CSS CYBER DEFENSE PROJECT

Trend Analysis

Contextualizing Cyber Operations

Zürich, June 2018

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

CSS
ETH Zurich

ETH zürich

Author: Dr. Robert S. Dewar

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: Robert S. Dewar (2018): Trend Analysis: Contextualizing Cyber Operations, May 2018, Center for Security Studies (CSS), ETH Zürich.

Contents

Executive Summary

Political and academic analyses of cyber operations provide extensive data on the actors conducting them, the tools they deploy and the methods or vectors they use to achieve their goals. These three aspects constitute the "who", "what" and "how" of cyber operations. Less attention is paid to the socio- and geopolitical contexts in which cyber operations occur – the "when" aspect. By examining a series of well-publicized cyber incidents, as well as drawing on current cyber security and defense policy and academic literature, this Trend Analysis provides a contextualization of some of the most high-profile incidences of the use of cyber operations. It is important to note, however, that this Trend Analysis does not address cyber-crime. Instead, the focus is on cyber operations in international relations.

The analysis identified five distinct socio- and geopolitical contexts in which cyber operations regularly occur. These are: open international conflict; civil war; political tension; economic tension and strategic rivalry. In international conflicts cyber operations occur as part of military campaigns, deployed as governments and commanders see fit in order to achieve tactical or military strategic objectives. In civil wars, such as that occurring at the time of writing in Syria, cyber operations including disinformation campaigns, hacktivism and recruitment have been undertaken by both sides in order to further wider social and political goals. In situations of interstate political tension, such as that observed between Russia and Estonia in the early 2000s, cyber operations can be used in attempts to destabilize one or other of the states involved. This was the case with the distributed denial of service (DDoS) operations experienced by Estonia in 2007. Cyber operations in the context of economic tension have been found to include state-sponsored or supported cyber-crime activities, such as the theft of money or information from central banks, a feature of (alleged) North Korean cyber operations. The analysis found that operations occurring in the contexts of political and economic tension generally take place where there is an asymmetry between the states involved. The final context identified shows that cyber operations occur in situations of strategic rivalry, where the states involved share relative political, economic and military parity and conduct cyber espionage or target government networks. The cyber operations occurring between the US and China serve as examples of this. Within these five distinct contexts, actors of all persuasions and motivations utilize any and all cyber tools at their disposal to achieve their ends, taking advantage of any weaknesses or vectors of attack that they can find.

In addition to identifying these five contexts, two important trends were identified during the analysis. The first addresses a temporal aspect of the "when" question – at what point in a conflict or rivalry do cyber operations take place? It was found that such operations do not occur at a critical juncture in a given sociopolitical context. For example, an international conflict does not have to reach a certain point before cyber operations are deployed. Rather, there is a continuous undercurrent of activity in cyberspace between the actors involved, much of which is low level.

The second trend identified is that there are very few large-scale cyber incidents taking place. This finding runs counter to much of the rhetoric emanating from the media and policy publications about the imminent outbreak of a cyber war or cyber Pearl Harbor. While major and destructive incidents do occur – such as Estonia 2007 or the deployment of Stuxnet – operations of this scale are relatively rare. A degree of strategic restraint is therefore advisable and possible on the part of the victim given the constant level of activity occurring in the background.

The exercise of identifying and codifying these five contexts, and placing them alongside the actors, tools and vectors utilized in cyber operations, is beneficial to academics and policy-makers because it provides a clearer picture of when and how cyber incidents occur: what are the possible combinations of actors, tools and vectors, and in what contexts do these combinations occur? What this codification does not do, however, is provide a typology of cyber incidents, or facilitate the prediction of when cyber operations are likely to occur. The almost continuous use of such operations makes predicting their use in any given context difficult if not impossible. No two cyber operations are the same and competent actors will utilize whatever tools and vectors get the job done. What this Trend Analysis does do, however, is highlight the need for holistic, resilience-based cyber security and cyber defense policies in order to address the multiple combinations of contexts, actors, tools and vectors that are possible.

Disclaimer

The data for this Trend Analysis was drawn from available open-source material which is of great value but is also problematic. Many incidents, both in the private and public sector, go unreported due either to their classified targets or fear of reputational damage. As a result, building a complete data set of international incidents is challenging. The incidents catalogued here are already in the public domain and are well documented in cyber security and defense literature. Extensive use was made of empirical Hotspot Analyses produced by the Center for Security Studies. As a result, the data set to be presented here is representative, but nevertheless comprehensive enough to draw the conclusions presented in the Trend Analysis.

1 Introduction

In 1993 Arquilla and Ronfeldt (1993) proclaimed that cyberwar was coming, a statement which has become a popular refrain among military strategists and government policy-makers. The prophesied cyberwar did not appear, however, and the debate is still ongoing as to whether such a situation will occur (Junio, 2013; Rid, 2012; Stone, 2013). From an academic perspective this debate is far from settled. However, the empirical reality facing policy-makers and legislators is that cyberspace *is* being considered as an operational arena. It is being used for strategic, tactical and political ends. Weaponized software such as viruses, worms and specially written pieces of code (Dewar, 2017) are being deployed with increasing frequency and increasing effectiveness.

