international norms in the field of information and telecommunications within the context of international security (United Nations General Assembly, 2015).
03.2016	A second hacker group, "APT28", breaches the DNC computer network as well (US Department of Homeland

03.2016	Security and Federal Bureau of investigation, 2016).
19.03.2016	The DNC suspects that it was hacked and hires the cybersecurity enterprise, CrowdStrike, to investigate the breach (Inkster, 2016, p. 23). The stolen data are, in part, from the email account of Clinton's campaign chairman, John Podesta, (Krieg and Kopan, 2016).
06.2016	The media reveal the DNC server breach. CrowdStrike suspects Russian hackers, with ties to their government, to have hacked the servers (Hosenball et al., 2016). The Kremlin denies any involvement in the cyberattacks (Rudnitsky et al., 2016).
07.2016	The voter registration systems of the states of Arizona and Illinois are hacked (Lartey, 2016; Reuters, 2016) as well as the servers from the Democratic Congressional Campaign Committee (DCCC) (McCain Nelson and Peterson, 2016). At the end of the month, thousands of stolen emails from the DNC servers breach are published on the Wikileaks and DCleaks websites (Hosenball et al., 2016). In a speech, the Republican candidate, Donald Trump, invites Russian hackers to penetrate again into DNC network and to steal more information. An investigation is started by the Federal Bureau of Investigation (FBI) to examine a possible collusion between Trump campaign's staff members with Russia (Borger, 2017a). A few days later, the Russian government announces the detection of a spying *malware*, affecting 20 different networks in Russian organizations (BBC News, 2016a).
15.08.2016	A hacker group, named "Shadow brokers", claims to have stolen data from the National Security Agency (NSA). The stolen data, they declares, was various *malware* developed by the "*Equation Group*", which they then put up for internet auction (Greenberg, 2016).
19.08.2016	Paul Manafort, Trump's campaign manager resignes after being suspected to have had contact with Russian intelligence officials (Torpey and Levett, 2017).
09.2016	The Russian hacker group, "APT28", accesses medical files of athletes on the World Anti-Doping Agency's network and leak them on the internet (Ingle, 2016).
07.10.2016	President Obama officially accuses Russia of being behind the DNC hack. He warns Russia of possible retaliation if Moscow was to intervene in the November 2016 presidential election (Strohm and Syeed, 2016). The Russian President does not confirm nor deny the Russian involvement in the DNC breach. He adds that USA was supporting and paying media outlets and non-governmental organizations to interfere in Russian politics (Ornos et al., 2017).
09.10.2016	Wikileaks publishes Podesta's emails that were stolen during the DNC breach in March 2016.
10.2015	The US Central Intelligence Agency (CIA) announces that it is ready to prepare a covert cyber operation to retaliate against Russia (Timm, 2016).
15.10.2016	Due to the lack of buyers, the hacker group "Shadow brokers" calls off the *malware* auction (Ashok, 2016).
30.10.2016	FBI director declares that they acquired new information on Hillary Clinton's use of her private email in 2013 and that the investigation was still ongoing (Borger, 2017a).
31.10.2016	The hacker group "Shadow Brokers" publishes a list of servers hacked by the NSA between 2000 and 2010 (Goodin, 2016).
08.11.2016	Donald Trump wins the US Presidential elections.
14.11.2016	Trump and Putin assures that they seek to reverse the growing tensions in their countries' relations (Ignatius, 2016).
25.11.2016	Russian government declares discovery of a plot targeting Russian banking systems with cyberattacks. Russia blames foreign spy agencies and claims that the attack was stopped before it could do any harm (Lowe and Zinets, 2016).
12.2016	President Obama suggests the creation of a cybersecurity ambassador in a report on cybersecurity to the incoming President. His or her role would be to develop international norms on states' behavior in cyberspace (Lee, 2016).
09.12.2016	The Washington Post publishes an article claiming that, after assessment, the US intelligence community asserted Russian interference in the presidential elections, which helped Donald Trump win the presidency (Entous et al., 2016).
15.12.2016	The security firm, Recorded Future, discovers that the US Election Assistance Commission's network

15.12.2016	was hacked after election day in November. The US Election Assistance Commission is responsible for controlling the security of the voting machines. The supposed hacker is believed to be Russian-speaking, but do not have any ties to the Russian government (Menn, 2016).
29.12.2016	The US Department of Homeland Security (DHS) and the FBI publishes a joint report on the cyberattacks during the presidential elections (US Department of Homeland Security and Federal Bureau of investigation, 2016).
29.12.2016	President Obama expels 35 Russian diplomats from US territory and closed two Russian compounds in USA as retaliation for the cyberattacks during the elections (BBC News, 2016b).
30.12.2016	The Russian Foreign Minister suggests expelling 35 US diplomats from Russian territory, but Russian President Putin rejected the proposition (BBC News, 2016c).
01.01.2017	The 35 expelled Russian diplomats leave the USA (BBC News, 2017a).
06.01.2017	The US National Intelligence Council publishes an unclassified version of their report on the Russian cyber activities in the US presidential election (National Intelligence Council, 2017).
08.01.2017	The group "Shadow Brokers" starts another auction of a new set of stolen *malware* from the NSA (Bing, 2017; Goodin, 2017).
11.01.2017	The news website Buzzfeed.com publishes a series of unverified reports alleging that Russia had compromising documents on US President Trump. Both Russia and Trump claim that these allegations are unfounded (Borger, 2017b).
20.01.2017	Donald Trump is inaugurated as the 45th US President.
31.01.2017	Russian authorities arrest four cybersecurity specialists, two of whom were working for the Federal Security Service (FSB). They are accused of treason and cooperation with the CIA (Walker, 2017).
14.02.2017	The US national security advisor, Michael Flynn, resigns because of contacts with the Russian ambassador to the USA and was considered vulnerable to Russian coercion (Borger, 2017c).
02.03.2017	The US Attorney General, Jeff Sessions, is accused of lying at his Senate confirmation hearing in January 2017 about meeting twice with the Russian ambassador to the USA during the election campaign (Siddiqui, 2017).
04.03.2017	President Trump accuses former President Obama of ordering the interception of his communications during the election campaign (Malkin and Yuhas, 2017).
06.03.2017	Series of documents, stolen from the CIA, is published on Wikileaks. They reveal several cyber-programs developed by the agency and disclose the use of technical vulnerabilities in internet-connected televisions, the development of a library of malware to store and categorize malicious software used by foreign agencies, and the use of the US consulate in Frankfurt as a covert base for the Center of Cyber Intelligence. The CIA does not comment on that leak. It is believed that the leak came from inside the agency or from a contractor, but was not due to a cyberattack (MacAskill et al., 2017).
20.03.2017	At a House Intelligence Committee Hearing, the FBI director confirms that his agency launched an investigation on Trump-campaign staff members for possible collusion with Russia. He adds that there is no information supporting the claim that Obama administration had wiretapped Trump's campaign (Borger and Ackerman, 2017).
22.03.2017	The House intelligence committee chairman, Devin Nunes, declares in a press conference that some members of Trump's team have been recorded after the elections when they had met with persons of interest under surveillance by the US intelligence. He states that these recording did not support President trump's claim of Obama ordering surveillance on his team during the elections and are not part of the FBI investigation on Trump team's ties with Russia (BBC News, 2017b).

3 Description

This section will first detail the various tools and techniques used by the perpetrators in the various cyberattacks on US institutions in order to understand how the perpetrators managed to enter into the networks and steal data. Secondly it will describe the types of victims targeted by the cyberattacks. Finally, it will

examine the alleged perpetrators of these intrusions and the evidence suggesting that they are be behind the cyberattacks.

3.1 Tools and techniques

The escalation in cyber-interactions between the USA and Russia is marked by a series of events. This section specifically details tools used in the incidents that occurred after the invasion of Crimea[5].

The penetration in US institutions' servers were *data breaches* conducted using an entry technique known as *spear phishing*, where emails are used to send a malicious link or content. Recipients of the emails sent by the hacker group "APT29" would be lured into clicking on a link or an attachment, seemingly coming from a legitimate sender that triggers the download of malware. The malicious software then implants a *Remote Access Tool (RAT)* in the computer allowing the perpetrators to remotely access the system and steal data without the computer users' knowledge. The hacker group "APT28" used a similar technique, luring their victims with fake emails, seemingly originating from legitimate businesses, tricking the recipient into giving their login credentials (username and password). The hackers then use the stolen information to access their victims' systems and install *malware* to gather specific data.

