Cyber and Information warfare in the Ukrainian conflict

Author(s):
Baezner, Marie; Robin, Patrice

Publication Date:
2017-06

Permanent Link:
https://doi.org/10.3929/ethz-b-000169634

Rights / License:
In Copyright - Non-Commercial Use Permitted
Cyber and Information warfare in the Ukrainian conflict

Zürich, June 2017

Version 1

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich
# Table of Contents

1. **Introduction** .................................................. 5

2. **Background and chronology** .................................. 6

3. **Description** .................................................... 7
   3.1 Tools and techniques ........................................... 7
       - DDoS ........................................................... 8
       - Website defacement ....................................... 8
       - Malware ...................................................... 8
   3.2 Targets .......................................................... 9
   3.3 Attribution and actors ......................................... 9
       - Pro-Ukrainian hacker groups ............................... 10
       - Pro-Russian hacker groups ................................. 10

4. **Effects** .......................................................... 11
   4.1 Social and political effects ................................... 11
   4.2 Economic effects ............................................... 12
   4.3 Technological effects ......................................... 12
   4.4 International effects ......................................... 13

5. **Consequences** .................................................. 14
   5.1 Raising awareness of propaganda and misinformation ... 14
   5.2 Limit the dependence on foreign technology ............... 14
   5.3 Leading by example against DDoS and website defacement 15
   5.4 Monitoring of the evolution of the conflict ............... 15
   5.5 Confidence Building Measures ............................... 15

6. **Annex 1** .......................................................... 16

7. **Glossary** ........................................................ 20

8. **Abbreviations** ................................................... 21

9. **Bibliography** .................................................... 22
Executive Summary

Russia’s cyber capabilities gained visibility with the intrusion into US computer networks during the 2016 election campaign. However, Russia has been building up and improving its cyber capabilities over the last ten years. The first demonstration occurred with the cyberattacks in Estonia in 2007, and continued with the Russo-Georgian war in 2008. In the Ukrainian conflict, Russia exhibited its capacity to combine cyber capabilities with electronic warfare, intelligence and kinetic capabilities.

This hotspot analysis examines the specific case of the cyber dimension in the Ukrainian conflict. A “hotspot” is understood as the cyber aspect in a particular conflict and relates to the series of actions taken in that context by states or non-state actors in cyberspace.

The main objective of this analysis is to better understand the events and the cyber-activities taking place during the Ukrainian conflict and their effects. An additional aim of this document is to evaluate how the victims reacted to the cyberattacks in order to learn from their actions.

Description

At the end of 2013, the Ukrainian President turned away from an association agreement with the European Union, which caused public demonstrations. A few months later, he fled to Russia and the Ukrainian conflict started with Russia invading the Crimean peninsula. Throughout the Euromaidan protests and the conflict, institutions and media outlets in Ukraine and Russia were the victims of Distributed Denial of Service (DDoS) attacks, website defacement, and Remote Administration Tools delivered by spear phishing emails. These cyberattacks were used to either disrupt, spy on or cause damage to the enemy. The warring parties used non-state actors as proxy forces to conduct these attacks and gave them plausible deniability.

Effects

The examination found that the cyber-activities in the context of the Ukrainian conflict affected the Ukrainian domestic level. There were also effects at the international level. The social and political effects in Ukraine are characterized by Crimea not having access to other sources of information than Russian ones and the Ukrainian population losing trust in its government’s credibility. The economic effects are marked by the costs of the damage of the various DDoS and website defacements and the expenses needed to replace equipment by cyberattacks on the Ukrainian power grid. The technological effects consist of the risks of depending on foreign technology, having troops physically tampering with telecommunications infrastructures, damage caused by cyberattacks on the Ukrainian power grid and the development of new malware.

At the international level, the effects are marked by low-intensity tit-for-tat logic between the warring parties in cyberspace, limited support to Ukraine from the international community, and the implementation of economic sanctions against Russia.

Consequences

Several consequences can be derived from the effects of the cyber-activities that occurred in the context of the Ukrainian conflict and Russian information warfare. States could try to limit the impact of the Ukrainian conflict by raising awareness in society about propaganda campaigns and misinformation. They should lead by example and enhance their cybersecurity against Distributed Denial of Service attacks and website defacement for state’s online infrastructures. Also, they could improve their cybersecurity by limiting their dependency on foreign technology and providing guidance for the private sector to follow in case of cyberattacks. States should monitor closely the evolution of the Ukrainian conflict and promote Confidence Building Measures at the international level.

---

1 Technical words written in italic 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

During the last ten years, Russia has shown that it is capable of developing its cyber capabilities and integrating it into its other military capabilities (e.g. kinetic, intelligence and electronic warfare (EW)). Russian actions began in 2007 with the use of Distributed Denial of Service (DDoS) on Estonian institutions’ websites. In 2008, during the conflict between Russia and Georgia, Russian capabilities had improved to the extent that cyber tools were successfully combined with kinetic forces. This hotspot analysis examines specific cases to better understand theoretical and abstract concepts of cyber-defense. The goal of the report is to analyze how victims were affected by cyberattacks and how they responded. This paper also serves as a basis for a broader comparison study between different hotspots that would also give advice on how states can improve their actions if faced with similar situations.

The hotspot analysis report will be regularly updated when new details are released or when new important events occur. The goal is to have a document as up-to-date as possible.

This report analyzes the specific case of cyber activities in the Ukrainian conflict. Since Vladimir Putin’s first election as Russian President, the relations between Ukraine and Russia have been tense. The strained relationship was punctuated with disputes in 2004 during the Orange Revolution in Ukraine and regularly over natural gas supplies. The tensions reached a new height when Ukraine started to get closer to the European Union (EU) and the Euromaidan protests ousted the Russia-friendly Ukrainian President Viktor Yanukovych. It finally broke into an open conflict with Russia invading the Crimean peninsula.

This case is relevant for study because it is an ongoing conflict that has an intense cyber-dimension. Even though this conflict has reduced in intensity in the physical and cyber-realm since its beginning, it remains significant in world politics and can also influence events in Syria, where Russia is also involved.

The hotspot analysis is divided in five sections and will proceed as follows. Section 2 describes the historical background and chronology of the events from Ukrainian independence in 1990 to the renewed violence in the Donbass region in January 2017. It records the events that shape the tense relationship between Russia and Ukraine and explains the conflict context in which the cyberattacks unfold.

In section 3, the report explains the various cyber-tools and techniques used during the Euromaidan protests and the Ukrainian conflict, who was targeted, and who were the perpetrators. It demonstrates that the tools and techniques used in this conflict display various levels of sophistication and serve different purposes. The reported cyberattacks included DDoS, website defacement, the principal goal of which is mainly to disrupt the good functioning of the websites, and several malware families, used to steal information. The victims of cyberattacks were mostly state institutions and media outlets in both Ukraine and Russia, but also warring groups and third parties, such as international organizations and other states. The perpetrators are summarized into two groups based on their affiliation and not on their geographic location. These two groups are: pro-Ukrainian hacker groups and pro-Russian hacker groups. Both Ukraine and Russia fight through proxies, which enables both governments to deny any involvement.

Section 4 examines the diverse effects of the cyber-aspects of the Ukrainian conflict on domestic and international levels. The effects were mostly felt on the Ukrainian domestic level in the social, political, economic and technological domains. The social and political effects in Ukraine were marked by a denial of access to non-Russian information in the Crimean peninsula and a loss in trust in the Ukrainian institutions in their role to protect society. Economically the effects were characterized by the high costs of DDoS and website defacement, as well as the costs of replacing damaged equipment in the power plant targeted by cyberattacks. The technological effects consist of the physical tampering of the Russian troops on telecommunications infrastructures in Ukraine, which also shows the dangers of relying on foreign technology; of the physical damage in power plants due to the cyberattacks, and the discovery of new malware. The effects on the international level are summarized by a low intensity tit-for-tat logic between the warring parties; even when critical infrastructure like power plants were targeted; and by the limited support that Ukraine received from the international community, and the implementation of economic sanctions on Russia.

