CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Strategic stability between Great Powers: the Sino-American Cyber Agreement

Zürich, December 2017

Version 1

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

CSS
ETH Zurich

ETH zürich

Authors: Marie Baezner, Patrice Robin

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

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

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

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

Please cite as: Baezner, Marie (2017): Hotspot Analysis: Strategic stability between Great Powers: the Sino-American Cyber Agreement, December 2017, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Strategic stability between Great Powers: the Sino-American Cyber Agreement

Targets:	Intellectual property and sensitive data from Chinese and US public and private institutions.
Tools:	Spear phishing[1] emails and messages, Remote Access Tool malware (Poison Ivy, Gh0stNet RAT, Zox, Hikit, Hydraq and other malware families) and Distributed Denial of Service attacks.
Effects:	Heightened tensions between the USA and China because of cyberespionage, divergences on international internet governance and establishment of Anti-Access/Area Denial zones by China in the East and South China Seas, conclusion of a 2015 bilateral agreement to not conduct or support economic cyberespionage.
Timeframe:	In cyberspace, approximately since 2000 and still ongoing.

The strategic stability between China and the USA rests on the knowledge that each state has the ability to respond to a nuclear first strike from the respective other. Both states also understand that a war between them would be devastating. However, expanding cyber capabilities and cyberespionage campaigns have generated new areas of friction and risk disturbing this strategic stability. The peak of tensions over cybersecurity was reached after Edward Snowden revealed the extent of the US cyberspace surveillance program and when Chinese hackers stole information from the US Office of Personnel Management. China and the USA subsequently committed to a bilateral agreement on cybersecurity in order to maintain stability.

This Hotspot Analysis explains the dynamics of the strategic relationship between the USA and China over cybersecurity and examines the effects caused by tensions in cyberspace on the domestic, economic, technological and international levels.

Description

The first Chinese cyberespionage campaign was exposed in 2006. Ever since, China and the USA have been wrangling over cyberespionage issues. China was often represented as the perpetrator and US public and private institutions as victims. However, the USA also targeted Chinese institutions and firms in cyberespionage operations, although there is no information about the tools or techniques that it used. China used spear phishing emails and messages for delivering commonly available Remote Access Tool malware in order to collect information on its victims.

Effects

This analysis of cybersecurity issues between China and the USA has found effects at the domestic political level in both states. The USA has struggled to find an appropriate way to retaliate against the cyberespionage campaigns led by China without risking an escalation into a physical conflict, while China has tried to control its domestic internet traffic and at the same time to avoid any social and political instability. Economically, the cyberespionage campaigns have represented an economic loss for the targeted institutions, both in China and the USA. On the technology side, theft of intellectual property has led to the loss of technological superiority for the targeted firms.

At the international level, the first effect is the risk that the tensions between China and its neighboring countries over the South and East China Seas have caused for the USA. If these tensions were to escalate, the USA could be dragged into a resulting conflict because of its alliances with states in the region. The second effect is the strategic impact of the tensions between the two states, which include the development of Anti-Access/Area Denial zones by China, i.e. zones where China is prepared to deploy cyber capabilities alongside military efforts. The tensions have also brought to light disagreement over international internet governance between China and the USA. In this context, the final effect discussed here consists of a 2015 agreement between China and the USA, in which both states commit to not conducting or supporting economic cyberespionage.

Policy consequences

Policy consequences resulting from the tensions between China and the USA in cyberspace and their effects are presented as recommendations in this paper. States may wish to improve their cybersecurity measures by promoting awareness campaigns on spear phishing and the use of two-factor authentication. It is also recommended that states monitor the development of tensions between China, the USA and China's neighbors. This would allow them to respond quickly to any exacerbation and take measures to mitigate the effects of a potential conflict involving these states, should the need arise. States could take the 2015 agreement as a first step for developing further international norms and bilateral agreements on cybersecurity.

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

1 Introduction

Strategic stability is understood as the stability resulting from the assurance between two nuclear states that each party has the ability to respond to a first strike (Colby, 2013, p. 48). China and the USA mutually acknowledge this stability and recognize that a war between the two would be devastating. However, increasing concerns over cybersecurity as well as tensions over other issues, including the East and South China Seas, have threatened this stability. Tensions over cybersecurity between China and the USA reached new heights when Edward Snowden revealed the extensive surveillance program of the US National Security Agency (NSA)[2] and when Chinese hackers stole information from the US Office of Personnel Management (OPM). The solution the two states agreed on in order to maintain stability and reduce tensions was to commit to a mutual cybersecurity agreement aimed at reducing misperceptions in cyberspace and increasing cooperation.

This Hotspot Analysis explores the tensions between China and the USA in cyberspace. The Chinese and US economies are highly interdependent, yet the two states are also in competition politically, militarily and economically. This Hotspot Analysis focuses on an analysis of the cyberespionage campaigns attributed to China and the USA, but also examines the role of both states' cyber capabilities and their implications for the physical realm.

A "hotspot" is understood as a zone of conflict or tensions that involves a component unfolding in cyberspace. A hotspot analysis evaluates specific cases to obtain a better understanding of cybersecurity issues and support theoretical concepts of cybersecurity. A report on Sino-American tensions and cyberespionage is relevant for research because it explains the specific tensions between two Great Powers in cyberspace, their different approaches to cybersecurity and resulting geopolitical implications.

It is intended that this document will be updated if and when new significant events between the two states occur and/or new elements of cyberattacks are identified. The objective is to continue to feed the document to keep it as up-to-date as possible. Also, a broader report will be integrating information from this Hotspot Analysis and others to compare the different cases and provide guidance for cybersecurity policies.

This Hotspot Analysis will proceed as follows. Section 2 provides details on the historical background and chronology of the main and recent events in the Sino-American tensions. The chronology gives an overview of the events in regard to cybersecurity, international internet governance and tensions in the South and East China Seas from the 1970s to 2016.

Section 3 reports on the various US and Chinese actors that may be involved in cyberespionage campaigns. It also shows that, while cyberespionage is aimed at a wide range of targets, all of them are of economic and strategic value. The analysis explains the specific features of the cybertools and techniques deployed and shows that some were used in more than one cyberespionage campaign.

In section 4, the report analyzes the effects of the tensions between the USA and China. It looks into the domestic effects on each country at the political and social levels and shows that the USA had trouble establishing an effective response to Chinese cyberespionage campaigns without provoking an escalation. This section also examines how China protects itself from foreign influence in its cyber and information space.

The analysis then explains the economic effects the relevant cyberespionage campaigns had on both countries. It shows that experts estimate the losses of intellectual property to run into the hundreds of billions of US$ per year for the US economy.

Technological effects take the form of theft of intellectual property and the loss of comparative technological advantage for the firms concerned. Also, both China and the USA tried to restrict access for information technology companies from the respective other state to their domestic markets.

The effects at the international level are examined first within the strategic context of tensions with China's neighbors and the risk of escalation due to provocations in the South and East China Seas. These tensions also risk dragging the USA into a conflict involving its allies in the region.

The analysis then focuses on both countries' growing cyber capabilities and their possible implications in conventional warfare. These capabilities are examined in relation to Anti-Access/Area Denial[3] (A2/AD) zones in the South and East China Seas as well as the two states' ability to deny adversaries access to cyberspace. The report also investigates the divergences between the two states regarding international governance of the internet, where China wants a state-oriented governance structure, while the USA promotes a user-oriented and loosely regulated governance structure.

The report analyzes the 2015 agreement on cybersecurity, in which China and the USA agreed to not conduct or support cyberespionage for economic goals. The agreement is a first step towards increased cooperation in the domains of cybercrime and cybersecurity and a reduced risk of misperceptions and escalation in cyberspace.

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

[3] Technical terms are explained in a glossary in section 7 at the end of the document.

Lastly, section 5 suggests recommendations deriving from the analysis. State actors may wish to use these recommendations to reduce the risk of being impacted by cyberespionage. This would require them to improve cybersecurity through awareness campaigns on spear phishing and increasing the use of two-factor authentication. This final section also suggests that the evolution of tensions between the USA, China and its neighboring countries should be closely monitored to avoid potential downstream impacts by a conflict in the region. It also recommends that international cybersecurity norms should be promoted and the 2015 agreement used as an example for further agreements.

2 Background and chronology

The strategic relationship between China and the USA has evolved and changed over the years. It is therefore important to understand its historical background and chronology to see how they relate to current tensions over cybersecurity. However, this is a rather broad subject that cannot be limited to cybersecurity issues. As a consequence, this Hotspot Analysis cannot cover every aspect of the relationship between the USA and China and will only focus on central issues related to cybersecurity.