It is therefore becoming commonplace for international and regional conflicts, political and economic tensions or strategic rivalries to include a digital or cyber component. These cyber operations have a number of important characteristics: they demonstrate ever-increasing technical capabilities on the part of the actors who use them; the technological sophistication of the tools themselves is becoming more and more advanced; and the number of actors who have access and recourse to those tools is also growing. Furthermore, as shown by the deployment of Stuxnet in 2010, cyber operations have evolved to the point where their deployment can have physically destructive consequences. As a result, there is a growing body of evidence pointing to the effective use of cybertools and cyberweapons by technologically advanced state and non-state actors and to the growing use of automated systems such as botnets to perpetrate large-scale digital disruption (Dewar, 2017; Goldman, 2012; Patterson, 2017; Rowe, 2012). Targets for such operations range from national critical infrastructures such as energy and communications networks to the hearts and minds of opponents through sophisticated cyber-influence campaigns. Recent studies analyzing the increasing numbers of cyber-competent actors, the increasing technical sophistication of malicious digital tools they are using and the vectors they exploit – the “who”, “what” and “how” of cyber operations – have shown that they are increasing in number and complexity. There has been a quantitative and qualitative growth in the numbers of attackers (who), the use of machine learning to perpetrate attacks (what) and the number of failures and systemic weaknesses that they can exploit (how).

What is absent from much of this commentary, particularly in the policy-development sphere, is a contextualization of the incidents in which cyber-operations occur: in what geo- or socio-political circumstances are cyber operations taking place? Are they stand-alone events or are they one part of a larger, ongoing conflict or incidence of strategic rivalry? Are they internal to a particular state or region - such as in a civil war - or are cyber operations being deployed in international conflicts between sovereign states? This is the "when" question – when do cyber operations occur?

The goal of this Trend Analysis is to supplement the “who”, “what” and “how” of cyber operations by answering this "when" question, providing the geo- and socio-political context in which cyber-operations occur. The examination of data gathered using a series of high-profile case studies, relevant academic literature, policy analyses and private sector reports demonstrates that cyber operations occur within five socio-political contexts:

1. Established international conflict;
2. Internal civil war;
3. Political tension between states;
4. Economic tension between states;
5. As a feature of wider strategic rivalry.

The Trend Analysis also examines another, temporal, aspect to this "when" question: at what point in any of these particular contexts do cyber operations occur? Do actors begin using cybertools at the commencement of, for example, a civil war or tension due to economic competition, or are they used as tools once a conflict or strategic rivalry becomes established? In seeking to answer this question the Trend Analysis identified two trends. The first is that there is an ever-present undercurrent of small-scale, low-level cyber operations occurring at all points in a given socio-political context. There is no critical point in a conflict or civil war at which cyber operations begin to be used by one or both sides. Instead, all sides deploy their full range of cyber capabilities, be that influence operations such as fake news or election manipulation or larger scale, more destructive acts such as those targeting critical national infrastructure.

The second trend is that there are very few major cyber incidents. For the purposes of this Trend Analysis a “major cyber incident” is one which could be classified as an armed attack under international law. According to the Tallinn Manual, in order to meet this qualification, the cyber operation or tool used must have the same destructive capability or effect as a conventional, kinetic operation (Schmitt, 2013). Very few of the incidences examined in this Trend Analysis meet this criterion. This demonstrates the trend for the constant undercurrent of cyber operations to be one of low-level, almost background operations.

The trends identified in the contextualization of cyber operations have important consequences for the development of defense and security policy. It makes predicting or prognosticating on the likely point at which cyber operations will occur almost impossible. If such operations are conducted at any and all points in a conflict or rivalry, then it is not possible to identify

markers or signs pointing to an imminent cyber operation. The anonymizing effects of the cyber domain and the speed at which cyber capabilities can be deployed further complicate this predictive activity. Nevertheless, the findings set out in this Trend Analysis should facilitate policy decisions regarding resource allocation and management as well as the development of resilient infrastructures.

The Trend Analysis will proceed as follows. The following section will briefly set out which actors, techniques and vectors are most commonly identified in cyber operations; this will establish the "who", "what" and "how" of such operations. The third section will focus on a number of important events in the historiography of cyber conflict. This examination will show that these events can be divided into the five socio- and geo-political contexts of open international conflict, internal civil war, political and economic tension and strategic rivalry. Throughout this analytical section, extensive use will be made of specialized, empirical Hotspot Analyses produced by the Center for Security Studies. The fourth section of the Trend Analysis will set out the two important trends discernable in this analysis and contextualization, while the fifth and final section will provide conclusions of use to practitioners and policy makers.

2 Actors, Technologies and Vectors: the "who", "what" and "how" of cyber operations

Due to the ubiquitous nature of the Internet and the ease with which information and tools can be shared the number of actors involved in malicious cyber incidents is increasing year on year. Not only are criminal actors increasing in number, but so too are incidents alleging state involvement. There are two sides to such involvement. On the one hand, state actors such as security agencies and military personnel, are engaging in cyber operations. This was the case in such incidents as the deployment of Stuxnet in 2010 and the ongoing Sino-American rivalry (Baezner and Robin, 2017a). In both of these contexts, government agencies are conducting cyber operations either to hinder rival activities (Stuxnet) or to gain a strategic or competitive advantage over their rivals (the Sino-American situation). On the other hand, non-state actors are increasingly being identified engaging in activities designed to have an effect at the national, state level. Analyses of the Syrian conflict, elections in European Union Member States between 2015 and 2017 and the conflict between Russia and Ukraine have shown that non-state actors supporting one or other side in a conflict have the capability and willingness to engage in sophisticated cyber campaigns with national consequences.

The increasing number of actors and level of resources at the state level are also translating into an increase in the sophistication of the tools and techniques being deployed. The digital payloads of cyberweapons have increased to the point where such devices can cause physical damage (Dewar, 2017). This was the case in 2010 when the aforementioned Stuxnet worm caused Iranian nuclear enrichment centrifuges to spin out of alignment and be damaged beyond repair. While the attack vector was alleged to have been "low tech" – an infected USB stick was used to cross the air gap in the enrichment facility's computer network – Stuxnet's payload demonstrated that the technological sophistication of cyberweapons has crossed from the digital to the real world, with real world applications. During the Russo-Georgian conflict of 2008, Georgian government and military communications were targeted as part of the Russian military's offensives, with the intention of disrupting the enemy's capacity to co-ordinate and respond effectively to a ground assault.

