CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Synthesis 2017: Cyber-conflicts in perspective

Zürich, September 2018

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Marie Baezner

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; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Please cite as: Baezner, Marie (2018): Hotspot Analysis: Synthesis 2017: Cyber-conflicts in perspective, September 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

In 2016 and 2017, cyber-incidents made headlines around the world and increasingly represent a tool of choice for many actors. The ramifications of effective cyberattacks was on full display, from Russian meddling in the US presidential election to the crippling of the globe's largest shipping company Maersk through NotPetya malware. However, not all these events had the same political ramifications. In 2016 and 2017, we analyzed five cyber-related conflicts in Hotspot Analysis reports. This Hotspot Synthesis gives an overview of these five cases and identifies and analyzes trends and particularities observed in the five Hotspot Analysis reports.

This Hotspot Synthesis argues that cyber-conflicts, understood as the use of cybermeans in strategic contexts or political conflicts, are different from cybercrime due to their political components. Increasingly, states politicize, militarize and securitize cyberspace as a strategic domain. This trend was observed in several policy documents analyzed in the CSS Cyber Defense Project's National Best Practice Snapshots Handbook (see Dewar 2018a). The study showed that cybersecurity was increasingly taken into account at the policy and Grand Strategy levels. In addition, the strategic choice of targets and the strategic attribution are other political aspects of cybersecurity that reflect the increasing politicization of the subject. State actors' motives in cyberspace are very different than those of cybercriminals. State actors choose their targets for other reasons than pure economic gain. Strategic attribution of cyberattacks by the targeted state is also a political choice and can act as a means to many an end (e.g., deterrence, provoke a reaction). Though a politicization of cyberspace and cybersecurity issues was observed, the technical innovations in the cybersphere remained rather limited. Malware developers did not invent new special features, but instead spent resources in developing more effective vectors to deliver malware. In addition, even if malware could be adapted to cause more damage, perpetrators have often shown restraint in the extent of their attacks.

The use of cyberspace, and the political dimensions inherent in cyber warfare, is also highly dependent on the context. This Hotspot Synthesis identified three main categories of contexts based on the Hotspot Analysis reports: internationalized civil wars (Syria), asymmetric military operations between states (Ukraine), and strategic relationships between great powers (USA-Russia, USA-China and elections in Europe). The study showed that in each category, actors used different tools and techniques and targeted other types of objectives.

The analysis of Hotspots in 2016 and 2017 also shed light on the disagreements between states regarding legitimate and illegitimate uses of cyberspace in strategic interactions. Cyberspace crosses all political and legal principles of the use of force. Cyberattacks are used to target civilians and non-civilians, in peace and in war, domestically and internationally. The versatility of cyberattacks creates a particular challenge for states, as they attempt to find common understanding on many elements of cybersecurity. The lack of definitional consensus regarding cybersecurity issues works to heighten tensions between states when cyber-activities are in play, as well as heighten the risks of misperception. In Hotspot Analysis reports, we identified two major points of contention: intelligence and information warfare. The disagreement on intelligence is rooted in the perceived goal of cyberespionage. Some states see a difference between cyberespionage for economic purposes and cyberespionage for national security purposes. The lack of a common set of norms increased tensions between states and augmented the risk of misperceptions in their relations. Information warfare can cause further conflict when cyberspace is used to influence electoral campaigns in foreign states. While some states consider the use of cyberspace as a vector to influence their own or other states' political processes as legitimate, other states do not. The ambiguity around the appropriate use of cyberspace also strained relations between states.

This Hotspot Synthesis is the first document in a series of reports. The series will analyze various cyber-activities in the context of their political conflicts and strategic relationships, as well as highlight trends in the use of cybertools.

1 Introduction

Cybersecurity has attracted a lot of media attention in 2016 and 2017. The cyberattack on the US Democratic National Committee raised significant awareness on the issues of cybersecurity in democratic election processes. Similarly, two ransomware[1] attacks called Wannacry and NotPetya paralyzed thousands of computers around the world. While both events had huge media coverage, these attacks did not have the same political consequences. This difference shows that cyberconflicts[2] and cybercrime are in fact separate concepts, and need to be analyzed as such.

The Hotspot Synthesis 2017's scope is the five Hotspot Analysis reports published in 2016 and 2017, and the cyber-incidents that took place in that timeframe. The specific reports are as follows: Cyber-conflict between the United States of America and Russia (2017); Cyber and Information warfare in the Ukrainian conflict (2017); The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict (2017); Strategic stability between Great Powers: the Sino-American cyber Agreement (2017); and Cyber and Information warfare in the elections in Europe (2017).[3] The Hotspot Synthesis 2017 examines the overarching themes highlighted in these five reports. Therefore, it is recommended to read this Hotspot Synthesis after reading the five Hotspot Analysis reports.

The aim of a Hotspot Synthesis is to situate all the Hotspot Analysis reports from 2016 and 2017 in a global context. The goal is to identify trends and/or specific particularities observed in Hotspots and analyze these trends.

The Hotspot Synthesis 2017 is organized as follows. Section 2 examines the particularities that separate cyber-conflict from cybercrime. The section identifies that cyber-conflicts has political and national security dimensions that cybercrime does not. This section focuses on the political and strategic choices behind identifying targets for cyber-operations in democracies and autocracies and at the strategic choice of publicly attributing.

Section 3 demonstrates that the context in which cybertools and techniques are used matters. This section shows that cyberattacks are often employed in conjunction with other military means. The section also highlights that the choice to use cybertools and techniques is a strategic one, and is highly dependent on the specific context.

Section 4 reveals that a constant challenge in cybersecurity is the lack of agreement concerning definitions and legitimate behaviors in cyberspace. The cyber domain transcends traditional political and legal principles by ignoring previously set boundaries and norms. For instance, cybertools were used in times of peace and war, against civilians and combatants, as well as domestically and internationally. This section demonstrates this challenge by highlighting two major disagreements on the definitions of the legitimate use of cybermeans: concerning intelligence and concerning information warfare. The former is derived from a lack of common understanding over the definition of cyberespionage. The latter analyzes competing understandings of the use of cybermeans for information warfare.

[1] Technical words are explained in a glossary in section 8.

[2] In this report, the term "cyberconflict" is understood as the use and the role of cybermeans in strategic contexts and political conflicts.

[3] The reports are summarized in tables in Annex 2.

2 Beyond cybercrime: The politicization of cyberspace

Since the discovery of Stuxnet in 2010, cybersecurity has ceased to be an issue for technical experts and has shifted to the agendas of politicians. Shortly after the malware was uncovered, several states published or updated their national cybersecurity strategies. These actions indicate the growing politicization of cybersecurity. Furthermore, states increasingly consider cyberspace as a strategic domain; as such, responses to everyday threats like cybercrime must be distinct from retaliatory actions following state-related cyber-activities. With this priority shift comes a progressive securitization of cyberspace as well as an increasing militarization, as armed forces prepare to fight wars and defend themselves in cyberspace.

The politicization, securitization, and militarization of cyberspace, as well as the increasingly popular distinction between cyber-conflict and cybercrime were observed in several documents of the CSS Cyber Defense Project that revealed the following phenomenon:

- A study of cybersecurity and cyberdefense strategies shows that states are increasingly integrating cyber issues at the security policy level and the Grand Strategy level (Dewar, 2018a).[4]
- The choice of targets in cyber-conflict (critical infrastructures and other targets of high value) reflect the political and national security dimensions of cyber-conflicts that cybercrime usually lacks.[5]
- The choice of some political actors to publicly attribute cyberattacks to other nations reflects a readiness to take a stand and possibly face the consequences
- However, the types of tools and techniques used in cybercrime and cyber-conflict are very similar. Trend Analyses demonstrate that cyberweapons[6] were rarely used, a fact confirmed in observations made in Hotspot Analysis reports. Therefore, it is not the tools that help to differentiate between different cyberphenomenon, but the intent of the attackers and the choice of targets.

2.1 Integration of cybersecurity at the policy level

During the last ten years, states not only developed dedicated cybersecurity and cyberdefense strategies, but also integrated cyber-related issues into their national security policies. These developments demonstrate that states perceive cyber warfare as legitimate threats to their societies and their own existence (Hare, 2010): in short, as national security threats.

A study of national security, cybersecurity and cyberdefense strategies showed that cyber issues grew in importance to the point that they are discussed at the highest policy level. No longer is cybersecurity solely an issue for experts anymore. During 2016 and 2017, there was also a growing recognition among states that cybersecurity is no longer a purely a technical concept, but has become relevant to society, the economy and defense.

The study also revealed how states perceive cyberthreats at the policy level and how they react to them. It demonstrated that not all states integrate cybersecurity the same way: For some, it is clearly a civilian issue with some separated tasks for defense ministries. For others, the role of defense ministries for cybersecurity is weaved into national security structures. The study also revealed that states do not use the same vocabulary for cybersecurity, as some prefer to talk about “digital” technology and others about “cyber” technology (Dewar, 2018a).