The strategic relationship between China and the USA is not confined to cyberspace; it is rather also the result of physical actions and provocations. China claims contested lands in the East and South China Seas and has built artificial islands to expand its territory and secure maritime shipping lanes. These actions have been denounced by neighboring countries, some of which are allies of the USA such as Japan or the Philippines.

In addition to these physical tensions, both China and the USA have used cyberspace for espionage. However, they disagree on the acceptable goals of such acts. The USA has acknowledged that it conducted cyberespionage, but only to gather information relevant for national security. On the other hand, it has accused China of conducting espionage to gather intellectual property that could be used for economic advantage. China has denied engaging in any cyberespionage.

The divergences between the two Great Powers went beyond cyberespionage campaigns, as they also take different positions regarding the broader issue of international internet governance. The USA, where the internet was originally developed, wants an open, user-oriented internet, whereas China demands a more state-oriented, controlled internet. To achieve this goal, China has built the so-called Great Firewall, i.e. a technical system for controlling internet traffic on Chinese territory. Later it also developed other tools such as the Great Cannon to disrupt traffic from and to specific websites.

The events described in the following chronology help understand the dynamics of the tensions between the USA and China regarding the aforementioned issues.

The following table summarizes the main events in the strategic relationship between China and the USA.

Rows colored in gray refer to cyber-related incidents[4].

[4] For a summary of the various cyberespionage campaigns in the context of the Sino-American relations, see Annex 1 in Section 6.

Date	Event
1970s	China asserts territorial claims on the Senkaku/Diaoyu Islands in the East China Sea and on other archipelagos in the South China Sea. Both regions are believed to contain important reserves of natural gas and oil. This assertion by China creates tensions with Japan, Malaysia, Vietnam, Brunei, Taiwan, Indonesia and the Philippines (Economy et al., 2017; Smith et al., 2017).
1978	China starts its transition from a planned economy to a mixed economy.
1989	The Chinese government violently represses students' protests in Tiananmen Square. Several countries react by imposing sanctions on China.
1996	China starts to set in place its Great Firewall to control domestic internet traffic (Brown and Yung, 2017a).
30.09.1998	The Internet Corporation for Assigned Names and Numbers (ICANN), a US-based organization that manages the Domain Names System (DNS), is created (Internet Corporation For Assigned Names and Numbers, 2017).
2004	The Chinese cyberespionage campaign Titan Rain, which targeted the US Department of Defense and defense contractors, is uncovered (Homeland Security News Wire, 2005).
2007	China shoots down a defunct Chinese satellite with a missile showing its ability to control the space domain.
2008	The USA shoots down an alleged Chinese spying satellite (Russell, 2015).
03.2009	A cyberespionage campaign targeting Tibetan activists and Non-Governmental Organizations (NGO) named GhostNet is revealed to the public (Kostadinov, 2013a).
01.2010	Google, Adobe and other US Information technology (IT) firms announce that they were victims of a Chinese cyberespionage campaign named Operation Aurora (Zetter, 2010a). As a consequence, Google announces that it will not censor web research on google.cn (Zetter, 2010b).
03.2011	24,000 sensitive files from a US defense contractor are stolen in a cyberespionage operation allegedly conducted by China (Jacobsson Purewal, 2011).
08.2011	The cybersecurity firm McAfee publishes a report revealing Operation Shady RAT, a Chinese cyberespionage campaign targeting various industries worldwide (Alperovitch, 2011).
09.2011	China and other Asian countries push the United Nations (UN) for an International Code of Conduct for cyberspace (Brown and Yung, 2017a).
2012	The USA shifts its military strategy and focus to Asia (Atanassova-Cornelis and Van der Putten, 2015). Xi Jinping becomes the new head of the Communist Party of China (CPC) (Davidson, 2016).
09.2012	The Japanese government purchases three islands from the owners of the privately owned Senkaku/Diaoyu archipelago. China contests the transaction (Smith et al., 2017).
22.01.2013	The Philippines applies to the UN Permanent Court of Arbitration for arbitration in relation to China. The request concerns alleged Chinese violations of the UN Convention on the Law of the Sea in the South China Sea (Economy et al., 2017).
02.2013	The cybersecurity firm Mandiant publishes a report about the People's Liberation Army (PLA) unit 61398[5], which is allegedly responsible for cyber-operations against English-speaking victims (Raud, 2016).
13.04.2013	China and the USA agree to establish a working group on cybersecurity (O'Brien and Shen, 2013).
06.2013	Edward Snowden, a former NSA contractor, leaks documents revealing the NSA's mass cyber-surveillance program and its cyberespionage Operation Shotgiant against the Chinese IT manufacturer Huawei. The campaign aimed at confirming links between Huawei and the Chinese PLA (Brown and Yung, 2017b; Spiegel Online, 2014).

[5] This actor is discussed in more detail in section 3.1 on Attribution and actors.

07-08.06.2013	US President Obama and Chinese President Xi Jinping meet at the Sunnylands Summit in California to discuss cybersecurity, climate change and North Korea (Price, 2013).
2014	The cybersecurity firm CrowdStrike (2014) publishes a report on the PLA unit 61486, which is allegedly responsible for cyberespionage campaigns against aerospace industries in Europe and the USA.
04.2014	US President Obama officially declares that the Senkaku/Diaoyu Islands are protected by the security treaty between the USA and Japan. However, he does not take a position on which state has sovereignty over the islands (Smith et al., 2017).
05.2014	The US Justice Department indicts five PLA officers for cyber-enabled economic espionage (Gady, 2016).
06.2014	The PLA launches its Cyberspace Strategic Intelligence Research Centre, which is tasked with producing high-quality intelligence research and assisting the Chinese authorities in developing solid national information security (Raud, 2016).
26.03.2015	China uses its Great Cannon against US websites for the first time. The targeted websites monitored the list of websites forbidden in China and suggested software for circumventing the Great Firewall.
04.2015	The USA discovers that its OPM networks were 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, 2017b).
05.2015	China and Russia sign an agreement on mutual non-aggression in cyberspace (Wei, 2016). The same month, China publishes its Defense White Paper which strongly emphasizes information and cyber warfare (Raud, 2016).
08.2015	China drills for oil near the Vietnamese coast, increasing tensions between the two states (Reuters, 2015).
24-25.09.2015	During a meeting in Washington, the USA and China agree to neither conduct nor support cyberespionage for economic purposes as well as on other measures to improve cybersecurity and fight cybercrime (McConnell, 2015).
22.10.2015	The United Kingdom and China sign an agreement on refraining from cyber-enabled economic espionage similar to the one between the USA and China (Brown and Yung, 2017c).
12.2015	The first round of Sino-US talks on cybercrime provided for in the agreement takes place (Segal, 2017).
02.2016	The CPC announces structural and organizational reforms of the PLA (Raud, 2016).
04.2016	The first joint cyberdefense exercise between China and the USA, which was provided for in the agreement, takes place (Gady, 2016). At the same time, there are reports that China has deployed fighter jets and radar systems on an island in the Paracel Archipelago, heightening tensions with Vietnam and Taiwan (Economy et al., 2017).
05.2016	The first meeting of a group of senior experts from China and the USA provided for by the agreement is held. Its discussions focus on international norms in cyberspace (Gady, 2016).
12.07.2016	The UN Permanent Court of Arbitration delivers its ruling in favor of the Philippines (Economy et al., 2017).
08.2016	The hotline between the US Department of Homeland Security and the Chinese Ministry of Public Security provided for by the agreement is set in place (Segal, 2017).
11.2016	China issues a new cybersecurity law (Moreshead, 2017).

3 Description

This section examines the various actors that are involved in cyber-activities in the USA and China and contribute to the tensions between the two states. It then explains the nature of the targets of these cyber-activities and details the type of tools and techniques deployed in various cyberespionage campaigns against US and Chinese firms.

3.1 Attribution and actors

Attribution in cyberspace is a complicated task which normally follows the "*cui bono*" (to whose benefit) logic. Attribution is therefore often based on circumstantial evidence and cannot be established with 100% certainty, as there is always the possibility that an alleged perpetrator has not in fact committed a particular cyberact. This Hotspot Analysis is mainly based on English-language media articles, cybersecurity reports and academic papers due to language limitations. These texts bring a certain point of view that is not neutral. It is essential to keep in mind that authors are not impartial and may have particular reasons for writing their papers at specific points of time.

The USA and China have both accused each other of conducting cyberespionage campaigns. In both cases, it has been assumed that relevant activities mostly involved state actors.