Not only are such tools having real-world effects, the technology has progressed to the point where effective attacks are being undertaken at the national level using automated systems. In 2007 Estonia suffered a series of sustained distributed denial of service (DDoS) attacks. According to Gaycken (2011, p. 110), these attacks were conducted using networks of infected computers – botnets – to flood Estonian servers with requests for information. These large botnets were able to sustain the DDoS requests for a period of several weeks through extensive use of automation.

There is evidence, however, of the involvement of both state and non-state actors in non-state activities. Recent analyses of North Korean, Chinese and American cyber operations highlight not just routine or commonly expected intelligence-gathering activities, but also point to increasing evidence of industrial or corporate espionage. State security and military agencies are deploying tools to enable a country to gain an edge in an increasingly competitive global economy. This shows that the gap between malicious state and corporate activities is closing and beginning to cross over. This has implications not only for securing digital assets against concerted attempts at intrusions but also for legislators and policy-makers who will need to develop legal and policy responses to state institutions engaging in corporate and/or commercial malicious activities.

Despite the increasing complexity of the relationships between state and non-state actors, the activities in which they engage and the increasing sophistication of the tools they are deploying, the vectors used by malicious actors to effect these operations center on exploiting systemic weaknesses in network architectures and digital systems. Hack records – lists of known and identified software vulnerabilities – can be found online. These are exploited due to the time delay between identifying the vulnerability, software developers issuing a corrective patch and end-users installing the patch. Zero-day exploits – where the vulnerability is unknown to developers and users – also remain a popular entry point for cyber operations (Ablon and Bogart, 2017). Such software vulnerabilities are not the only vectors for successful malicious cyber operations, however. Large scale data thefts, such as the theft of 3million user accounts from the PlayStation network in 2011, can be used to extract security information for further thefts or identity breaches. Cyber sabotage operations, such as the ransomware NotPetya (Henley and Solon, 2017), can also be conducted to hinder or prevent the use of networked systems, causing large-scale disruption.

The most popular vector for malicious intrusions remains, however, the human factor. Successful phishing campaigns, insecure passwords, oversharing of personal information on social media and the use of USB memory sticks remain popular methods for inserting malware into secure networks (as was the case with Stuxnet) or extracting personal, proprietary or classified data.

The examination of the technology used by actors undertaking cyber operations and the vectors used to deploy those tools also points to some areas where current vulnerabilities are being identified but could increase in the future. As more and more

everyday devices are being connected to the Internet, the absence of a systemic security architecture and infrastructure in the emergent Internet of Things (IoT) makes this phenomenon an attractive target, particularly for criminal activity. Incidents such as TRITON, where a Trojan horse was used to install malware in Schneider industrial control software used in critical infrastructures (Hay Newman, 2018; Johnson et al., 2017), demonstrate that the wired world may be moving from a position of hyper connectivity to one of hyper vulnerability. The drive to connect critical national infrastructures such as utilities and transport to the Internet could serve to increase the vulnerability of those critical assets.

This examination shows that the range and interrelation of actors, technologies and vectors is both large and complex. The main issues are summarized in Table 1 below. There are two features of this tabulation which are immediately clear. The first is that a typology or correlation between actors, technologies and vectors is not possible to produce. Particular actors do not employ particular tools in a particular manner. Malicious actors develop bespoke solutions for their activities, seeking to use the tool and vector best suited to their specific needs. This will make predicting the precise combination of actors, tools and vectors challenging for defenders. The second feature highlighted by this tabulation is that very little contextualization in academic or policy analyses of when such tools and vectors are utilized. This raises the question: in which socio- or geo-political contexts do cyber operations and incidents take place? In short, we know the "who", "what" and "how", but not the "when".

Table 1: Summary of Actors, Technologies and Vectors of Cyber Operations

Actors	Technologies	Vectors
• Quantitative and qualitative growth of attackers • Robotization/automation of attackers (attacker is an algorithm) • Intensification of use of cyberweapons (loss/removal of all constraints) • Privatization of security and intelligence (dependence and loss of state sovereignty and of individuals) • State actors involved in non-state activities	• Machine learning, Artificial Intelligence etc. (towards technological singularity) • Multiple failures discovered and exploited early or late • "Hack record" of objects and services that are acquired and/or used	• Human failure (cyber influence) • Sabotage (as per NotPetya) • Large scale data theft (weak clouds) • Absence of IoT security (higher probability of large scale attacks) • From hyper connectivity to hyper vulnerability (as per TRITON) • CIAAT – Critical Infrastructure as a target • SAAT – Security as a target

3 Providing context: When do cyber operations occur?

One of the most significant contexts in which cyber operations occur is criminal activity. The Hackmageddon aggregator[1] posts data on a full range of incidents and, statistically speaking, the vast majority intrusions, extractions and deployments of malware occur with the object of criminal gain. However, a sizeable minority of incidents occur with socio- or geopolitical objectives. This section of the Trend Analysis will explore and set out these non-criminal contexts.

Three of the cyber incidents with the highest profile and greatest impact in the historiography of cyber security and cyber conflict occurred within a span of only three years. These were the Estonian DDoS intrusions of 2007, the use of cyber operations in combat during the Russo-Georgian conflict of 2008 and the discovery of the Stuxnet worm and its effects in 2010. While these incidents raised the profile of cyber operations in the public and political consciousness and raised the bar for the impact of malicious cyber activities, these incidents also provided non-anecdotal evidence of state involvement and activities in cyber conflicts.

These incidents also shared one important feature: they were not isolated or standalone events. Each of the three incidents occurred within or as part of a specific, ongoing geopolitical context. The DDoS attacks on Estonia in 2007 were part of an escalation in political tension between Estonia and Russia. This tension reached a diplomatic zenith with the decision of the Tallinn city council to move a Soviet war memorial from the center of that city to its outskirts. This decision sparked an angry response from Russians living in Estonia and from the Russian government.