2.2 Political and national security dimension

While cybersecurity is an increasingly influential issue at the security policy level, analyses must not confuse cybercrime with cyber-conflict. The difference between the two, apart from the intent of the attack, can be observed through 1) the strategic choices of targets - those public or private entities most affected by an attack - and 2) the calculated use of public attribution, with its inherent political challenges. Hotspot Analysis reports demonstrated that by the end of 2017, states and non-states actors had integrated cybermeans as optional tools for political conflicts and strategic contexts.

Strategic choice of target

In cybercrime, targets are chosen solely for their economic value (EY, 2014). This is not the case in cyber-conflicts or in strategic relationships where targets are chosen in accordance with broader strategic aims (apart from several cases of purely opportunistic attacks that happened in the context of the civil war in Syria (Baezner and Robin, 2017a)).

[4] For more information on the study of cybersecurity policies of various states, see National Best Practice Snapshots (Dewar, 2018a).

[5] This may depend on the country and if organized crime is involved in cybercrime.

[6] In this report, the definition of the term “cyberweapon” is based on Dewar’s definition: The user of a cybertool intends to cause damage and the capability of the cybertool is the cause of damage. Only when these two conditions are met can a cybertool qualify as a cyberweapon (Dewar, 2017).

The choice of target is also influenced by the purpose of the attack. If the perpetrator wants the cyberattack to remain undetected, the choice of targets and tools would be limited to those that would be less visible, or have a delayed or minimal effect. However, if the attacker wants its cyberattack to be known by the public, the choice of target and tools would lean towards a more visible and/or costlier vulnerability for the targeted state (Borghard and Lonergan, 2017; Libicki, 2009). The targets observed in Hotspot Analysis reports were classified into three categories: computer networks of state institutions (mostly targeted to gather intelligence, to find compromising information, or to protest against the state); media outlets (mostly targeted by distributed denial of service (DDoS)[7] attacks and website defacements to protest against something and/or promote a specific message); computer networks of non-state actors (mostly targeted to gather economic or national security intelligence) (Baezner and Robin, 2017a, 2017b, 2017c, 2017d, 2017e).

These types of objectives were targeted because their information assets or computer networks have strategic and political, not economic, value. The choice to target these particular entities reflects political considerations and decisions, which is consistent with the growing importance of cyber issues in politics. However, there are clear distinctions between the political contexts in democratic versus autocratic government systems.

Strategic attribution on the rise

Publicly attributing cyberattacks to a particular actor remains a core difficulty in cybersecurity, both for law enforcement and nation states. Attribution is mainly carried out by states, private cybersecurity companies or research institutes. Those are the actors that have the necessary resources to conduct a proper attribution investigation (Davis II et al., 2017; Rid and Buchanan, 2015). Importantly, complete and credible attribution in international politics needs to be supported by non-technical analysis and knowledge on the geopolitical context (Rid and Buchanan, 2015). This non-technical attribution is largely predicated on a logic that seeks to see who benefits from the cyberattack, also called "*cui bono.*" There is a possibility that technical evidence incriminating an actor may have been altered to specifically look like one particular actor is behind the cyberattack, thus falsely incriminating the group. It is also difficult to attribute a cyberattack to a specific state actor because states use proxy groups to perpetrate cyberattacks, giving them plausible deniability in case of discovery.

According to Edwards et al. (2017), the decision to publicly attribute depends on the vulnerability of the attacker, the victim's knowledge about this potential vulnerability, potential gains from the attribution, and the intensity of belief that the perceived attacker is indeed the perpetrator. What becomes increasingly clear from the emerging evidence, however, is that attribution is also a political choice. In other words, public attribution as an act of political communication (between the attributing state and the accused party as well as between the attributing state and its population) is an important aspect of the attribution itself. In the context of conflicts or strategic relationships, as seen in Hotspot Analysis reports, public attribution has political ramifications and comes with certain costs and benefits. A state can be blamed for a cyberattack to:

- provoke a reaction from the accused party;
- deter further attacks;
- warn perpetrators that there will be a response;
- warn other potential victims to take cybersecurity measures against a particular perpetrator;
- engage a discussion on norms;
- persuade international partners to support sanctions;
- mobilize citizens to support the government's actions;
- or raise awareness on cybersecurity among the population (Borghard and Lonergan, 2017; Davis II et al., 2017; Rid and Buchanan, 2015).

States can also choose *not* to publicly attribute a cyberattack (Davis II et al., 2017; Libicki, 2009). This decision may be made because states do not have the resources to conduct investigations leading to an attribution, do not consider their evidence sufficiently conclusive, or do not want to face public pressure to respond to the event. In addition, a public accusation could render attribution more difficult to perform in the future. Perpetrators of cyberattacks learn from publicly available attribution reports how to avoid such attribution in the future. Attackers could also become increasingly bold in their cyberattacks, if no retribution follows attribution (Davis II et al., 2017; Rid and Buchanan, 2015).

To be credible, attribution must be supported by strong technical evidence, as well as evidence from the intelligence community and political considerations. Furthermore, the attribution process needs to be sufficiently transparent in order to be credible. An observed problem is that states attribute cyberattacks, but do not disclose their evidence to protect sensitive sources and methods. This lack of transparency hinders the credibility of attribution and its effectiveness (Davis II et al., 2017).

[7] Abbreviations are listed in Section 9.

2.3 Little innovation in cyberweapons

The Hotspot Analysis reports show that actors in strategic contexts most often use commonly available cybertools that are also used by cybercriminals. This was particularly noticeable in the cases of Ukraine, Syria and China. The case of the Syrian civil war in particular illustrated how non-state actors used malware that was readily available online to spy on their adversaries (Baezner and Robin, 2017a; Galperin et al., 2013; Regalado et al., 2015; Scott-Railton, 2014; Scott-Railton et al., 2016). In a few Hotspots, notably China, publicly available malware was technically modified to perform additional tasks. Actors can also use combinations of available and customized malware in the same campaign (Baezner and Robin, 2017d; Novetta, 2014).

These observations demonstrate the growing difficulty in distinguishing state-sponsored acts, independent groups, and cybercriminals based on the tools and techniques alone. This is exacerbated by a recent trend identified by the Swiss Reporting and Analysis Centre for Information Assurance (MELANI), termed "cybercrime as a service" (Reporting and analysis centre for information assurance MELANI, 2017). Cybercriminals sell their services to other, more strategically inclined cyberattackers. It enables the client to have greater access to sophisticated cybertools and expertise for their cyberattack.

Even though the majority of malware analyzed in the Hotspot Analysis reports is easily available in the public domain, some older malware was modified to more effectively infect particular targets or avoid detection. Cybertools were primarily used to gather intelligence, and little physical damage resulted. As a cyberweapon by definition causes physical damage, it can be said that almost no cyberweapons were used in the context of conflicts and strategic relationships. This corroborates the findings of the CSS Cyber Defense Trend Analysis (Dewar, 2017) on cyberweapons. There it was also shown that cyberweapons have been rarely used. When they were deployed, cyberweapons constituted only minor tools in larger strategic conflicts. In the conflicts analyzed by the Hotspot Analysis reports, cyberweapons were used in only two occasions: in the Syrian civil war, and to gain strategic advantage in the rivalry between China and the USA (Baezner and Robin, 2017d, 2017a; Dewar, 2017). This lack of apparent innovation in malware development also indicates that skills and resources are applied not to malware development, but to the social engineering aspects of cyberattacks. Spear phishing emails and messages became more targeted, more precise, and more difficult to identify (Dewar, 2018b). The calculated and personalized attacks imply that perpetrators spent a large amount of time and resources to research their targets and adapt their spear phishing campaigns accordingly. This practice also differentiates state-sponsored actors from cybercriminals, who tend to use phishing in a more automated and indiscriminate manner.

There are a number of potential explanations behind the stagnant and relatively unsophisticated nature of popular cybertools. More advanced tools are expensive to develop, require comprehensive testing, and in many cases can only be used once. After an attack, there is a greater likelihood that the exploited vulnerabilities would have been discovered and patched (Axelrod and Iliev, 2014).

2.4 Restraint

The cases studied in the Hotspot Analysis reports demonstrate that while cybertools may appear to be an easily accessible tool with high disruptive potential, actors conducting cyberattacks show restraint in their use. This also indicates that there might be a widespread misperception in the nature and level of actual cyber risk. As cybertools are relatively easy and cheap to acquire, many states may be preparing for high impact cyberattacks. The reality shows that perpetrators used surprising restraint while conducting cyberattacks, by choosing to deploy easily available cybertools with low impact potential.

