CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Use of cybertools in regional tensions in Southeast Asia

Zürich, August 2018

Version 1

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

CSS
ETH Zurich

ETH zürich

Author: Marie Baezner

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

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

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

Please cite as: Baezner, Marie (2018): Hotspot Analysis: Use of cybertools in regional tensions in Southeast Asia, August 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Targets:	Government and military agencies, businesses, Association of Southeast Asian Nations (ASEAN)[1] entities and meetings.
Tools:	Various malware[2] families, website defacements, Distributed Denial of Service (DDoS) attacks.
Effects:	Use of website defacements and DDoS attacks as patriotic reactions, economic loss due to cyberespionage, discovery of new malware, cyberespionage campaigns from China and other actors causing increased tensions, patriotic hackers reacting to physical events and risking an escalation, use of cyber capabilities in Anti-Access/Area Denial (A2/AD) strategy, ASEAN as platform for cooperation and development of cybernorms.
Timeframe:	From early 2000s and still ongoing.

Southeast Asia has a dynamic and growing economy and is an important shipping route. Yet tensions born from disputed territorial claims over islands in the South China Sea constitute a risk for the stability of the region. While China is an important economic partner for the region, it also acts as an adversary. Malicious cyber-activities have thrived in Southeast Asia, employing a range of techniques from cyberespionage campaigns to patriotic hacking.

This Hotspot Analysis examines cyber-activities in Southeast Asia and their role in affecting regional dynamics. The aim of this analysis is to better understand how cybertools interact with and exacerbate regional tensions.

Description

In part due to conflicting territorial claims and substantial economic growth, Southeast Asia has been the theater of various cyberattacks. The majority of these affronts originated from Chinese actors, which in all likelihood hold ties to the Chinese government. These groups engaged in cyberespionage against foreign government and military agencies, businesses in Southeast Asia and ASEAN entities. Regional actors, like APT32 a Vietnamese hacker group, also conducted cyberespionage campaigns against government officials in neighboring states, local dissidents and businesses using customized and freely available malware. However, the most prominent actors in Southeast Asian cyberspace were the patriotic hackers from several Southeast Asian states who defaced websites and launched DDoS attacks in response to military clashes in the South China Sea.

Effects

The social effects of cyber-activities in Southeast Asia consist of patriotic hackers using website defacements and DDoS attacks to provoke their adversaries and garner attention. Their goal is to respond to what they consider as an infringement of their state's sovereignty and to generate fear among their adversary's population.

The economic effect of these cyberattacks are the financial losses generated by cyberespionage campaigns. Businesses that have had their intellectual property stolen have lost economic advantage.

The technological effect includes the discovery of new customized malware that was used to spy on targets in Southeast Asia. Some malware families were highly sophisticated and could steal information from air-gapped networks.

The effects at the international level were numerous. First, China was the primary perpetrator behind many of the cyberespionage campaigns in Southeast Asia which went on to exacerbate tensions in the region. Tensions were more easily inflamed due to existing hostilities between Southeast Asian states over territorial claims in the South China Sea. Cyberespionage campaigns also increased the risk of misinterpretation in cyberspace and the potential to escalate an incident to the point of conventional warfare. APT32, a Vietnamese actor, also engaged in cyberespionage against domestic targets and neighboring states' government agencies – even those of supposed allies. Second, patriotic hackers' attacks also risked escalating tensions. Patriotic hacking is more likely to inflame tensions as these attacks are often reactions to physical clashes and concern contested subjects. Third, China is establishing A2/AD zones in the South China Sea and cyber capabilities are included in its strategy. Cyber capabilities could be used in the event of a conventional war to disrupt communications or GPS localization. Finally, cybersecurity awareness and capacity is highly variable among Southeast Asian states. ASEAN is used as a platform to promote and discuss cybersecurity issues and cooperation to bring all ASEAN member states to a more unified level of cybersecurity.

Policy Consequences

The policy recommendations that may help mitigate possible cyberattacks, similar to these found in Southeast Asia, focus on improving cybersecurity measures and monitoring the development of tensions in the South China Sea.

[1] Abbreviations are listed in Section 9.

[2] Technical terms are explained in a glossary in Section 8.