Using *zero-day vulnerabilities* or unpatched vulnerabilities of software already installed on the machines, the *malware* would then send data back to servers belonging to the hacker groups. These operations proceed without the knowledge of the users, permitting attackers to stealthily steal emails, sensitive information, or other personal data. These techniques are also used for reconnaissance of network architecture and intelligence collection on a network's vulnerabilities with the aim of preparing a future attack. The attackers can then use the *backdoor* opened by the *RAT* to retrieve files and data (Dilanian et al., 2016). The use of *spear phishing*, a targeted technique, suggests that the victims were not chosen at random. The *spear phishing* emails were precisely designed to fit their victims. The use of *zero-day vulnerabilities* is not normally a method for inexperienced hackers, but rather individuals or groups with considerable knowledge, resources and time (Thielman and Ackerman, 2016).

The information released on the tools used by the attackers during the 2016 US election were mostly focused on the techniques, but also suggested that *malware* from the "Dukes" family[6] was used. It was probably the "SeaDuke" *malware* toolset, which is used as secondary *backdoor* (Calabresi and Rebala, 2016; F-Secure, 2015; Lipton et al., 2016).

The perpetrators also used the publication of stolen information and misinformation to influence the US elections. By releasing stolen information at strategic times in the campaign, they tried to influence public opinion. The goal was the same when releasing misinformation through the use of *trolls*, who wrote hateful comments on social media websites and spread rumors. This method does not require any special technical knowledge. English-written news channels funded by the Russian state, like RT (formerly Russia Today) and Sputnicknews were also used in order to shape public opinion on the candidates (Inkster, 2016, p. 28).

Regarding the cyber-incidents in Russia, there has been no information on the tools or techniques used.

3.2 Targets

In this cluster of cyber incidents, the majority of targets were located in the USA with a couple of events in Russia. In the USA, the targets could be categorized into two groups: State institutions, and political parties. The first group concerns the White House, the US State Department, the Pentagon, the Joint Chiefs of Staff, the voter registration system, and the NSA. These institutions are all linked to foreign affairs, military or voting processes. They represent a certain intelligence value for a foreign power, which makes them primary targets for cyberespionage.

The targets within the US political party were the DNC and the DCCC. Political parties are particularly interesting targets for foreign intelligence services because they have access to some policy-relevant documents, but do not have technical protection measures as high as government institutions. These particularities make political parties as good a target as state institutions. The incidents targeting the DNC were highly specific in their choice of target. A principal victim of the DNC hack was the presidential election candidate, Hillary Clinton. Stolen, and subsequently published, emails showed that the chairwoman of the DNC favored Clinton over her Democratic Party rival, Bernie Sanders. The Chairwoman later resigned from her position as a result of the emails' publication (Hosenball et al., 2016). The leakage of information in this regard throughout the election campaign was reported to be used in order to discredit Hillary Clinton as a legitimate presidential candidate (National Intelligence Council, 2017).

There is little information about cyberattacks in Russia and their targets. In July 2016, the FSB declared that 20 organizations belonging to state, scientific and defense institutions were the targets of a spying *malware* (BBC News, 2016a). No further details were given on the victims, nor details on information on what was stolen or how the *malware* infected the networks. In October 2016, the Ukrainian hacker group, "Cyber Hunta", leaked emails claiming to have originated from one of Putin's counselors, Vladislav Surkov. These emails contained elements attesting ties between the Russian government and pro-Russia Ukrainian separatists. The USA officially announced that it had no responsibility in this hack

[5] For a detailed classification of the recent cyberattacks in the USA and Russia see Annex 1.

[6] The "Dukes" malware family contains nine different pieces of malware (F-Secure, 2015).

(Miller, 2016). Finally, in November 2016, the FSB announced to have evaded a cyber-plot targeting Russian online banking systems. Apart from accusing foreign intelligence services, the Russian officials did not give more information on this event (Lowe and Zinets, 2016).

3.3 Attribution and actors

In all US incidents, the US government suspected Russian involvement, but officially accused Russia only in the case of the DNC hack, which Russia denied (Dunn Cavelty, 2016). In this incident and others, investigators claimed that they had evidence, like *IP addresses* or the language environment of the computers used to create the infected attachments, pointing to Russian hacker groups, "APT28" and "APT29", as the responsible perpetrators of the attacks. These groups are also suspected to have ties to the Russian government (Rudnitsky et al., 2016) and are used as *proxy* actors. This gives Russia plausible deniability when the malicious actions are discovered and helps to confuse and blur reality and complicate attribution.

In the case of the US DNC breach, experts from the cybersecurity firm, CrowdStrike, asserted that the attacking groups were: "APT29"[7], and "APT28"[8]. This firm presented technical evidence showing that the hacker group "APT29" had been operating within the US DNC's network for approximately a year before it was discovered, and that the hacker group "APT28" had infiltrated the same network in March 2016 (US Department of Homeland Security and Federal Bureau of investigation, 2016). Furthermore, the investigation obtained several indicators supporting the idea of the involvement of these two hacker groups: the *IP addresses* originating from Russia, the *malware* found on infected computers known to have been used by the Russian hacker groups, and that the timing of the groups' hacking activities matched Moscow working-day schedules and Russian holidays (Inkster, 2016).

The hacker group "APT29" is suspected of having ties to the FSB, the main Russian intelligence and security institution and successor to the KGB and other intelligence agencies. The hacker group is believed to have been active since a series of cyberattacks in Chechnya in 2008 (F-Secure, 2015, p. 4) and was uncovered during the investigations of the cyberattacks on the US State Department and White House in 2015 (Thielman and Ackerman, 2016). The hacker group "APT29" is also believed to be responsible for the attack the US Joint Chiefs of Staff in July 2015 (Alperovitch, 2016).

The hacker group "APT28" is believed to be linked to the Main Intelligence Directorate (GRU), the Russian foreign military intelligence service. This hacker group was discovered first in 2008 during the conflict between Russia and Georgia. The group has been accused of hacking the networks of defense, energy, government, and media companies, and more recently of the intrusion into TV5Monde and the German Bundestag servers in April 2015. However, it seems that the hacker group "APT28" tends to target military or defense-related assets, which corroborates the possibility of the group being tied to the GRU. Moreover, the group is known to conduct elaborate phishing schemes like the ones that tricked John Podesta into giving out his email login credentials (Alperovitch, 2016).

Both hacker groups have substantial resources, raising suspicion that they receive state support or sponsorship. Both groups are focused on information gathering, specifically embarrassing information or sensitive data, but not as basis for extortion. The fact that they do not use the stolen information for coercion suggests that they are not driven by financial enrichment. Also it corroborates the idea that they are sponsored by a state. Furthermore, both hacker groups adjust their attacks on targets to reflect Russian political objectives (Thielman and Ackerman, 2016). However, the fact that "APT28" breached the DNC network after "APT29" suggest that the two hacker groups lacked coordination regarding their victim. This suggests that the lack of coordination also exists between the two government bodies to which the hacker groups are allegedly tied. Apart from these two groups, it is believed that the Russian government has ties with approximately five other hacker groups (Rudnitsky et al., 2016).

In the case of the DNC breach, an online figure, named "Guccifer 2.0", claimed responsibility for the hack and the distribution of the information gathered to Wikileaks and DCleaks. This entity claimed to be Romanian, but investigators and cybersecurity experts believe that the identity of "Guccifer 2.0" was probably built up to confuse the investigators and that the entity behind it is in reality Russian. In a joint report, the US intelligence community assessed that the hackers were from the GRU (National Intelligence Council, 2017).

In the case of the NSA breach, the alleged perpetrator was a hacker group called "Shadow brokers". The group has tried to sell *malware,* supposedly stolen from the "*Equation group*", through online auctions. The group appeared for the first time in cyberspace with the NSA breach of August 2016 and the first auction that followed. Experts who have analyzed the sample of *malware* provided by the group assessed that the material could be coming from the NSA (Emm et al., 2016, p. 6). The hacker group did not find any buyers for the stolen *malware* and called off the first auction in October 2016. They came back later with a new auction in January 2017, claiming to be their last action before disappearing. Experts added further that a group who could hack into the NSA network must have had support from a state or help from the inside (Greenberg, 2016; Suiche, 2016). The latter argument is supported by the fact that no external servers would contain such a big sample of cyber-tools in one place and that it might have been stolen from an internal network of the NSA, accessed with a USB-drive (Bing, 2017; Goodin, 2017). Experts

[7] The hacker group is also known as "Cozy Bear", "Dukes" or "CozyDuke".