There are several possible reasons for this restraint: First, it could be due to a fear of escalation. Actors using such tools may have realized that proxy groups, and their cyberweapons, could prove difficult to control. Additionally, there would be a greater potential for misperception in cyberspace that could involuntarily prompt an escalation (Borghard and Lonergan, 2017). Furthermore, no state can ever be perfectly secure against cyberattacks. As such, the decision to invite retaliatory cyberattacks is not an easy one. Second, actors may have found cheaper ways to achieve their strategic goals. Sophisticated cybertools can be extremely costly to develop, to test, and to control. These tools also need to be used at specific times. If they were employed in the wrong context, the attack might cause an escalation. However, if cyberattacks were unduly delayed, the vulnerabilities that they seek to exploit might have been patched in the meantime (Axelrod and Iliev, 2014). Therefore, more conventional means could be advantageous in certain circumstances. Third, simplistic and unsophisticated cybertools may still be effective enough to gain strategic advantage without innovation. In some cases, the strategic goals of a cyberattack might be a low-intensity attack or a small disruption, and therefore such tools would be sufficient to achieve these objectives.

3 Context matters: Cybermeans are adjunct, not stand-alone

The Hotspots studied in 2016 and 2017 were very diverse, particularly in the type of conflicts. Despite the diversity, cybermeans were used in all of them. This confirms that cyberspace is of growing importance in the strategic domain.

Comparing these five cases highlights that cybertools were used in combination with other, conventional means. The choice to use cybertools depends on the resources available, the broader context and the way actors interact with one another beyond the cybersphere. Broadly speaking, the contexts examined in Hotspot Analysis reports can be categorized as the following: An internationalized civil war (Syria); an asymmetric military operation (Ukraine); or a strategic relationship between great powers (USA-Russia; Elections in Europe; and China-USA).

3.1 Internationalized civil war: Syria

The Hotspot Analysis report on the civil war in Syria showed that in that context, cyber-activities were primarily of low intensity. Cyberattacks consisted mainly of hacktivism, using DDoS attacks and website defacements against opposing groups and media outlets. The cybersphere proved a potent influence on public opinion and was used to protest against the Syrian government. There were also a few instances when malware was used to spy on members of anti-government groups. The goal of these infiltrations was to gather information on the structures and locations of the targets. While the attacks were effective in gathering intelligence, they did not cause any physical damage. This confirms that in the particular context of an internationalized civil war, cybermeans were used in complement with conventional means by all actors (Baezner and Robin, 2017a; Grohe, 2015).

3.2 Asymmetric military operation between states: Ukraine

The Hotspot Analysis report on the conflict in Ukraine showed that in that specific context, like in Syria, cyber-activities were of low-level intensity but peaked in intensity at critical moments of the conflict. In these cases, cyberattacks caused significant disruption and hardship against the intended target. For example, the Ukrainian power grid was infiltrated in December 2015, and power was cut for approximately 250,000 persons for several hours. There was also lasting damage to electric substations.

Cyber-activities in Ukraine were largely demonstrations by non-state actors on both sides acting in parallel to military operations. Cybermeans were used to influence public opinion largely through hacktivism, but malware was also used in combination with other conventional military means, including: to prepare the battlefield (i.e. a malicious Android application revealing the location of Ukrainian artillery units); and for sabotage (i.e. malware penetrations of power plants) (Baezner and Robin, 2017b; Crowdstrike, 2016; F-Secure, 2014).

3.3 Strategic relationship between powers: USA-Russia, Elections in Europe, and China-USA

In the context of strategic relationships between powers, cybermeans were used in conjunction with a number of different elements. Their primary use was for intelligence gathering, or for sowing disinformation and propaganda. However, cybermeans played a significant role in shaping these strategic relationships. In various instances, we see both their escalation potential and how states seek to mitigate this risk.

In the two cases of Russian election meddling, in the US presidential election and in Europe, cybertools were used to influence political opinions and undermine democratic processes. However, these cases also clearly show that it was difficult for Russia to anticipate and control the effects of their actions. From what is known about Russia's intentions, it seems likely the interferences failed to create the expected effects to have a US President friendlier to Russia and undermine US democracy. As a result, Russia is now even more isolated, faces additional economic sanctions and is confronted with heightened tensions with the West (Baezner and Robin, 2017c, 2017e; Thiessen, 2017).

In the Hotspot Analysis report on the strategic relationship between China and the USA, cybertools were mainly used for intelligence gathering, but notably also had a stabilizing effect on the relationship through the establishment of a bilateral agreement on cybersecurity. The two powers disagreed, however, on the use of cybermeans for intelligence purposes (mainly the gathering of material for economic purposes, versus the gathering of material for "purely" national security purposes). This led to a heightening of tensions between the two states until the 2015 Agreement, informed by the broader context of their sometimes strained relationship (see Baezner and Robin, 2017d; Brown and Yung, 2017a).

4 Determining the legitimate use of cybermeans: shaping behavioral norms

Given the growing focus on cybersecurity in political debates and the importance of the context surrounding the use of cybertools in conflict, the next challenge for states will be to define the line between legitimate and illegitimate cyberbehavior in strategic interactions.

Cybertools have been a challenge for the traditional political and legal principles that governed the legitimate use of force. Cybertools are used domestically and internationally, in times of war and in times of peace, and against both civilian and non-civilian targets. There is no commonly accepted definition for cyber-conflict among states, and no agreement on what behaviors are considered legitimate and illegitimate in cyberspace (Borghard and Lonergan, 2017). The definitional differences form the basis for consistent disagreement, and contribute to heightened tensions between states.

In addition to the complexities that arise from misattribution and the use of proxies, in order to create stability, states need to find common ground concerning norms for the use of cybertools in strategic contexts. This would enable states to move past the tit-for-tat logic that has characterized much of state-on-state cyberattacks, where states accuse each other of being perpetrators and victims successively.

The Hotspot Analyses showed the two main points of disagreement over the use of cybertools between states: China and the USA mainly disagreed on the use of intelligence that was gathered through cyberespionage, and the USA and European states disagreed with Russia on appropriate information warfare tactics.

4.1 Disagreements on the purpose of intelligence

China and the USA disagree sharply on the acceptable purpose of intelligence gathered through cyberspace. The USA draws a distinction between cyberespionage for economic purposes and cyberespionage for national security purposes, but China did (and probably does) not. National security justifications are tolerated by both states, though the USA considers economic cyberespionage highly illegitimate. (Harris, 2016). This difference in understanding increased tensions and risks of misperceptions in cyberspace between the two powers.

Edward Snowden's revelations on US mass surveillance of the internet created an opportunity for more dialogue between the two states. The USA justified its actions by stating that it was for national security purposes, and was therefore legitimate. China has always officially denied conducting cyberespionage, but it is an open secret that China used proxy groups to spy on adversaries (Borghard and Lonergan, 2017; Raud, 2016). Chinese cyberespionage was not limited to economic aims, but was also about ensuring strategic gains; Chinese firms are not separate from the state and stolen information could be used to help develop Chinese armaments or high-tech companies. China also complained about US soft power in Chinese political and social spheres and its potential destabilizing effects for the regime. It is partly the continuing fear of destabilization that pushed China to tightly control the content on the internet within its territory (Baezner and Robin, 2017d; Lindsay, 2015).

In a promising development, the two states were able to reduce tensions by establishing a bilateral agreement on cybersecurity to normalize the separation between cyberespionage for economic purposes from strategic cyberespionage and to reduce misperception in cyberspace. This agreement was signed in September 2015 and has since been implemented. An indirect goal for the US was also to push China to recognize the difference between economic and national security cyberespionage.

4.2 Disagreements on information warfare

Public outcry concerning the elections in the USA and in European countries demonstrates that there were significant disagreements between the West and Russia on the use of cyberspace in connection with information warfare. Russia, in its military doctrine, underlined the importance of using non-military means and tightly controlling the information space to gain advantage in conflicts (Nocetti, 2015). Russia is afraid of a potential domestic revolution, and therefore tries to dominate its domestic information space (Giles, 2012). At the international level, Russia \tried to influence elections in the West by spreading misinformation on the internet through Russian media outlets on anti-Russian candidates and publishing more favorable stories on pro-Russian candidates. The tactic also aimed to erode the credibility of democratic processes in the West by confusing the population on the veracity of news articles (Beuth et al., 2017).

The West interpreted Russia's attempts to influence their democratic processes and public opinion as a clear issue of national security. Russian actions were then automatically deemed an illegitimate use of cyberspace.

It seems like the Kremlin's efforts to influence Western elections did not work as intended. As a result of the cyber-campaign, Russia became more isolated

than before. Support for pro-Russian candidates did not prompt a thawing of US-Russian relations, and nowhere in the West did tensions ease after the elections. The USA did not reduce its commitment to NATO, and in fact, its members agreed to spend more in the name of defense. Additionally, Western public opinion became increasingly polarized toward the notion of Russian interference, and new sanctions were issued against Russia by Western states (Thiessen, 2017).