1 Introduction

Southeast Asia is a growing market, providing an attractive environment for investment and technological developments. The region is also an important crossroad for the global shipping sector as half of all international shipping travels through the South China Sea. However, tensely disputed territorial claims in the area threaten to destabilize the region. China may be a principal economic partner of the region, but it also serves as an adversary. Closely connected technological growth in the region has helped states to develop their economies, but has also brought new vulnerabilities. In the case of Southeast Asia, malicious cyber-activities are flourishing. The principal technique is cyberespionage, which largely originated from China. In addition to cyberespionage, physical clashes in the South China Sea often prompted website defacements[3] and Distributed Denial of Service (DDoS)[4] attacks from Southeast Asian patriotic hackers online.

This Hotspot Analysis examines cyber-activities in Southeast Asia and the role they play in affecting regional tensions and clashes. Cyberattacks are among a number of tools at the disposal of Southeast Asian states that can be used to respond to increased tensions over territorial claims. The goal of the analysis is to provide a better understanding of the mechanics of the use of cybertools in regional tensions.

The Hotspot Analysis will be updated as new information is discovered or significant changes occur. The aim of an update is to keep the document relevant with current information and as accurate as possible. This analysis will also be used in a broader report that is intended to compare various Hotspot Analyses and to provide recommendations to states on ways to improve their cybersecurity policies.

This Hotspot Analysis is organized as follows: Section 2 describes the historical and international context in Southeast Asia to help better understand the setting in which cyber-activities take place. A chronology summarizes the major physical events in the South China Sea and cyber-incidents throughout Southeast Asia.

Section 3 details the various actors involved in cyber-activities in Southeast Asia. This section shows that the majority of actors originate from China, but actors from other states also play a significant role. Following this, the various types of targets in Southeast Asian are described. This will show that perpetrators did not only target governments and businesses, but also an international organization: the Association of Southeast Asian Nations (ASEAN). Finally, details on the tools and techniques used by the various actors in their campaigns in Southeast Asia will be outlined.

Section 4 analyzes the effects of cyber-activities in Southeast Asia. The first subsection concerns the social consequences of these cyber-activities. These results largely consist of website defacements and DDoS attacks getting more attention than cyberespionage campaigns, and thereby generating more fear in the population.

The second subsection focuses on the economic repercussions of cyber-activities in Southeast Asia. The economic effect on the region is limited to the loss in economic comparative advantage due to cyberespionage. Because of its lucrative technological market and its growing digitalized economy, Southeast Asia attracts cyberespionage and cybercriminals.

The third subsection describes the technological consequences. This effect is concentrated on the discovery of sophisticated malware families that were only observed in Southeast Asian targets' networks.

The fourth subsection analyzes four international effects of cyber-activities in Southeast Asia. First, cyberespionage originates mainly from China, but also from other regional actors like Vietnam. Cyberespionage from China is not a surprise and aligns with the state's growing interest in technological industry and the fact that China is the primary economic partner of the region. Cyberespionage originating from Vietnam is more difficult to explain, but was most likely for economic advantages and intelligence. Second, patriotic hackers conducted their cyberattacks as reactions to physical events in the South China Sea. These cyberattacks also risked escalating existing tensions among the involved states. Third, China is establishing Anti-Access/Area Denial (A2/AD) zones in the South China Sea and effective cybertools are part of its strategy to disrupt communications and GPS localization in the event of a conventional conflict. Finally, states in Southeast Asia use ASEAN as a platform to discuss cybernorms and develop cooperation in cybersecurity.

Finally, Section 5 suggests a series of policy recommendations for mitigating the risk for states to be impacted by similar cyberattacks as the ones seen in Southeast Asia. It proposes ways to improve cybersecurity and recommends closely monitoring developments in the South China Sea.

[3] Technical terms are explained in a glossary in Section 8.

[4] Abbreviations are listed in Section 9.

2 Background and chronology

Southeast Asia is an important global trading route, and approximatively half of all commercial shipping passes through the South China Sea. The region is also rich in oil, natural gas and fish. Because of its strategic and economic advantages, the South China Sea also plays host to a number of territorial disputes. This includes the conflicting Chinese and Vietnamese claims over the Paracel Islands, and Chinese and Filipino claims over the Spratly Islands (FireEye Inc. and Singtel, 2015). The tensions created by these ongoing turf wars regularly escalate into localized disputes in which cyber-activities also play a role. Various cyberactors from these states attempt to influence events on the ground through either hacktivism or cyberespionage.

Simultaneously, cooperation among Southeast Asian states has also increased significantly since the 1960s. ASEAN serves as a framework and forum for states to discuss all range of issues including cybersecurity. ASEAN can also include external partners in discussions, including India, China, Japan and Australia to better learn from one another.