Finally, section 5 proposes some consequences that result from the analysis of the hotspot which state actors can apply to decrease the risks to be impacted by the effects of the cyber-activities resulting from the conflict or to find themselves in a similar situation. It suggests improving cybersecurity by raising awareness in society of the issues of propaganda and misinformation; to lead by example with better protection against DDoS or website defacement for state’s online infrastructures, and to limit dependency on foreign technology. It also recommends closely monitoring the development of the Ukrainian conflict and to promote Confidence Building Measures (CBM) in cyberspace to reduce mistrust among states.

---

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

4 Technical words written in italic are explained in a glossary in section 7 at the end of the document.
2 Background and chronology

Both the historical background and chronology of the Ukrainian conflict are important in understanding the context in which it developed.

Ukraine gained its independence at the fall of the Soviet Union, but Russia still tried to maintain a certain control or influence on former Soviet Republics. The relations between Russia and Ukraine were characterized by disputes, including the Orange Revolution during the Ukrainian elections in 2004 and those over natural gas supplies. Ukraine started first to get closer to the EU with an association agreement, but later turned back to Russia instead. This decision precipitated the Euromaidan protests and provoked the departure of Ukrainian President Yanukovych. In parallel with the protests, DDoS and website defacement occurred on Ukrainian websites. A few months later when Russia invaded Crimea there was also an increase in cyber-activities in Ukraine and Russia that remained more or less at a low level. However there were two spikes: two attacks against the Ukrainian power grid.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.12.1994</td>
<td>Ukraine becomes a member of the Nuclear Non-Proliferation Treaty by returning its nuclear weapons to Russia. In the Budapest memorandum on Security Assurances, Ukraine is assured that its territorial integrity and political independence would not be threatened by Russia (Besemeres, 2014; United Nations, 1994).</td>
</tr>
<tr>
<td>03.2005-01.2006</td>
<td>In March 2005, Russia accuses Ukraine of diverting natural gas bound for EU states and not paying taxes over natural gas supplies. On 1st of January 2006, Russia cuts off natural gas supply to Ukraine, with effects on European states that depend on the gas supply transiting through Ukraine (BBC News, 2006).</td>
</tr>
<tr>
<td>08.2008</td>
<td>Following skirmishes between pro-Russian rebels and Georgian armed forces, Russia invades Georgia. The Russian military uses a combination of kinetic capabilities and cyberattacks on Georgian institutions’ websites (Giles, 2016a, pp. 4–5).</td>
</tr>
<tr>
<td>12.2011</td>
<td>After Putin’s victory in the legislative elections, the opposition organizes demonstrations to protest against the election results. During the protests, the Russian armed forces use automated DDoS to disrupt media and social media pages in order to stop the discussion over the elections (Giles, 2012).</td>
</tr>
</tbody>
</table>

12.2011: stop the discussion over the elections

11.2013: The Ukrainian President Yanukovych rejects the Association Agreement with the EU. In consequence, the pro-European Euromaidan movement organizes protests, but is violently repressed. In parallel, Ukrainian institutions’ websites are targeted by DDoS attacks (Ukraine investigations, 2014).

18-21.02.2014: Violence against protesters intensifies causing the deaths of several demonstrators. The DDoS attacks continue on Ukrainian websites and on Ukrainian members of Parliament’s cell phones. The Ukrainian Parliament agrees to a change in constitutional law and to return to the setting before the constitution of 2004.

22.02.2014: Ukrainian President Yanukovych flees to Russia. The Ukrainian Parliament elects Oleksandr Turchynov as acting President until the planned presidential election of 25th May 2014 (Pakharenko, 2015).

27-28.02.2014: Pro-Russian groups organize demonstrations in various Ukrainian big cities and non-uniformed soldiers seize airports and other strategic sites in Crimea. They cut off Crimean communications with the external world in a raid on the Ukrainian telecommunications infrastructures and tamper with the fiber optic cables (Gordon, 2014; Martin-Vegue, 2015).

01.03.2014: The Russian Parliament authorizes the use of force against Ukraine (Lally et al., 2014).

02.03.2014: Russian troops enter Crimea (Maurer, 2015).

07-14.03.2014: As retaliation for the invasion, various Russian websites are targeted by DDoS attacks (Ukraine investigations, 2014).

16.03.2014: The referendum on the annexation of Crimea by Russia is accepted by the Crimean population (Geers, 2015, p. 10).

16-18.03.2014: Various DDoS attacks on Ukrainian and Russian websites are reported (Ukraine investigations, 2014).

17.03.2014: USA and European States agree on a first round of sanctions against Russia (Geers, 2015, p. 10).

18.03.2014: President Putin signs a bill on the annexation of Crimea (White, 2014).

For a detailed table of the cyberattacks during this period and during the Ukrainian conflict, see the Annex 1.
The war in the Eastern Ukrainian region of Donbass starts between pro-Russian separatists and the Ukrainian armed forces. In parallel, cyberattacks on Russian and Ukrainian websites continue. USA and European states agree on a second round of sanctions on Russia (Shahani, 2015).

A pro-Russian hacker named “CyberBerkut” hacks the servers of the Central Election Commission (CEC) and infects the election networks with a malware. The Ukrainian cyber emergency response team manages to remove the malware from the network in time for the election (Weedon, 2015).

Petro Poroshenko is elected as the new President of Ukraine (Geers, 2015, p. 10).

President Poroshenko declares a seven-day ceasefire for the pro-Russian separatists to put down their weapons. During that ceasefire, cyberattacks coming from pro-Russian hacker groups stop as well (Shahani, 2015).

Malaysia Airlines’ flight MH17 from Amsterdam to Kuala Lumpur is shot down by combatants in Ukraine resulting in approximately 300 dead (Geers, 2015, p. 10).

The USA and European states expand the sanctions against Russia (BBC News, 2014).

Russia issues an embargo on agricultural goods from the countries that established sanctions against Russia (Walker and Rankin, 2014).

The warring parties agree in the Minsk Protocol to a ceasefire in the Donbass region. The ceasefire collapses in January 2015.

Poroshenko’s political party wins the majority in the Ukrainian parliamentary elections. During the campaign several DDoS attacks and hacks are observed against Ukrainian institutions (Martin-Vegue, 2015).

Russia creates a new cyber warfare-specific military unit in Crimea (Pakharenko, 2015, p. 62).

The new Russian military doctrine is published, which also details the concept of information warfare (Giles, 2016a, p. 27).

Warring parties sign a new ceasefire agreement, the Minsk II Protocol. The protocol is violated shortly after the signing (Weaver and Luhn, 2015).

The EU creates a StratCom Task Forces, whose goal is to identify and correct disinformation coming from Russian-speaking media (European Union, 2015).

A cyberattack on Ukrainian power grid leaves approximately 250,000 inhabitants without power for several hours (Zetter, 2016).

An international investigation reports that flight MH17 was shut down by a Soviet-built BUK missile launched from the Donbass region (Harding, 2016).

A Ukrainian hacker group leaks hacked emails from a key counsellor of Vladimir Putin, Vladislav Surkov. His emails reveal that he was communicating on regular basis with leaders of pro-Russian separatists in Ukraine (Windrew, 2016).

Russia withdraws from the International Criminal Court (Reuters, 2016a).

Ukraine tests missiles in the Black Sea, West of Crimea, and is accused of violating Russian territorial waters (BBC News, 2016a).

Several cyberattacks target Ukrainian banks, state’s agencies and Ministries (Miller, 2016a).

Power goes out for an hour in the region of Kiev after a new cyberattack on the Ukrainian power grid (Goodin, 2017).

In Eastern Ukraine, clashes between Ukrainian forces and separatist groups intensify after several calmer months (BBC News, 2017).

3 Description

This section will describe the different tools and techniques used during the Euromaidan protests and the Ukrainian conflict. The objective is to better understand what tools and techniques were used, how they work and what are their purposes. Then, it will explain who the targets of these cyberattacks were and who perpetrated them.

3.1 Tools and techniques

In the conflict between Ukraine and Russia, the cyberattacks can be classified into three types: DDoS attacks, website defacement and malware infection by
spear phishing⁶. The first two tools are more qualified as cyber-disruption while the latter is more oriented toward cyber-espionage for intelligence collection and to prepare the battlefield for further kinetic offensives or cyberattacks (Torruela, 2014, p. 121).