In 2008 Russia and Georgia were engaged in a military conflict over the disputed region of South Ossetia. The use of cyber operations in this conflict is well documented. Of interest is the fact that these operations were put to direct strategic use. They were designed to weaken the Georgian government and military's resolve and ability to communicate just prior to a Russian conventional campaign. In this sense cyber operations were used in much the same way as an artillery bombardment prior to an infantry maneuver. The context here is that cyber operations were used as part of a state military's arsenal during an open international conflict.

Finally, the Stuxnet worm was deployed to halt or at least hinder the Iranian nuclear weapons program. Although it was not part of an existent international conflict as was the case Georgia, the Stuxnet deployment was part of ongoing political tension between the US and Iran.

The point here is that these three incidents occurred within two types of recognizable and identifiable geopolitical context. The Georgian incident occurred within the context of an open international conflict, while the DDoS attacks on Estonia and the deployment of Stuxnet occurred within the context not of conflict but high political tension. This implies that cyber incidents, at least those which do *not* have criminal gain as their objectives, do not occur in a vacuum. They are not isolated, standalone events but are part of a longer, larger chronology or context. By analyzing the events and political landscapes surrounding the various events outlined in Sections 1 and 2 of this Trend Analysis, it is possible to identify a total of five distinct socio- and geopolitical contexts.

3.1 Context 1: Open International Conflict

This is perhaps the least surprising socio- or geopolitical context in which to find instances of cyber operations. Governments and militaries have always used the latest tools, techniques and capabilities to gain a tactical or strategic advantage over an adversary in a military conflict. In 2008 Russia and Georgia engaged in such a military conflict. As part of their military campaign, Russian forces targeted Georgian communications networks in order to restrict that state's ability to use the Internet, both to coordinate their forces but also to restrict the Georgians' capacity to communicate with the international community (Hagen, 2013, p. 196). The vectors and techniques involved included DDoS attacks and website defacement, techniques similar to these deployed against Estonia a year earlier. By 2008, however, these techniques were more robust and sophisticated, indicating a degree of maturation. Of particular note is that the cyber component of Russian operations took place a matter of weeks before land and air assaults (Joyner, 2012, p. 161).

Another international conflict in which cyber operations played a prominent role was that between Russia and Ukraine which began in earnest in 2013. Both sides in the conflict deployed cyber tools and undertook cyber operations (Baezner and Robin, 2017b). DDoS campaigns, patriotic hacking and the propagation of malware was undertaken by both pro-Russian and pro-Ukrainian actors.

Setting aside the fact that Russia appears as an actor in both instances, and also setting aside the fact that state authorization or involvement in these operations cannot be definitively or categorically proven

[1] www.hackmageddon.com

due to the attribution problem, cyber operations are being routinely used in interstate conflicts, and used to good effect. However, the conflicts in which cyber operations take place need not be inter-state. As evidenced by the large-scale use of hacking tools, data breaches and website defacement in the Syrian conflict, cyber operations are also a significant component of intra-state civil wars.

3.2 Context 2: Civil War

The ongoing conflict in Syria provides an example of an internal, civil conflict which combines both conventional, kinetic hostilities between the actors involved and extensive use of cyber operations. The conflict itself arose as one of a series of violent and non-violent anti-government actions in the Middle East between 2010 and 2012, known collectively as the Arab Spring. In the Syrian situation, the Arab Spring manifested itself as a series of protests against the government of Bashar al-Assad which escalated into a full-scale civil war between numerous anti-government actors and the Syrian military loyal to Assad. The cyber component of this internal conflict consisted of social media propaganda campaigns, website defacements and limited cyberespionage activities (Baezner and Robin, 2017c, p. 6).

While cyber activities were conducted by both sides in the conflict, the majority of operations were conducted by pro-regime actors such as the Syrian Electronic Army. The Syrian government itself carried out the interception of email communications and on at least two occasions shut down the Internet itself in Syria. Nevertheless, anti-government actors such as the Free Syrian Army and Hackers of the Syrian Revolution were able to utilize online capabilities to infiltrate government communications networks and to promote their respective causes, publish details of alleged government atrocities and as platforms for recruitment (Baezner and Robin, 2017c, p. 11).

Two aspects of the Syrian conflict are of particular note. First, while the kinetic aspect of this context was largely contained within Syria's borders[2], the cyber component of this conflict spilled over to have effects outside the country. Not only did this involve internal actors targeting external entities such as media outlets unsympathetic to one side in the conflict or the other, it also included external actors such as US citizens targeting pro-regime networks to render cyber aid to the insurgents (Baezner and Robin, 2017c; Grohe, 2015). Cyber operations have therefore become an important feature of the Syrian civil war, and it is not unreasonable to assume that such activities will be a key facet of other such internal conflicts should they occur in the future.

The second aspect of note is that cyber operations were used throughout the conflict, and are still being employed by both sides. The fighting did not reach a certain point or critical mass after which the use of cyber tools became a viable option. Almost from the commencement of the Arab Spring, cyber tools and operations were used by all sides to gain followers, spread dis- or misinformation or attempt to gain tactical advantages over adversaries.

Cyber operations are not only being conducted as part of a physical, kinetic conflicts, however. Although the Estonian DDoS attacks of 2007 were described in some circles as an act of state-on-state aggression, armed conflict between Russia (the alleged perpetrator) and Estonia did not occur. Although relations between these two countries at the time could not have been described as warm, there was no open military conflict. There was, however, a situation of severe political tension.