US state actors

In the USA, cyber-operations are handled by the Cyber Command. The Cyber Command, established in 2009 as a sub-unit under the US Strategic Command, is responsible for defensive and offensive military cyber-operations. It is directed by the head of the NSA and is located in Fort Meade in Maryland, where the NSA is based. It uses NSA infrastructures and networks. In July 2017, the Trump administration announced that it will separate the Cyber Command from the NSA, arguing that the mission of the NSA is only to gather intelligence, whereas military cyber-operations are both offensive and defensive (Baldor, 2017).

The NSA is a US intelligence agency within the US Department of Defense that is responsible for Signal Intelligence (SIGINT) and the security of US information systems. The NSA may also enable Computer Network Operations (CNO) (NSA/CSS, 2016). Edward Snowden revealed that the NSA was conducting worldwide mass surveillance of the internet and was physically tapping hardware (Greenwald et al., 2013).

Chinese state actors

In China, cyber-operations are conducted by two departments of the PLA General State Department: the Third Department and the Fourth Department.

The Third Department, which is responsible for SIGINT and the defense of information systems, is divided into 12 bureaus, three research institutes and 16 regional bureaus.

The Second Bureau[6] deals with CNO. This Bureau is located in Shanghai and targets mostly English-speaking victims in order to obtain political, economic and military intelligence (McWhorter, 2013; Raud, 2016).

The Third Department also comprises the 12th Bureau[7], which monitors satellite communications and space networks and conducts space-based SIGINT (Raud, 2016). In 2014, the US-based cybersecurity firm CrowdStrike issued a report on the 12th Bureau cyberespionage campaign against aerospace industries in Europe and the USA. According to the report, the unit has been active since 2007 and is also located in Shanghai (CrowdStrike Global Intelligence Team, 2014).

The Fourth Department has a Computer Network Attack force and is responsible for electronic countermeasures by using a combination of Electronic Warfare (EW) and CNO (Raud, 2016).

China announced in February 2016 that it was reforming the structure of the PLA and would create three new organizations, among them the Strategic Support Force (SSF). The SSF will have a strong focus on cyber-operations and intelligence (Davidson, 2016). It will be composed of three forces: space troops (responsible for recognition and navigation of satellites); cybertroops (in charge of defensive and offensive hacking); and EW troops (responsible for jamming, disrupting radars and communications). SSF will then be responsible for all aspects of information warfare (Raud, 2016).

Chinese non-state actors

Chinese non-state actors have also played a role in heightening tensions with the USA. Jeffrey Kwong's research of 2012 cited in Raud (2016) argued that most of the cyberattacks attributed to China were in fact committed by independent hacktivists. He explained that the Chinese government tolerated hacktivist groups to act on behalf of China in cyberspace but asserted that these groups were often more nationalistic than the Chinese state and, if left uncontrolled, could start a conventional war with another state. Kwong referred to the Chinese cyber militia, which consists of civilians with specific knowledge of IT or certain languages who take

[6] The Second Bureau is also known as Unit 61398, APT1, Shady RAT, Comment Crew and Comment Group.

[7] The 12th Bureau is also known as Unit 61486 and Putter Panda.

part in military cyber exercises and support the PLA but are not directly under the PLA's command (Raud, 2016).

The cybersecurity firm Novetta identified one group, which they named Axiom. It was this group that was behind the Hikit campaign, although it remains unclear whether it had ties to the Chinese government. The group targeted victims that were of strategic value for the Chinese government. Axiom seemed highly organized and technically sophisticated. It was able to produce custom-made malware and used extensive compromised and legitimate Command and Control infrastructures (C&C). Their hacking behavior also suggested that they pursued long-term strategic goals, as they took time to study their targets' networks to identify the right victims and to leave backdoors to access their computers again later if necessary. These elements led the Novetta experts to believe that the group had access to extensive financial and physical resources (Novetta, 2014).

3.2 Targets

The targets of cyberattacks and cyberespionage in the context of the strategic relationship between China and the USA were diverse. However, the choice of victims was by no means random, as all victims had strategic, economic and/or intelligence value.

Victims in China

There is only limited information available about Chinese victims of US cyberattacks or cyberespionage. This might be due to the fact that this Hotspot Analysis bases its research on mainly Western sources, but it is also possible that US cyber-operations were more efficient and/or conscious about covering their tracks. The USA also differentiated between cyberespionage for economic purposes, which it considered illegal, and cyberespionage for national security purposes, which it considered acceptable. However, the two states have very different political systems, and while US firms are separated from the US government, Chinese firms are not, making it more difficult to differentiate between espionage for economic and national security purposes.

It was reported that the USA had spied on the Chinese IT manufacturer Huawei. The campaign was allegedly aimed at finding links between Huawei and the PLA, but the USA was unable to confirm any such ties. It argued that the cyberespionage campaign only served national security reasons and that none of the intelligence collected would be disclosed to Huawei's competitors in the USA. However, Huawei is also of strategic interest to the USA, as this technology firm lays internet cables between Asia and Africa and its customers have included Iran, Afghanistan, Pakistan, Kenya and Cuba (Sanger and Perlroth, 2014; Spiegel Online, 2014). Furthermore, Snowden's revelations showed that the US intelligence community also used cybermeans to spy on the former Chinese President Hu Jintao, the Chinese Trade Ministry, Chinese banks and Chinese telecommunication companies (Spiegel Online, 2014). These targets were consistent with espionage for national security, but the collected information could also be used for economic competitive advantage. It was further revealed that the USA spied on Chinese firms to gain advantage in trade negotiations, which could also be qualified as economic espionage (Lindsay, 2015a). These revelations showed that there are certain contradictions in the USA's position on cyberespionage.

Victims in the USA

Chinese cyber-operations are better documented by Western media and cybersecurity firms than those of the US. This creates an imbalance that may suggest that the USA was more frequently affected by cyberespionage than China. However, any such perception would be biased due to the lack of reporting on cyber-incidents in China. Chinese cyber-operations targeted a very diverse range of victims located both in the USA and in other countries, but this Hotspot Analysis is only concerned with victims in the USA. Each time a Chinese cyberespionage campaign was uncovered, it was found to have affected approximately twenty victims, which can be generally grouped into the following categories: technology firms (e.g. Google, Adobe), industrial companies (e.g. pharma companies, banks), US military (e.g. Pentagon, US Navy and US Marine Corps, contractors), US government and public institutions (e.g. OPM and the candidates in the 2008 presidential elections), academia, journalists and NGOs located in the USA (e.g. the Tibetan mission in New York City). All these targets represented some sort of intelligence, economic or strategic value to China.

3.3 Tools and techniques

Both China and the USA conducted several cyberespionage campaigns against one another, with each campaign relying on various methods of infection, tools and types of malware. This sub-section describes the most common tools and techniques observed in the context of these cyberespionage campaigns.

In most of the campaigns, victims were infected via spear phishing. They received specially designed emails or messages to lure them into clicking on a link to a malicious website or opening an infected attachment file. When the victim clicked on the link or opened the attachment, a piece of malware was downloaded that usually set a backdoor to allow the attacker to access the computer remotely. The most commonly used malware applications were the following:

Poison Ivy

Poison Ivy[8], one of the most frequently used Remote Access Tools (RATs), has been freely available on the internet since 2005. Its features include key logging, capturing screen shots, activating cameras and microphones, and stealing files and passwords. Poison Ivy is used by many cybercriminals because of its easy-to-use graphical interface, but it has also been identified in many espionage campaigns including the GhostNet, Hikit, Night Dragon and Byzantine campaigns (FireEye Inc., 2014).

Gh0stNet RAT

Gh0stNet RAT[9] was mainly used in the GhostNet cyberespionage campaign against Tibetan activists and NGOs, but was also found in other campaigns. This RAT is capable of activating cameras and microphones, recording key strokes and retrieving and downloading documents (Markoff, 2009).

Zox

The Zox malware family is also called Gresim. This malware family was observed in the Hikit campaign and was used by the threat actor Axiom. Zox malware is capable of uploading, downloading, writing, deleting and moving files. Some versions have spreading capabilities. The earliest samples date back to 2008. Zox uses the PNG file format to communicate with C&C (Novetta, 2014).

Hikit

Hikit is also known as Hikiti. Investigations by Novetta (2014) revealed that Hikit was used specifically by the threat actor Axiom in the Hikit campaign. Novetta experts found that each Hikit sample was customized to fit its target and that each sample communicated with a specific C&C server. This malware, which has been active since 2011, includes some code parts that came from open sources. Hikit is capable of uploading and downloading files on infected machines and creating *ad hoc* networks of infected machines running in parallel to the victim's network (Novetta, 2014).