DDoS

An increase of DDoS attacks was observed against various webpages at the beginning of the Euromaidan protests and during the invasion of Crimea. In a DDoS attack, perpetrators overload targeted websites with requests causing disruption in the services of the websites and preventing legitimate users accessing these pages. This technique requires the use of multiple computers infected by botnets or the coordination of a large number of users. The attacker would command these computers compromised with botnets to send requests to the targeted network without the users of the infected computers knowing it. This kind of cyberattack was used multiple times by both parties of the conflict, for instance Ukrainian media websites were targeted by pro-Russian hackers in November 2013 or Russian media webpages were attacked by pro-Ukrainian hackers in December 2013. DDoS attacks can also serve as distraction to monopolize the attention of the emergency team of the targeted institution. While they are occupied by stopping the DDoS attack, the perpetrator(s) can conduct other malicious activities on this network, like installing a backdoor or malware in order to steal data (NSFocus Inc., 2016, p. 4).

Website defacement

Website defacement has also been observed as a tool used by both parties in the Ukrainian crisis. The technique where a hacker breaches a web server using an SQL injection to gain administrative access is considered to be a cyber-version of vandalism. Once the system has been entered, the attacker changes the visual appearance of the website or replaces with its own webpage. It is a technique usually used by hacktivists to spread political messages. For instance, the website of the Russian media, RT, was defaced in March 2014. The attackers replaced the words “Russia”, “Russian” and “military” with the word “Nazi” (Perlroth, 2014; Storm, 2014).

Malware

Several malware, believed to be linked to the Ukrainian conflict, have been observed throughout the conflict. The security firm, FireEye, reported that since the beginning of the war there has been an increase of the use of malware connected to Russian and Ukrainian servers (Geers, 2014). Four malware groups have been identified in this context: “BlackEnergy”, “Snake”, “Operation Armageddon” and “X-Agent”.

“BlackEnergy” is a family of malware usually used by cybercriminals. It was also employed in a campaign named “Sandworm” (Zetter, 2014). The first version of “BlackEnergy” was used to gain access to networks in order to launch DDoS attacks. The Second version, “BlackEnergy2”, was updated with new functionalities enabling it to steal data. The last version, “BlackEnergy3”, was updated to target Supervisory Control and Data Acquisition (SCADA) systems and added a new feature, “KillDisk”, which rendered the infected computers unusable. This version was used to attack the Ukrainian power grid system in December 2015 (E-ISAC, 2016; FireEye Inc., 2016). Attackers used spear phishing emails or a compromised attachment to infect computers. The malware would then install a backdoor for the attackers to have access to the network. The last two versions of the malware were employed to gather information and were implanted in specific targets, like NATO, the Ukrainian government or the Ukrainian power grid system.

The “Snake” malware was discovered in 2014, but had been active since at least 2010 or 2011. It is similar to an older malware, “Agent.btz”, used to infiltrate the US military network in 2008. Victims got infected either by opening spear phishing emails or by visiting watering hole websites, which consist of infecting a webpage with a malware hoping that the target would visit it and get infected. Once the malware has infected a machine, it would wait until the user opens a web browser, simultaneously opening a backdoor to communicate with the attackers without the user’s knowledge (InfoSecurity, 2014; Paganini, 2014a). It is designed to copy and delete files, connect to infected servers, load and execute other malware. The “Snake” malware is composed of two elements: A rootkit and a driver. The former takes control of the computer and hides its activities from the user in order to steal data and capture the network traffic. The driver injects codes in the web browser to hide its traffic of exchanged information with the attackers’ servers and sets a hidden file to store its configuration and stolen information (Paganini, 2014b; Symantec Security Response, 2014). The amount of computers infected by “Snake” increased in Ukraine after the start of the Euromaidan protests. There were only eight cases of “Snake” infection in Ukraine in 2013, as compared to 14 new cases between January 2014 and March 2014. In total, there have been 32 cases observed since 2010 (Sanger and Erlanger, 2014).

“Operation Armageddon” is a Remote Administration or Access Tool (RAT) that targeted Ukrainian government, law enforcement and military networks. It was discovered in September 2014 by the US security firm LookingGlass. Security experts and Ukrainian officials suspect Russia of creating and using this malware (Witty, 2015). Its purpose was to gather

⁶ Even though the use of trolls to spread propaganda and misinformation is a technique used in the Russian information warfare, this aspect will not be considered as a tool for cyberattacks in this section. However, it will be examined in the section on attribution and actors.

⁷ This malware is also known as “Urobouros” or “Turla”.


information about its victims, probably to gain the advantage on the battlefield in Eastern Ukraine (Weedon, 2015, p. 72). This practice demonstrates that cyberespionage can be used as a tool to support physical warfare. It is believed that this malware has been active since at least 2013 when Ukraine started the discussions about the Association Agreement with the EU. It infected machines through spear phishing emails with a compromised Microsoft Word attachment. It has been observed that sometimes stolen documents would be injected with the malware and sent to new targets of spear phishing emails (Hackett, 2015).

“X-Agent” is a malicious application found on Android and Apple smartphones. It was revealed to the public in December 2016, but has been active since 2013. The application was first created as a legitimate software by a Ukrainian artillery officer in order to prepare artillery targeting data faster. The legitimate software was injected with the malware and sent to new targets of spear phishing emails (Crowdstrike, 2016).

3.2 Targets

In this series of cyberattacks there were various victims, but most were located in Ukraine and Russia. In this analysis, they are classified by activity and country of origin: Ukrainian institutions, Ukrainian media outlets, Russian institutions, Russian media outlets, Russian groups, and third parties.

Ukrainian institutions sustained various kinds of cyberattacks during the Euromaidan protests and during the war with Russia. During the invasion of Crimea, the government website was down for 72 hours because of a DDoS attack, and the cell phones of the members of Parliament were overwhelmed with SMS to prevent them communicating to coordinate a response. The attacks were not limited to DDoS and defacement of websites. Government networks were also targeted by malware campaigns like “Snake” and “Sandworm”. Ukrainian institutions were targeted for intelligence gathering with malware, for protest or retaliation with DDoS (Ukraine investigations, 2014; Weedon, 2015).

Ukrainian media outlets, newspapers, TV channels, and news agencies suffered mostly from DDoS attacks and website defacement during the Euromaidan protests and during the early stages of the war. They were targeted to either prevent them from reporting the events or as retaliation for the way they portrayed the events (Ukraine investigations, 2014; Weedon, 2015).

Russian institutions sustained mostly DDoS attacks and website defacement from Ukrainian hacker groups. For example, at the beginning of the war, the website of the Kremlin was the victim of a DDoS attack as well as the website of the lower parliamentary chamber. They were mainly targeted as retaliation for Russia’s actions in Ukraine and Crimea. They more recently suffered from data theft from a Ukrainian hacker group, “Cyber Hunta”. This group stole emails from one of President Putin’s counselor’s emails, revealing links between the Kremlin and separatists groups in Eastern Ukraine (Windrew, 2016).

Russian media outlets suffered mostly from DDoS and defacement attacks. The goal would have been to either disrupt the website, when attacked by DDoS, or ridicule the media webpage by defacing it.

Third parties include NATO, Organization for Security and Co-operation in Europe (OSCE), organizations and countries not directly involved in the conflict who were victims of various cyberattacks in relation to the Ukrainian conflict. Various NATO websites were hit by DDoS attacks at the start of the war and NATO servers were infected by the same malware that infected Ukrainian institutions, “Snake” and “Sandworm”. The former has also been found in the Belgian, Lithuanian and British networks (Paganini, 2014a). NATO was also probably targeted for intelligence collection. Additionally, the DDoS attacks could have been made in retaliation or as a signal for NATO to stop its enlargement (Giles, 2015). The OSCE, which discovered a spying malware in its system in November 2016, was probably targeted to gather information on observers operating in Ukraine or elsewhere in the world (BBC News, 2016b). The Dutch Safety Board has been targeted for several days at the releasing of its report of the investigation into the crash of the flight MH17 (Foxall, 2016). It might have been targeted to protest and disrupt the publication of the report.