3.3 Context 3: Political tension

As discussed above, the background to the DDoS attacks on Estonia in 2007 was grounded in a cooling of relations between that country and Russia which reached a low-point following the city of Tallinn's decision to move a Soviet-era memorial to the Second World War. The ensuing weeks of DDoS attacks on Estonian government and banking systems was and is still seen as the first incidence of state-on-state cyber-attacks in the public domain. While this cannot be categorically verified[3], the key point here is that, despite the hostile political relationship between the two states, the cyber activities were not part of, or a precursor to, any kind of conventional warfare such as the use of ground troops or airborne assaults, as would be the case a year later in Georgia. The cyber operations were, however, part of a continuous state of distrust, suspicion and diplomatic tension on the parts of these two states. Relations have waxed and waned between Estonian independence from the USSR but the underlying political tension has not improved.

The same can be said of the USA's relationship with Russia. Since 2008 allegations have ping-ponged back and forth regarding state or state-sanctioned cyber operations on both sides of the Atlantic. These operations and allegations reached a high point during the 2016 US elections, when allegations were made of Russian interference in that election with the goal of encouraging a victory for Donald Trump. Investigations into these allegations are still continuing, but the point here is that the simmering undercurrent of political tension, distrust and malicious cyber activity has

[2] Setting aside the humanitarian and refugee crises which occurred in neighbouring countries such as Turkey.

[3] Due to the attribution problem

continued but not escalated to the point of kinetic conflict.

Those cyber operations occurring in the context of political tension need not be limited to hacktivism or political interference, but can have concrete effects. Such an example is the political context in which the Stuxnet worm was deployed. In 2002 President George W. Bush declared Iran to be part of an "axis of evil" alongside North Korea and Iraq. Since that time, concerns were raised in the international community when the Iranian government confirmed that they were enriching uranium at Natanz for civilian purposes. Such an activity is one of the initial steps towards developing nuclear weapons. The international community, led by the US, sought to pressure Iran into abandoning its nuclear program. This political context led to the development of alternative measures to halt or hinder that program. In 2010 the Stuxnet worm was found to have infected a large number of devices world-wide, but 60% of these were located in Iran (Baezner and Robin, 2017d), and the majority of those locations were in supervisory control and data acquisition systems (SCADA) associated with nuclear enrichment centrifuges. It is noteworthy that one of the most sophisticated cyber operations, one which involved a cyberweapon causing physical damage, was not deployed as part of an open international conflict but in the context of a political tension. In this context, cyber operations need not therefore be restricted to propaganda and influence campaigns or espionage. They can include actions which have kinetic, real world, destructive consequences.

Tension between states is not restricted to political interaction, however. It occasionally manifests itself in commercial and industrial competition, i.e. as *economic* tension. This is the fourth geo-political context in which cyber operations take place.

3.4 Context 4: Economic Tension

Competition for resources and markets for trade has been a feature of international conflict and diplomatic tension for centuries. In the 21st century such economic considerations are becoming more complex due to the highly interrelated and interdependent nature of globalized commerce. Ideologically opposing states nevertheless trade openly with each other.

However, the ubiquitous nature of the Internet and online commercial activity means that inter-state economic tensions are also manifesting as (alleged) direct theft of resources, not just the acquisition of proprietary data. This is particularly the case where there is a distinct asymmetry in political, economic or military capabilities and capacities. The relations between the US and the Democratic People's Republic of Korea (DPRK) serve as an example of this. Despite the DPRK government's rhetoric, it is fair to assume that US political, economic and military capabilities far exceed those of North Korea. Nevertheless, there is a concerted cyber campaign being conducted by DPRK agents. A forthcoming study of DPRK cyber operations has identified a number of campaigns designed to achieve direct, discreet thefts of funds from national central banks (Baezner and Robin, In Press, p. 11). Hacker groups with alleged links to the North Korean government conducted a number of spear-phishing attacks targeting financial institutions with the objective of long-term infiltration, not just one-off "heists".

Such activities are difficult to corroborate or confirm with information in the public domain. What *can* be confirmed is the monetary impact of such economic tension, particularly in the case of alleged Chinese activities against the US. Although figures for Chinese financial losses due to cyber industrial espionage are difficult to acquire, a US Intellectual Property Commission report estimated the US and Western losses to be around $300bn per year (Kihara, 2014). It should be pointed out, however, that this figure includes losses attributed to cybercrime, a phenomenon deliberately omitted from this Trend Analysis. Nevertheless, the nature of the economic tension between these and other important commercial states is such that the line between state-sponsored cyber espionage targeting foreign industries and criminal activity is becoming increasingly blurred thanks to the anonymizing effect of cyberspace. While it is fair to say that competition for resources and markets is manifesting itself in cyber operations, it remains to be seen whether such economic tension will escalate. Thus far, in the economic context, the incidents and incidences of cyber operations have remained an action apart from activities which could have political or military ramifications.

3.5 Context 5: Strategic Rivalry

The final context in which cyber operations can be frequently observed and which have an effect is in strategic rivalry between major international powers. Strategic rivalry differs from political and economic tension in that the latter is symptomatic of asymmetric interstate relationships. Rivalry by contrast emerges where there is a level of parity between the states in either the political, economic or military spheres. It involves states with similar levels of international influence and similar capacities for exercising that influence. A rivalry is described by Vasquez (1993) as:

> "A relationship characterized by extreme competition, and usually psychological hostility, in which the issue positions of contenders are governed primarily by their attitude towards each other".

This means that, while not engaging in military hostilities, relations between rival states remain cold with a number of actions carried out by both sides as they jockey for position in a given situation. The relations between China and the US provide an effective example of such strategic rivalry. Both states have a degree of parity in political, economic and military capabilities and power. They are the two largest economies in the world, both have large military resources and both are recognized nuclear powers. While not engaged in direct military action against one another, both states are targeting the same developing markets in South and South-East Asia and Africa (Reynolds, 2015).