Hydraq

Hydraq[10] is a Trojan horse that opens a backdoor on infected computers. It was found in Operation Aurora, which targeted Google and other technology companies. It is capable of downloading, modifying, executing, copying and deleting files, and restarting or shutting down infected computers (Symantec Corporation, 2011).

Overall, malware infection was not the only way tensions between China and the USA were expressed in cyberspace, though. China developed and used its Great Cannon, a tool capable of directing, injecting and deleting data traffic to and from websites. Attacks by the Chinese Great Cannon can cause Distributed Denial of Service (DDoS) attacks on targeted websites, rendering the affected websites unavailable to users and possibly causing thousands of US$ in economic losses as well as reputation damage to website owners (Marczak et al., 2015; Radware, 2015).

[8] Poison Ivy is also known as Breut or Darkmoon (Novetta, 2014).

[9] Gh0stNet RAT is also known as Gh0st, Moudoor or Mydoor (Novetta, 2014).

[10] Hydraq is also known as McRAT, HydraQ, Hidraq, Naid, Homux, HomeUnix, MdmBot or Roarur (Novetta, 2014).

4 Effects

This section explains the effects of both the various cyberespionage campaigns and the increasing cyber capabilities of both actors at the national level in China and the USA, in the economic and technological domains, and at the international level.

At the US domestic level, this Hotspot Analysis focuses on social and political effects caused by the Chinese cyberespionage campaigns. At the Chinese domestic level, the report concentrates on China's desire to control the flow of information within its territory, including in cyberspace.

In the economic domain, the analysis looks into the economic losses caused by the cyberespionage campaigns and the theft of intellectual property.

In the technological field, the report examines effects on companies whose intellectual property was stolen.

Finally, this Hotspot Analysis studies the strategic context and the implications of the tensions between China and its neighboring countries on Sino-American relations. It analyzes the development of A2/AD zones by China and the role of cybermeans in these zones as well as their implications for the USA. In relation to A2/AD zones, it also examines the disagreement between the USA and China over international internet governance. Finally, the report looks into the bilateral agreement on cybersecurity concluded by China and the USA in September 2015 and its consequences for the evolution of the relations between both countries.

4.1 Social and political effects

The various cyberespionage campaigns and physical provocations occurring in the East and South China Seas put pressure on the Sino-American relationship and increased mistrust between the two states. These tensions were also felt at the domestic level in both states.

The USA detected attacks on economic and state secrets by Chinese hackers. These campaigns specifically alarmed the US government, which differentiates between cyberespionage for national security purposes and cyberespionage for economic purposes. Spying for national security purposes is tolerated internationally and will most likely never be restricted, as states are responsible for protecting their people against foreign threats and espionage is a means to prevent foreign attacks. However, economic espionage is not seen as necessary by states and is not an accepted practice (Harris, 2016). The USA was concerned to see its businesses lose comparative economic advantage as their intellectual property was stolen. Also, the USA could not be seen to allow China to act freely in cyberspace and needed to take action. Had the USA not counteracted Chinese cyberespionage, it would have appeared as a weak and easy target for other nations or non-state actors wishing to conduct similar cyberespionage actions against US enterprises or institutions. Furthermore, the US response to cyberespionage needed to be proportionate to deter China and other actors effectively from conducting cyberespionage while avoiding escalation into a conventional conflict. On that particular subject, Torruella (2014) presented a ranking system of potential responses to various cyberattacks. He classified the theft of data as "cyber disruption" and proposed a response between blocking and reporting the theft, which the USA did multiple times. Torruella also suggested the use of a "cyber response", and it is possible that the USA used a response of this type against China (Torruella, 2014, p. 121).

The indictment of five PLA members by a US Grand Jury in May 2014 showed that the USA was ready to initiate legal proceedings to discourage China and other countries from further cyberespionage (Lindsay, 2015b). This step additionally signaled to US companies that the government was willing to protect them. The indictment also signaled a shift in the US response to cyberespionage on US firms from defensive to offensive action and that a certain line had been crossed in the relationship (Chabrow, 2014). The USA also warned China in 2015 that it would impose economic sanctions and take diplomatic measures if the cyberespionage did not stop. Nevertheless, these measures were mostly symbolic, as the PLA members concerned were never jailed and economic sanctions would also have penalized the US economy, which is interdependent on the Chinese economy (Sanger and Perlroth, 2014).

China in turn was concerned that Western states were trying to exert influence on its domestic political and social activities. China wanted to preserve its political and social stability by controlling access to flows and contents of information. The Great Firewall serves to safeguard the Chinese population against accessing information that is beyond the control of the Chinese authorities. China accused the USA of influencing the Chinese population through soft power and was anxious about the perceived risk of Westernization among its population. It also criticized US websites that suggested software and tools for circumventing the Great Firewall. China regarded these actions as a way for the USA to interfere in Chinese domestic affairs and to heighten tensions (Lindsay, 2015b).

4.2 Economic effects

The main economic effects observed as a result of the tensions between the USA and China in cyberspace consist of the economic losses caused by the cyberespionage campaigns. The reported victims were mostly US and European firms which had information stolen by Chinese perpetrators. The US Assistant

Attorney-General for National Security, John Carlin, estimated that by 2016 thousands of US businesses had been affected by cyberespionage. A 2013 US Intellectual Property Commission Report estimated the economic loss of intellectual property to amount to approximately US$300 billion per year (Kihara, 2014). A study by the think tank Center for Strategic and International Studies and the cybersecurity firm McAfee (2014) revealed in a report released in 2014 that all types of intellectual property theft (cybercrime and state-sponsored) combined cost the US economy between US$200 and 250 billion per year. These figures only take into account quantifiable losses, but the actual cost of cyberespionage to the US economy would be substantially higher if other costs such as opportunity costs, reputational damage to firms and investments in cybersecurity were factored in as well (Kihara, 2014).

This estimation needs to be put into perspective further, as many companies did not report that they had been targeted by cyberattacks. On the other hand, the threat caused by China to US enterprises tended to be exaggerated: as Lindsay (2015c) argued, the anxiety felt by US enterprises about losing competitive advantages was inflated, as it seemed that China struggled to translate stolen information into economic benefits.

Chinese businesses were also victims of cyberespionage, but no estimates of Chinese economic losses are available.

4.3 Technological effects

The various cyberespionage campaigns led by both China and the USA resulted in the loss of comparative technological advantages for the targeted firms as well as in increased mistrust in foreign technology.

Firms lost not only economic advantage due to economic cyberespionage, but also technological advantage. The hackers who stole information were able to sell it to competitors of the affected firms, which in the case of China are often state-owned companies. This technology could then be developed without needing to allocate resources to research, saving both time and money. This in turn allowed industries to compete directly with the original developers of technology. In the case of military goods, it also raised the issue of loss of strategic advantage in addition to the loss of technological superiority.

The theft of intellectual property from US firms by China needs to be put into perspectives, as Lindsay (2015c) argued that China appeared to struggle translating stolen information into significant benefits. Lindsay asserted that organizational challenges within the PLA, including information overload and a highly compartmentalized bureaucracy, prevented and/or slowed down the process of the PLA converting information usefully (Lindsay, 2015a). Gilli and Gilli (2017) added that while China had relatively easy access to significant US technological secrets, it was unable to translate these into concrete military advantages because of increasing technological complexity. They argued that this increased complexity renders technological imitation and replication more difficult.

Concerns over compromised technology also pushed the USA and China to restrict foreign technology companies' access to their respective domestic markets. The USA blocked certain Chinese IT firms from the US domestic market because of concerns of built-in backdoors in the products (Sanger and Perlroth, 2014). China in turn mistrusted US IT companies and tried to restrict their access to the Chinese IT and internet market (Lindsay, 2015b).

4.4 International effects

This sub-section examines the effects of the tensions between the USA and China in cyberspace on the international level. First, the strategic context showed that Eastern Asian allies of the USA were directly concerned about growing Chinese cyberpower and territorial expansion. Second, the strategic effects of such tensions can be seen in the development of A2/AD zones by China and their implications for the US projection of force in the region. Third, both states have different views on international internet governance, adding further tensions. Fourth, the two states concluded a bilateral agreement on cybersecurity in September 2015.