3.3 Attribution and actors

Attribution in cyberspace remains a complicated task. It normally follows the “cui bono” (to whose benefit) logic, but there will always be uncertainties on perpetrators. The sources used for this report are mainly academic journals, main Western media and cybersecurity firms. There is the possibility that the presented technical evidence was set in a certain way by an actor to incriminate another actor.

In the specific case of the Ukrainian conflict, the attribution issue is especially complicated because of the quantity of attacks and the fact that both sides use proxies. The use of proxies gives states the advantage of plausible deniability. If the attacks are successful, the state benefits from the results of the attacks. However if they fail, or are compromised, the state can dissociate itself from these groups by declaring that they acted on their own initiative without any government support (Maurer, 2015, p. 81). The distinction between state actors and non-state actors is also unclear as both tend to share their tools. For instance, it was reported that the “BlackEnergy” toolkit was normally used by cybercriminals for DDoS attacks. However the attack on the Ukrainian power plant showed that this tool could also be used for espionage and to gain access to more political targets (F-Secure, 2014).
The actors come from both states and constitute two categories of groups: pro-Ukrainian hacker groups and pro-Russian hacker groups. The difference between the two categories is not geographical because some groups target their own country’s institutions. Moreover some pro-Russian hacker groups would perpetrate their attacks from the Eastern Ukrainian territories to bypass the territorial filters blocking IP addresses coming from Russia (Ukraine investigations, 2014). The following list is non-exhaustive and only details the main active groups on both sides. It is also possible that some of these groups are in reality the same groups, but have different names and would have been classified as two different groups.

**Pro-Ukrainian hacker groups**

- “Cyber Hunta”: The hacktivist group composed of several volunteers whose goal is to expose Moscow’s involvement in the conflict in Ukraine. They claim not to be associated to the Ukrainian government (Miller, 2016b).
- “Cyber Hundred”
- “APT28”
- “APT29”11: This hacker group was first discovered in 2008 during the conflict between Russia and Georgia. The group is believed to have ties to the Russian Main Intelligence Directorate (GRU), which is the foreign military intelligence office. They are highly professional and use malware developed on computers with Russian language settings. They are known to design their malware to fit their targets and to use spear phishing to infect their victims, as well as using zero-day vulnerabilities. They infiltrated the networks of Russian dissidents, European security organizations, defense contractors, Western governmental institutions, and media outlets. They are one of the two groups who allegedly hacked into the US Democratic National Committee in 201610. The choice of their targets seems to be the typical targets that a military intelligence service like the GRU would concentrate on. “APT28”’s malware have been found in Ukrainian government’s networks and artillery troops’ smartphones (Crowdstrike, 2016; Koval, 2015; Weeldon, 2015). The security firm ThreatConnect believes that they are linked to “CyberBerkut” as they took turns in spear phishing campaigns against the investigative journalist group, named Bellingcat (Ashok, 2016).
- “APT29”
- “CozyDuke”

**Pro-Russian hacker groups**

- “CyberBerkut”: The hacker group supports separatist groups in Eastern Ukraine, but it remains uncertain if the hacker group is composed of pro-Russian Ukrainians or Russians. “CyberBerkut” has claimed to be behind several cyberattacks, going from DDoS of NATO websites to the implantation of malware into the CEC. Rumors claimed that former members of the Ukrainian special police forces, “Berkut”, are behind “CyberBerkut”. Others claimed that “CyberBerkut” is in reality the Russian hacker group “APT28” (Miller, 2016b) or that they work together against common enemies (Ashok, 2016). It is said that “CyberBerkut” is assisted with expertise and financing from the Russian government (Kerkkänen and Kuronen, 2016).
- “APT28”
- “APT29”

---

9 This hacker group is also known under the names “Sofacy”, “Fancy Bear”, “Pawn Storm”, “Strontium” or “Sednit”.
10 For more information about the Democratic National Committee hack, please see: Baezner, Marie; Robin, Patricia (2016): Hotspot Analysis: Cyber-conflict between the United States of America and Russia, December 2016, Center for Security Studies (CSS), ETH Zürich.
11 This hacker group is also called “Cozy Bear”, “The Dukes” or “CozyDuke”.

---

The hacker group is also known as “KiberSotnya” or “CyberMaidan”.

---

The hacker group is also known as “CyberMaidan”. 
constantly trying to reduce or eliminate any forensic evidence. This level of organization and the use of highly sophisticated software suggests that they are state-financed (FireEye Inc., 2015).

- “Anonymous Ukraine”: This hacker group is the branch of the hacktivist movement “Anonymous” in Ukraine. It is however internally divided on its opinions regarding the conflict in Eastern Ukraine. Some of its members are pro-Ukrainian who tend to be closer to “Cyber Hundred” and “Null Sector”. While others are pro-Russian and closer to “CyberBerkut”. The pro-Russian element is prominent, having claimed several attacks on NATO, US and EU governments’ websites (Carr, 2014).

- “Quedagh”: This name has been assigned to this group by analysts from the security firm, F-Secure, after the group employed the “BlackEnergy” toolkit against political targets. F-Secure suspects that the group was also involved in the conflict between Russia and Georgia in 2008. The hacker group has used different versions of the toolkit since 2010. The evolution of their version of the toolkit shows that they were patient and observed their victims to adapt their malware to their targets (F-Secure, 2014, p. 4).

- Trolls: They are used by the Russian government to spread pro-Russian propaganda in social media, blogs and forums abroad and in Russia. They are organized in “troll farms or factories”: institutions from which trolls post their messages, comments or posts. One of these troll farms was discovered in St. Petersburg, where trolls were arranged in sectors responsible for different media, and given quotas of comments and posts to write per day. The Ukraine government and the Ukrainian conflict subjects are said to have been the prominent targets of trolls (Volchek and Sindelar, 2015).

- Nashi Youth Movement and Russian Patriotic Hackers: “Nashi” means “ours” and the Nashi Youth Movement was a political youth movement for young Russians aged between 17 and 25 years old. The organization was created in 2005 as a reaction to the activist movement of the Orange Revolution in Ukraine. The movement was openly pro-Putin and was reported to have harassed and spied on opposition activists (Shachtman, 2009). The movement was terminated after the resignation of its president following changes in the Russian government in 2012 (Hartog, 2016). The group claimed responsibility for the cyberattacks on Estonian institutions in 2007 and was also known to have organized pro-Russian protests in Finland and Estonia (Stratfor, 2012). Even though the movement was terminated in 2012, some of its members might continue to be involved in cyber-activities as patriotic hackers, individuals or groups of individuals perpetrating hacking activities on their own initiative against what they perceive to be enemies of Moscow (Denning, 2011, p. 178).

4 Effects

This section analyzes the various effects of the cyber-aspect of the Ukrainian conflict on the Ukrainian domestic level and the international level. At the Ukrainian domestic level, the report looks at the damage to society caused by the cyber-activities in the context of the conflict. It also focuses on the economic costs of such cyberattacks for the private sector and governmental institutions. It examines the technological damage resulting from the conflict, but also technological innovations.

At the international level, it focuses on the international effects of the cyberattacks and the Ukrainian conflict on international order and cooperation.

4.1 Social and political effects

On the social level, people from East Ukraine and Crimea, which are mostly Russian-speaking regions, are totally isolated from the information coming from the outer world. They can only listen to Russian radio or watch Russian television. Therefore they have very limited access to other forms of media and cannot forge other opinions than that provided by Russian media. On the other hand, people from the Western part of Ukraine, have limited access to Russian-speaking media (Lange-Ionatamishvili and Svetoka, 2015; Nocetti, 2015; Selhorst, 2016). Maintaining this isolation is an important part of Russian information warfare, where the goal is to control public opinion and indirectly shape decisions in favor of Russia (Lewis, 2015). Russian propaganda is judged to be highly effective. It broadcasts through a large number of channels, going from traditional television to social media and chat rooms. This enables propaganda to reach a larger number of people, and publish news faster than traditional media channels not limited by the need to check facts before publication (Paul and Matthews, 2016). They also try to increase the credibility and the visibility of their news platforms by inviting experts or famous guests, such as Julian Assange and Larry King (Besemer, 2014).