The following chronology provides an overview of the history of cybersecurity cooperation between Southeast Asian states, the various disputes related to the South China Sea, and the subsequent cyber-activities that often arise in response. The chronology includes the major cyberactors involved in Southeast Asia and their primary methods.

Rows colored in gray refer to cyber-related incidents[5].

Date	Event
1951	The USA and the Philippines sign a Mutual Defense Treaty (Glaser, 2012).
08.08.1967	Indonesia, Malaysia, the Philippines, Singapore, and Thailand sign the ASEAN Declaration that creates ASEAN (ASEAN University Network, 2012).
1971	China installs military infrastructure on islands belonging to the disputed Paracel Islands.
1974	China and Vietnam confront one another militarily about maritime issues in the South China Sea (Lt. Cmdr. Benson, 2012).
07.01.1987	Brunei joins ASEAN (ASEAN University Network, 2012).
1988	China and Vietnam clash militarily over maritime issues in the South China Sea (Lt. Cmdr. Benson, 2012).
28.07.1995	Vietnam joins ASEAN.
23.07.1997	Laos and Myanmar join ASEAN (ASEAN University Network, 2012).
1999	The Philippines beaches a military ship on the shores of the Second Thomas Shoal in the Spratly Islands and uses it as a military post (Glaser, 2015).
30.04.1999	Cambodia joins ASEAN (ASEAN University Network, 2012).
01.04.2001	A US military plane collides mid-air with a Chinese fighter jet and causes an international dispute.
04.2001	Chinese patriotic hackers target US websites as retaliation for the aircraft collision (Kozy, 2015).
2002	ASEAN members and China sign the Declaration on the Conduct of Parties in the South China Sea, designed to regulate state relations in the South China Sea (Glaser, 2012).
2005	The Philippines issues its national cybersecurity strategy.
2006	Malaysia issues its national cybersecurity strategy.
2009	Japan and ASEAN members hold their first Information Security Policy Meeting (Parameswaran, 2017).
05.03.2009	Chinese People's Liberation Army (PLA) vessels maneuver close to US Navy ships in the South China Sea, aggravating existing tensions.
2011	Vietnam accuses China of cutting the cables of ships surveilling oil and gas reserves in the Vietnamese Exclusive Economic Zone (EEZ) (Glaser, 2012).
09.2011	China and other Asian countries push for a United Nations (UN) international code of conduct for information security (Brown and Yung, 2017).
06.2011	Chinese and Vietnamese patriotic hackers engage in a tit-for-tat website defacement and DDoS attack campaign over the allegation that China cut cables of oil and gas surveilling ships (Balduzzi et al., 2018).
10.2011	China and Vietnam sign an agreement outlining principles for solving maritime issues (Glaser, 2012).

[5] A more detailed list of cyber-activities in Southeast Asia can be found in Annex 1.