Strategic context

The tensions also affected the countries near Chinese areas of influence and Asian allies of the USA. China's territorial expansion and establishment of A2/AD zones had an impact on the security interests of Japan, South Korea, Taiwan, Vietnam, Singapore, Indonesia, Malaysia and the Philippines (Van der Putten, 2017). Not only were these states anxious about their own security, but they also were concerned that they may need to choose between China and the USA at some point if the tensions were to escalate into a conventional conflict. Some countries may be tempted to leave a partnership or alliance with the US in the belief that China would be better able to ensure regional stability and secure shipping lanes than the USA (Atanassova-Cornelis and Van der Putten, 2015).

These neighboring states could potentially trigger an escalation between the USA and China, as the USA would need to intervene if Taiwan declared independence or Vietnam or Indonesia seized contested islands. These issues have been ongoing sources of friction, but could easily result in an escalation if concrete, one-sided action was taken (Gompert and Libicki, 2014). It falls to the USA to prevent escalation

and protect its economic, political and security interests in the region.

Figure 1: East Asian Maritime Claims (Stratfor Worldview, 2017)

Strategic effects

The strategic effects of the tensions between China and the USA in cyberspace were not limited to the cyberespionage campaigns, but also concerned the use of A2/AD zones in the East and South China Seas by China. A2/AD is an asymmetric defensive approach that can be summarized as the use of all military domains, including cyberspace, by a state to prevent or deter an adversary from entering a specific area.

China has security, economic and intelligence interests in the East and South China Seas because of natural resources and their strategic value for the Chinese military and intelligence. However, Chinese territorial claims in these regions threaten other states, including US allies and partners such as Japan, Vietnam and the Philippines (Van der Putten, 2017). China is aware that it cannot compete with the USA in a conventional war. China modernized its navy to secure its freedom of action in these seas, but also developed shore-based anti-ship ballistic and cruise missiles and maritime strike aircraft (Hempel, 2016). All these military technologies combined with cyber and space technologies serve to deny a potential adversary access to specific areas. The Chinese doctrine highlights the need to control the information space early on in a conflict in order to deny its opponents' Command and Control (C2) capabilities and to secure a quick victory (Cheng, 2014; Raud, 2016). Cyber capabilities are useful in this regard to disrupt GPS localization or communications. Kazianis (2013a) argued that cyber-operations are ideal for A2/AD because they are suitable for damaging an adversary's C2. Cyber-operations can also be conducted through proxy groups, allowing the attacking state to deny any involvement. China has already shown that it has the ability to disrupt satellites through either conventional or cybermeans, and the

development of A2/AD zones has given China additional weight in its discussions with the USA regarding the stabilization of their relationship.

The USA felt specifically targeted by the Chinese A2/AD zones as they directly impact on the USA's projection of force in the region. As a consequence, the USA developed the Joint Operational Access Concept and the AirSea Battle Operational Concept. These concepts involve the deployment of a large number of submarines carrying long-range missiles capable of destroying Chinese C2 systems and the development of cyber capabilities targeting Chinese missile systems (Cheng, 2014; Gompert and Libicki, 2014; Kazianis, 2013b).

A2/AD can also be performed in cyberspace. Russell (2015) argued that states can conduct cyberblockades and deny internet access to other states. She claimed that cyber A2/AD can be achieved by means of cyberattacks to shut down internet exchange points or by physically tampering with internet infrastructures. The goal would be to disrupt and/or deny the flow of information in cyberspace. This is a relevant tactic, as military forces in both China and the USA rely heavily on cyberspace for relaying information to and from C2 centers. States could target submarine or terrestrial cables or satellites in this type of action.

However, it would be difficult for the USA to deny access to cyberspace to China by tampering with submarine or terrestrial cables. China has more than a dozen landing stations where submarine cables come to shore and connect to the terrestrial network. For a cyber A2/AD to be efficient, all these cables would need to be cut simultaneously (Russell, 2015). The same applies if China wanted to cut US access to cyberspace. The USA has dozens of landing points on the Pacific coast and just as many on the Atlantic coast (TeleGeography, 2017). While either state would still be able to tap cables and thus to spy on the respective other, this would not impair access to cyberspace.

In terms of internet access via satellites, both the USA and China have confirmed abilities to destroy satellites. China shot down a defunct satellite with a missile in 2007, and the USA shot down a satellite in 2008. Satellites in orbit furthermore often run on outdated technology and are therefore vulnerable to hacking (Russell, 2015), although merely hacking satellites would not deny cyberspace access to either China or the USA.

The development of A2/AD zones by China and the possibility that A2/AD could also be used in cyberspace have demonstrated a shift in the doctrinal debate over the definition of cyberwar. The debate stopped being about the eventualities of and preparation for a potential cyber Pearl Harbor and instead shifted to the strategic use of cyber capabilities in combination with other domains in the context of conflicts. This change of focus has not only given more weight to cyber issues in the doctrinal debate, as it started to investigate more realistic scenarios, but is also indicative of a normalization of the subject.

Internet governance

The context of the strategic relationship between China and the USA over cyberspace had another international consequence illustrated by these countries' disagreement on international internet governance. China opposed the current internet governance by the Internet Corporation for Assigned Names and Numbers (ICANN), a private not-for-profit organization based in the USA that regulates the technical coordination of the Domain Name System (DNS). China criticized US control of internet governance as being hypocritical, claiming that it only served US interests and the US intelligence community. The countries' different views on internet governance focused on sovereignty, with the USA promoting a multi-stakeholder governing body and China, along with Russia and some members of the Shanghai Cooperation Organization, preferring a stronger and more formalized internet governance organization similar to the International Telecommunications Union (ITU). These latter states were concerned about foreign interference in their domestic management of the internet and hoped that a more state-oriented governance structure would prevent such behavior (Lindsay, 2015c). In this regard, China, Russia and other Asian states issued an international Code of Conduct for information security via the UN in 2011, suggesting international norms and rules for greater cooperation, security and transparency in cyberspace (Brown and Yung, 2017b, 2017a).

Bilateral agreement

The 2015 agreement on cybersecurity was concluded as the Obama administration's response to the OPM hack. The USA had considered retaliating with economic sanctions and diplomatic measures, but instead decided to develop a bilateral agreement. The 2015 agreement was made at a time when the tensions between the two states had reached new heights, with intensified cyberespionage campaigns by China and Edward Snowden's revelations, which diminished US legitimacy regarding cybersecurity issues. Given the heightened tensions, the risks of misperception of each state's cyber-activities increased as well. The goal of the 2015 agreement on cybersecurity was to reduce these risks and stabilize relations between China and the USA (Chabrow, 2015; Lindsay, 2015a). The 2015 agreement formed part of a broader discussion that included agreements on military relations, law enforcement, counterterrorism and people-to-people exchanges. The 2015 agreement on cybersecurity was built around seven measures, with both states agreeing to:

- Provide timely responses to requests for information and assistance in case of malicious cyber-activities
- Investigate cybercrime, collect electronic evidence and mitigate malicious cyber-activities coming from their respective territories
- Inform each other on the status of the aforementioned investigations
- "[Not] conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors"
- Make efforts to identify and promote international norms of state behavior in cyberspace
- Create a high-level joint dialogue mechanism on fighting cybercrime and related issues, which will also be used to review the timeliness of the requests for information.
- Create a hotline for escalation issues related to cybersecurity (The White House, Office of the Press Secretary, 2015).

Cybersecurity experts have stated that cyber-intrusions originating from China seem to have decreased since 2015, but they also argue that cyberattacks coming from other countries have increased over the same period. They hypothesize that China may have outsourced or used proxies for its cyberespionage activities (Olenick, 2017). Other explanations for the decreased number of cyberattacks on the USA attributed to China include the possibility that China may have become better at covering its tracks or that it has redirected its focus or objectives on other, easier targets (Harold, 2016; Segal, 2016). Also, China has conducted a vast anti-corruption campaign within its administration, which may have discouraged PLA units that used to engage in hacking to supplement their salaries from continuing to pursue such practices (Brown and Yung, 2017c).

The remaining elements of the 2015 agreement have since been implemented. Representatives of the US Department of Homeland Security and the Chinese Ministry of Public Security met in December 2015 and June 2016 and agreed on guidelines for requests of information and assistance under the agreement. The hotline has been operational since August 2016 (Segal, 2016). This hotline is somewhat similar to the red phone instated after the Cuban missile crisis in 1962. The cybersecurity hotline serves to reduce the risk of misperceptions in the cybersecurity domain by creating a direct line of communication between the two states.