The significant amount of cyberattacks on the Ukraine’s institutions probably also put a strain on the people’s faith in these institutions, increasing a feeling of insecurity. DDoS attacks and defacement impaired the trust of the population in their institutions and their ability to protect their own population. This is also the logic behind the creation of various hacker groups in Ukraine, like Dokukin’s “Ukrainian Cyber Troops/Army”. At the beginning of the conflict the Ukrainian authorities were visibly lacking the capacities to deal with the various cyberattacks. Therefore, private initiatives, like Dokukin’s, decided to help the
government and the Ukrainian population against trolls and other Russian cyber activities (Kerkkänen and Kuronen, 2016). Another good example of diminishing people’s trust in their government, was the distributed denial of telephone service attack launched on the call center of the Ukrainian power supplier during the blackout of December 2015. The call center was submerged by fake phone calls and could not answer the legitimate calls coming from the customers who called regarding their lack of power. This situation would lead Ukrainians to think that Ukrainian energy suppliers are not prepared for such incidents (Zetter, 2016).

4.2 Economic effects

The economic effects of the cyberattacks in the context of the Ukrainian conflict mostly concern the consequences of the DDoS and defacement attacks. DDoS attacks usually generate direct costs for businesses in the form of loss of revenue and loss of productivity. The average economic damage is estimated to be 22,000 USD per minute of unavailability of a website and the average duration of such attack was estimated to 54 minutes (Kenig, 2013). Therefore such attacks can cost a substantial amount of money for the targeted businesses. However every business is affected differently by DDoS attacks and other costs like investigation, technical response, customer support and public relations costs further add to the bill. Indirect costs like damage to reputation, theft of critical data and opportunity costs are also to be taken into account and can also have serious consequences (NSFocus Inc., 2016). In the context of the Ukrainian conflict, the victims of such attacks were mostly media outlets, banks and governmental websites. For the first two types of victim, the revenue loss might be the most important concern. For governmental institutions, whose websites were targeted, the reputational damage and the indirect costs generated by such attacks are the greatest issues. In their cases, the population can begin to doubt the ability of the institution to perform their tasks or protect the public (especially when they were unable to protect their own websites from a cyberattack).

*Website defacement* has similar economic consequences to DDoS attacks. If the defacement involves a redirection of the visitors to another website, the targeted webpages might lose customers for the time of the defacement. It would also cause a loss in trust in the owners of the defaced websites. The attack would show that they have weaknesses in their webpage security and might have other vulnerabilities, which render them untrustworthy (Paladion Networks, 2015).

The malware infection can be as economically damaging for the victims as a DDoS attack. However it seems that in the Ukrainian conflict, malware were used for collecting information for intelligence purposes and not for enrichment or cybercriminal activities. The intrusion has similar costs to the DDoS because victims must hire emergency teams to stop the interference, and start an investigation. It also has an impact on the reputation of the institution for the same reasons as for DDoS and defacement attacks (BanffCyber Technologies, 2016).

4.3 Technological effects

In the context of the conflict in Ukraine, there were physical attacks on telecommunications infrastructures as well as cyberattacks on critical infrastructures. In particular, when Ukraine was invaded in March 2014, the so-called “little-green-men” raided the Crimean infrastructures of the Ukrainian telecommunications provider, UkrTelecom. They tampered with the internet exchange point of Crimea in order to isolate the peninsula from the rest of the world and prevent it communicating what was happening. In this case the physical damage was not the results of a cyberattack, but a material interference in the functioning of the internet in Crimea. Russia, who admitted in April 2014 that the “little-green-men” were Russian troops, did not try to shut down the internet in Ukraine entirely for two reasons (Karmanau and Isachenkov, 2014). First, it would have been too difficult because Ukraine has six internet access points which all go through Kiev. Second, Russia already owns the main telecommunications companies in Ukraine and the latter relies mostly on Russian hardware for its telecommunications infrastructures (Libicki, 2015, p. 50; Tucker, 2014). In addition, many Ukrainians use Russian social media, like vKontakte and Russian internet resources, like email addresses, allowing the Russian authorities to intercept and read or listen to all conversation happening on these platforms. Even some Ukrainian officials used email accounts provided by Russian companies, which allowed the Russian government to easily obtain the information they needed without any cyberattacks (Pakharenko, 2015; Poludenko-Young, 2015). This partly explains why there have been so few attacks on communication infrastructures in real and cyber realms and that dependence on another state for technology can have significant consequences.

The first cyberattacks on critical infrastructures occurred in December 2015, when several Ukrainian power plants were shut down for several hours. The attacks involved the “BlackEnergy3” malware. It was reported by the investigators that the power plants targeted were still not back to full production levels two months after the attacks. The attackers overwrote the codes of the firmware of 16 substations. In consequence, operators could not log into the system of the substations remotely and had to control them manually. Furthermore, the malware contained a payload named “KillDisk” that erased and crashed the infected computers. The infected machines could not be restarted. All the stored data and information were lost and needed to be replaced.

This particular attack on the power plants might have been a response to the physical attack of a pro-Ukrainian group on power substations in Crimea. However the forensic investigation showed that the
infection had already started in spring 2015. The investigators claimed that the attackers could have done a lot more damage than just shutting down the power for several hours. They assume that the attack was only a message to show of what they were capable (Zetter, 2016).

The second cyberattack on critical infrastructures happened in December 2016 and was very similar to the one a year earlier. It attacked a power plant near Kiev and caused a power outage for approximately one hour. The attack used the same “BlackEnergy” malware and the “KillDisk” payload as well. The malicious software were planted in the system with a spear phishing campaign. However the incident caused less significant material damage than the one in 2015 (Goodin, 2017).

The techniques used in cyberspace in the Ukrainian conflict are not new and did not reach the same intensity as during the conflict between Georgia and Russia in 2008 (Perlroth, 2014; Weedon, 2015). The novel element in this conflict has been the emergence of new malware, like “Snake”, “Operation Armageddon”, and “X-Agent”, which also revealed the development of criminal malware for intelligence and offensive operations, like “BlackEnergy”. The discovery of the malware targeting smartphones, “X-Agent”, was also a significant technological development during the conflict. This represents a completely new element in the dimension of intelligence collection and communication on the battlefield. These new malware could trigger a cyber-arms race among states fearing cyberattacks from Russia. These states might build new cyber-defensive measures or offensive capabilities in order to defend themselves. There is also the risk that the malware used during the conflict will utilized for criminal purposes.

4.4 International effects

After the Euromaidan protests and subsequent annexation of Crimea in March 2014, the number of cyberattacks related to Ukraine and Russia increased. With this intensity, people were expecting to see the development of a cyberwar between the two states, but this scenario never happened. In reality, the conflict occurred simultaneously in cyberspace and the physical world: cyber-means were used in combination with, and in support of kinetic operations. In this case, a possible pattern of escalation of activities in cyberspace and a spilling over into the physical realm did not occur, because the conflict escalated in parallel in both spheres. Cyber-operations have been used in advance in order to support kinetic operations with the collection of intelligence and misinformation. Moreover, the part of the conflict taking place in cyberspace was significant at the beginning of the war then settled, and remained at a more or less constant intensity since. The cyberattacks were limited to mainly cyber-disruptive and enabling-operations attacks, like DDoS, website defacement, and intelligence collection malware (Torruella, 2014, p. 121). There seems to have been a renewed intensity since December 2015, but even in these cases the damage was intentionally limited. The cyberattack on the Ukrainian power grid in December 2015 and 2016 could have caused an escalation in the conflict. However, the attackers limited themselves in the damage they caused. A US Air Force expert, who helped the Ukrainian authorities with the investigation, stated that the attackers could have done a lot more damage, but stopped after several hours (Zetter, 2016).

The expert suggested that both attacks were just to show what the perpetrators were capable of. This self-restriction could also be understood as a way to avoid to further escalation of the conflict, thus risking a significant response from Ukraine or its allies. Critical infrastructures and human lives are considered as “red lines” not to be crossed if actors wish to contain a conflict (Lin, 2012).