In terms of cyber operations Baezner and Robin (2017a) describe the relationship between China and the US, for example, as one replete with diplomatic spats, proxy confrontations, antagonistic messages and tit-for-tat acts of malicious cyber activity. Such activities in cyberspace this situation has been in existence at least since the initiation of China's so-called "Great Firewall" in 1996 (Brown and Yung, 2017). The cyber activities themselves involved primarily cyberespionage – including attempts to acquire or access classified files on government servers or the networks of government contractors – and instances of industrial espionage. What sets these activities apart from political or economic tensions is the nature of that which is being targeted and by whom. American technology and pharmaceutical companies are routinely being targeted by hackers with alleged connections to the Chinese state (Baezner and Robin, 2017a, p. 10). Other popular targets for such activities are Western aerospace companies, particularly those with government contracts. One example of alleged Chinese hacking and industrial espionage was the swift development of the J-20 stealth fighter jet for the Chinese air force. The US alleges that this was made possible only after a Chinese hacker obtained plans for the American air force's F22 and F35 jets, enabling the Chinese military to produce their "version", an allegation strongly denied by Beijing. Despite these denials, the targeting of American military contractors by agents conducting cyber operations raises these incidents above those found to be occurring in "simple" economic tension.

A final point to make is that, as with civil war and international conflict, cyber operations do not occur at any specific, predictable point in the chronology of a strategic rivalry. Such operations can be found throughout that chronology. Relations do not need to deteriorate to a specific level or experience a specific flashpoint for cyber operations to commence. There is instead an almost constant undercurrent of cyber activity occurring at all points in the rivalry.

3.6 Contextualizing Cyber Operations

Given the evidence for the existence of five distinct contexts in which cyber operations occur, the table produced for Section 2 of the Trend Analysis – the summation of actors, technologies and vectors – can be updated. Adding these contexts provides a more complete picture of the state of play of cyber operations (see Table 2 below).

Table 2: Actors, Technologies, Vectors and Geopolitical Contexts of Cyber Operations

Context	Actors	Technologies	Vectors
• Open international conflict • Internal civil war • Political tension • Economic tension • Strategic Rivalry	• Quantitative and qualitative growth of attackers • Robotization/automation of attackers (attacker is an algorithm) • Intensification of use of cyberweapons (loss/removal of all constraints) • Privatization of security and intelligence (dependence and loss of state sovereignty and of individuals)	• Machine learning, Artificial Intelligence etc. (towards technological singularity) • Multiple failures discovered and exploited early or late • "Hack record" of objects and services that are acquired and/or used	• Human failure (cyber influence) • Sabotage (as per NotPetya) • Large scale data theft (weak clouds) • Absence of IoT security (higher probability of large scale attacks) • From hyper connectivity to hyper vulnerability (as per TRITON) • CIAAT – Critical Infrastructure as a target • SAAT – Security as a target

It is tempting at this point to declare that a typology for cyber operations can be developed now that the four geopolitical contexts in which cyber operations are deployed and utilized have been explored and set alongside the actors, tools and vectors involved in the operations themselves. However, if the analysis of context, actors, technologies and vectors of cyber incidents and operations does nothing else, it shows that there is no standard pattern or combination of these four elements. While one incident occurring in the context of open international conflict may demonstrate an increased involvement of private, non-state actors using sophisticated AI technology to target critical infrastructure, another example occurring in the same context may have a completely different combination of actors, vectors and technologies. This exercise of contextualization cannot therefore be taken as predictive or as a means to prognosticate on the types of actors involved or the vectors expected to be utilized in any given context. The four columns in Table 2 below represent features common to all manner of cyber operations.

An important reason for this lack of consistency or standard pattern is the wide variation in the goals of the actors themselves. Within each geo- and sociopolitical context, there are numerous goals the actors seek to achieve, ranging from undermining trust in a national government to foment insurrection and regime change to acquiring intelligence on an enemy state's military capability. This range of goals has a direct impact on the tools and vectors chosen by those actors to achieve those goals. Actors choose specific tools – such as DDoS attacks or spear-phishing – to achieve specific outcomes within a particular context. The lack of a standard patter of cyber operations within a context, coupled with the range of possible goals and motivations of the actors deploying those cyber operations means that it is not possible to create a formal, working typology or predictive combination of these four elements. That being the case, however, there are two important trends which have been identified in this analysis.

4 Trends in the use of Cyber Operations

4.1 Trend 1: An almost constant undercurrent of cyber activity

As set out in Section 3 above, it is not possible to create a standard model or predictive typology for cyber incidents and operations. Actors – malicious or otherwise – use all technologies and vectors available to them to achieve their goals, no matter the context. That being said, there are two identifiable trends which arise from this analysis.

The first is that there is no tipping point in a given context when cyber operations begin to be used. A context such as an open international conflict or situation of economic tension does not need to reach a critical juncture in its chronology before one side or the other decides to use its cyber capabilities. Instead, the data shows that there is an almost perpetual undercurrent of cyber operations occurring continually throughout the timescape of a given context. This undercurrent can be seen in the extract from Baezner's forthcoming synthesis of hotspot data provided in Appendix 1 (Baezner, In Press).

As Appendix 1 shows, in the 12 months between October 2014 and October 2015, 33 cyber incidents occurred across five specific historical examples representing instances of all five geopolitical contexts. The examples themselves were at various stages in their timescapes. Some had recently commenced (Ukraine), while others had been going on for some time or had settled into a pattern of retaliatory rivalry (US-Russia). There is no one event within a specific context which sparked the initiation of cyber operations. Instead, such were deployed almost immediately and continued to be used throughout the relationship between the actors. The only factor contributing to timing of any sort was an actor's access to particular capabilities or resources. Such capabilities were widely accessible only from the mid-2000s.