08.04.2012	The Chinese Coast Guard restricts access to Filipino fishermen to the Scarborough Shoal reef, which has abundant fish, oil, and gas reserves.
04-05.2012	Chinese and Filipino patriotic hackers engage in a tit-for-tat defacement campaign in reaction to the Scarborough Shoal dispute (Glaser, 2015; Passeri, 2012).
15.11.2012	Xi Jinping becomes the General Secretary of the Communist Party of China (Davidson, 2016). He adopts a more aggressive stance in regard to territorial claims in the South China Sea (ThreatConnect and Defense Group, 2015).
22.01.2013	The Philippines files a complaint to the United Nations Permanent Court of Arbitration (UNPCA) against China over issues in the South China Sea (Economy et al., 2017).
05.2013	Filipino and Taiwanese patriotic hackers engage in a tit-for-tat website defacement and DDoS attack campaign over an incident between a Taiwanese fishing boat and the Filipino Coast Guard (Balduzzi et al., 2018).
11.2013	China establishes an Air Defense Identification Zone (ADIZ) in the East China Sea, raising tensions with the USA and Japan. States in the South China Sea fear that China would try to establish similar zones there (ThreatConnect Research Team, 2014).
2014	APT32, a Vietnamese Advanced Persistent Threat (APT), targets a Vietnamese security firm, a German company doing business in Vietnam, and the Vietnamese diaspora in Southeast Asia with spear phishing emails (Carr, 2017).
03.2014	China tries to stop the resupply of the beached military ship on the Second Thomas Shoal, worsening tensions with the Philippines (Glaser, 2015).
08.03.2014	Malaysian Airlines flight MH370 disappears in flight en route to China.
11.03.2014	Naikon, a Chinese APT, targets countries involved in the search effort for the flight MH370 using spear phishing emails with an attachment related to the flight disappearance (Raiu and Golovkin, 2015).
05.2014	China deploys a deep-sea oil rig in Vietnamese EEZ that starts a dispute with Vietnam (Glaser, 2015).
05.2014	Chinese patriotic hackers deface Vietnamese government websites as part of the maritime dispute. Goblin Panda, a Chinese APT, targets the Vietnamese government with spear phishing emails as part of the oil rig incident (Kozy, 2015).
12.2014	Japan and ASEAN Defense Ministers hold an informal meeting where cybersecurity issues are discussed (Parameswaran, 2017).
2015	ASEAN launches its Cyber Security Agency (Heinl, 2018).
04-05.2015	While China builds infrastructure on the Spartly Islands, Filipino and Vietnamese patriotic hackers unite for a campaign of website defacements and DDoS attacks against Chinese websites (Balduzzi et al., 2018).
09.07.2015	A Chinese APT infects the UNPCA website to spy on visitors to the page researching the disagreement between the Philippines and China (ThreatConnect Research Team, 2014).
01.12.2015	APT16, a Chinese APT, targets the Taiwanese media and government with a spear phishing campaign (Jiang et al., 2015; Winters, 2015).
2016	Vietnam develops a strategic plan to strengthen its cybersecurity.
2016	Indonesia and Russia sign a cooperation agreement on cybersecurity issues (Baka, 2016).
2016	The Philippines creates a cybersecurity working group within the ASEAN Defense Ministers Meeting structure and ASEAN holds its first Ministerial Meeting on cybersecurity (Heinl, 2018; Parameswaran, 2017).
2016	China allows Filipino fishermen to access the Scarborogh Shoal again (Mogato, 2017).
2016	Singapore issues its national cybersecurity strategy.
2016	APT32 spies on Filipino technology firms and a Chinese hospitality developer (Carr, 2017).

07.2016	A Chinese patriotic hacker, 1937cn, hacks into the network of three large Vietnamese airports and defaces the flight information screens with pro-China slogans (Baka, 2016).
12.07.2016	The UNPCA delivers its ruling in favor of the Philippines on the issues in the south China Sea (Economy et al., 2017).
08.2016	Tropic Trooper, an APT of unknown origin, targets Taiwanese government officials and a Taiwanese energy company with spear phishing emails (Ray et al., 2016).
10.2016	Singapore announces its intentions to create an ASEAN Cybersecurity Capacity Program (ACCP) (Parameswaran, 2016).
2017	Japan and the UK hold a workshop on cybersecurity in Brunei for Southeast Asian states (Matsubara, 2018).
2017	ASEAN issues a Cybersecurity Cooperation Strategy (Heinl, 2018).
2017	APT32 targets the Vietnamese diaspora in Australia and Filipino government officials with spear phishing emails (Carr, 2017).
01.2017	Numbered Panda, a Chinese APT, targets the Taiwanese government with a new sample of the malware IXESHE (Crowdstrike, 2018).
04.2017	Singapore launches the ACCP (Heinl, 2018).
03.2018	The cybersecurity firm ESET publishes a report on APT32's new backdoor targeting corporations and governments in Vietnam, the Philippines, Laos, and Cambodia (ESET, 2018).
06.2018	ASEAN and Japan launch the ASEAN - Japan Cybersecurity Capacity Building Center (AJCCBC) in Thailand (Parameswaran, 2018).

3 Description

This section details the numerous actors conducting cyberattacks in Southeast Asia. While the majority of actors originate from China, smaller perpetrators from throughout the region still have significant capabilities and influence. The section also summarizes the types of targets that these actors attack and their tools.

3.1 Attribution and actors

Attribution is a significant, and challenging, part of cybersecurity. Attribution is usually determined through digital forensics, using technical evidence and analysis to interpret which actors may benefit from the cyberattack (the logic of "*cui bono*"). However, attribution can never be determined with complete certainty. Actors can confuse investigators by disguising technical evidence as originating from an alternative source. It is important to bear in mind that there is always the possibility that the alleged perpetrator of a cyberattack may not be the actual attacker. In addition, this Hotspot Analysis is based on sources in the English language from academia, media and cybersecurity firms. These sources usually deliver points of view and opinions that other, non-English language sources may not hold.