The conflict in Ukraine showed that, just like in 2008 during the conflict between Georgia and Russia, the latter is ready to use military force as a foreign policy instrument. The use of cyber-means by Russia has developed since the conflict of 2008 in the Caucasus. After the conflict with Georgia, Russia created an “information troop”, which later was transformed into “troll farms” (Giles, 2016a, pp. 29–30). A difference with the conflict in Georgia was that, in 2008, Russia had more trouble controlling the “information space” and was seen as the loser of the information war (Nocetti, 2015, p. 26). On the other hand, in 2014, Ukraine found itself completely isolated from information from the outside world and it was difficult for foreign media to obtain accurate information about what was happening there. The fact that Western media could not confirm the presence of Russian military in Ukraine for approximately the entire year of 2014 proved that Russian tactics of isolating Ukraine’s “information space” were more effective than in 2008. Propaganda and misinformation were judged by Western countries as too easy and obvious to detect. However, the Russians were able to pollute information feeds, causing confusion about the reliability of the information coming from that region (Giles, 2015, pp. 25–27). Russia also made use of its proxy forces in the physical part of the conflict in Ukraine to complicate the situation. This gave Russia the ability to deny any physical involvement in the conflict. This method was also applied with success in cyberspace. It was well illustrated with the figure of “CyberBerkut”, which some sources claimed to be a pro-Russian hacker group from Ukraine, while others asserted that in fact it was a Russian hacker group, “APT28” (Koval, 2015, p. 57).

At the international level, after the annexation of Crimea, Ukraine found itself isolated from any help and at the mercy of efficient Russian information warfare. In December 1994, the USA, Great Britain, France and China promised Ukraine, in the Memorandum on Security Assurances, to seek assistance from the UN Security Council in case of any aggression from Russia (United Nations, 1994). In reality, the former Soviet Republic is geographically too close to Russia and too far from Western Europe to benefit from any significant military support from the Western states. Apart from
some material and educational help, Western countries’ armies have not done much to prevent Russia from annexing Crimea or to stop the conflict in Eastern Ukraine (Besemeres, 2014). Assistance from NATO came in the form of funding and know-how to protect Ukraine’s cyberspace, but no NATO troops were deployed. In September 2014, it was agreed at the NATO Summit to create five funds to help Ukraine, one of them is the Cyber Defense Trust Fund to help to train personnel and advise Ukrainian authorities on cyber-policies (Fiscutean, 2015). NATO also conducts regular international military exercises in the Ukrainian region in order to demonstrate that the region is not forgotten. The USA is also helping Ukrainian forces by training troops and donating equipment such as radars, Humvees and medical supplies (Gould, 2015).

Western states did however impose economic sanctions on Russia after the annexation of Crimea. These sanctions were not forced on Russia specifically because of the cyberattacks in Ukraine. Nevertheless, the bans and embargos had some impact on the Russian economy. The goal of these sanctions was for Western states to put pressure on Russian markets over the long-term to show their disapproval of the war in Ukraine and the annexation of Crimea. The sanctions restricted access to European and American capital markets by Russian financial, energy and defense businesses, an import and export ban on arms-trading, an export ban on dual-use goods, restricted access to sensitive technologies, and a restriction on services linked to oil production (Gros and Mustilli, 2016). These sanctions had an impact on the Russian economy, causing it to shrink by 1.5% in 2015, but which are still considered limited. In reality, the fall in oil price in 2015 had more impact on the Russian economy than the sanctions (Emmott, 2016). While the impact of these sanctions was limited, they have nevertheless put the Russian economy under pressure, but without influencing Russian policy regarding Ukraine.

5 Consequences

This section consists of proposing several measures that states could apply to decrease the potential impact of activities similar to the Ukrainian conflict occurring in cyberspace.

5.1 Raising awareness of propaganda and misinformation

Throughout the conflict, Russia has used a combination of cyber, EW, intelligence and kinetic capabilities to control communications inside Ukraine or from Ukraine (Giles, 2016b). This comprehensive approach needs to be acknowledged and understood in order to better counter it.

Based on this case, a primary danger was Russia’s focus on information warfare using propaganda, systematic internet trolling and misinformation. It is important that states admit that such cyber-activities may be less sophisticated technically than direct cyberattacks on critical infrastructures, but can also do a great deal of damage in society. This issue needs to be debated openly in the highest political circles in order to raise awareness among political leaders and society. As it is difficult for democracies to counter propaganda. Freedom of the press and free speech are significant democratic principles, but they also provide a space in which propaganda and misinformation can easily spread. Russian media outlets, like RT or Sputniknews, understand this vulnerability and exploit it.

In addition to an open debate on misinformation and propaganda, states can take other measures to mitigate their effects. In order to be effective, however, it is important that democracies truly understand the effects of propaganda and misinformation to be able to shape effective awareness programs. Such programs should explain to the population the difficulties surrounding information warfare. A government agency could warn domestic audiences about disinformation campaigns, give tips on how to detect them and denounce them, but must also integrate other actors, like the media. They should also clarify what trolls are and their role in propaganda operations (Tatham, 2015). Education and awareness campaigns can be designed to help the population to discern propaganda materials more easily and keep a more critical point of view toward what they read or watch. It would also be important for democracies to reveal and correct misinformation and inconsistencies in news in order to limit the effects of propaganda (Paul and Matthews, 2016).

5.2 Limit the dependence on foreign technology

The case of the Ukrainian conflict showed that the reliance on foreign technology to operate critical infrastructures could be fatal in case of conflicts. Therefore, when possible, it is important to keep the dependence on foreign companies for hardware or software to a minimum. Relying on foreign technology is problematic for security and logistic reasons. For example, the foreign supplier may have to travel to the country for maintenance or to update the product. During that time, the supplier might collect intelligence on how the product was used and its purposes. They might also be tempted to sell the information they collect to other states. It is better for a state’s security to produce hardware and software itself when it has the possibility and the capacity. When that is not possible, the state should set its priorities on the security aspects of such actions. Independent controls of the hardware and software should be run regularly, or inserted into foreign assets, to detect any real and perceived vulnerabilities left (intentionally or accidentally) by the supplier.
The fact that an important proportion of Ukrainians use email services provided by Russian companies also facilitated the intelligence collecting work of Moscow. The fact that foreign email services providers can easily read and save email discussions and information needs to be highlighted and explained to the users. Education and awareness campaigns could help to raise knowledge among the population the issue. Governments could also suggest domestic alternatives or encourage companies to develop them.

The physical attack on the Ukrainian communication infrastructure in Crimea underlined the fact that the protection of such infrastructures needs to be addressed in combination with cyber strategies. Especially that it has been reported that Russia showed interest in undersea internet cables, land telecommunication links and communication satellites. This particular attention could be for collecting intelligence on the vulnerabilities on the infrastructures themselves or to get access to the information that they transport (Giles, 2016b, pp. 11–13).

5.3 Leading by example against DDoS and website defacement

**DDoS attacks and website defacement** were often used during the Ukrainian conflict. These forms of attacks are only considered as cyber-disruptions, but can also be expensive for the victims. States should show by example in terms of website security, thereby reinforcing their credibility, and encouraging private actors to engage proper website security. It is also important for capable states to assist other actors who might be less capable of dealing with attacks on their own. A standard operating procedure could be created to guide businesses in case of DDoS or website defacement.

5.4 Monitoring of the evolution of the conflict

Western states are not direct victims of cyberattacks from either party of the conflict, but private companies or individuals may be indirectly affected. States that are active on the mediation scene in Ukraine through the OSCE might be specifically targeted. Their position increases the risks of becoming a victim of cyberattacks in the future. As a matter of a fact, the OSCE was targeted by a cyberattack allegedly perpetrated by “Fancy Bear” in December 2016 (BBC News, 2016b; “What Effect Will U.S. Sanctions Have On Russia?,” 2016). States should closely monitor the cyber-activities in the Ukrainian region to evaluate if the risks of direct and indirect cyberattacks on their infrastructures, individuals or businesses increase.