[8] The hacker group is also known as "Fancy Bear", "Sofacy", "Sednit", "Strontium" or "Pawn Storm".

have stated that the group might also be related to the former NSA employee, Harold Thomas Martin, who was arrested in October 2016 with 50 Terabytes of stolen data (Goodin, 2016).

There will always be uncertainties when it comes to attribution in cyberspace. Attribution would normally follow the "*cui bono*" (to whose benefit) logic, but even with this reasoning, it is not possible to be entirely certain that a particular actor who benefits from the attack is indeed the perpetrator. Evidence presented by official US reports, main Western media and cybersecurity firms seems to point to Russia as the perpetrator. While Russia would certainly profit from the victory of Donald Trump, it is still possible that this technical evidence was "*spoofed*". They might have been created to falsely incriminate the Russian government. Location settings in computers can be altered and the *malware* used are also available on the black market (Gaycken, 2016). Furthermore, it was assumed that these entities had ties with the Russian authorities, which the latter consistently denied.

These incidents may also be simply about foreign intelligence collection. According to Michael Hayden, the former NSA chief, his organization has collected information on foreign political parties and institutions (Timm, 2016), thus it could be plausibly assumed that foreign intelligence services also gather information about the USA. As previously stated, state institutions and political parties are high value targets for intelligence agencies and are often victims of such attacks.

On the Russian side, because very little information has been published, it is difficult to determine the actors behind the cyber-incidents.

4 Effects

This section examines the effects of the various cyber-incidents at the domestic and international level. At the domestic level, the analysis focuses on the effects on social and domestic politics. It studies how US society and election processes were affected by the incidents and how the US government responded to them. The two other points of focus are how the incidents affected the state's economy and how they impacted its technological development.

At the international level, the report analyses the impacts of the cyberattacks on the relations between the two countries and the international community.

4.1 Social and internal political effects

Socially and politically, the most visible effect of these cyberattacks has been their influence on the proceedings of the US presidential elections. Foreign attempts to influence US elections are not a new phenomenon. For instance, in 1968, the Kremlin allegedly ordered the Russian ambassador in Washington to help the Democrat candidate, Hubert Humphrey, to win the elections against the Republican and anti-communist candidate, Richard Nixon (Higgins, 2017). Also, in 1982, Russian intelligence launched a misinformation campaign against the Republican candidate, Ronald Reagan. They pictured him as a militarist candidate corrupted by the defense industry (Ornos et al., 2017). In both past cases, Russian efforts to influence the outcome of the US elections failed. In 2016, the novelty of these incidents is found in the tools used to try to influence the presidential elections and public opinion. Technology offered new possibilities. Cyberattacks and leaks of stolen information on the internet enable a wider audience to be reached and can have an important impact on US elections. Using the internet, any group or organization can enter any homes with a connection. As a result, the successful breaches and leaks of embarrassing stolen data diminished public faith in the credibility of the US presidential election process, its integrity and legitimacy. The report from the US intelligence community and the joint report from the DHS and the FBI argue that the goal of the DNC breach was not to directly interfere with the results of the elections in favor of Donald Trump, but rather to cast doubts on the legitimacy of the election process. A certain mistrust of the US state institutions already existed among the US population. Russia used the cyberattacks on the DNC to deepen that distrust (Ornos et al., 2017). This tactic aligns with the concept of "information warfare" included in the Russian *Gerasimov doctrine*. The Russian aim is to control the adversary's "information space" by complicating the distinction between truth and lies, while blurring the line between peace and war time and finally to make the USA take "decisions that benefit the adversary's interests", in this case Russia (Nocetti, 2015, pp. 7–8). By denying its involvement in the cyberattacks, Russian authorities contributed to the general confusion, cast doubts on the events and gave the impression that there were no reliable facts (Giles, 2016, p. 40). Conway (2003) argues that the internet changed the power-balance of information by shifting it from organizations or people who own and control traditional media to other actors who disseminate information that has not been processed online.

Also, Russia used embarrassing information stolen in the DNC breach to discredit Hillary Clinton. They leaked this information at strategic times in the campaign in order to make her appear an unsuitable candidate (National Intelligence Council, 2017). To exaggerate the effect, Russia not only used cyberattacks on political institutions to confuse the population and discredit Hillary Clinton, but also manipulated news on social media and specific media platforms like RT and Sputniknews. This tactic also contributed to the confusion of the population on the reliability of mainstream media and increased mistrust toward them. Hillary Clinton had asserted several times during the election campaigns that she was in favor of a "no-fly zone" in Syria. This option was fiercely criticized in the USA because it would pose high risks of escalation in Syrian airspace with Russia (Ackerman, 2016). Russia targeting the Democrat candidate would align with a possible fear of Russia to see a "no-fly zone" instated in

Syria. Such measures would remind people of the international intervention in Libya, which ended with the death of Qaddafi. Such a scenario in Syria would not be welcomed by Russia. Therefore, it was in Russia's interest to prevent the Democrat candidate being elected (Ornos et al., 2017).

The US government responded to the attack by expelling 35 Russian diplomats and closing two compounds. However, it took them approximately four months to officially accuse Russia of perpetrating the DNC breach. The slowness of the response made the US look indecisive in its response to the hack. Yevgenia Albats, an author of a book about the KGB and James Comey, FBI director, argue that Russia wanted the cyberattack to be discovered in order to demonstrate that it has the capacity to breach into computers in USA. The facts that the USA was slow to respond and that the retaliation was rather mild disappointed some US officials who argue that it signaled to Russia that it can act in cyberspace with impunity.

There are various reasons the Obama administration waited until October 2016 to officially accuse Russia. First, by responding to cyberattacks, the responder also reveals his cyber-capabilities. Therefore states need to evaluate if the effects of the response compensate the exposition of such aptitudes, which could be of better use when kept secret (Grohe, 2015). Second, the Obama administration did not want to act too rashly in fear to appear partisan in the conflict. They wanted to be sure that the cyberattacks were actually coming from Russia. This assumption was then confirmed by all 17 US intelligence agencies. Third, the US administration was more focused on maintaining the integrity of the presidential elections than on retaliating. They feared that a retaliation before the day of the elections would provoke direct interference in the voting process. Fourth, the US government, reassured by polls results claiming Hillary Clinton as winner of the elections, was so sure that the Democrat candidate would win that they feared that retaliation before November 2016 would feed Trump's possible discourse on rigged elections. Fifth, the US intelligence community was waiting for Russia to cross a certain line in its cyber-activities against the US, like directly interfering in the election process. It was never proven that Russia had ever crossed that line. Finally, the US State Department feared that a too strong response to the cyberattacks would impact the peace negotiations in Syria where the cooperation with Russia is needed (Ornos et al., 2017).

4.2 Economic effects

Apart from the indirect cost of the cyber-incidents, there was no economic impact for the USA. State institutions and the DNC had to hire cybersecurity services to stop the intrusions and determine the damage, which induced certain costs. Russia, on the other hand, could be facing new sanctions on top of the ones that were implemented after the annexation of Crimea in March 2014. These sanctions included travel bans and the freezing of assets of Russian nationals in the USA. Russia retaliated with its own sanctions on European states and the USA. New sanctions would add pressure to the already fragile Russian economy (Financial Times, 2016).

4.3 Technological effects

Technologically, the impact of an escalation in cyberspace between Russia and the USA might be that both would invest more money in cyber-defense and cyber-offense capabilities, with the possibility of a cyber-arms-race emerging. The knowledge of the attacks by Russian actors is embarrassing for the USA and highlights that the USA's cyber-defense is not impenetrable. Therefore, the USA needs to take new cybersecurity measures. The same might be the case with Russia which also reported that its institutions were the targets of attacks (Allen, 2016).

The cyberattacks on USA institutions also showed that democratic processes like elections or votes are at risk. An effect of these cyberattacks might be technical developments in order to secure and protect these processes from such attacks. Inquiries have already been made in the USA to classify elections and voting infrastructures as critical infrastructures in order to benefit from higher security measures (Hay Newman, 2016).