The 2015 agreement appears to be a good first step for states to discuss cybersecurity issues and establish cooperation. While the agreement alone will not solve cybercrime or cyberespionage issues, it has been a good start for decreasing the tensions that had grown between the two states over cyberspace. Through increased dialogue and cooperation, the agreement may also help to reduce the risk of miscalculation in cyberspace. The 2015 agreement also appears to have been a victory for the USA, as it got China to agree on differentiating between cyberespionage for economic and national security purposes. The fact that China consented to discuss the issue was already a step forward for the USA, knowing that China's previous narrative was to deny any hacking originating from its territory. The 2015 agreement also demonstrated to US businesses that their authorities took the issue of cyberespionage seriously. It was further seen as a positive step forward by China, which considered the agreement as a way to reduce tensions and increase cooperation (Brown and Yung, 2017c). China had repeatedly complained about being the victim of cyberattacks originating from the USA and Western states' lack of interest in cooperating on cybercrime issues (Kshetri, 2013; O'Brien and Shen, 2013). Further bilateral dialogue on cybersecurity issues may emerge between the USA and China, facilitated by the infrastructures set in place by the 2015 agreement.

Nevertheless, the 2015 agreement had its limits. It has been difficult to evaluate its implementation, for example: while it is easy to assess whether the hotline or dialogue have been implemented, it is more difficult to estimate the number of cyberattacks conducted or supported by either the USA or China. Besides, neither the US administration nor the Chinese government has control over all individuals living within their respective territories, and nor do they have the ability to prevent all private involvement in malicious cyber-activities (Olenick, 2017). Cyber-activities by individuals in one of the two states may then be interpreted as having been conducted or supported by the respective other state. Individual actions in cyberspace may be even more difficult to manage for the USA, as it has less control over internet traffic on its territory than China (Brown and Yung, 2017b). Moreover, the 2015 agreement does not provide for any enforcement measures, and if one party to the agreement fails to comply with the agreement, the other therefore has no means to punish it (Tiezzi, 2015). Finally, it is difficult to draw a line between the two supposedly distinct types of cyberespionage. The USA admitted to conducting cyberespionage for national security purposes, but this sometimes involved intrusions into business networks. The reasons for activities of this kind would be hard to explain in case of detection (Brown and Yung, 2017c).

The agreement was internationally perceived as a positive sign. It also signaled to other states that both the USA and China were open to concluding agreements of this kind with other states. Nevertheless, there are doubts whether such an agreement could potentially work between the USA and Russia, as the relations between the USA and Russia are different from those

between the USA and China, their economies are less interdependent and Russia seems less interested in intellectual property than China (Olenick, 2017). However, the USA and Russia did sign an accord in 2013 to try to reduce misperceptions in cyberspace by creating a direct line of communications and a procedure for exchanging technical information between both states' Computer Emergency Response Teams (Nakashima, 2013). Cyberattacks from Russia did not appear to decrease after the 2013 agreement, but instead intensified and became more obvious compared to cyberattacks originating from China (Korolov, 2017).

5 Policy consequences

This section suggests several measures that states may wish to follow to reduce the risk of falling victim to cyberespionage and/or being impacted by the tensions between China and the USA over cyberspace.

5.1 Improving cybersecurity

Most cyberespionage campaigns used spear phishing emails or messages to access networks, and cybersecurity therefore needs to be improved at the technical and human levels. Technically, firms working with sensitive data or intellectual property can boost security via two-factor authentication logins to ensure that attackers cannot use stolen user login credentials to access systems without authorization. Effective access rights management, that is strictly limiting access to sensitive information to those employees who need it, can also help limit the risk of having sensitive information fall into the wrong hands.

At the human level, states could promote awareness campaigns about spear phishing as a first step towards sensitizing staff in the public and private sectors. Offline or online cybersecurity courses could be offered to improve knowledge of the issue, and staff could be occasionally exposed to fake spear phishing emails to check their understanding of the issue.

5.2 Monitoring tensions between China and the USA

The tensions between China and the USA in both the physical and the cyber realm have the potential to escalate into a conflict. It is therefore essential to monitor closely how the relationship between the two states evolves in order to anticipate a possible conflict. The tensions surrounding the East and South China Seas, the A2/AD zones, international internet governance and cyberespionage campaigns are specific elements of tensions that demand international attention.

States may wish to prepare contingency plans in the event of an escalation or if China decides to block maritime straits or shipping lanes. States could also discuss international internet governance in international forums in order to identify solutions that may suit both China and the USA.

5.3 Promotion of international dialogue and international norms

The 2015 agreement on cybersecurity between China and the USA is a good first step toward other international agreements. The United Kingdom concluded a similar agreement with China in October 2015, only a month after the USA (UK Foreign &

Commonwealth Office, 2015). Other states may wish to make similar agreements on cybersecurity with China or other states. If enough states do so, the issues raised in such agreements could one day be transformed into international norms. The USA, China and United Kingdom could help promote such agreements internationally.

6 Annex 1

Non-exhaustive table of the different cyberespionage campaigns between China and the USA since 2000:

Campaign	Time period	Victim(s)	Alleged perpetrator's origin	Infection methods	Malware used	Damage
Titan Rain	01.01.2003-01.04.2006	US military and institutions	China	MSN Messenger and spear phishing emails	Myfip worm	Theft of unclassified but sensitive information (Brenner, 2005; Maness and Valeriano, 2014).
Shady RAT	01.08.2006-01.01.2010	71 victims from a variety of sectors, 49 of which were in the USA	China	Spear phishing emails	Unknown	Unknown (Alperovitch, 2011; Maness and Valeriano, 2014).
GhostNet	27.05.2007-01.08.2009	Tibetan missions and NGOs in the USA and elsewhere	China	Spear phishing emails	Gh0stNet RAT	Theft of information and structure about Tibetan activists and NGOs around the world (Kostadinov, 2013a, 2013b; Maness and Valeriano, 2014).
2008 US Presidential elections campaign	01.08.2008-04.08.2008	Obama and McCain campaigns	China	Unknown	Unknown	Theft of campaign information (Glendinning, 2008; Maness and Valeriano, 2014).
Hikit	01.09.2008-27.10.2014	Journalists, environmental groups, pro-democracy groups, IT companies, academics and governmental institutions worldwide	China	Spear phishing emails and compromised websites	Gh0stNet RAT, Poison Ivy, Zox, Hikit and other commonly available or customized malware	Theft of information (Maness and Valeriano, 2017; Novetta, 2014).
Night Dragon	01.11.2009-11.02.2011	US critical infrastructure companies	China	SQL Injection and spear phishing	Gh0stNet RAT and other commonly available RATs	Theft of sensitive intellectual property (Maness and Valeriano, 2014; McAfee Foundstone Professional Services and McAfee Labs, 2011).

Campaign	Time period	Victim(s)	Alleged perpetrator's origin	Infection methods	Malware used	Damage
Byzantine series	30.10.2008-30.06.2011	US institutions	China	Spear phishing emails	Gh0stNet RAT	Theft of information (Grow and Hosenball, 2011; Maness and Valeriano, 2014).
Operation Aurora	01.06.2009-01.01.2010	US IT companies (Google, Adobe and others)	China	Spear phishing emails, instant messages and compromised websites	Hydraq Trojan horse	Theft of intellectual property (Maness and Valeriano, 2014; McAfee Labs and McAfee Foundstone Professional Services, 2010; Symantec Security Response, 2010).
NSA fourth party collection	01.07.2009-ongoing	Chinese hackers targeting the US Department of Defense	USA	Unknown	Unknown	Collection of stolen information from previous hacks (Appelbaum et al., 2015; Maness and Valeriano, 2017).
Operation Shotgiant	10.03.2010-2014	Huawei (Chinese IT company)	USA	Unknown	Unknown	Theft of source code of Huawei products, list of customers, internal documents (Maness and Valeriano, 2014; Sanger and Perlroth, 2014; Spiegel Online, 2014).
US top national security email hacks	01.04.2010-10.08.2015	Top US national security officials	China	Spear phishing emails	Unknown	Theft of emails (Maness and Valeriano, 2017; Thielman, 2015).
Operation Beebus	12.04.2011-07.02.2013	Contractors of the US Department of Defense	China	Spear phishing emails	Unknown	Theft of intellectual property and industrial secrets (Maness and Valeriano, 2017; Paganini, 2013).