In this case, the disagreement could not be improved through an international agreement. It is also unlikely that this impasse will easily be resolved, as it reflects fundamentally different understandings of the role of cybersecurity. Whereas the West mainly considers the risks to its critical infrastructures and computer networks as the core issue, Russia and to some extent China have always considered information security "fair game" in international relations.

5 Conclusion

This Hotspot Synthesis is the first in a series of reports that are geared towards highlighting the most noteworthy trends in the use of cybertools in conflict situations and in strategic interactions more broadly. Our study reveals four main elements: First, public attributions by state actors have increased as a matter of political and strategic choice. Second, the cybertools and techniques used were not necessarily innovative and/or highly sophisticated, reflecting an overall poor state of information security in many networks. Third, cybermeans are never used as a standalone tool of war but always in conjunction with other means in existing conflictual contexts. Fourth, overall, the use of cybertools in conflict or strategic relationships shows a considerable level of restraint from all parties. All four elements together demonstrates how tightly connected cyber-operations are to their political contexts, and cyber issues need to be analyzed as such.

6 Annex 1

Table representing the chronology of all the cyber-related events observed in the five Hotspot Analysis reports.

Strategic stability between Great Powers: the Sino-American cyber Agreement	The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict	Cyber and Information warfare in the Ukrainian conflict	Cyber-conflict between the United States of America and Russia	Cyber and Information warfare in the elections in Europe

Date	Event
1996	China starts to set up its Great Firewall to control domestic traffic on the internet (Brown and Yung, 2017b).
2004	The Chinese cyberespionage campaign, Titan Rain, is discovered. The campaign was targeting the US Department of Defense and defense contractors (Homeland Security News Wire, 2005).
08.2008	Theft of US Presidential election campaign information by China.
03.2009	A cyberespionage campaign named GhostNet, targeting Tibetan activists and Non-Governmental Organizations, is revealed to the public (Kostadinov, 2013).
01.07.2009	Start of the US National Security Agency's (NSA) collection of stolen information by Chinese hackers on the US Department of Defense.
01.2010	Google, Adobe and other US Information technology firms announce that they were victims of a cyberespionage campaign from China named Operation Aurora (Zetter, 2010a). As a consequence, Google announced that it will not censor web research on google.cn (Zetter, 2010b).
11.02.2011	Discovery of the Chinese cyberespionage campaign Night Dragon against US critical infrastructures.
03.2011	24,000 sensitive files from a US defense contractor are stolen in a cyberespionage operation allegedly conducted by China (Jacobsson Purewal, 2011).
05.2011	The Syrian Electronic Army (SEA) launches its first cyberattack with a DDoS attack on OrientTV.
05.2011	Data theft by The Syrian Supreme Council of the Revolution of Assad's family emails.
05.2011	Data breach and spamming of opposition's Facebook pages by SEA.
16.05.2011-19.06.2011	Defacement of approximately a hundred of websites by SEA.
06.2011	Defacement and spamming of opposition's Facebook pages by SEA.
04.06.2011	Public internet access is shut down by the Syrian government (Blight et al., 2012).
24.06.2011	Defacement by SEA of the French Embassy to Syria's website.
30.06.2011	Discovery of the Chinese cyberespionage campaign, Byzantine Series, against US institutions.
07.2011	Defacement by Anonymous of the Syrian Ministry of Defense.
07.2011	Defacement by SEA of the University of California website.
23.07.2011	Data breach by SEA of Anonymous' social media website.
08.2011	The cybersecurity firm McAfee publishes a report revealing the Operation Shady RAT. It was a Chinese cyberespionage campaign targeting various industries worldwide (Alperovitch, 2011).
29.08.2011	Spamming and trolling by SEA of The Atlantic website.
30.08.2011	Defacement by SEA of the wrong Facebook page of Columbia university.
26.09.2011	Defacement by SEA of the Harvard university webpage.
12.2011	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).
02.2012	The Anonymous hacker group declares war against the Syrian regime and SEA.
02.2012	Infiltration of the text-message service of the Syrian national TV station Addounia by opposition forces.
02.2012	Defacement by SEA of Al Jazeera English.

28.02.2012	Defacement by SEA of Qatar Foundation Twitter account.
04.2012	Defacement by SEA of Al Arabyia Twitter account.
26.04.2012	Defacement by SEA of Linkedin blog website.
07.2012	Phishing campaign by SEA on Al Jazeera Twitter account.
07.2012	Data breach and leak of information by SEA of the opposition force.
07.2012	Data breach and leak of information by Anonymous against the Syrian Government.
03.08.2012	Phishing and defacement by SEA on Reuters' website and blog.
05.08.2012	Phishing and defacement by SEA on Reuters' website, blog and Twitter account.
06.08.2012	Defacement by the opposition forces on a Russian official's Twitter account.
09.2012	Phishing and defacement by SEA on Al Jazeera Arabic.
11.2012	Phishing campaign and use of RAT against opposition forces by an unknown actor.
29.11.2012-01.12.2012	The Syrian government shuts down the Internet for three days (Chulov, 2012).
01.2013	Phishing campaign and use of RAT against opposition forces by an unknown actor.
02.2013	The cybersecurity firm Mandiant publishes a report about the People's Liberation Army (PLA) unit 61398, which is responsible for cyber-operations on English-speaking victims (Raud, 2016).
03.02.2013	Data theft from the Ministry of Transport in Israel by SEA.
07.02.2013	Defacement by SEA of Sky News Arabia.
07.02.2013	Discovery of the Chinese cyberespionage campaign Operation Beebus against contractors of the US Department of Defense.
26.02.2013	Defacement by SEA of Agence France-Presse Twitter account.
03.2013	Phishing and defacement by SEA on The Daily Telegraph Twitter account.
01.03.2013	Defacement by SEA of Qatar Foundation Twitter account.
04.03.2013	Phishing and defacement by SEA on France24 TV Twitter account.
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).
17.03.2013	Defacement by SEA of Human Rights Watch website and Twitter account.
21.03.2013	Phishing and defacement by SEA on BBC Weather, BBC Arabic and BBC Ulster Radio Twitter accounts.
15.04.2013	Data theft and defacement by SEA on US National Public Radio website and Twitter account.
20.04.2013	Defacement by SEA on Gamerfood (software company) website.
20.04.2013	Defacement by SEA on CBS News Twitter account.
22.04.2013	Phishing and defacement by SEA on Sepp Blatter (former President of the International Federation of Association Football) Twitter account.
23.04.2013	Phishing and defacement by SEA on Associated Press Twitter account.
29.04.2013	Phishing and defacement by SEA on The Guardian.
05.2013	The US firm Network Solutions LLC seizes hundreds of Syrian websites' Domain Names of Syrian organizations including the SEA's website. The seizure takes place after US trade sanctions on Syria of 2012.
03.05.2013	Data theft by SEA on the Qatar Armed Forces.
04.05.2013	Defacement by SEA on E! Online Twitter account.
06.05.2013	Phishing and defacement by SEA on the Onion webpage and Twitter account.
17.05.2013	Phishing and defacement by SEA on Financial Times webpage and Twitter account.
24.05.2013	Phishing and defacement by SEA on ITV Twitter account.
25.05.2013	Compromising and defacement by SEA of the Sky News Android app.
06.2013	Repacking of the software Freegate by an unknown actor against the opposition forces.
06.2013	Edward Snowden, a former NSA contractor, leaks documents revealing the NSA's global mass cyber-surveillance program and its cyberespionage campaign Operation Shotgiant against the Chinese IT manufacturer Huawei. The campaign's objective was to prove a link between Huawei and the Chinese PLA (Brown and Yung, 2017c; Spiegel Online, 2014).
05.06.2013	Data theft by SEA from Turkish government's networks.
18.06.2013	Defacement by Jabhat al-Nusra Electronic Army (JNEA) of Syrian state-owned Addounia TV Channel website.
16.07.2013	Data theft by SEA of Truecaller (international telephone directory).