4.4 International effects

Politically, a resurgence of Cold War rhetoric was observed during the last few years creating an atmosphere of suspicion at every move from the key players of Russia, NATO or the USA. The visible result is that each protagonist responds to the other with a counter-move in a "tit-for-tat" logic. For example, NATO had a civilian disaster emergency exercise in November 2016 in Montenegro, while Russia was engaged at the same time in a military exercise in Serbia (BBC News, 2016d). Another example is the USA suspending the talks on the ceasefire in Syria as a consequence of the discovery that Russia had helped Syrian government troops launch an attack in Aleppo. At roughly the same time, Russia announced that it has suspended its participation in one agreement on nuclear energy research and development of 2013 and quit another agreement of 2010 on cooperation in the conversion of research reactors to low-enriched uranium fuel (Klion, 2016; World Nuclear News, 2016).

The last known action in this cycle is the expulsion of Russian diplomats by former US President Obama as retaliation for the cyberattacks. This measure was said to be one of many and some might be of covert nature. This action sent the message that the USA is unwilling to disengage. These examples demonstrate how the "tit-for-tat" logic is already in place in the physical world and seems to be transposed into cyberspace as well.

The tensions between the USA and Russia could also intensify into cyberspace disputes, thus risking an

increased possibility of a conventional war (Bamford, 2016; Lin, 2012). For example, in order not to appear weak, the USA had to respond to the attacks, and former US President Obama publically accused Russia of perpetrating the various cyberattacks on US institutions and political parties. Furthermore, former US Vice President Biden and the CIA asserted the possibility of undertaking a covert cyber operation to respond to these attacks (Timm, 2016). One response announced in December 2016 was the expulsion of Russian diplomats. This action shows that the dispute has already spilled over from cyberspace to the diplomatic sphere. However, Obama also assured that this would not be the only retaliation and that other measures may be taken in the future (Gambino et al., 2016). Such announcements might seek to deter further intrusion by Russia, but could also have the opposite effect. For example, problematically for the USA, Biden's declaration of retaliation signaled Russia that if a cyber-incident did occur on its territory, USA would be the primary suspect. Then Russia would probably want to react in order not to appear weak itself. This would feed the escalation-cycle (Bamford, 2016). Deterrence only works if the adversary believes the threat to be credible. The evidence gathered in previous cyber-incidents suggests that in case of cyberattack both states proved to be capable of generating credible cyber-threats. However, the covert nature of cybersecurity makes it hard for a state to demonstrate its cyber capabilities in order to scare its adversaries off.

In addition, the uncertainty of attribution is another problem for the credibility of the threat. Even if the US response is proportionate to the Russian cyberattacks, there could be an increase in intensity or a misinterpretation, resulting in further escalation. If the conflict in cyberspace reaches a certain point in intensity, prolongs itself in time, or targets a certain type of victim or infrastructure, it could reach a tipping point. This point could be reached when, for example, one of the states is tempted to take the advantage by spilling the conflict over to the conventional realm. In that regard, the US cyber strategy highlights that a kinetic response to a cyberattack could be regarded as appropriate (Farrell and Glaser, 2016; Lin, 2012, p. 61).

On the other hand, both states might not desire further escalation, preferring to restrain the conflict to cyberspace. Each would follow the "tit-for-tat" logic and accuse each other while never reaching a tipping point where the conflict spills over to a conventional war. Such a tipping point would be linked to the intensity of the attack or the nature of the targets. Both nations would keep the cyberattacks small enough not to trigger a bigger reaction. The same would be observed on the choice of targets, with both avoiding certain critical or sensitive targets, for instance critical infrastructures. In order to contain the conflict in cyberspace, both states would have to demonstrate their restraint by selecting options with low risk of miscalculation (Lin, 2012, pp. 64–66).

In the future, it might also be possible to see a de-escalation in the form of the emergence of an international treaty or at least further bilateral treaties between the USA and Russia on cyberattacks. For example, during the last few years, businesses in the USA were often hacked and spied on by the Chinese military. These intrusions were mostly cyber-economic-espionage and were said to have supported the theft of billions of dollars' worth of intellectual property (Bamford, 2016). In September 2015, the USA and China signed an agreement engaging both countries not to support or conduct cyber-theft of intellectual property. Moreover, the parties have made the commitment not to use cyberattacks against each other's critical infrastructures in peace-time and to support the establishment of international behavioral norms in cyberspace (Rosenfeld, 2015). Both states also highlighted the fact that they could not control each individual in their country and therefore could not be held responsible for individual acts. Since then it seems that the number of attacks on commercial targets has diminished (Timm, 2016). Former President Obama suggested the creation of a position of cybersecurity ambassador to deal with bilateral or multilateral treaties concerning cyber-norms (Lee, 2016).

For this kind of de-escalation to take effect, the termination of the conflict at hand must be the stated aim of both parties. A clear common understanding of the terms of agreement is required and must be based on trust-building efforts, as well as the assurance of mutual adherence. The difficulty of tracking the implementation of such agreements in cyberspace has been an obstacle preventing more states consenting to such solutions (Lin, 2012, pp. 62–64). Nevertheless, a dialogue on cyberspace already exists between the USA and Russia since July 2013. This cooperation includes *Confidence Building Measures (CBM)* such as the creation of working groups on the issue of ICT security, exchange of information between the two national Computer Emergency Response Teams (CERT), and the creation of a direct communication line to directly manage ICT incidents (Segal, 2016; The White House, Office of the Press Secretary, 2013). In October 2016, former President Obama used the latter to inform Russian President Putin that the USA was accusing Russia of interference in the election process (Ignatius, 2016). Furthermore, Russia and the USA take part in the UN GGE supporting the future establishment of international norms on actions in cyberspace. They stated that international law can be applied in cyberspace and therefore, the rules of proportionality and limited collateral damage should also be respected in cyberattacks (Ignatius, 2016; United Nations General Assembly, 2015). These examples demonstrate that even though the two states are involved in a "tit-for-tat" logic in their relations on a tactical level, there was still a dialogue on the strategic level, at least until 2015. The recent cyberattacks in USA and the election of Donald Trump as US President, bring new uncertainties.

There are significant concerns that similar attacks may be perpetrated in Europe, where elections will take place in 2017. Specifically Germany and France expressed their fear of seeing the development of a similar scenario as in the USA happening during their

election campaigns. It would not be the first time for Russia to target European institutions as "APT28" has already been accused of hacking into the network of the German Lower House of Parliament, the Bundestag, in 2015 (AFP, 2016). On its side, France claimed in January 2017 to have stopped approximately 24,000 cyberattacks in 2016 and declared that they feared a Russian cyberattacks as well (Europe 1, 2017).

5 Consequences

This section details several measures that states could apply to reduce their risks to be faced with similar situation as the USA during its presidential elections.

5.1 Improvement of cybersecurity

States can also concentrate on improving their cybersecurity. Emphasis has to be placed on measures to raise awareness of the issue and most specifically of human errors. The various attacks on the US institutions and political party showed that *spear phishing* is an effective delivery means for malicious cyber-tools. The Internet Society report of 2016 stated that social engineering techniques, like *spear phishing*, were often successfully used in attacks to steal data. The report recommends raising the knowledge of computer users on such issues with education and proper technological tools. In order to take more cautionary behavior in regard to such attacks, users require a better understanding of the risks and possible damage of *malware* intrusions in networks. Users could already be taught at a young age about proper *cyber hygiene* in order to recognize fake emails more easily, and be more careful before opening links or attachments. A simple standard operating procedure could also be implemented to report any suspicious emails or links in order to more quickly identify malicious emails (Internet Society, 2016, pp. 121–122).

Technological solutions could also help in the improvement of states' cybersecurity. A solution to limit *spear phishing* emails being confused with legitimate emails could be to request that partners implement email authentication systems like the *Sender Policy Framework (SPF)*. The *SPF* certifies that the *IP address* of a sender is indeed from the sender, and enables receivers to detect phishing emails. With such a system users would be able to identify fraudulent emails and avoid infecting the networks (Openspf, 2010). *SPF* is one authentication method, among others. Another technological solution would be a *two-factor authentication*. If login credentials and passwords are stolen, a *two-factor authentication* can limit the damage because the procedure would prevent any attackers who do not have the second authentication factor from infiltrating systems (Internet Society, 2016, p. 122). Entirely secure systems do not exist, therefore in addition to more sophisticated login techniques, if a *data breach* occurs, encryption could help to mitigate the damage. Strong encryption can prevent data thieves from reading the data, thus reducing its value. If the thieves cannot crack the encryption, these data would be useless to them. To some extent an encrypted system could also serve as a deterrent for cyberattacks specifically targeting data. It would become too demanding in resources to try to steal them (Internet Society, 2016, p. 126).