Such a constant use of cyber capabilities in all contexts demonstrates that these capabilities rarely if ever are used in isolation. There is no event or context in which cyber capabilities were the *only* resource deployed. Rather, an actor deploys them as part of a full spectrum or arsenal of available tools. Similarly, there is no geopolitical context in which cyber operations are the *only* feature of actor interaction. Stuxnet is an example of this. The defining feature of the political tension between Iran and the USA (and arguably the rest of the world) over Iran's nuclear program was the damage caused by a sophisticated piece of malware. Yet the situation of tension had been going on for years by 2010, the year Stuxnet was identified and publicized. By this point there had been discussions and debates at the United Nations and its Security Council, bilateral and multilateral attempts to stop the Iranian program and several rounds of international sanctions. These tensions, however, reached a zenith (or nadir depending on perspective) with the deployment of Stuxnet as a direct, active but plausibly deniable attempt to hinder Iran's enrichment capabilities. Therefore, not only do cyber operations occur constantly in a particular context, but they occur rarely, if ever, in isolation.

4.2 Trend 2: There are very few large-scale cyber operations

The example of Stuxnet also highlights a feature of the second identifiable trend in the contextualization of cyber incidents and operations. Of the global events where cyber operations occurred, there are very few where the cyber component of the event constitutes a major incident. This Trend Analysis accepts the position of the Tallinn Manual, where, under international law, a cyber operation can rise to the level of an armed attack if the effects of the cyber operation, or the cyber component of an operation, are equivalent to those of a kinetic attack, i.e. the damage caused is the same as would have been caused were a conventional, physical attack undertaken. By way of example, Stuxnet, under international law, can be classified as an armed attack because physical damage occurred which could have been caused by kinetic weapons (Dewar, 2017, p. 6). If this not unreasonable metric is adopted and applied to the numerous cyber incidents which have occurred, then relatively few incidences of the use of cyber operations qualify as armed attacks, or "large scale incidents".

There are two important points to make here. The first is that this confirms the first trend identified: the other incidences of cyber operations constitute an undercurrent of almost perpetual cyber activity, some of which is malicious. Second, none of those other incidents of cyber operations escalated into an armed attack. The incidences which were of a scale to qualify as armed attacks under international law were singular events. They may have been part of an escalation of a wider contextualized conflict, but the cyber component of that conflict did not gradually increase in complexity, number or severity. This is important because it provides evidence which runs counter to some of the arguments and positions of those proponents of an imminent cyber apocalypse or cyber Pearl Harbor. A great deal of hype surrounding the devastating effects of cyber operations has been and continues to be published (Hansen and Nissenbaum, 2009). Such fears and prognostications of doom have thus far not materialized. Furthermore, the evidence set out in this Trend Analysis shows that such an event is unlikely ever to materialize.

5 Conclusions

The analysis of important incidents in the historiography of cyber operations has enabled five broad socio- and geopolitical contexts to be identified. This provides insights into when cyber operations are used, not just how or by whom. It should come as no surprise that actors with increasing access to cyber capabilities should seek to deploy sophisticated technologies via a variety of vectors in the contexts of kinetic conflict such as interstate or civil war. Similarly, where states are engaged in rivalries, cyber operations are undertaken as part of intelligence-gathering campaigns. A legal grey area occurs when such techniques are employed in the context of economic tension given that industrial espionage is proscribed but recent events have alleged a certain level of state involvement in activities normally associated with crime. This is an issue of which policy-makers are, and should be, aware.

Another aspect of significance for policy-makers is one of timing. The analysis has found that there is no one specific point in a political tension, international conflict or strategic rivalry at which cyber operations commence. Instead there is an almost constant undercurrent or susurrus of activity in cyberspace, much of which is criminal in nature, but some of which may be carried out by malicious, or enemy, state actors. Policy-makers and those responsible for responding to cyber incidents should be aware of this undercurrent and not simply wait for a singular flashpoint triggering the commencement of cyber operations.

The aggregation of cyber operations into four distinct categories – contexts of occurrence, actors involved and their attributes, the technology employed and the vectors utilized – provides a useful summary and distillation of the key features of those operations, features to be expected in any given context. While a predictive typology has not proved feasible, having the core components of cyber incidents and operations clearly defined, and the contexts in which one would expect such operations to occur, can be of benefit to policy-makers and researchers wishing to identify important and relevant cyber security policy areas on which to focus their efforts. The research undertaken for this Trend Analysis may not provide a predictive framework, but should enable more effective and efficient resource management when attempting to develop policy and technical solutions. Particular attention should be paid to the context of economic tension. Given the fuzzy legal situation surrounding cyber operations in this context precise solutions may be challenging from a diplomatic perspective, but maintaining a position of observation on emerging or ongoing tensions or strategic rivalries may increase preparedness and hence improve defense.

That being said, a measure of perspective and self-control should also be exercised. As stated above, this Trend Analysis found that there is an almost constant undercurrent of cyber operations and activity taking place in all four contexts where such activities are to be found. Maintaining a watchful eye on this undercurrent is therefore beneficial and to be advised, but knee-jerk responses and constant reaction to every identified threat or action should be avoided. Not all cyber activities are successful or effective and policy decisions need to be made as to the best use of defensive resources given not all operations can be or require to be responded to directly. This strategic restraint is particularly important given the trend identified in Section 4.2, that very few cyber operations are of a scale or severity that warrants a national security or military response. Just as cyber operations come with a measure of plausible deniability on the part of the perpetrator, this deniability makes restraint a reasonable and acceptable response on the part of the victim.