Numerous actors are involved in cybersecurity issues in Southeast Asia. The strategic nature of the region attracts a variety of actors that seek to gain tactical and/or economic advantages over other states. While Southeast Asia is a lucrative market for technological investment, with a growing market of internet users and an increasing digital economy, cybersecurity development and awareness throughout the area requires improvement. Due to limited levels of cyber literacy, Southeast Asian states tend to be passive actors when it comes to cybersecurity (Matsubara, 2018). This may make it easier for major cybersecurity actors, primarily Chinese hacker groups, to wreak significant damage. This is also true of non-Chinese cyberthreats, most notably a Vietnamese APT and other APTs whose origin could not be identified. Additionally, patriotic hackers from Southeast Asian states were involved in website defacements and DDoS attacks during maritime disputes in the South China Sea.

Chinese actors involved in Southeast Asia

Naikon

The cybersecurity firm ThreatConnect has identified Naikon[6] as being part of the Chinese PLA's 2nd

[6] Naikon is also known as Unit 78020 in the PLA's 2nd Reconnaissance Bureau and Lotus Panda.

Reconnaissance Bureau. Naikon has been active since at least 2010 and targets government officials, military agencies, media and energy firms in ASEAN member states. ThreatConnect and Kaspersky Lab have stated that Naikon is highly successful at infiltrating their victims' systems to gather geopolitical intelligence. Naikon is well-organized and has separate campaigns for each targeted state, but sometimes reuses cybertools or infrastructure in other campaigns. Naikon relies on socially engineered spear phishing emails with decoy attachments on regional geopolitical issues to infect its targets' networks. Naikon uses a combination of legitimate cybertools and the group's own customized malware in their campaigns. The APT's goal is to stay undetected for as long as possible in a network to gather as much information as possible. (Aquino, 2013; Baumgartner and Golovkin, 2015a, 2015b; ThreatConnect and Defense Group, 2015).

APT30

The cybersecurity firm FireEye believes that APT30 is sponsored by the Chinese government and has been active since at least 2005. APT30 targets governments and industries in Southeast Asia for intelligence that aligns with the strategic needs of the Chinese government. The APT has been particularly interested in information on ASEAN meetings. APT30 attaches specifically crafted documents in spear phishing emails to better lure their targets. APT30 uses a very limited number of malware, despite the fact they have been active for more than ten years. FireEye has argued that APT30 may not have modernized its cybertool arsenal because the group consistently modified, updated and improved its malware. These abilities demonstrate that the APT has the skills and resources to adapt its cybertools to its varying needs. APT30 also demonstrated an ability to steal information from air-gapped networks (FireEye Labs, 2015).

Kaspersky Lab has identified some similarities between Naikon and APT30 but the evidence is insufficient to prove the two groups are one entity. The cybersecurity experts recognized that a keylogging tool from Naikon was very similar to a keylogging tool from APT30. Both groups also seemed to have shared strings of code for their malware (Baumgartner and Golovkin, 2015a, 2015b). These similarities and crossovers make other cybersecurity experts believe that APT30 and Naikon may in fact be the same group.

Numbered Panda

Numbered Panda[7] is a Chinese APT believed to have ties to the PLA. The APT is thought to have been active since at least 2009. Numbered Panda usually spies on journalists, government officials and defense industries in East and Southeast Asia. Numbered Panda delivers its malware through spear phishing emails with lure documents on regional geopolitical events (FireEye Inc., 2018; Meyers, 2013).

APT16

APT16 is a group from China that targets high-tech companies, media outlets, financial institutions, and government officials in Taiwan, Hong Kong and Japan. APT16 seems to be interested in intelligence gathering and has demonstrated the ability to quickly use recently discovered exploits. APT16 usually infiltrates its victims through spear phishing emails. Based on the resources used and the types of targets, it is very likely that APT16 also has ties to the Chinese government (FireEye Inc., 2018; Jiang et al., 2015; Winters, 2015).

Goblin Panda

Goblin Panda[8] is an APT from China that targeted the Vietnamese government during the dispute over the oil rig in 2014. The APT group has also targeted institutions in Myanmar. Goblin Panda and Naikon sometimes target the same victims. However, it is unclear if Naikon and Goblin Panda conduct coordinated cyberattacks or are aware of the other's presence in their victims' networks. it is likely that Goblin Panda has ties to the Chinese government (Baumgartner and Golovkin, 2015a; Crowdstrike, 2018; Kozy, 2015).