The hacks on US institutions showed that democratic institutions like elections or voting processes and political parties could become the target of cyberattacks, and that they are vulnerable to such attack. This situation highlights the fact that in democracies voting systems' infrastructures should be considered as critical infrastructures just like water and energy supplies. Voting systems infrastructures could benefit from the same type of security attention and measures as the other critical infrastructures. Such measures imply an increase in protection measures and the benefit of an expansion of cooperation between the various concerned actors. This issue is even more important in democracies using electronic voting systems. The case of the DNC breach also showed that political parties can be targeted by cyberattacks. The former NSA chief, Michael Hayden also explained that political parties may not only be victims of espionage by political opponents for political purposes, but also by foreign actors for intelligence collection. Therefore, raising awareness on this issue through education programs could also help to mitigate the risks and damage caused by such *data breaches*.

5.2 Raising awareness of propaganda and misinformation

Finally the case of the *data breaches* during the US elections showed that societies are targeted by "information warfare" operations. Propaganda and *trolls* represent an important danger for society. It is more difficult for democracies to counter propaganda as they cannot censor what media outlets publish and/or what is posted on social media. Often media outlets are also privately owned, which adds another challenge to democracies to control the content of such media (Conway, 2003). Freedom of the press and free speech are significant democratic principles, but they also enable propaganda to spread. Therefore, state actors cannot act alone against propaganda and should also involve the entire society in the process. It is easy for uninformed people to mistaken fake information for genuine information. Some media outlets understand this vulnerability and do not hesitate to exploit it. They are designed to look exactly like an official and credible media outlet and broadcast legitimate information coupled with misinformation. Propaganda is hard to counter, but some measures can be taken to mitigate its effects. For that matter, it is important for societies to truly understand the effects of propaganda to be able to shape an effective awareness program. Such a program should warn about disinformation campaigns, and give tips on how to spot them. It also should clarify what are *trolls* and their role in propaganda operations (Tatham, 2015). Education or awareness campaigns could help the

population to discern more easily propaganda materials and keep a more critical point of view toward what they read or watch. It would also be important for democracies, media and other members of civil society to reveal and correct false information and inconsistencies in news in order to limit the effects of propaganda (Paul and Matthews, 2016).

5.3 Observation of the evolution of relations between the USA and Russia

The evolution of the relations between the USA and Russia would need to be carefully monitored. The recent election of Donald Trump to the US presidency has introduced considerable uncertainty in terms of how events might develop further. President Trump said that he wanted to improve relations with Russia and named a Secretary of State who has previously been in contact with the Russian President and Russian officials for business (Krauss and Schwartz, 2016). In December 2016, in his address to the Russian Federal Assembly, President Putin showed optimism about the relationship with the new US Administration and the US Secretary of State's nomination was perceived as a friendly move (Lain, 2016). Russian media also saw the election of Trump as a positive sign for Russia (Ornos et al., 2017). However, after the congressional confirmation hearings, some discrepancies in discourses on the issue of the involvement of Russia in the DNC breach have appeared between the President and his Secretary of Defense and CIA Director. During the election campaign, Trump expressed his will to reduce US involvement in NATO. However, the US Secretary of State and the US Secretary of Defense have assured full support of NATO. Former British General Sir Alexander Shirreff fears that it would be the beginning of the end of post-World War alliances. He argued that such measures would create instability in the world order and that Europe would see a rise of nationalism. They observed that when NATO withdrew troops from Eastern Europe, Russia took the opportunity to intensify its provocative stance by moving troops closer to Baltic States' border and moving nuclear-capable missiles closer to European territory (Ornos et al., 2017).

Following former President Obama's decision to expel Russian diplomats, President Putin stated that he would not expel US diplomats and not continue the escalation. This lack of reaction suggests that Vladimir Putin expected a better dialog with Trump (Lain, 2016). According to the media, US intelligence agencies were alarmed by the lack of reaction and investigated the communications from the Russian embassy in Washington to Moscow. They discovered that Michael Flynn, Trump's then national security advisor, had met the Russian ambassador to discuss new sanction terms for Russia. Flynn later had to resign for lying about these meetings (Ornos et al., 2017).

In the extreme case of further escalation in cyberspace or a possible spillover in the physical realm in the frame of a new Cold War era, a conflict would not affect every state the same way. Some might be directly concerned, while others indirectly. Not being involved directly in a conflict would not protect states from being affected by cyber-incidents, like *DDoS* attacks on the USA or Russian websites or by infected emails originating from partners from both countries. Information technology located in third party states could possibly be used in further cyberattacks, like the use of a vulnerable server belonging to a third party state, for the purpose of covering the perpetrators' tracks. For these reasons, it will be important to carefully monitor the next actions of both countries in cyberspace and the physical world as it would set the tone for the forthcoming period.

5.4 Promotion of Confidence Building Measures

States could promote the establishment of *CBM* in order to develop international norms for cyberspace in the future. Until now, countries have only agreed that international law could apply to states' activities in cyberspace, but there are no international norms to regulate them. The difficulties of attributing actions to actors in cyberspace increase ambiguities that lead to international tensions. Clearer international protocols, agreements or guidelines may help to mitigate such issues. *CBM* would help to increase transparency, trust and improve relations among states in regard to states' actions in cyberspace. *CBM* could be developed in bi-lateral processes or in regional/international fora. Stauffacher and Kavanagh (2013) proposed a series of *CBM* in the context of cybersecurity consisting of: transparency measures (dialog on cyber policies/strategies/doctrine, exchange of military personnel, joint simulation exercises, and so forth); compliance indicators and monitoring of transparency measures (e.g. agreement on forbidden targets like hospitals, joint mechanisms in crisis management like hotlines); cooperative measures (e.g. development of a common terminology, development of joint guidelines in case of incidents, joint threat assessments); communication and collaborative mechanisms (e.g. communication channels in case of escalation); and restraint measures (e.g. pledge to remove incentives for first strike offensive or retaliation actions, exclude cyber offensive operations on third parties countries). These measures could later develop into international norms or treaties which combine a mutual understanding of certain principles for states' actions in cyberspace. Such norms would also enhance cooperation among states resulting in greater dialog which would also reduce confusion relating to states' cyber-activities. This would improve security in both cyber and physical realms (Brake, 2015; Farrell, 2015).

6 Annex 1

Table of the different techniques used in the recent cyberattacks between the USA and Russia:

G = government institutions, M = Media, PP = Political Party, IO = International Organization				
Date	**Victim**	**Type of victim**	**Technique / Tool**	**Damage**
10.2014	US State Department unclassified network	G	*Spear phishing* with a malicious link	Access to thousands of computers across the USA and in embassies Access to sensitive information that could be relevant to foreign intelligence services Theft of emails concerning the Ukrainian conflict (Howarth, 2015)
10.2014	White House unclassified network	G	*Spear phishing* with a malicious email coming from the US State Department	Access to sensitive information available on the unclassified network like the President's daily schedule (Perez and Prokupecz, 2015)
Early 2015	Pentagon unclassified network	G	Use of unspecified old vulnerabilities in the network	Unknown (Crawford, 2015)
Summer 2015	First breach into DNC network	PP	*Spear phishing* with a malicious link or attachment	Embarrassing emails later published on the Wikileaks and DCLeaks websites (Taylor, 2016)
07.2015	US Joint Chiefs of Staff email server	G	*Spear phishing* emails forwarded from a university which has been victim of a phishing wave	Stolen personnel credentials, passwords, and information with no intelligence value. After the network was taken down, it took the US Joint Chiefs of Staff almost two weeks to restart their email servers (Martin, 2016; Starr, 2015).
03.2016	Second breach into the DNC network and John Podesta's email account	PP	*Spear phishing* email disguised as one coming from Gmail	Embarrassing emails later published on the Wikileaks and DCLeaks websites and research on Republican candidate Donald Trump (Krieg and Kopan, 2016)
07.2016	Arizona and Illinois voter registration system	G	Use of unspecified *malware*	Theft of 20,000 personal data from voters in Illinois No data were stolen in Arizona (Lartey, 2016; Reuters, 2016)
07.2016	DCCC and Clinton's election campaign networks	PP	*Spear phishing* similar to the DNC case	Access to voter analysis data (McCain Nelson and Peterson, 2016)
08.2016	NSA and "*Equation group*" servers	G	Unspecified	Information, a list of *IP addresses* of hacked servers, and a claimed *malware* sample later auctioned on social media (Goodin, 2016; Greenberg, 2016)
09.2016	World Anti-Doping Agency	IO	Phishing	Stolen medical files of athletes (Ingle, 2016).
12.2016	US Election agency	G	*SQL Injection*	Stolen list of user names and passwords, later tried to be sold on the "underground electronic markets" (Barysevich, 2016; Menn, 2016).