19.07.2013	Defacement by SEA on Reuters Twitter account.
21.07.2013	Data theft by SEA on Tango (video and text messaging service).
23.07.2013	Defacement by SEA on Daily Dot News website.
24.07.2013	Phishing and data theft by SEA on Viber (Telephone services).
08.2013	Data theft by Anonymous on SEA.
06.08.2013	Defacement by SEA on Channel4 Blog.
14.08.2013	Post of malicious link by Electronic National Defense Forces (ENDF) on an opposition's Facebook page.
15.08.2013	Phishing and defacement by SEA on Outbrain (advertising service).
20.08.2013	Defacement by ENDF on an opposition's Facebook page.
27.08.2013	Defacement by SEA on The New York Times website.
29-30.08.2013	Defacement by SEA on The New York Times website, the Huffington Post British website and the Twitter images (Twimg.com) website.
09.2013	Post of malicious link by an unknown actor against opposition forces.
02.09.2013	Defacement by SEA on US Marine Corp recruitment webpage.
11.09.2013	Defacement by SEA on Several Fox News Twitter accounts.
13.09.2013	Data theft by JNEA from a computer of a regional commander of the Syrian National Defense Forces.
14.09.2013	Post of a malicious link by an unknown actor against opposition forces.
30.09.2013	Defacement by SEA on the Global Post website and Twitter account.
10.2013	The Commander of the Iranian Cyber War Headquarters, the cyberunit of the Iranian Revolutionary Guard Corps is assassinated. He was suspected of working with SEA. The Israeli secret services, the Mossad, is accused by Iranian authorities (Grohe, 2015, p. 144).
07.10.2013	Phishing campaign by an unknown actor, possibly Al Nusra, against pro-opposition NGO.
14.10.2013	Phishing campaign by an unknown actor, possibly Al Nusra, against opposition forces.
21.10.2013	Hack by SEA on Qatar *Domain Name* System
28.10.2013	Defacement by SEA on the Organization for Action Gmail account.
11.2013	The Ukrainian President Yanukovych rejects the Association Agreement with the European Union. 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).
11.2013	Malware campaign by an unknown actor (possibly from Lebanon) against opposition forces, media activists, and humanitarian aid workers in Syria.
07.11.2013	DDoS attack by CyberBerkut against the NATO Cooperative Cyber Defence Centre Of Excellence website.
09.11.2013	Phishing and defacement by SEA on Vice webpage.
12.11.2013	Hack by SEA on Matthew VanDyke (US news reporter) Twitter account and email.
15.11.2013	Databreach by the Anonymous on the Ukrainian customs services.
15-18.112013	Defacement by SEA on Anti-Shabiha (Alawite militia) website.
24-25.11.2013	DDoS attack by a pro-Russian actor on the Ukrainian newspaper Ukraiska Pravda websites.
26.11.2013	DDoS attack by a pro-Russian actor on the TV channel Hromadske website.
26.11.2013	Information wiped by a pro-Russian actor on the news website censor.net
29.11.2013	Defacement by SEA on Time Magazine.
04.12.2013	DDoS attack by a pro-Ukrainian actor against the pro-Russian newspaper Ukrainskaya Pravda.
10.12.2013	Data breach and defacement by Clash hackerz, a group affiliated with Anonymous, against the website of the Ukrainian region of Brovary.
28.12.2013	Theft of login credentials by Anonymous of the email service of the Ukrainian Volyn regional state administration website.
2014	The cybersecurity firm CrowdStrike (2014) publishes a report on the PLA unit 61486, which has been held responsible for cyberespionage campaigns against aerospace industries in Europe and the USA.
01.01.2014	Phishing and defacement by SEA on Skype website, Facebook and Twitter accounts.
07.01.2014	DDoS attack by a pro-Russian actor against the Ukrainian TV5 Channel News website.
09.01.2014	DDoS attack by a pro-Russian actor against the webpage maidan.ua.org.

11.01.2014	Defacement by SEA on Xbox Twitter accounts.
15.01.2014	Hack by SEA of 15 Saudi government's websites and a state-owned Saudi magazine.
16.01.2014	DDoS attack by a pro-Russian actor against the website of the Greek-Catholic Church in Ukraine.
22.01.2014	Defacement by SEA on Microsoft Office blog website.
23.01.2014	Defacement by SEA on CNN Twitter account.
28.01.2014	DDoS attack by a pro-Russian actor against the Ukrainian TV channel website espresso.tv.
31.01.2014	Defacement by the Ukrainian neo-fascist party Svoboda on 30 Ukrainian government and media websites.
03.02.2014	Hack by SEA of Ebay website and Paypal website.
06.02.2014	Defacement by SEA on Facebook website.
11.02.2014	Data breach by the Anonymous on a regional office of the Ukrainian Democratic Alliance for Reform party.
14.02.2014	Phishing and defacement by SEA on Forbes website.
17.02.2014	Data theft by SEA of Forbes employees and users.
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 a return to the status quo prior to the constitution of 2004.
27-28.02.2014	Non-uniformed soldiers 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).
03.2014	Closure of the Ukrainian government's website for 72 hours by an unknown actor.
03.2014	DDoS attack on Ukrainian media outlets' websites by an unknown actor.
03.2014	Discovery of the Snake malware in the Ukrainian government's network.
02.03.2014	Defacement of the pro-Russian website RT by an unknown actor.
04.03.2014	DDoS attack on the RT video website Ruptly by an unknown actor.
11.03.2014	Repacking of the Psiphon software by an unknown actor against opposition forces.
12.03.2014	Hack and defacement by SEA on 3 FC Barcelona Twitter accounts.
07-14.03.2014	As retaliation for the invasion, various Russian websites are targeted by DDoS attacks (Ukraine investigations, 2014).
14.03.2014	Defacement by SEA on US Central Command.
16-18.03.2014	Various DDoS attacks on Ukrainian and Russian websites are reported (Ukraine investigations, 2014).
24.03.2014	Leak of credit card information by Anonymous.
26.04.2014	Defacement by SEA on RSA Conference website.
05.2014	Data theft by CyberBerkut on Ukrainian Privatbank.
05.2014	The US Justice Department indicts five PLA officers for cyber-enabled economic espionage (Gady, 2016).
06.05.2014	Defacement by SEA on The Wall Street Journal Twitter account.
24.05.2014	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 Computer Emergency Response Team (CERT) manages to remove the malware from the network in time for the election (Weedon, 2015).
18.06.2014	Hack by SEA of The Sun webpage and The Sunday Times webpage.
22.06.2014	Hack by SEA of Reuters' webpage.
30.06.2014	Defacement by SEA on Israel Defense Forces blog website.
04.07.2014	Defacement by SEA on Israel Defense Forces Twitter account.
26.07.2014	Data breach and leak of information by CyberBerkut on the email of the Ukrainian Colonel Pushenko.
09.08.2014	Data breach and leak of information by CyberBerkut on the Regional department of the law enforcement in Dnepropetrovsk, Ukraine.
10.2014	Several servers of the White House and the US Department of State are hacked (Perez and Prokupecz, 2015).
10.2014	DDoS attack by an unknown actor on the Ukrainian Central Election Commission's (CEC) website.
02.10.2014	Defacement by SEA on UNICEF Twitter account.

25.10.2014	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).
27.10.2014	Discovery of the Chinese cyberespionage group Axiom behind the Hikit campaign.
11.2014	Spear phishing campaign and malware, possibly by ISIS, against Citizen journalists posting on the website "Raqqah is being slaughtered silently".
20-21.11.2014	Defacement by CyberBerkut on several Ukrainian governmental websites.
27.11.2014	Disruption by SEA on Gigya comment system.
16.12.2014	Phishing and defacement by SEA on International Business Times website.
2015	Spear phishing campaign by APT28 against Bellingcat.
2015	Development of an internet surveillance tool by the Syrian regime against the opposition forces.
Early 2015	An unclassified network from the Pentagon is hacked (Crawford, 2015; Stewart, 2015).
01.2015	Defacement by the Cyber Caliphate against US Central Command Youtube and Twitter accounts.
02.01.2015	Data breach and leak by Anonymous against the Ukrainian law enforcement and justice organizations.
07-08.01.2015	The Ukrainian hacker group CyberBerkut launches a DDoS attack against the German government's networks. The attack is to protest against the visit of the Ukrainian Prime Minister to Germany (Stelzenmüller, 2017).
21.01.2015	DDoS attack by SEA against Le Monde website.
02.2015	Anonymous declares war against Islamic State in Iraq and Syria (ISIS) (Ruhfus, 2015).
10.02.2015	Defacement by the Cyber Caliphate against International Business Times website, Newsweek Twitter account and a subsidiary Newsweek Tumblr website.
12.02.2015	Defacement by SEA on the Syrian Observatory for Human Rights Facebook page.
27.02.2015	Data theft on phones of the US Private military contractor involved in Ukraine, Green Group Defense Service, by CyberBerkut.
09.03.2015	Discovery of the Chinese cyberespionage campaign against the University of Connecticut Engineering Department.
26.03.2015	China uses its Great Cannon against US websites for the first time. The targeted websites were monitoring the list of websites forbidden in China and proposing software to circumvent the Great Firewall.
30.03.2015	Hack by SEA of Endurance International Group INC (A world leader in web hosting service).
04.2015	The USA discovers that the Office of Personnel Management's (OPM) networks have been breached. The hack is attributed to China (Moreshead, 2017). After the OPM breach, the USA threatens China with economic sanctions and diplomatic measures (Brown and Yung, 2017c).
13.04.2015	Defacement by ISIS of Australian airport website.
25.04.2015	Discovery of the operation Armageddon in Ukrainian government's network.
04-05.2015	Targeted intrusions in the network of the Ukrainian Ministry of Defense by an unknown actor.
08.05.2015	The German Bundestag is the victim of a cyberattack in which approximately 16GB of data are stolen. The attack is attributed to the Russian hacker group APT28 who is also believed to have ties to the Russian military intelligence (GRU) (Le Miere, 2017).
14.05.2015	Defacement by SEA on the Washington Post.
15.05.2015	Discovery of the Chinese cyberespionage campaign against the Penn State Engineering branch.
08.06.2015	Defacement by SEA on US Army website.
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 Democratic National Committee (DNC) computer network (US Department of Homeland Security and Federal Bureau of investigation, 2016).
10.08.2015	Discovery of the Chinese cyberespionage campaign targeting the emails of top US national security officials.
18.08.2015	DDoS attack by CyberBerkut on several Ukrainian websites.
16.09.2015	Discovery of the Chinese cyberespionage campaign Operation Iron Tiger against US information technology, telecommunications, energy and manufacturing firms.
10.2015	Spear phishing campaign and malware by Group5 against opposition forces.
13.10.2015	Spear phishing campaign, probably by APT28, against the Dutch Safety Board (investigative body for the crash of the flight MH17).