Campaign	Time period	Victim(s)	Alleged perpetrator's origin	Infection methods	Malware used	Damage
Penn State Engineering breach	01.09.2012-15.05.2015	Penn State College of Engineering	China	Unknown	Unknown	Theft of information on students and staff (Maness and Valeriano, 2017; Vinton, 2015).
Operation Iron Tiger	15.01.2013-16.09.2015	US IT, telecom, energy and manufacturing companies, but also victims in Asia	China	Spear phishing	Gh0stNet RAT, PlugX and other malware	Theft of emails, intellectual property and strategic planning documents (Chang et al., 2015; Maness and Valeriano, 2017).
University of Connecticut Engineering Hack	24.09.2013-09.03.2015	University of Connecticut School of Engineering	China	Unknown	Unspecified malware	Theft of research data and login credentials (Breen, 2015; Maness and Valeriano, 2017).
OPM hack	15.03.2014-17.03.2015	The US Office of Personnel Management	China	Unknown	PlugX RAT	Theft of information on federal employees (Koerner, 2016; Schmidt et al., 2015).

7 Glossary

Anti-Access/Area Denial (A2/AD): The act of denying and/or limiting an adversary's ability to freely operate and use its capabilities on and/or in a specific contested region on either land, sea, air, space and cyberspace or in all of these realms (Russell, 2015, p. 154).

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

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).

Command and Control (C2): "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission" (US Department of Defense, 2017, p. 43).

Command and Control infrastructure (C&C): A server through which the person controlling malware communicates with it in order to send commands and retrieve data (QinetiQ Ltd, 2014, p. 2).

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

Domain Name Service (DNS): Domain Name Service (DNS): The address structure that translates Internet Protocol addresses into a string of letters that is easier to remember and use (Internet Corporation For Assigned Names and Numbers, 2016).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

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

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

Portable Network Graphics (PNG) file: A computer file, usually an image, using an extensible format with a compression algorithm to allow data to be flawlessly reconstructed from the compressed data (PNG Homesite, 2017).

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.

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

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).

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

Trojan horse: Malware hidden in a legitimate program in order to infect and hijack a system (Ghernaouti-Hélie, 2013, p. 441).

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

Worm: Standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012, p. 81).

8 Abbreviations

A2/AD	Anti-Access/Area-Denial
C2	Command and Control
C&C	Command and Control infrastructure
CNO	Computer Network Operations
CPC	Communist Party of China
DDoS	Distributed Denial of Service
DNS	Domain Name System
EW	Electronic Warfare
ICANN	Internet Corporation for Assigned Names and Numbers
IT	Information Technology
ITU	International Telecommunications Union
NGO	Non-Governmental Organization
NSA	National Security Agency - USA
OPM	Office of Personnel Management - USA
PLA	People Liberation Army - China
PNG	Portable Network Graphics
RAT	Remote Access/Administration Tool
SIGINT	Signal Intelligence
SSF	Strategic Support Force - China
UN	United Nations

9 Bibliography

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

Appelbaum, J., Gibson, A., Guarnieri, C., Müller-Maguhn, A., Poitras, L., Rosenbach, M., Ryge, L., Schmundt, H., Sontheimer, M., 2015. NSA Preps America for Future Battle [WWW Document]. Spieg. Online. URL http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html (accessed 29.7.17).

Atanassova-Cornelis, E., Van der Putten, F.-P., 2015. Strategic Uncertainty and the Regional Security Order in East Asia [WWW Document]. E-Int. Relat. URL http://www.e-ir.info/2015/11/24/strategic-uncertainty-and-the-regional-security-order-in-east-asia/ (accessed 12.7.17).

Baldor, L.C., 2017. US to create independent military cyber command [WWW Document]. ABC News. URL http://abcnews.go.com/Technology/wireStory/us-create-independent-military-cyber-command-48675223 (accessed 19.7.17).

Breen, T., 2015. UConn Responds to Data Breach at School of Engineering [WWW Document]. Uconn Univ. Conn. URL http://today.uconn.edu/2015/07/uconn-responds-to-data-breach-at-school-of-engineering/ (accessed 28.7.17).

Brenner, B., 2005. Myfip's Titan Rain connection [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/news/1120855/Myfips-Titan-Rain-connection (accessed 20.7.17).

Brown, G., Yung, C.D., 2017a. 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 10.7.17).

Brown, G., Yung, C.D., 2017b. 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 10.7.17).

Brown, G., Yung, C.D., 2017c. 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 10.7.17).

Center for Strategic and International Studies, McAfee, 2014. Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II. McAfee, Santa Clara, CA.

Chabrow, E., 2015. Cyber Lexicon: U.S., China Speak Different Languages [WWW Document]. Bank Info Secur. URL https://www.bankinfosecurity.com/blogs/cyber-lexicon-us-china-speak-different-languages-p-1936 (accessed 18.9.17).

Chabrow, E., 2014. The Real Aim of U.S. Indictment of Chinese [WWW Document]. Bank Info Secur. URL https://www.bankinfosecurity.com/real-aim-us-indictment-chinese-a-6854 (accessed 18.9.17).

Chang, Z., Lu, K., Luo, A., Pernet, C., Yaneza, J., 2015. Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors, TrendLabs Research Paper. TrendMicro.

Cheng, D., 2014. The U.S. Needs an Integrated Approach to Counter China's Anti-Access/Area Denial Strategy [WWW Document]. Herit. Found. URL http://www.heritage.org/defense/report/the-us-needs-integrated-approach-counter-chinas-anti-accessarea-denial-strategy (accessed 11.7.17).

Colby, E.A., 2013. Defining Strategic Stability: Reconciling Stability and Deterrence, in: Strategic Stability: Contending Interpretations. Strategic Studies Institute and U.S. Army War College Press, Carlisle, PA, pp. 47–83.

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

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

Davidson, L., 2016. China's Strategic Support Force: The New Home of the PLA's Cyber Operations? [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog-post/chinas-strategic-support-force-new-home-plas-cyber-operations (accessed 13.7.17).

Economy, E.C., Kurlantzick, J., Blackwill, R.D., 2017. Territorial Disputes in the South China Sea [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/global/global-conflict-tracker/p32137#!/conflict/territorial-disputes-in-the-south-china-sea (accessed 26.7.17).

FireEye Inc., 2014. POISON IVY: Assessing Damage and Extracting Intelligence (Special Report). FireEye Inc., Milpitas, CA.

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 7.6.17).

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

Gilli, A., Gilli, M., 2017. Military-Technological Superiority, Systems Integration and the Challenges of Imitation, Reverse Engineering, and Cyber-Espionage.

Glendinning, L., 2008. Obama, McCain computers "hacked" during election campaign [WWW Document]. The Guardian. URL https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa (accessed 20.7.17).

Gompert, D.C., Libicki, M., 2014. Cyber Warfare and Sino-American Crisis Instability. Survival 56, 7–22. https://doi.org/10.1080/00396338.2014.941543

Greenwald, G., MacAskill, E., Poitras, L., 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed 13.11.17).

Grow, B., Hosenball, M., 2011. Special report: In cyberspy vs. cyberspy, China has the edge [WWW Document]. Reuters. URL http://www.reuters.com/article/us-china-usa-cyberespionage-idUSTRE73D24220110414?pageNumber=1 (accessed 20.7.17).

Harold, S.W., 2016. The U.S.-China Cyber Agreement: A Good First Step [WWW Document]. RAND Corp. URL https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html (accessed 11.7.17).

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 20.9.17).

Hempel, A., 2016. A Guide to Chinese Naval Anti-Access/Area Denial (A2/AD) [WWW Document]. WhiteFleet.net. URL https://whitefleet.net/2016/08/21/a-pocket-guide-to-chinese-naval-anti-accessarea-denial-a2ad/ (accessed 11.7.17).

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 3.8.17).

Internet Corporation For Assigned Names and Numbers, 2017. ICANN History Project [WWW Document]. Internet Corp. Assigned Names Numbers. URL https://www.icann.org/history#timeline (accessed 26.7.17).

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 4.11.16).

Internet eXchange Federation, n.d. Definition of an Internet Exchange Point [WWW Document]. IX-FInternet Exch. Fed. URL http://www.ix-f.net/ixp-definition.html (accessed 12.12.16).

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 7.6.17).

Kazianis, H., 2013a. The Real Anti-Access Story: Cyber [WWW Document]. The Diplomat. URL http://thediplomat.com/2013/05/the-real-anti-access-story-cyber/ (accessed 10.7.17).

Kazianis, H., 2013b. America's Anti-Access Nightmare Coming True [WWW Document]. RealClear Def. URL http://www.realcleardefense.com/articles/2013/05/21/americas_anti-access_nightmare_coming_true_106609.html (accessed 12.7.17).

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

Koerner, B.I., 2016. Inside the Cyberattack That Shocked the US Government [WWW Document]. Wired. URL https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (accessed 3.8.17).