Icefog

Kaspersky Lab identified Icefog[9] as a Chinese APT that had been active since at least 2011. Icefog targets defense industries and telecom companies in Taiwan, South Korea, and Japan. They infect their victims through spear phishing emails exploiting known vulnerabilities. Kaspersky Lab has stated that Icefog is not a highly sophisticated group, but it is nevertheless effective. The specificity of this APT is to use Command and Control infrastructure (C&C) only for the period of time needed to infect and get the required information. Icefog's campaigns are extremely focused and operate in a "hit-and-run" modus. Kaspersky Lab added that the group may be a group of mercenaries hired for cyberespionage campaigns (Kaspersky Lab, 2013).

[7] Numbered Panda is also known as IXESHE, TG-2754, APT12, BeeBus, Calc Team, Group 22, DynCalc, Crimson Iron and DNSCalc.

[8] Goblin Panda is also known as Cycldek.

[9] Icefog is also known as Dagger Panda.

DragonOK

DragonOK is an APT originating from China and targeting high-tech industries in Japan and Taiwan. Its motive may be to gain economic competitive advantage. The group uses spear phishing emails to infect its victims. It is unclear if the group is a group of cybercriminals or a state actor (Haq et al., 2014).

Danti

Danti is an APT group that primarily targets Central Asian states, but also India, Myanmar, Nepal and the Philippines. Apart from the fact that Danti manages to rapidly make use of a recently discovered exploit in subsequent attacks, Danti's methods for infecting its victims and its cybertools of choice remain unknown. Kaspersky Lab has stated that Danti may be related to DragonOK or NetTraveller, another APT from China not listed here (GReAT, 2016).

Pirate Panda

Pirate Panda[10] is an APT group that targets Vietnamese, Indian, Tibetan, and Filipino entities, and Chinese pro-democracy activists. The group is known to use spear phishing emails to infect its targets. It is likely that Pirate Panda has ties to the Chinese government (Guarnieri and Schloesser, 2013; Kozy, 2015; Parys, 2017; Schultz, 2013).

Hurricane Panda

Hurricane Panda[11] is an APT group from China active in economic cyberespionage. The group does not target specifically Southeast Asian companies and industries, but is active throughout the region. Hurricane Panda specifically targets large telecom, technology, healthcare, aerospace and energy companies around the world. The group uses zero-day exploits in spear phishing emails and watering hole attacks to infect its victims. The use of zero-day exploits indicates that Hurricane Panda is a well-resourced and highly sophisticated group, further suggesting the group has ties to the Chinese government (Alperovitch, 2014; Francou, 2015; Symantec Security Response, 2015).

Vietnamese actors

APT32

FireEye has identified APT32[12] as a Vietnamese actor. APT32 targets foreign companies doing business in Vietnam and in China, Vietnamese journalists and the diaspora, and Vietnam's neighboring countries. The element that differentiates APT32 from Chinese cyberespionage is the fact that APT32's campaigns are usually timed with business discussions between the foreign companies and the Vietnamese government. Despite this, APT32's motivations are unclear. The Vietnamese APT group chooses targets that align with the Vietnamese government's interests, but there is no conclusive evidence that the group has ties to the state apparatus. APT32 seems to have significant resources as well as the technical skills required to develop its own malware. The APT group uses spear phishing emails and watering hole attacks to infect its victims. APT32 employs a combination of its own malware and commercially available tools (Carr, 2017; ESET, 2018; FireEye Inc., 2018; Gomez and Valeriano, 2017; Metzger, 2017; Reuters Staff, 2017).

Other actors involved in Southeast Asia

Platinum

Platinum[13] is an APT from an unidentified location in Southeast Asia and has been active in the region since 2009. Platinum targets government institutions, defense agencies, intelligence agencies, diplomatic institutions and telecom companies in Malaysia, Indonesia, China, Singapore, India and Thailand. The group is well-resourced and technically skilled as it uses zero-day exploits in spear phishing emails or drive-by attacks to infect its victims. Platinum employs its own malware to gather information. The group regularly updates its malware to avoid detection (GReAT, 2016; Windows Defender Advanced Threat Hunting Team, 2016).

Hellsing

Kaspersky Lab pinpointed Hellsing as operating from somewhere in Southeast Asia. This group was discovered during Naikon's spear phishing campaign targeting countries participating in the search mission for flight MH370. Hellsing did not succumb to Naikon's attempts and instead sent a spear phishing email back to Naikon. Like other APTs, Hellsing targets the Malaysian, Filipino, Indonesian, and Indian governments; US diplomatic agencies; and ASEAN entities. Hellsing employs its own malware, but some code strings appear to share similarities with Goblin Panda's malware. Hellsing's infrastructure also seems to

[10] Pirate Panda is also known as KeyBoy.