The final takeaway from this research and contextualization is that no two cyber operations are the same. Such activities are defined by opportunism and the bespoke nature of the operation itself. Canny actors choose the best combinations of technology and vectors for a specific purpose in a specific operation regardless of the wider geopolitical context. This demonstrates a “whatever works” mentality which makes cyber operations challenging to defend against and even more challenging to predict. The tabulation provided here in Section 3.6 of context, actors, technologies and vectors – the “when”, “who”, “what” and “how” of cyber operations – is designed to facilitate preparedness and resilience on the part of those seeking to defend digital and real-world assets. To date this is still the optimum cyber defense posture.

6 Appendix 1

Table representing the chronology of all the cyber-related events observed in five Hotspot Analysis reports. Taken from Baezner and Robin's forthcoming Hotspot Synthesis

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
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 cyber-espionage 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 by SEA against Le Monde website.
02.2015	The Anonymous collective 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 cyber-espionage campaign against the university of Connecticut Engineering Department.
26.03.2015	China uses for the first time its Great Cannon against US websites. 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 (One of 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 of 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 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 Washington Post.

15.05.2015	Discovery of the Chinese cyber-espionage 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 cyber-espionage campaign on emails of top US national security officials.
18.08.2015	DDoS by CyberBerkut on several Ukrainian websites.
16.09.2015	Discovery of the Chinese cyber-espionage 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	Posted pro-ISIS messages, published passwords to the accounts and phone numbers of the directors of the US Central Intelligence Agency (CIA), the US Federal Bureau of Investigation and the NSA by the Cyber Caliphate against 54'000 Twitter accounts (mostly based in Saudi Arabia).
23.12.2015	A cyberattack on 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 as well (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 cyber security 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).
05.2016	Data theft and leak of information by the Myrotvorets a Ukrainian nationalist hacker group against alleged pro-Russian Ukrainian journalists.
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, to have hacked the servers (Hosenball et al., 2016). The Kremlin denies any involvement in the cyberattacks (Rudnitsky et al., 2016).
07.2016	The voter registration systems of the states of Arizona and Illinois are hacked (Lartey, 2016; Reuters, 2016) as well as the servers from the Democratic Congressional Campaign Committee (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). 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.
08.2016	Data theft and leak of information by the Myrotvorets a Ukrainian nationalist hacker group against alleged pro-Russian Ukrainian journalists.
15.08.2016	A hacker group, named Shadow brokers, claims to have stolen data from the NSA. The stolen data, they declares, was various malware developed by the Equation Group, which they then put up for internet auction (Greenberg, 2016).

7 References

Ablon, L., Bogart, A., 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Rand Corporation.

Arquilla, J., Ronfeldt, D., 1993. Cyberwar is coming! Comp. Strategy 12, 141–165. https://doi.org/10.1080/01495939308402915

Baezner, M., In Press. 2017: Cyber Conflicts in Perspective - Hotspot Synthesis.

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

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

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

Baezner, M., Robin, P., 2017d. Hotspot Analysis: Stuxnet.

Baezner, M., Robin, P., In Press. Hotspot Analysis: Cyber disruption and cybercrime: Democratic People's Republic of Korea.

Brown, G., Yung, C.D., 2017. 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 7.10.17).

Dewar, R.S., 2017. Trend Analysis 2: Cyberweapons: Capability, Intent and Context in Cyberdefense.

Gaycken, S., 2011. Cyberwar: Das Internet als Kriegsschauplatz. Open Source Press, Munich, Germany.

Goldman, D., 2012. Gauss: State-sponsored cyberweapon targets bank accounts [WWW Document]. CNNMoney. URL http://money.cnn.com/2012/08/09/technology/gauss-cyberweapon-bank-accounts/index.html (accessed 4.19.17).

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

Hagen, A., 2013. The Russo-Georgian War 2008, in: Healey, J. (Ed.), A Fierce Domain: Conflict in Cyberspace 1986-2012. CCSA, USA, pp. 194–204.

Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. Int. Stud. Q. 53, 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hay Newman, L., 2018. Menacing Malware Shows the Dangers of Industrial System Sabotage [WWW Document]. WIRED. URL https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/ (accessed 3.15.18).

Henley, J., Solon, O., 2017. "Petya" ransomware attack strikes companies across Europe and US [WWW Document]. the Guardian. URL http://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe (accessed 3.15.18).

Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., Glyer, C., 2017. Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure « Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (accessed 3.15.18).

Joyner, J., 2012. Competing Transatlantic Visions of Cybersecurity, in: Reveron, D.S. (Ed.), Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, pp. 159–172.

Junio, T.J., 2013. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. J. Strateg. Stud. 36, 125–133. https://doi.org/10.1080/01402390.2012.739561

Kihara, S., 2014. A rising China: Shifting the economic balance of power through cyberspace. Naval Postgraduate School, Monterey, CA, USA.

Patterson, D., 2017. Cyberweapons are now in play: From US sabotage of a North Korean missile test to hacked emergency sirens in Dallas [WWW Document]. TechRepublic. URL https://www.techrepublic.com/article/cyberweapons-are-now-in-play-from-us-sabotage-of-a-north-korean-missile-test-to-hacked-emergency/ (accessed 10.24.17).

Reynolds, B., 2015. The Economics of U.S.-China Rivalry [WWW Document]. URL https://www.chinausfocus.com/foreign-policy/the-economics-of-u-s-china-rivalry

Rid, T., 2012. Cyber War Will Not Take Place. J. Strateg. Stud. 35, 5–32.

Rowe, N.C., 2012. The ethics of cyberweapons in warfare. Ethical Impact Technol. Adv. Appl. Soc. 195.

Schmitt, M.N. (Ed.), 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. CUP.

Stone, J., 2013. Cyber War Will Take Place! J. Strateg. Stud. 36, 101–108. https://doi.org/10.1080/01402390.2012.730485

Vasquez, J., 1993. The War Puzzle. Cambridge: Cambridge University Press.

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.