Korolov, M., 2017. Russia, China -- and the US -- are biggest geopolitical cybersecurity threats [WWW Document]. CSOonline.com. URL https://www.csoonline.com/article/3156554/it-strategy/russia-china-and-the-us-are-biggest-geopolitical-cybersecurity-threats.html (accessed 20.9.17).

Kostadinov, D., 2013a. GhostNet – Part I [WWW Document]. Infosec Inst. URL http://resources.infosecinstitute.com/ghostnet-part-i/#gref (accessed 7.6.17).

Kostadinov, D., 2013b. GhostNet – Part II [WWW Document]. Infosec Inst. URL http://resources.infosecinstitute.com/ghostnet-part-ii/ (accessed 8.6.17).

Kshetri, N., 2013. Cyber-victimization and cybersecurity in China. Commun. ACM 56, 35. https://doi.org/10.1145/2436256.2436267

Lindsay, J.R., 2015a. Exaggerating the Chinese Cyber Threat.

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

Lindsay, J.R., 2015c. Inflated Cybersecurity Threat Escalates US-China Mistrust. New Perspect. Q. 32, 17–21. https://doi.org/10.1111/npqu.11521

Maness, R.C., Valeriano, B., 2017. The Dyadic Cyber Incident and Dispute Data, Versions 1.5 Incidents only 20 jan.

Maness, R.C., Valeriano, B., 2014. The Dyadic Cyber Incident and Dispute Data, Versions 1.

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 19.7.17).

Markoff, J., 2009. Vast Spy System Loots Computers in 103 Countries [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2009/03/29/technology/29spy.html (accessed 24.7.17).

McAfee Foundstone Professional Services, McAfee Labs, 2011. Global Energy Cyberattacks: "Night Dragon." McAfee, Santa Clara, CA.

McAfee Labs, McAfee Foundstone Professional Services, 2010. Protecting Your Critical Assets Lessons Learned from "Operation Aurora." McAfee, Santa Clara, CA.

McConnell, B., 2015. What Do the Obama-Xi Agreements Mean for Cyber? [WWW Document]. China-US Focus. URL http://www.chinausfocus.com/peace-security/what-do-the-obama-xi-agreements-mean-for-cyber (accessed 7.6.17).

McWhorter, D., 2013. Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (accessed 18.5.17).

Microsoft, 2016. SQL Injection [WWW Document]. Microsoft TechNet. URL https://technet.microsoft.com/en-us/library/ms161953(v=SQL.105).aspx (accessed 29.11.16).

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 7.6.17).

Nakashima, E., 2013. U.S. and Russia sign pact to create communication link on cyber security [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html?utm_term=.43685f50a5a5 (accessed 20.9.17).

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

NSA/CSS, 2016. Frequently Asked Questions About NSA [WWW Document]. NSA/CSS. URL https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml (accessed 13.11.17).

O'Brien, R.D., Shen, S., 2013. The U.S., China, and Cybersecurity: The Ethical Underpinnings of a Controversial Geopolitical Issue [WWW Document]. Carnegie Counc. Ethics Int. Aff. URL https://www.carnegiecouncil.org/publications/articles_papers_reports/0156 (accessed 20.9.17).

Olenick, D., 2017. U.S.-China Cyber Agreement: Flawed, but a step in the right direction [WWW Document]. SC Mag. US. URL https://www.scmagazine.com/us-china-cyber-agreement-flawed-but-a-step-in-the-right-direction/article/633533/ (accessed 11.7.17).

Paganini, P., 2013. Operation Beebus, another chinese cyber espionage campaign [WWW Document]. Secur. Aff. URL http://securityaffairs.co/wordpress/12216/hacking/operation-beebus-another-chinese-cyber-espionage-campaign.html (accessed 29.7.17).

PNG Homesite, 2017. Portable Network Graphics [WWW Document]. PNG Homesite. URL http://www.libpng.org/pub/png/#history (accessed 17.10.17).

Price, P., 2013. Sunnylands Summit With U.S. And China Presidents Ends On Positive Note [WWW Document]. Forbes. URL https://www.forbes.com/sites/pamprice/2013/06/10/sunnylands-summit-with-u-s-and-china-presidents-ends-on-positive-note/#5585a6101a84 (accessed 19.7.17).

QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.

Radware, 2015. DDoS HANDBOOK.

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

Reuters, 2015. China oil rig to keep drilling in waters disputed with Vietnam [WWW Document]. Reuters. URL http://www.reuters.com/article/us-southchinasea-china-vietnam-idUSKCN0QU0UG20150825 (accessed 26.7.17).

Rosenblatt, S., Cipriani, J., 2015. Two-factor authentication: What you need to know (FAQ) [WWW Document]. CNet. URL https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ (accessed 14.12.16).

Russell, A.L., 2015. Strategic anti-access/area denial in cyberspace. IEEE, pp. 153–168. https://doi.org/10.1109/CYCON.2015.7158475

Sanger, D.E., Perlroth, N., 2014. N.S.A. Breached Chinese Servers Seen as Security Threat [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html (accessed 14.7.17).

Schmidt, M.S., Sanger, D.E., Perlroth, N., 2015. Chinese Hackers Pursue Key Data on U.S. Workers [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0 (accessed 28.7.17).

Segal, A., 2017. The Continued Importance of the U.S.-China Cyber Dialogue [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog-post/continued-importance-us-china-cyber-dialogue (accessed 11.7.17).

Segal, A., 2016. The U.S.-China Cyber Espionage Deal One Year Later [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog-post/us-china-cyber-espionage-deal-one-year-later (accessed 11.7.17).

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 4.11.16).

Smith, S., Economy, E.C., Snyder, S.A., Blackwill, R.D., 2017. Tensions in the East China Sea [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/global/global-conflict-tracker/p32137#!/conflict/tensions-in-the-east-china-sea (accessed 26.7.17).

Spiegel Online, 2014. NSA Spied on Chinese Government and Networking Firm [WWW Document]. Spieg. Online. URL http://www.spiegel.de/international/world/ns

a-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html (accessed 14.7.17).
Stratfor Worldview, 2017. East Asian Maritime Claims.
Symantec Corporation, 2011. Trojan.Hydraq [WWW Document]. Symantec. URL https://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-99 (accessed 3.8.17).
Symantec Security Response, 2010. Hydraq - An Attack of Mythical Proportions [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions (accessed 3.8.17).
TeleGeography, 2017. TeleGeography Submarine Cable Map [WWW Document]. TeleGeography. URL https://www.submarinecablemap.com/ (accessed 26.7.17).
The White House, Office of the Press Secretary, 2015. FACT SHEET: President Xi Jinping's State Visit to the United States [WWW Document]. White House. URL https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed 13.7.17).
Thielman, S., 2015. Chinese hack of US national security details revealed days after Russian hack [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2015/aug/10/chinese-national-security-officials-hack (accessed 29.7.17).
Tiezzi, S., 2015. The Limits of a US-China Cyber Deal [WWW Document]. The Diplomat. URL http://thediplomat.com/2015/09/the-limits-of-a-us-china-cyber-deal/ (accessed 10.7.17).
Torruella, R.A., 2014. Determining Hostile Intent in Cyberspace. Jt. Force Q. 75 114–121.
UK Foreign & Commonwealth Office, 2015. UK-China Joint Statement 2015 [WWW Document]. GOV.UK. URL https://www.gov.uk/government/news/uk-china-joint-statement-2015 (accessed 13.7.17).
US Department of Defense, 2017. DOD Dictionary of Military and Associated Terms.
Van der Putten, F.-P., 2017. The East and South China Sea Tensions [WWW Document]. Clingendael. URL https://www.clingendael.nl/publication/east-and-south-china-sea-tensions (accessed 12.7.17).
Vinton, K., 2015. Penn State College Of Engineering Network Disabled Following Two "Incredibly Serious" Cyber Attacks [WWW Document]. Forbes. URL https://www.forbes.com/sites/katevinton/2015/05/15/penn-state-college-of-engineering-network-disabled-following-two-incredibly-serious-cyber-attacks/#5976416350c4 (accessed 29.7.17).
Wei, Y., 2016. China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty [WWW Document]. Henry M Jackson Sch. Int. Stud. URL https://www.theglobalist.com/cyber-diplomacy-us-china-problem/ (accessed 12.7.17).
Wired Staff, 1997. The Great Firewall of China [WWW Document]. WIRED. URL https://www.wired.com/1997/06/china-3/ (accessed 19.7.17).
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 13.7.17).
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 13.7.17).

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.