7 Glossary

Backdoor: Part of a software code allowing hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

Confidence Building Measures (CBM): Various procedures that can be established to build trust and prevent escalation between state-actors (United Nations, n.d.).

Cyber hygiene: Analogy to personal hygiene in regard with one's security and practices in cyberspace in order to protect networks and personal computers (European Union Agency for Network and Information Security, 2016).

Data breach: Event in which information of a sensitive nature is stolen from a network without the users' knowledge (TrendMicro, 2017).

Distributed Denial of Service (DDoS): Act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Equation Group: A group of hackers using highly sophisticated and complex malwares. They are suspected to be have ties to the NSA (Kaspersky Lab, 2015, p. 3).

Gerasimov doctrine: Also called "non-linear warfare" or "hybrid warfare": a concept of war where all the actors are fighting each other, making alliances but also breaking them during the battle. The actors only follow their own objectives and will use cyber, economic, military and psychological operations to achieve them (Miller, 2016; The Economist, 2014).

Internet Protocol (IP) address: A numerical address assigned to each device that uses the internet communications protocol allowing computers to communicate with one another (Internet Corporation For Assigned Names and Numbers, 2016).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Metadata: Information describing and explaining other data, like the date of creation of a document, the resolution of an image or the identifier of a specific device (National Information Standards Organization (U.S.), 2004).

Proxy: In computing it is an intermediate server acting in place of the end-users. This allows users to communicate without direct connections. This is often use for more safety and anonymity in cyberspace (Ghernaouti-Hélie, 2013, p. 438). This is also used in the physical world when one actor in a conflict uses third parties to fight in their place.

Remote Administration / Access Tool (RAT): Software giving remote access and control to a computer without having physical access to it. RATs can be legitimate software, but also malicious (Siciliano, 2015).

Sender Policy Framework (SPF): Technical system validating email-senders as coming from a authenticated connection in order to prevent email spoofing (Openspf, 2010).

Spear phishing: A sophisticated malicious technique that not only imitates legitimate webpages, but also selects the potential targets and adapts the malicious email to them. Often the email looks like it comes from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Spoofing: Act to usurp IP address in order to commit malicious acts like breaching a network (Ghernaouti-Hélie, 2013, p. 440).

SQL Injection: A cyberattack technique in which a malicious code is injected into an entry field for execution and is executed by an SQL database (Microsoft, 2016).

Troll: A person submitting provocative statements or articles to an internet discussion in order to create a fight and drag more people into it (Williams, 2012).

Two-factor authentication: A login procedure that involves two elements from the following three: something the user knows (ex: password), something the user has (ex: card) or something the user is (ex: biometric) (Rosenblatt and Cipriani, 2015).

Website defacement: Cyberattack replacing a website's page or elements by another page or elements (Ghernaouti-Hélie, 2013, p. 442).

Zero-day exploit / vulnerabilities: Security vulnerabilities from which software developers are not aware, which could be used to hack a system (Karnouskos, 2011, p. 2).

8 Abbreviations

CBM	Confidence Building Measures
CERT	Computer Emergency Response Team
CIA	US Central Intelligence Agency
DCCC	US Democratic Congressional Campaign Committee
DDoS	Distributed Denial of Service
DHS	US Department of Homeland Security
DNC	US Democratic National Committee
EU	European Union
FBI	US Federal Bureau of Investigation
FSB	Federal Security Service of Russia
GRU	Main Intelligence Directorate of Russia
ICT	Information and Communications Technologies
IP	Internet Protocol
KGB	USSR Committee for State Security
NATO	North Atlantic Treaty Organization
NSA	US National Security Agency
RAT	Remote Administration Tool
SPF	Sender Policy Framework
SQL	Structure Query Language
UN	United Nations
UN GGE	United Nations Group of Governmental Experts

9 Bibliography

Ackerman, S., 2016. Why Clinton's plans for no-fly zones in Syria could provoke US-Russia conflict [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2016/oct/25/hillary-clinton-syria-no-fly-zones-russia-us-war (accessed 3.21.17).

AFP, 2016. Russian cyber-attacks could influence German election, says Merkel [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2016/nov/08/russian-cyber-attacks-could-influence-german-election-says-merkel (accessed 11.29.16).

Allen, N., 2016. Barack Obama warns of Cold War-style "cyber arms race" with Russia [WWW Document]. The Telegraph. URL http://www.telegraph.co.uk/news/2016/09/05/barack-obama-warns-of-cold-war-style-cyber-arms-race-with-russia/ (accessed 12.1.16).

Alperovitch, D., 2016. Bears in the Midst: Intrusion into the Democratic National Committee [WWW Document]. CrowdStrike Blog. URL https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (accessed 11.1.16).

Ashok, I., 2016. Shadow Brokers cancels auction of stolen NSA "cyberweapons" as bidders fail to turn up [WWW Document]. Int. Bus. Times. URL http://www.ibtimes.co.uk/shadow-brokers-cancels-auction-stolen-nsa-cyberweapons-bidders-fail-turn-1586753 (accessed 11.2.16).

Bamford, J., 2016. Commentary: Don't be so sure Russia hacked the Clinton emails [WWW Document]. Reuters. URL http://www.reuters.com/article/us-russia-cyberwar-commentary-idUSKBN12X075 (accessed 11.3.16).

Barysevich, A., 2016. Russian-Speaking Hacker Selling Access to the US Election Assistance Commission [WWW Document]. Rec. Future. URL https://www.recordedfuture.com/rasputin-eac-breach/ (accessed 12.21.16).

BBC News, 2017a. Russian diplomats expelled by Obama over hacking leave US [WWW Document]. BBC News. URL http://www.bbc.com/news/world-us-canada-38484735 (accessed 1.3.17).

BBC News, 2017b. Trump team "incidentally monitored" after election [WWW Document]. BBC News. URL http://www.bbc.com/news/world-us-canada-39358363 (accessed 3.30.17).

BBC News, 2016a. Russia cyber attack: Large hack "hits government" [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-36933239 (accessed 10.31.16).

BBC News, 2016b. US expels Russian diplomats over cyber attack allegations [WWW Document]. BBC News. URL http://www.bbc.com/news/world-us-canada-38463025 (accessed 1.3.17).

BBC News, 2016c. Russia-US row: Putin rules out tit-for-tat expulsion of diplomats [WWW Document]. BBC News. URL http://www.bbc.com/news/world-us-canada-38464612 (accessed 1.3.17).

BBC News, 2016d. Nato-Russia tensions move to Balkans with military drills [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-37834388 (accessed 11.2.16).

Bing, C., 2017. Shadow Brokers' latest leak could have come from beyond NSA staging servers [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/shadow-brokers-nsa-microsoft-windows-exploits-2017/ (accessed 1.16.17).

Borger, J., 2017a. What we learned from the hearing on the Trump campaign's Russia ties [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/mar/20/trump-campaign-russia-hearing-key-points (accessed 3.22.17).

Borger, J., 2017b. John McCain passes dossier alleging secret Trump-Russia contacts to FBI [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/jan/10/fbi-chief-given-dossier-by-john-mccain-alleging-secret-trump-russia-contacts (accessed 1.16.17).

Borger, J., 2017c. Trump security adviser Flynn quits after leaks suggest he tried to cover up Russia talks [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/feb/13/michael-flynn-resigns-quits-trump-national-security-adviser-russia (accessed 2.14.17).

Borger, J., Ackerman, S., 2017. Trump-Russia collusion is being investigated by FBI, Comey confirms [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/mar/20/fbi-director-comey-confirms-investigation-trump-russia (accessed 3.22.17).

Brake, B., 2015. Strategic risks of ambiguity in cyberspace. Contigency Plan. Memo. 11.

Calabresi, M., Rebala, P., 2016. Here's The Evidence Russia Hacked The Democratic National Committee [WWW Document]. Time. URL http://time.com/4600177/election-hack-russia-hillary-clinton-donald-trump/ (accessed 2.1.17).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. doi:10.1080/18335330.2012.653198

Conway, M., 2003. Cybercortical Warfare: The Case of Hizbollah.org. Presented at the European Consortium for Political Research Joint Sessions of Workshops, Edinburgh, UK, p. 17.