[11] Hurricane Panda is also known as Black Vine, TEMP.Avengers and Zirconium.

[12] APT32 is also known as Ocean Lotus, APT-C-00, SeaLotus and Cobalt Kitty.

[13] Platinum is also known as TwoForOne.

overlap with the infrastructure of a Chinese APT named Mirage[14] (Raiu and Golovkin, 2015).

Tropic Trooper

The origin of Tropic Trooper is unknown, but the group has been active in Southeast Asia since at least 2011. The APT group targets Taiwanese government officials and energy companies, and Filipino military agencies. Tropic Trooper uses spear phishing emails taking advantage of common exploits to infect its victims. The group uses its own malware to gather information. Some of its malware does share similarities with Pirate Panda's malware. The cybersecurity firm Trend Micro did not consider Tropic Trooper to be highly sophisticated, but recognized that the APT group was nevertheless successful in its campaigns (Alintanahin, 2015; Ray et al., 2016).

APT5

APT5's origin is unknown. The APT group has been active since 2007 and targets large telecom and technology companies. The APT group appears to frequently target satellite communications. APT5's motivations may be to access the communication systems themselves or to gain economic knowledge. The APT group uses its own malware, referred to as LEOUNCIA (FireEye Inc., 2018; FireEye Inc. and Singtel, 2015).

Sowbug

Sowbug is an APT group active in the Pacific region and Southeast Asia, and has been in operation since at least 2015. However, the group's origin is unknown. Sowbug targeted foreign policy and diplomatic institutions in Brunei, Malaysia and South America. The group seems to be well-resourced and uses its own malware (Symantec Security Response, 2017).

Hacktivists and Patriotic hackers

In addition to the APTs, patriotic hackers also conducted cyberattacks in relation to events in Southeast Asia. Patriotic hackers were particularly active during maritime disputes in the South China Sea, defacing and blocking websites with DDoS attacks. Patriotic hackers were observed during the standoff between Vietnam and China in 2011; between the Philippines and China in 2012; between Taiwan and the Philippines in 2013; between Vietnam and China in 2014; and between Vietnam, the Philippines and China in 2015. It is unclear if the patriotic hackers involved in these disputes are individuals or organized groups. Hacktivists and patriotic hackers in involved in Southeast Asia seem to have the same modus operandi as hacktivists and patriotic hackers in Syria, India and Pakistan. Vulnerabilities in websites are identified, and then exploited. (Baka, 2016; Balduzzi et al., 2018; Kozy, 2015; Passeri, 2012).

3.2 Targets

Actors in Southeast Asia target a large variety of marks, for a number of reasons. Targets can be subdivided into three main categories, with an additional two 'special cases'. The three major categories are: government and military agencies, businesses (e.g. energy, telecom and high-tech), and ASEAN entities. The two special cases are: Taiwan and businesses with ties to Vietnam.

Government and military agencies

APTs active in Southeast Asia frequently targeted government and military agencies. The objective of these attacks was to better understand the operations of neighboring states and regional rivals. These cyberattacks were largely consistent with the aims of regular intelligence gathering for national security purposes, and often aligned with state interests.

Businesses

APTs consistently targeted businesses involved in technology, communications and energy. The motivation for these attacks may have been to gain an economic advantage over these businesses. In the case of energy companies, however, there would be additional advantage gained if information was uncovered concerning oil and/or gas explorations performed in the South China Sea. The motivations to target telecom companies can also differ from regular economic espionage. By targeting telecom companies, an actor may also be attempting to gain access to large-scale communications for intelligence purposes.

ASEAN entities

Many APTs with ties to Chinese or Southeast Asian states targeted ASEAN entities. Their motivations may be related to gaining an advantage in important discussions and negotiations debated in ASEAN meetings or to gather intelligence on the talks themselves. Such intelligence gathering would be consistent with regular espionage for national security purposes and aligns with Southeast Asian and neighboring states' interests.

[14] Mirage is also known as Playfull Dragon, GREF and Vixen Panda.

Taiwan

Taiwan is unique in Southeast Asia due to its disputed status. This position makes it more prone to cyberattacks and espionage from China, which likely wants to gain information on Taiwanese government organizations. Taiwan is also a high-value target for cyber-campaigns because of its emerging economy and its flourishing high-tech industry, making it an especially fruitful target for economic cyberespionage (Ray et al., 2016).