5.5 Confidence Building Measures (CBMs)

The promotion of **CBM** in cyberspace in times of peace and war could help to reduce uncertainties and misperceptions. Until now, States have only agreed that international law could apply to states’ activities in cyberspace, but **CBM** could help to increase trust and transparency among states in cyberspace. The difficulties of attributing actions to actors in cyberspace could raise ambiguities that lead to further international tensions. Clearer international protocols, agreements or guidelines negotiated in bi-lateral processes or in regional/international fora may help to mitigate such issues. 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).
- **Restraint measures** (e.g. pledge to remove incentives for first strike offensive or retaliation actions, exclude cyber offensive operations on third parties countries).

Such measures would also enhance cooperation among states resulting in greater dialog, which could also evolve into international norms or treaties. This could improve security in both cyber and physical realms (Brake, 2015; Farrell, 2015; Stauffacher and Kavanagh, 2013).
6 Annex 1

Non-exhaustive table of the different cyberattacks that happened in the Ukrainian “Euromaidan” protests and the conflict with Russia:

<table>
<thead>
<tr>
<th>Date</th>
<th>Victim</th>
<th>Type of victim</th>
<th>Alleged perpetrator</th>
<th>Technique/Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>07.11.2013</td>
<td>CCDOE website</td>
<td>IO</td>
<td>CyberBerkut or Anonymous Ukraine</td>
<td>DDoS (Carr, 2014)</td>
</tr>
<tr>
<td>15.11.2013</td>
<td>Ukraine Customs Services</td>
<td>G</td>
<td>Anonymous</td>
<td>Unspecified data breach (Kovacs, 2013a)</td>
</tr>
<tr>
<td>24-25.11.2013</td>
<td>Newspaper Ukrainka Pravda website</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>26.11.2013</td>
<td>TV channel Hromadske website</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>26.11.2013</td>
<td>News website censor.net</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>Wiped all information on the website (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>31.11.2013</td>
<td>Ukrainian Ministry of Internal Affairs website</td>
<td>G</td>
<td>Protesters of the “Euromaidan” movement</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>04.12.2013</td>
<td>Pro-Russian news website of Ukrainskaya Pravda</td>
<td>M</td>
<td>Pro-Ukrainian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>10.12.2013</td>
<td>Ukraine Brovary region website</td>
<td>G</td>
<td>Anonymous affiliated group called Clash Hackerz</td>
<td>Unspecified data breach and defacement (Kovacs, 2013b)</td>
</tr>
<tr>
<td>28.12.2013</td>
<td>Emails from the Ukrainian Volyn regional state administration website</td>
<td>G</td>
<td>Anonymous</td>
<td>Credentials and password to the email accounts obtained by a phishing campaign (Johnstone, 2013)</td>
</tr>
<tr>
<td>07.01.2014</td>
<td>Ukrainian TV 5 Channel News website</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>09.01.2014</td>
<td>The webpage maidan.ua.org</td>
<td>O</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>16.01.2014</td>
<td>Website of the Greek-Catholic Church in Ukraine</td>
<td>O</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>28.01.2016</td>
<td>Ukrainian TV channel website espresso.tv</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>31.01.2014</td>
<td>30 Ukrainian government and medi websites</td>
<td>G/M</td>
<td>Ukrainian neo-fascist party “Svoboda”</td>
<td>Defacement (Waqas, 2014)</td>
</tr>
<tr>
<td>11.02.2014</td>
<td>A regional office of the Ukrainian Democratic Alliance for Reform party</td>
<td>O</td>
<td>Anonymous</td>
<td>Unspecified data breach (Johnstone, 2014)</td>
</tr>
<tr>
<td>18.02.2014</td>
<td>Ukrainian members of Parliament’s cell phones</td>
<td>G</td>
<td>Unknown</td>
<td>Cell phones flooded by SMS to prevent them to use their phones (Weedon, 2015)</td>
</tr>
<tr>
<td>Date</td>
<td>Location</td>
<td>Actor</td>
<td>Method</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>03.2014</td>
<td>Ukrainian government’s website</td>
<td>G</td>
<td>Unknown</td>
<td>Shut down for 72 hours (Weedon, 2015)</td>
</tr>
<tr>
<td>03.2014</td>
<td>Ukrainian media outlets’ websites</td>
<td>M</td>
<td>Unknown</td>
<td>DDoS (Weedon, 2015)</td>
</tr>
<tr>
<td>03.2014</td>
<td>Ukrainian government’s network</td>
<td>G</td>
<td>Unknown</td>
<td>Snake malware (Sanger and Erlanger, 2014)</td>
</tr>
<tr>
<td>02.03.2014</td>
<td>Pro-Russian news website RT.com</td>
<td>M</td>
<td>Unknown</td>
<td>Defacement, replacing certain words by “nazi” (Perlroth, 2014)</td>
</tr>
<tr>
<td>04.03.2014</td>
<td>Ruptly (a video website part of RT)</td>
<td>M</td>
<td>Unknown</td>
<td>DDoS (Kovacs, 2014)</td>
</tr>
<tr>
<td>07.03.2014</td>
<td>The Kremlin’s website</td>
<td>G</td>
<td>Cyber Hundred or Null Sector or other pro-Ukrainian actor</td>
<td>DDoS (Maurer, 2015)</td>
</tr>
<tr>
<td>14.03.2014</td>
<td>Russian President’s website and Bank of Russia’s websites</td>
<td>G</td>
<td>Cyber Hundred or Null Sector or other pro-Ukrainian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>14.03.2014</td>
<td>Russian news portal lenta.ru</td>
<td>M</td>
<td>Cyber Hundred or Null Sector or other pro-Ukrainian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>16.03.2014</td>
<td>Several NATO websites</td>
<td>IO</td>
<td>CyberBerkut</td>
<td>DDoS (Bejtlich, 2015)</td>
</tr>
<tr>
<td>18.03.2014</td>
<td>Regional TV of Rivne in Western Ukraine</td>
<td>M</td>
<td>CyberBerkut</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>18.03.2014</td>
<td>Ukrainian news portal zik.ua</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>24.03.2014</td>
<td>7 million of credit cards</td>
<td>O</td>
<td>Anonymous</td>
<td>Data breach and leak (Passeri, 2014a)</td>
</tr>
<tr>
<td>03.04.2014</td>
<td>Website of the Coordination Council of Sevastopol</td>
<td>G</td>
<td>Pro-Ukrainian actor</td>
<td>Defacement and rerouting (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>04.04.2014</td>
<td>Websites of Ukrainian Main Prosecutor Office and of Ukrainian Ministry of internal Affairs</td>
<td>G</td>
<td>CyberBerkut</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>09.04.2014</td>
<td>Ukrainian Main Prosecutor’s Office’s webpage</td>
<td>G</td>
<td>CyberBerkut or other pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>09.04.2014</td>
<td>Ukrainian blog RoadNews</td>
<td>M</td>
<td>Pro-Russian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>10.04.2014</td>
<td>The Russian Lower Parliament Chamber’s (Duma) website</td>
<td>G</td>
<td>Pro-Ukrainian actor</td>
<td>DDoS (Ukraine investigations, 2014)</td>
</tr>
<tr>
<td>05.2014</td>
<td>Ukrainian Privatbank</td>
<td>O</td>
<td>CyberBerkut</td>
<td>Data theft (The Moscow Times, 2014)</td>
</tr>
<tr>
<td>25.05.2014</td>
<td>Ukrainian Central Election Commission’s website</td>
<td>G</td>
<td>CyberBerkut</td>
<td>Defacement and unspecified malware (Koval, 2015; Weedon, 2015)</td>
</tr>
<tr>
<td>26.07.2014</td>
<td>Email of the Ukrainian Colonel Pushenko</td>
<td>G</td>
<td>CyberBerkut</td>
<td>Data breach and leak (Passeri, 2014b)</td>
</tr>
<tr>
<td>09.08.2014</td>
<td>Regional department of the law enforcement in Dnepropetrovsk, Ukraine</td>
<td>G</td>
<td>CyberBerkut</td>
<td>Data breach and leak (Passeri, 2014c)</td>
</tr>
<tr>
<td>10.2014</td>
<td>Ukrainian Central</td>
<td>G</td>
<td>Unknown</td>
<td>DDoS (Martin-Vegue, 2015)</td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Actor A</td>
<td>Actor B</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>24.10.2014</td>
<td>City billboard in Kiev</td>
<td>G/O</td>
<td>CyberBerkut</td>
<td>Depiction of Ukrainian members of Parliament as war criminals (Lange-Ionatamishvili and Svetoka, 2015)</td>
</tr>
<tr>
<td>20-21.11.2014</td>
<td>Several Ukrainian governmental websites</td>
<td>G</td>
<td>CyberBerkut</td>
<td>Defacement of the websites with a message on Joe Biden being a fascist (Shevchenko, 2014)</td>
</tr>
<tr>
<td>2015</td>
<td>Bellingcat</td>
<td>O</td>
<td>APT28</td>
<td>Spear phishing campaign (Ashok, 2016)</td>
</tr>
<tr>
<td>02.01.2015</td>
<td>Ukrainian law enforcement and justice organizations</td>
<td>G</td>
<td>Anonymous</td>
<td>Data breach and leak (Passeri, 2015a)</td>
</tr>
<tr>
<td>27.02.2015</td>
<td>US Private military contractor involved in Ukraine, Green Group Defense Service</td>
<td>O</td>
<td>CyberBerkut</td>
<td>Access to information on the phones (Passeri, 2015b)</td>
</tr>
<tr>
<td>25.04.2015</td>
<td>Ukrainian government’s network</td>
<td>G</td>
<td>Unknown</td>
<td>Operation Armageddon malware (Bejtlich, 2015)</td>
</tr>
<tr>
<td>04-05.2015</td>
<td>Ukrainian Ministry of Defense</td>
<td>G</td>
<td>Unknown</td>
<td>Targeted intrusions into the network (Crowdstrike, 2016, p. 5)</td>
</tr>
<tr>
<td>13.10.2015</td>
<td>The Dutch Safety Board (investigative body for the crash of the flight MH17)</td>
<td>O</td>
<td>Allegedly APT28</td>
<td>Spear phishing and an another unspecified type of cyberattack (Foxall, 2016)</td>
</tr>
<tr>
<td>18.08.2015</td>
<td>Several Ukrainian websites</td>
<td>O</td>
<td>CyberBerkut</td>
<td>DDoS (Passeri, 2015c)</td>
</tr>
<tr>
<td>01.2016</td>
<td>Kiev Boryspil Airport</td>
<td>O/G</td>
<td>Unknown  (probably Russian group)</td>
<td>Similar to the malware from the power grid, probably “BlackEnergy3” (Bolton, 2016; Polityuk and Prentice, 2016)</td>
</tr>
<tr>
<td>02.2016</td>
<td>Bellingcat website and email from a Bellingcat journalist</td>
<td>O</td>
<td>CyberBerkut</td>
<td>Defacement and leak of document stolen from the journalist’s email account (Ashok, 2016; Crowdstrike, 2016, p. 5)</td>
</tr>
<tr>
<td>06.05.2016</td>
<td>Emails of Boris Dobrodeev, former boss of the Russian social network, vKontakte</td>
<td>O</td>
<td>Anonymous</td>
<td>Data breach and leak (Passeri, 2016)</td>
</tr>
<tr>
<td>05.2016</td>
<td>Alleged pro-Russian Ukrainian journalists</td>
<td>M</td>
<td>Myrotvorets a Ukrainian nationalist hacker group</td>
<td>Data breach and leak (Cimpanu, 2016)</td>
</tr>
<tr>
<td>07.2016</td>
<td>20 Russian organizations (governmental, scientific and defense institutions)</td>
<td>G</td>
<td>Unknown</td>
<td>Unspecific malware (BBC News, 2016c)</td>
</tr>
<tr>
<td>07.2016</td>
<td>Ukrainian artillery</td>
<td>G</td>
<td>APT28</td>
<td>Malicious application for Android and Apple smartphones that intercepts communications and gives away location of the users (Crowdstrike, 2016).</td>
</tr>
<tr>
<td>24.08.2016</td>
<td>Ukrainian Ministry of Defense and Ukrainian National Guard’s Twitter and Instagram accounts</td>
<td>G</td>
<td>Pro-Russian or Russian actor named “SPRUT”</td>
<td>Defacement of their Twitter and Instagram account (Starks, 2016).</td>
</tr>
<tr>
<td>08.2016</td>
<td>Alleged pro-Russian Ukrainian journalists</td>
<td>M</td>
<td>Myrotvorets a Ukrainian</td>
<td>Data breach and leak (Cimpanu, 2016)</td>
</tr>
<tr>
<td>Date</td>
<td>Organization</td>
<td>Group</td>
<td>Hacker group</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>25.10.2016</td>
<td>Surkov’s emails</td>
<td>G</td>
<td>CyberHunta</td>
<td>“special software” (Miller, 2016b)</td>
</tr>
<tr>
<td>11.2016</td>
<td>OSCE</td>
<td>IO</td>
<td>Allegedly APT28</td>
<td>Unspecified (BBC News, 2016b)</td>
</tr>
<tr>
<td>06-08.12.2016</td>
<td>Ukrainian Ministry of Finance</td>
<td>G</td>
<td>Unknown</td>
<td>DDoS attack in simultaneous to a breach into the system (Zetter, 2017).</td>
</tr>
<tr>
<td>06-08.12.2016</td>
<td>Ukrainian State Treasury</td>
<td>G</td>
<td>Unknown</td>
<td>DDoS attack in simultaneous to a breach into the system (Zetter, 2017).</td>
</tr>
</tbody>
</table>
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).