Crawford, J., 2015. Russians hacked Pentagon network, Carter says [WWW Document]. CNN Polit. URL http://edition.cnn.com/2015/04/23/politics/russian-hackers-pentagon-network/ (accessed 10.25.16).

Dilanian, K., Arkin, W.M., Windrew, R., 2016. U.S. Govt. Hackers Ready to Hit Back If Russia Tries to Disrupt Election [WWW Document]. NBC News. URL http://www.nbcnews.com/news/us-news/u-s-hackers-ready-hit-back-if-russia-disrupts-election-n677936 (accessed 11.14.16).

Dunn Cavelty, M., 2016. Cyberspace wird zum politischen Schlachtfeld. Neue Zür. Ztg. 7.

Emm, D., Unuchek, R., Garnaeva, M., Liskin, A., Makrushin, D., Sinitsyn, F., 2016. IT Threat Evolution in Q3 2016. Kaspersky Lab HQ.

Entous, A., Nakashima, E., Miller, G., 2016. Secret CIA assessment says Russia was trying to help Trump win White House [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.bd0e7bc92277 (accessed 12.14.16).

Europe 1, 2017. Cyberattaque : "un risque d'instrumentalisation" de l'élection présidentielle [WWW Document]. Eur. 1. URL http://www.europe1.fr/societe/cyberattaque-un-risque-dinstrumentalisation-de-lelection-presidentielle-2944991 (accessed 2.1.17).

European Union Agency for Network and Information Security, 2016. Review of Cyber Hygiene practices. European Union, Heraklion, Geece.

Farrell, H., 2015. Promoting Norms for Cyberspace [WWW Document]. Counc. Foreign Relat. URL http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358 (accessed 1.18.17).

Farrell, H., Glaser, C.L., 2016. The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine.

Financial Times, 2016. America's dilemma over Russian cyber attacks [WWW Document]. Financ. Times. URL https://www.ft.com/content/8a75f954-9151-11e6-a72e-b428cb934b78 (accessed 12.1.16).

F-Secure, 2015. The Dukes: 7 years of Russian cyberespionage. F-Secure, Helsinki.

Gambino, L., Siddiqui, S., Walker, S., 2016. Obama expels 35 Russian diplomats in retaliation for US election hacking [WWW Document]. The Guardian. URL

https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack (accessed 1.10.17).

Gaouette, N., Labott, E., 2016. Russia, US move past Cold War to unpredictable conflict [WWW Document]. CNN Polit. URL http://edition.cnn.com/2016/10/12/politics/us-russia-tensions-cold-war/ (accessed 10.24.16).

Gaycken, S., 2016. Blaming Russia for the DNC hack is almost too easy [WWW Document]. Counc. Foreign Relat. URL http://blogs.cfr.org/cyber/2016/08/01/blaming-russia-for-the-dnc-hack-is-almost-too-easy/#more-3752 (accessed 10.31.16).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Giles, K., 2016. Russia's "new" tools for confronting the West: continuity and innovation in Moscow's exercise of power. Chatham House, London.

Giles, K., 2012. Russia's Public Stance on Cyberspace Issues, in: 2012 4th International Conference on Cyber Conflict (CYCON 2012): Tallinn, Estonia, 5 - 8 June 2012. IEEE, Piscataway, NJ, pp. 63–76.

Goodin, D., 2017. NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage [WWW Document]. Ars Tech. URL http://arstechnica.com/security/2017/01/nsa-leaking-shadow-brokers-lob-molotov-cocktail-before-exiting-world-stage/ (accessed 1.16.17).

Goodin, D., 2016. New leak may show if you were hacked by the NSA [WWW Document]. Ars Tech. URL http://arstechnica.com/security/2016/10/new-leak-may-show-if-you-were-hacked-by-the-nsa/ (accessed 11.2.16).

Greenberg, A., 2016. Hackers claim to auction data they stole from NSA-linked spies [WWW Document]. Wired. URL https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/ (accessed 10.25.16).

Grohe, E., 2015. The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict. Comp. Strategy 34, 133–148. doi:10.1080/01495933.2015.1017342

Hay Newman, L., 2016. Officials Are Scrambling to Protect the Election From Hackers [WWW Document]. Wired. URL https://www.wired.com/2016/09/elections-loom-officials-debate-protect-voting-hackers/ (accessed 12.20.16).

Higgins, A., 2017. Russians Ridicule U.S. Charge That Kremlin Meddled to Help Trump [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2017/01/07/world/europe/russians-ridicule-us-charge-that-kremlin-meddled-to-help-trump.html?partner=google_editors_choice (accessed 2.7.17).

Hosenball, M., Volz, D., Landay, J., 2016. U.S. formally accuses Russian hackers of political cyber attack [WWW Document]. Reuters. URL http://www.reuters.com/article/us-usa-cyber-russia-idUSKCN12729B (accessed 10.24.16).

Howarth, F., 2015. US State Department Hack Has Major Security Implications [WWW Document]. SecurityIntelligence. URL https://securityintelligence.com/us-state-department-hack-has-major-security-implications/ (accessed 11.1.16).

Ignatius, D., 2016. In our new Cold War, deterrence should come before detente [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/opinions/global-opinions/in-our-new-cold-war-deterrence-should-come-before-detente/2016/11/15/051f4a84-ab79-11e6-8b45-f8e493f06fcd_story.html?utm_term=.674ce7f32101 (accessed 11.18.16).

Ingle, S., 2016. Wada cyber attack: Williams sisters and Simone Biles targeted by Russian group [WWW Document]. The Guardian. URL https://www.theguardian.com/sport/2016/sep/13/wada-russian-cyber-attack-espionage-group (accessed 12.16.16).

Inkster, N., 2016. Information Warfare and the US Presidential Election. Survival 58, 23–32. doi:10.1080/00396338.2016.1231527

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 11.4.16).

Internet Society, 2016. Global Internet Report 2016. Internet Society.

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. IEEE, pp. 4490–4494. doi:10.1109/IECON.2011.6120048

Kaspersky Lab, 2015. Equation Group: Questions and Answers. Kaspersky Lab HQ, Moscow.

Kessler, G., 2015. Hillary Clinton's e-mails: a timeline of actions and regulations [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/news/fact-checker/wp/2015/03/10/hillary-clintons-emails-a-timeline-of-actions-and-regulations/ (accessed 11.8.16).

Klion, D., 2016. The US-Russia discord will be an ugly fact for the next President [WWW Document]. The Guardian. URL https://www.theguardian.com/commentisfree/2016/oct/09/us-russia-discord-weight-on-the-next-president-hacking-dnc-election (accessed 10.24.16).

Krauss, C., Schwartz, J., 2016. Secretary of State Nominee Is a Flexible Pragmatist [WWW

Document]. N. Y. Times. URL http://www.nytimes.com/2016/12/13/business/energy-environment/rex-tillerson-secretary-of-state-exxon-mobil.html (accessed 12.14.16).

Krieg, G., Kopan, T., 2016. Is this the email that hacked John Podesta's account? [WWW Document]. CNN Polit. URL http://edition.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks/ (accessed 11.8.16).

Lain, S., 2016. The Vlad and Donald Show: Russia–US Relations Get Personal [WWW Document]. RUSI. URL https://rusi.org/commentary/vlad-and-donald-show-russia%E2%80%93us-relations-get-personal (accessed 1.4.17).

Lartey, J., 2016. US investigates if Russia may be trying to influence election - report [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2016/sep/05/russia-influence-us-presidential-election-investigation (accessed 10.25.16).

Lee, D., 2016. Obama presses Trump on cybersecurity [WWW Document]. BBC News. URL http://www.bbc.com/news/technology-38193663 (accessed 12.5.16).

Lin, H., 2012. Escalation Dynamics and Conflict Termination in Cyberspace. Strateg. Stud. Q. 6, 46–70.

Lipton, E., Sanger, D.E., Shane, S., 2016. The Perfect Weapon: How Russian Cyberpower Invaded the U.S. [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0 (accessed 12.19.16).

Lowe, C., Zinets, N., 2016. Russia says foreign spies plan cyber attack on banking system [WWW Document]. Reuters. URL http://www.reuters.com/article/us-russia-cyberattack-banks-idUSKBN13R0NG (accessed 12.5.16).