08.11.2015	The Cyber Caliphate posted pro-ISIS messages, published passwords of 54,000 Twitter accounts (mostly based in Saudi Arabia) and phone numbers of the directors of the US Central Intelligence Agency (CIA), the US Federal Bureau of Investigation and the NSA.
23.12.2015	A cyberattack on the Ukrainian power grid leaves approximately 250'000 inhabitants without power for several hours (Zetter, 2016).
01.2016	Discovery of the same malware as in the Ukrainian power grid.
02.2016	Data theft and defacement by CyberBerkut of Bellingcat.
03.2016	A second hacker group, APT28, breaches the DNC computer network (US Department of Homeland Security and Federal Bureau of investigation, 2016).
03.2016	A member of SEA is arrested in Germany and is extradited in May 2016 to the USA (Cimpanu, 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).
06.05.2016	Data theft and leak of information by Anonymous from emails of Boris Dobrodeev, former boss of the Russian social network, vKontakte.
06.2016	The media reveal the DNC server breach. CrowdStrike suspects Russian hackers, with ties to their government, as the perpetrators (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 (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).
07.2016	A few days later, the Russian government announces the detection of a spying malware, affecting 20 different networks in Russian organizations (BBC News, 2016).
07.2016	Discovery of a malware from APT28 targeting Ukrainian artillery units.
15.08.2016	A hacker group, named Shadow Brokers, claims to have stolen data from the NSA. The stolen data, they declare, included various malware developed by the Equation Group, which they then put up for internet auction (Greenberg, 2016).
24.08.2016	Defacement of Twitter and Instagram accounts of Ukrainian Ministry of Defense and Ukrainian National Guard by a Pro-Russian or Russian actor named SPRUT.
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).
10.2016	The website of Macron's party, En Marche! (EM), is targeted by a cyberattack (Chebil, 2017).
09.10.2016	Wikileaks publishes Podesta's emails that were stolen during the DNC breach in March 2016.
25.10.2016	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).
31.10.2016	The hacker group Shadow Brokers publishes a list of servers hacked by the NSA between 2000 and 2010 (Goodin, 2016).
011.2016	Breach of the Organization for Security and Cooperation in Europe's network by APT28
08.11.2016	Donald Trump wins the US Presidential elections.
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).
06-14.12.2016	Several cyberattacks target Ukrainian banks, state agencies and ministries (Miller, 2016).
17.12.2016	Power goes out for an hour in the region of Kiev after a new cyberattack on the Ukrainian power grid (Goodin, 2017).
15.12.2016	The security firm Recorded Future discovers that the US Election Assistance Commission's network 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 did not have any ties to the Russian government (Menn, 2016).
14.02.2017	Emmanuel Macron's website was down for a while

06.03.2017	A 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).
05.05.2017	A few hours before the mandatory pre-vote campaign media blackout, a series of documents stolen from EM computers are released on the internet under the name of MacronLeaks (Untersinger, 2017).

7 Annex 2

Each table summarizes a Hotspot Analysis report:

Table summarizing the **Hotspot Analysis: Cyber-conflict between the United States of America and Russia**

Description	Tools and techniques	Spear phishing Remote Access Tools malware (XTunnel, Duke malware family) Disinformation
	Targets	US State institutions Democratic National Committee
	Attribution and Actors	Attacks attributed to APT28 and APT29 (Russian actors)
Effects	Social effects	Attempt to discredit and delegitimize US democratic processes by creating doubts and confusion within the population. Political parties are easy targets for cyberattacks. They have to prove that they are trustworthy to the public and have less protected networks than state institutions. The Democratic candidate, Hillary Clinton, was discredited as a trustworthy candidate. Doubts and confusion on the veracity of news and media. Harder to differentiate facts from fiction. US government showed that it was hard to find a right way to respond to cyberattacks.
	Economic effects	Very little direct economic impacts due to the cyberattacks during the US presidential election, only cybersecurity expenses to get rid of the intruders.
	Technological effects	Discussion to classify voting processes as critical infrastructures.
	International effects	Tit-for-tat logic in cyberspace between the USA and Russia. The situation in cyberspace between the USA and Russia could escalate, remain the same, or deescalate. Greater awareness that democratic processes can be targeted by cyberattacks. The cyberattacks that happened during the US presidential election prompted European states with upcoming elections to modify and further protect their democratic processes.

Table summarizing the **Hotspot analysis: Cyber and Information warfare in the Ukrainian conflict**

Description	Tools and techniques	Distributed Denial of Service attacks Website defacements Spear phishing	Malware (BlackEnergy, Snake, Operation Armageddon, X-Agent) Disinformation and propaganda
	Targets	Ukrainian institutions Ukrainian media outlets	Russian media outlets Russian institutions
	Attribution and Actors	Pro-Ukrainian hacker groups (Cyber Hunta, Cyber Hundred, Null Sector, Ukrainian Cyber Troops/Army) Ukrainian patriotic hackers	Pro-Russian hacker groups (CyberBerkut, APT28, APT29, Anonymous Ukraine, Quedagh) Pro-Russian trolls The Russian youth movement Nashi Russian patriotic hackers
Effects	Social effects	The Crimean population cannot access information not provided by Russia. Increasing mistrust from the Ukrainians in their government's capabilities to protect them against cyberattacks. Plausible deniability for states in their possible involvement in cyberattacks because of the use of independent hacker groups.	
	Economic effects	Costs caused by Distributed Denial of Service attacks and website defacements, as well as indirect costs caused by the cybersecurity response to the attacks. In addition, there were economic ramifications due to the damage done to businesses reputation. Costs due to damaged hardware after a malware attack.	
	Technological effects	Ukraine was highly dependent on Russian technology for telecommunications. This ensured Russia faced no real opposition while commandeering such facilities. The cyberattacks on the Ukrainian power grid damaged computers and electrical substations. All needed to be replaced. Discovery of new malware. The attacks on the Ukrainian power grid could have been a test for Russian cyber capabilities.	
	International effects	Tit-for-tat logic in cyberspace between Ukraine and Russia. However, the intensity of the cyberattacks remained rather low. Little help from Western states for Ukraine to fight pro-Russian groups. Use of information as a weapon in the conflict and at the international level.	

Table summarizing the **Hotspot Analysis: the use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict**

Description	Tools and techniques	Distributed Denial of Service attacks Website defacements Spear phishing Freely available malware (DarkComet RAT, njRAT, XtremeRAT, Backdoor.breut, ShadowTech RAT)	Customized malware Malicious Android application Disinformation and propaganda
	Targets	Syrian government institutions and pro-government groups Anti-government groups Islamist groups	Third party states Third party organizations Media outlets
	Attribution and Actors	Syrian government institutions and pro-government groups (the Syrian Electronic Army, the Syrian Malware Team, the Electronic National Defense Forces, a group from Lebanon, Group5 from Iran) Anti-government groups (the Supreme Council of the Revolution, the Free Syrian Army, the Hackers of the Syrian revolution) Islamist groups (the Cyber Caliphate, the cyberbranch of Jabhat al-Nusra, the cyberunit of Ahrar al-Sham) State actors (Iran, Turkey, Israel, Russia, the USA) Non-aligned groups (Anonymous, Oliver Tucket)	
Effects	Social effects	Influential propaganda from all groups to procure funding, to recruit, to influence public opinion and to discredit adversaries. Blurring of the line between combatants and non-combatants as anybody with an internet connection can take part in the propaganda campaigns, Distributed denial of Service attacks or website defacements. Increasing distrust among members of anti-government groups due to several defacements of social media profiles by pro-government groups.	
	Economic effects	Costs caused by Distributed Denial of Service attacks and website defacements, as well as indirect costs caused by the cybersecurity response to the attacks and damage done to the reputation. Drop in stock market caused by the defacement of the Twitter account of the Associated Press.	
	Technological effects	The Syrian government shut the internet down on more than one occasion during the conflict to prevent communications between anti-government groups. The cyberattacks were never technically sophisticated or of high intensity.	
	International effects	Internationalization of the conflict with targets and actors from all around the world. No escalation between states in cyberspace, but the use of cyberspace as additional domain to other military domains. Cyberspace was mainly used for preparing operations and psychological warfare. European states, the USA and the Arab League issued economic sanctions against the Syrian government.	