Botnet: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

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

Data breach: Event in which information of 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).

Euromaidan movement: Literally means “European Square” is a movement of protest in support of the European Union Association Treaty that was denied by former Ukrainian President Yanukovych (Chervonenko, 2013).

Hacktivism: use of hacking techniques for political or social activism (Ghernaouti-Hélie, 2013, p. 433).

Internet exchange point: facility that interconnects two or more independent internet networks in order to facilitate internet traffic (Internet eXchange Federation, n.d.).

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).

Firmware: A software program programmed on a hardware device providing the instructions for the device communication with the other hardware. The firmware is stored in the flash read-only memory of the device (TechTerms, 2016).

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

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).

Patriotic hacking: is also sometimes called nationalistic hacking. It is a group of individuals originating from a specific state and who engage in cyberattacks to defend against actors that they perceive to be enemies of their country (Denning, 2011, p. 178).

Payload: the malware harmful results (PCmag, 2016).

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).

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

Rootkit: program downloading itself in the infected system and taking control of certain functions (Lindsay, 2013).

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

SQL Injection: it is a cyberattack technique in which a malicious code is injected into code lines that will be executed by a SQL server (Microsoft, 2016).

Supervisory Control And Data Acquisition (SCADA): Computer programs used to control industrial processes (Langner, 2013, p. 9).

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).

Troll farm or factory: Place running round the clock to produce trolling messages and posts (Volchek and Sindelar, 2015).

Watering hole attacks: a targeted legitimate website is injected with a malicious code redirecting users to a compromised website infecting the users accessing it (TechTarget, 2015).

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

Worm: standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012).
8 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBM</td>
<td>Confidence Building Measures</td>
</tr>
<tr>
<td>CEC</td>
<td>Ukrainian Central Election Commission</td>
</tr>
<tr>
<td>CCDOE</td>
<td>NATO Cooperative Cyber Defence Centre of Excellence</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EW</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>FSB</td>
<td>Federal Security Service - Russia</td>
</tr>
<tr>
<td>GRU</td>
<td>Main Intelligence Directorate - Russia</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technologies</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>OSCE</td>
<td>Organization for Security and Co-operation in Europe</td>
</tr>
<tr>
<td>RAT</td>
<td>Remote Administration Tool</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>SQL</td>
<td>Search Query Language</td>
</tr>
</tbody>
</table>
9 Bibliography


Crowdstrike, 2016. Use of Fancy Bear Android malware in tracking of Ukrainian field artillery units.


Cyber and Information warfare in the Ukrainian conflict

Foxall, A., 2016. Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain.

F-Secure, 2014. BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks. F-Secure, Helsinki.


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


much-can-a-ddos-attack-cost-your-business/ (accessed 1.23.17).


Cyber and Information warfare in the Ukrainian conflict


r/identity-protection/what-is-rat/ (accessed 11.4.16).


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.