MacAskill, E., Thielman, S., Oltermann, P., 2017. WikiLeaks publishes "biggest ever leak of secret CIA documents" [WWW Document]. The Guardian. URL https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance (accessed 3.10.17).

Malkin, B., Yuhas, A., 2017. FBI director challenges Trump claims over Obama wiretap – reports [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/mar/06/fbi-director-challenges-trump-over-obama-wiretap-claims-reports (accessed 3.6.17).

Martin, D., 2016. Russian hack almost brought the U.S. military to its knees [WWW Document]. CBS News. URL http://www.cbsnews.com/news/russian-hack-almost-brought-the-u-s-military-to-its-knees/?ftag=CNM-00-10aab7e&linkId=32446094 (accessed 12.21.16).

McCain Nelson, C., Peterson, K., 2016. Hackers target Clinton campaign, House Democratic Campaign Committe [WWW Document]. Wall Str. J. URL http://www.wsj.com/articles/house-democratic-campaign-committees-computers-hacked-1469807247 (accessed 10.27.16).

Menn, J., 2016. U.S. election agency breached by hackers after November vote [WWW Document]. Reuters. URL http://www.reuters.com/article/us-election-hack-commission-idUSKBN1442VC?il=0 (accessed 12.16.16).

Microsoft, 2016. SQL Injection [WWW Document]. Microsoft TechNet. URL https://technet.microsoft.com/en-us/library/ms161953(v=SQL.105).aspx (accessed 11.29.16).

Miller, C., 2016. Inside The Ukrainian "Hacktivist" Network Cyberbattling The Kremlin [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html (accessed 11.3.16).

National Information Standards Organization (U.S.), 2004. Understanding metadata. NISO Press, Bethesda, MD.

National Intelligence Council, 2017. Assessing Russian Activities and Intentions in Recent US Elections (Intelligence Community Assessment No. ICA 2017-01D). National Intelligence Council.

Nocetti, J., 2015. Guerre de l'information : le web russe dans le conflit en Ukraine. Focus Strat. 62, 1–47.

Openspf, 2010. Sender Policy Framework [WWW Document]. Send. Policy Framew. URL http://www.openspf.org/Introduction (accessed 1.3.17).

Ornos, E., Remnick, D., Yaffa, J., 2017. Trump, Putin, and the New Cold War [WWW Document]. New Yorker. URL http://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war (accessed 3.13.17).

Paul, C., Matthews, M., 2016. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It (No. PE-198-OSD), Perspectives. RAND Corporation, Santa Monica, CA.

Perez, E., Prokupecz, S., 2015. How the U.S. thinks Russians hacked the White House [WWW Document]. CNN Polit. URL http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/ (accessed 10.25.16).

Reuters, 2016. Hacking of two state voter databases prompts FBI to call for better security [WWW

Document]. The Guardian. URL https://www.theguardian.com/technology/2016/aug/29/arizona-illinois-voter-registration-systems-hacked-fbi (accessed 10.25.16).

Rosenblatt, S., Cipriani, J., 2015. Two-factor authentication: What you need to know (FAQ) [WWW Document]. CNet. URL https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ (accessed 12.14.16).

Rosenfeld, E., 2015. US-China agree to not conduct cybertheft of intellectual property [WWW Document]. CNBC. URL http://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html (accessed 11.3.16).

Rudnitsky, J., Micklethwait, J., Riley, M., 2016. Putin says DNC hack was a public service, Russia didn't do it [WWW Document]. Bloomberg. URL http://www.bloomberg.com/politics/articles/2016-09-02/putin-says-dnc-hack-was-a-public-good-but-russia-didn-t-do-it (accessed 10.25.16).

Sanger, D.E., 2017. Putin Ordered "Influence Campaign" Aimed at U.S. Election, Report Says [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0 (accessed 1.10.17).

Segal, A., 2016. Do U.S. efforts to deter Russian cyberattacks signal the end of cyber norms? [WWW Document]. Counc. Foreign Relat. URL http://blogs.cfr.org/cyber/2016/11/07/do-u-s-efforts-to-deter-russian-cyber-attacks-signal-the-end-of-cyber-norms/ (accessed 11.14.16).

Siciliano, R., 2015. What is a Remote Administration Tool (RAT)? [WWW Document]. McAfee Blog. URL https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rat/ (accessed 11.4.16).

Siddiqui, S., 2017. Sessions did not disclose meetings with Russian ambassador during Trump campaign [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/mar/02/jeff-sessions-russian-ambassador-trump-campaign (accessed 3.10.17).

Starr, B., 2015. Official: Russia suspected in Joint Chiefs email server intrusion [WWW Document]. CNN Polit. URL http://edition.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/ (accessed 10.25.16).

Stauffacher, D., Kavanagh, C., 2013. Confidence Building Measures and International Cyber Security. ICT4Peace, Geneva, Switzerland.

Stewart, P., 2015. Pentagon says evicted Russian hackers, global cyber threat grows [WWW Document]. Reuters. URL http://www.reuters.com/article/us-usa-pentagon-cyber-idUSKBN0NE29E20150423 (accessed 11.1.16).

Strohm, C., Syeed, N., 2016. U.S. Publicly blames Russia for hacking to disrupt elections [WWW Document]. Bloomberg. URL http://www.bloomberg.com/news/articles/2016-10-07/u-s-confirms-russia-behind-hacking-attacks-to-disrupt-elections (accessed 10.24.16).

Suiche, M., 2016. Shadow Brokers: The insider theory [WWW Document]. Medium.com. URL https://medium.com/@msuiche/shadowbrokers-the-insider-theory-ded733b39a55#.kst1wpftx (accessed 11.29.16).

Tatham, S., 2015. The solution to Russian propaganda is not EU or NATO propaganda but advanced social science to understand and mitigate its effect in trageted population (No. 4), Policy Paper. National Defence Academy of Latvia - Center for Security and Strategic Research, Riga, Latvia.

Taylor, H., 2016. DNC breach was likely Russia, not 400-pound hacker, law enforcement says [WWW Document]. CNBC. URL http://www.cnbc.com/2016/09/27/dnc-breach-was-likely-russia-not-400-pound-hacker-law-enforcement-says.html (accessed 10.25.16).

The Economist, 2014. War by another name [WWW Document]. The Economist. URL http://www.economist.com/news/europe/21606290-russia-has-effect-already-invaded-eastern-ukraine-question-how-west-will (accessed 10.27.16).

The White House, Office of the Press Secretary, 2013. FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security [WWW Document]. White House. URL https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol (accessed 11.14.16).

Thielman, S., Ackerman, S., 2016. Cozy Bear and Fancy Bear: did the Russians hack Democratic party and if so, why? [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc (accessed 10.25.16).

Timm, T., 2016. If the US hacks Russia for revenge, that could lead to cyberwar [WWW Document]. The Guardian. URL https://www.theguardian.com/commentisfree/2016/oct/19/russian-hacking-us-retaliation-cyberwar-international-treaty (accessed 11.1.16).

Torpey, P., Levett, C., 2017. Trump associates' links with Russia: what we know so far [WWW

Document]. The Guardian. URL https://www.theguardian.com/us-news/ng-interactive/2017/mar/02/donald-trump-russia-campaign-moscow (accessed 3.10.17).
TrendMicro, 2017. Definition [WWW Document]. TrendMicro. URL http://www.trendmicro.com/vinfo/us/security/definition/data-breach (accessed 1.17.17).
United Nations, n.d. Military Confidence-building [WWW Document]. U. N. Off. Disarm. Aff. URL https://www.un.org/disarmament/cbms/ (accessed 3.16.17).
United Nations General Assembly, 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (No. 15–12404). United Nations.
US Department of Homeland Security, Federal Bureau of investigation, 2016. GRIZZLY STEPPE – Russian Malicious Cyber Activity (No. JAR-16-20296).
Walker, S., 2017. Russia accuses cybersecurity experts of treasonous links to CIA [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/jan/31/russian-cybersecurity-experts-face-treason-charges-cia (accessed 2.1.17).
Williams, Z., 2012. What is an internet troll? [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2012/jun/12/what-is-an-internet-troll (accessed 12.5.16).
World Nuclear News, 2016. Russia withdraws from US nuclear cooperation [WWW Document]. World Nucl. News. URL http://www.world-nuclear-news.org/NP-Russia-withdraws-from-US-nuclear-cooperation-07101601.html (accessed 11.29.16).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.