Table summarizing the **Hotspot Analysis: Strategic stability between Great Powers: the Sino-American Agreement**

Description	Tools and techniques	Distributed Denial of Service attacks through the use of the Chinese Great Cannon Spear phishing Remote Access Tools malware (Poison Ivy, Gh0stNet RAT, Zox, Hikit, Hydraq)
	Targets	Intellectual property from US private and public institutions Sensitive data from US public institutions Sensitive information from Chinese institutions
	Attribution and Actors	US National Security Agency Chinese Third and Fourth Departments of the People Liberation Army General State Department
Effects	Social effects	The USA tried to find the best way to answer Chinese cyberespionage. The USA indicted five members of the People's Liberation Army in 2014. China feared American attempts to interfere in its politics and criticizes the American use of soft power in China, as well as the US promotion of tools to circumvent the Chinese Great Firewall.
	Economic effects	The US institutions that were victims to Chinese economic cyberespionage evaluated the economic loss of the stolen intellectual property at US$ 300 billion per year.
	Technological effects	Loss of technological advantages for the firms that were victims of cyberespionage campaigns from either the USA or China. China and the USA try to restrict their domestic market and disincentive the use of the other's hardware and software technologies out of fear of backdoors.
	International effects	In September 2015, the USA and China agreed not to commit or support cyberespionage for economic purposes. The agreement reduced the increasing tensions between the two states, but in practice, it is still unclear if the scope or number of cyberespionage campaigns diminished. China sets Anti-Access/Areal Denial zones in the East and South China Seas. These zones were created to deny and deter adversaries from entering a particular zone. In these Anti-Access/Areal Denial zones, Chinese cybertools disrupt the adversaries' communications and GPS equipment. The USA feels particularly threatened by the Chinese Anti-Access/Areal Denial zones as they affect US force projection in the Asia-Pacific region. The USA developed strategies to counter Anti-Access/Areal Denial zones. Anti-Access/Areal Denial zones can also be used in cyberspace, when a state prevents access to cyberspace for another state. This can be done by disrupting the physical infrastructures of the internet. This situation is unlikely in the case of the China and the USA. It would prove extremely challenging for either party to disrupt all internet exchange points of the other state simultaneously. The situation in East and South China Seas also exacerbated tensions between China and its neighbors. Several of them are allies or partners of the USA and if the tensions escalate, it might drag the USA into a conflict with China. China criticizes American dominance in global internet governance. The USA wants to keep an open internet managed by the users. China wants to have a more state-oriented internet governance.

Table summarizing the **Hotspot Analysis: Cyber and Information warfare in the elections in Europe**

Description	Tools and techniques	Spear phishing Social bots Disinformation and propaganda
	Targets	Election candidates who positioned themselves for the European Union and for sanctions against Russia over Ukraine State institutions
	Attribution and Actors	Russia APT28 in the case of the MacronLeaks (was not officially attributed) Russian media outlets Trolls (Far-right and far left parties' sympathizers, pro-Russia sympathizers, US alt-right)
Effects	Social effects	European states' election processes were considered more resilient than the USA. European states have a more diverse political setting than the USA, and media are less polarized than in the USA. Discredit on democracy processes. European states took measures to mitigate the risks of cyberattacks during their elections. They put pressure on social media platforms to close fake accounts that amplified disinformation stories. Extremist party sympathizers were spreading disinformation campaigns. The situation prompts the question: are cyberattacks during elections becoming a norm?
	Economic effects	No direct economic effects.
	Technological effects	European states decided to abandon electronic solutions for elections and voting processes. The offer of fact-checking services increased in European states to counter disinformation campaigns.
	International effects	International cooperation between Western states against Russian interference. International cooperation among extremist parties' sympathizers to exchange materials and ideas for disinformation campaigns.

9 Glossary

Chinese Great Cannon: A Chinese technical weapon to hijack traffic to specific IP addresses to shut down websites and/or to change unencrypted parts of websites with malicious content (Marczak et al., 2015).

Chinese Great Firewall: Legal and technical measures to control the flow of information and access to websites for internet users in China (Wired Staff, 1997).

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

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

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

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

Ransomware: Malware that locks the user's computer system and only unlocks it when a ransom is paid (Trend Micro, 2017).

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

Social bots: Bot is a shorter term for robot. It is an automated program that runs routine tasks on social media but can also define fake social media accounts that are used to repost messages or news and/or to spam (Chu et al., 2012; Hegelich, 2016).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Website defacement: Cyberattack replacing website pages or elements by other pages or elements (Ghernaouti-Hélie, 2013, p. 442).

10 Abbreviations

CEC	Central Election Commission (Ukraine)
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency (USA)
DDoS	Distributed Denial of Service
DNC	Democratic National Committee (Political party in the USA)
ENDF	Electronic National Defense Forces (Pro-Syrian government group)
EM	En Marche! (French political party)
EU	European Union
ISIS	Islamic State of Iraq and the Levant (Syrian Islamist group)
JNEA	Jabhat al-Nusra Electronic Army (Syrian Islamist group)
MELANI	Swiss Reporting and Analysis Centre for Information Assurance
NATO	North Atlantic Treaty Organization
NSA	National Security Agency (USA)
OPM	Office of Personnel Management (USA)
PLA	People Liberation Army (China)
RAT	Remote Administration or Access Tool
SEA	Syrian Electronic Army (Pro-Syrian government)

11 Bibliography

Alperovitch, D., 2011. Revealed: Operation Shady RAT (White Paper). McAfee, Santa Clara, CA.

Axelrod, R., Iliev, R., 2014. Timing of cyber conflict. Proc. Natl. Acad. Sci. 111, 1298–1303. https://doi.org/10.1073/pnas.1322638111

Baezner, M., Robin, P., 2017a. Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict.

Baezner, M., Robin, P., 2017b. Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict.

Baezner, M., Robin, P., 2017c. Hotspot Analysis: Cyber-conflict between the United States of America and Russia.

Baezner, M., Robin, P., 2017d. Hotspot Analysis: Strategic stability between Great Powers: the Sino-American cyber Agreement.

Baezner, M., Robin, P., 2017e. Hotspot Analysis: Cyber and Information Warfare in elections in Europe.

BBC News, 2016. Russia cyber attack: Large hack "hits government" [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-36933239 (accessed 31.10.16).

Beuth, P., Brost, M., Dausend, P., Dobbert, S., Hamann, G., 2017. War without blood [WWW Document]. Zeit. URL http://www.zeit.de/digital/internet/2017-02/bundestag-elections-fake-news-manipulation-russia-hacker-cyberwar/komplettansicht (accessed 03.10.17).

Blight, G., Pulham, S., Torpey, P., 2012. Arab spring: an interactive timeline of Middle East protests [WWW Document]. The Guardian. URL https://www.theguardian.com/world/interactive/2011/mar/22/middle-east-protest-interactive-timeline (accessed 24.02.17).

Borghard, E.D., Lonergan, S.W., 2017. The Logic of Coercion in Cyberspace. Secur. Stud. 26, 452–481. https://doi.org/10.1080/09636412.2017.1306396

Brown, G., Yung, C.D., 2017a. Evaluating the US-China Cybersecurity Agreement, Part 3 [WWW Document]. The Diplomat. URL http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/ (accessed 10.07.17).

Brown, G., Yung, C.D., 2017b. Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity [WWW Document]. The Diplomat. URL http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/ (accessed 10.07.17).

Brown, G., Yung, C.D., 2017c. Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace [WWW Document]. URL http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ (accessed 10.07.17).

Chebil, M., 2017. Quels risques de piratage pèsent sur la présidentielle française ? [WWW Document]. Fr. 24. URL http://www.france24.com/fr/20170113-quels-risques-piratage-pesent-presidentielle-francaise-anssi-cyber-attaques-russie (accessed 16.08.17).

Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S., 2012. Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? IEEE Trans. Dependable Secure Comput. 9, 811–824. https://doi.org/10.1109/TDSC.2012.75

Chulov, M., 2012. Syria shuts off internet access across the country [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2012/nov/29/syria-blocks-internet (accessed 24.02.17).

Cimpanu, C., 2016. Syrian Electronic Army Hacker Pleads Guilty to Online Extortion Charges [WWW Document]. Softpedia. URL http://news.softpedia.com/news/syrian-electronic-army-hacker-pleads-guilty-to-online-extortion-charges-508804.shtml (accessed 13.02.17).

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

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 25.10.16).

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

CrowdStrike Global Intelligence Team, 2014. CrowdStrike Intelligence Report: Putter Panda. CrowdStrike.

Davis II, J.S., Boudreaux, B., Welburn, J.W., Aguirre, J., Ogletree, C., McGovern, G., Chase, M.S., 2017. Stateless Attribution Toward International Accountability in Cyberspace. Rand Corp.

Dewar, R.S., 2018. National Best Ptractice Snapshots, Working Paper (May 2018).

Dewar, R.S., 2018b. Trend Analysis: Contextualizing Cyber Operations. Cyber Defense Project 19.

Dewar, R.S., 2017. Trend Analysis: Cyberweapons: Capability, Intent and Context in Cyberdefense. Cyber Defense Project 24.

Edwards, B., Furnas, A., Forrest, S., Axelrod, R., 2017. Strategic aspects of cyberattack, attribution, and blame. Proc. Natl. Acad. Sci. 114, 2825–2830. https://doi.org/10.1073/pnas.1700442114

EY, 2014. Cyber threat intelligence: how to get ahead of cybercrime.

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

Gady, F.-S., 2016. The China-US Cyber Spying Deal: Where Are We Now? [WWW Document]. China-US Focus. URL http://www.chinausfocus.com/peace-security/the-china-us-cyber-spying-deal-where-are-we-now (accessed 07.06.17).

Galperin, E., Marquis-Boire, M., Scott-Railton, J., 2013. Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns. Electronic Frontier Foundation.

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

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. Hackers trigger yet another power outage in Ukraine [WWW Document]. Ars Tech. URL http://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/ (accessed 19.01.17).

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 02.11.16).

Gordon, M.R., 2014. NATO Commander Says He Sees Potent Threat From Russia [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2014/04/03/world/europe/nato-general-says-russian-force-poised-to-invade-ukraine.html (accessed 18.11.16).

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 25.10.16).

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

Hare, F., 2010. The cyber threat to national security: Why can't we agree?, in: Conference on Cyber Conflict: Proceedings 2010. Cooperative Cyber Defence Centre of Excellence, Tallinn, pp. 211–225.

Harris, E., 2016. Comparing Cyber-Relations: Russia, China, and the U.S. [WWW Document]. Mackenzie Inst. URL http://mackenzieinstitute.com/comparing-cyber-relations-russia-china-and-the-u-s/ (accessed 20.09.17).

Hegelich, S., 2016. Invasion of the social bots.

Homeland Security News Wire, 2005. The lesson of Titan Rain: Articulate the dangers of cyber attack to upper management [WWW Document]. Homel. Secur. News Wire. URL http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management (accessed 03.08.17).

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 24.10.16).

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 16.12.16).

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

Jacobsson Purewal, S., 2011. 24,000 Pentagon Files Stolen in Major Cyberattack [WWW Document]. PCWorld.com. URL http://www.pcworld.com/article/235816/Pentagon_Files_Stolen_in_Major_Cyberattack.html (accessed 07.06.17).

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 08.11.16).

Kostadinov, D., 2013. GhostNet – Part I [WWW Document]. Infosec Inst. URL

http://resources.infosecinstitute.com/ghostnet-part-i/#gref (accessed 07.06.17).

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 08.11.16).

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 25.10.16).

Le Miere, J., 2017. France is latest in long list of countries that have allegedly had elections hacked by Russia [WWW Document]. Newsweek. URL http://www.newsweek.com/russia-election-hacking-france-us-606314 (accessed 11.07.17).

Libicki, M.C., 2009. Sub Rosa Cyber War. Cryptol. Inf. Secur. Ser. 53–65. https://doi.org/10.3233/978-1-60750-060-5-53

Lindsay, J.R., 2015. The Impact of China on Cybersecurity: Fiction and Friction. Int. Secur. 39, 7–47. https://doi.org/10.1162/ISEC_a_00189

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 05.12.16).

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 10.03.17).

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R.J., Paxson, V., 2015. China's Great Cannon [WWW Document]. Citiz. Lab. URL https://citizenlab.ca/2015/04/chinas-great-cannon/ (accessed 19.07.17).

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 21.12.16).

Martin-Vegue, T., 2015. Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it [WWW Document]. CSOonline.com. URL http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html (accessed 17.11.16).

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 27.10.16).

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 16.12.16).

Miller, C., 2016. Ukraine Searches For Culprit After Cyberattacks On Finance Ministry, Treasury [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/ukraine-cyberattacks-finance-ministry-treasury-infrastructure-russia/28172004.html (accessed 20.01.17).

Moreshead, C., 2017. The Next Step in US-China Relations: Norms in Cyberspace [WWW Document]. China-US Focus. URL http://www.chinausfocus.com/peace-security/the-next-step-in-us-china-relations-norms-in-cyberspace (accessed 07.06.17).

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

Novetta, 2014. Operation SMN: Axiom Threat Actor Group Report. Novetta.

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 25.10.16).

Raud, Mi., 2016. China and Cyber: Attitudes, Strategies, organisation. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Regalado, D., Villeneuve, N., Scott-Railton, J., 2015. Behind the Syrian conflict's digital front lines, Special Report. FireEye Inc., Milpitas, CA.

Reporting and analysis centre for information assurance MELANI, 2017. Information Assurance: Situation in Switzerland and internationally - Semi-annual report 2016/II (July-December) (Semi-annual situation report). MELANI, Bern.

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 25.10.16).

Rid, T., Buchanan, B., 2015. Attributing Cyber Attacks. J. Strateg. Stud. 38, 4–37. https://doi.org/10.1080/01402390.2014.977382

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 25.10.16).

Ruhfus, J., 2015. Syria's Electronic Armies [WWW Document]. Al Jazeera. URL http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html (accessed 13.02.17).

Scott-Railton, J., 2014. Maliciously Repackaged Psiphon Found [WWW Document]. Citiz. Lab. URL https://citizenlab.org/2014/03/maliciously-repackaged-psiphon/ (accessed 21.02.17).

Scott-Railton, J., Abdulrazzak, B., Hulcoop, A., Brooks, M., Kleemola, K., 2016. Group5: Syria and the Iranian Connection [WWW Document]. Citiz. Lab. URL https://citizenlab.org/2016/08/group5-syria/ (accessed 14.02.17).

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 04.11.16).

Spiegel Online, 2014. NSA Spied on Chinese Government and Networking Firm [WWW Document]. Spieg. Online. URL http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html (accessed 14.07.17).

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 25.10.16).

Stelzenmüller, C., 2017. The impact of Russian interference on Germany's 2017 elections [WWW Document]. Brookings. URL https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/ (accessed 01.10.17).

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 01.11.16).

Thiessen, M.A., 2017. Putin's interference in our election clearly backfired [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/opinions/putins-interference-in-our-election-clearly-backfired/2017/08/03/32fa548c-77be-11e7-9eac-d56bd5568db8_story.html?utm_term=.a01909f69b9a (accessed 13.11.17).

TrendMicro, 2017. Ransomware [WWW Document]. TrendMicro. URL https://www.trendmicro.com/vinfo/us/security/definition/ransomware (accessed 19.02.18).

Ukraine investigations, 2014. Cyber Wars: The Invisible Front [WWW Document]. Ukr. Investig. URL http://ukraineinvestigation.com/cyber-wars-invisible-front/ (accessed 17.11.16).

Untersinger, M., 2017. « MacronLeaks » : ouverture d'une enquête judiciaire en France [WWW Document]. Le Monde. URL http://www.lemonde.fr/pixels/article/2017/05/06/macronleaks-debut-d-un-long-et-fastidieux-travail-d-enquete_5123577_4408996.html?xtmc=cyber_attaque&xtcr=11 (accessed 26.09.17).

US Department of Homeland Security, Federal Bureau of investigation, 2016. GRIZZLY STEPPE – Russian Malicious Cyber Activity (No. JAR-16-20296).

Weedon, J., 2015. Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 67–77.

Windrew, R., 2016. Payback? Russia gets hacked, revealing Putin aide's secrets [WWW Document]. CNBC. URL http://www.cnbc.com/2016/10/28/payback-russia-gets-hacked-revealing-putin-aides-secrets.html (accessed 03.11.16).

Wired Staff, 1997. The Great Firewall of China [WWW Document]. WIRED. URL https://www.wired.com/1997/06/china-3/ (accessed 19.11.17).

Zetter, K., 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid [WWW Document]. Wired. URL https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed 23.11.16).

Zetter, K., 2010a. Google Hack Attack Was Ultra Sophisticated, New Details Show [WWW

Document]. Wired. URL https://www.wired.com/2010/01/operation-aurora/ (accessed 13.07.17).

Zetter, K., 2010b. Google to Stop Censoring Search Results in China After Hack Attack [WWW Document]. Wired. URL https://www.wired.com/2010/01/google-censorship-china/ (accessed 13.07.17).

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.