Businesses with ties to Vietnam

Businesses in negotiations with Vietnam are disproportionately targeted in cyberspace, though the targeting differ from regular cyberespionage. APT32 launched campaigns against foreign businesses that were involved in Vietnam. APT32's motivations are unclear, but it might have been to gain an advantage over the businesses before concluding the deals, or to gain other economic advantages.

3.3 Tools and techniques

A variety of cybertools and techniques were utilized by actors in Southeast Asia. Attackers would regularly use spear phishing and watering hole attacks to infect their victims, but they also often made use of their own malware[15]. This subsection looks broadly at the malware developed by the APTs and at website defacements orchestrated by patriotic hackers.

Malware

Actors in Southeast Asia employed malware mostly of their own design, though sometimes in combination with more common and freely available cybertools. Customized malware gave remote access of the victim's computer to the attackers. Yet, the level of sophistication of the malware used varied from actor to actor. The malware enabled attackers to search for files or documents in their victim's computer without alerting their marks. Perpetrators could download or upload other pieces of malware to their victim's computer, take screenshots, and register keystrokes. APT30 even developed a malware able to retrieve information from air-gapped computers. This particular malware would first search for a USB drive connected on the computer and copy itself on it. When the USB drive was then connected to the air-gapped computer, the malware would infect it. It would then proceed to search for specific files and copy them to the USB drive, which would then transfer the files to the first infected and connected computer (FireEye Labs, 2015).

Website defacement

Contrary to covert cyberattacks mimicking traditional espionage, website defacements were highly public. Patriotic hackers defaced websites during disputes between states over territory in the South China Sea. The goal of website defacement is to harass the other party by changing the visual aspect of a website or redirecting a website to another by exploiting pre-existing vulnerabilities in the websites (Balduzzi et al., 2018). DDoS[16] attacks can be categorized as website defacement when their aim is also to harass or to draw public attention by opportunistically targeting vulnerable websites.

[15] A detailed list of malware used in Southeast Asia can be found in a table with a list of actors, targets in annex 2.

[16] DDoS attacks can also have other aims, including creating a diversion to draw the target's attention elsewhere so the attackers can perform other types of attacks (i.e. planting a malware or stealing data) (Zetter, 2016).

4 Effects

This section analyzes the effects of Southeast Asian cyber-activities by exploring the impact of cyberattacks and the use of cybertools at the domestic level and at the international level. At the domestic level, this section examines the effects of these cyber-activities on societies, on the economy and on the technology. This section also looks at the role of cybersecurity in international relations and in relation to ongoing territorial disputes in Southeast Asia.

4.1 Social effects

Societal fall-out from the various cyberattacks was largely restricted to inconvenience and irritation. Patriotic hackers used website defacements and DDoS attacks in response to on-the-ground territorial disputes in the South China Sea. In this context, DDoS attacks should be considered as a form as defacement because their aim was simply to attract attention. Patriotic hacking primarily originated from China, the Philippines, Taiwan and Vietnam. The goal of DDoS and defacement attacks was to get garner attention, as well as humiliate and harass the other party. These attacks tend to get a lot of media coverage and response from the population. Such publicity makes DDoS attacks and website defacements effective tools to impress and scare targeted audiences. While these types of attacks tend to attract more attention than other types of cyberattacks like cyberespionage, defacement tends to not require technical sophistication. Perpetrators usually claim their attacks and use the media coverage to further promote their demands and narrative. In addition to sending a message, website defacements and DDoS attacks are designed to generate fear in the targeted populations, reminding the people that they are vulnerable (Balduzzi et al., 2018).

In Southeast Asia, an important pattern emerged. Website defacements and DDoS attacks were always launched in reaction to specific events in the South China Sea. Territorial squabbles in the area triggered retaliatory attacks in cyberspace. This is consistent with other incidents of patriotic hacking, for example between India and Pakistan.[17]

However, it is likely that website defacements and DDoS attacks have a different social dimension in Southeast Asia as compared to India and Pakistan. The observed tit-for-tat cyberattacks may be tied to the social concept of “face”, which is very important to the Chinese culture. ”Face” could be understood as a form of personal prestige that individuals or entities will seek to protect and maintain. Losing face is considered a disgrace (Cheng, 1986). Not responding to a cyberattack may be perceived as losing face. Therefore, responding to a cyberattack in kind may also be a way for the populations to ensure their nation’s honor.

4.2 Economic effects

The Information and Telecommunications Technology (ICT) sector in Southeast Asia is a rapidly growing market. This expansion is also perceptible online, through the growing Southeast Asian digital economy. Unfortunately this growth also attracts interest from competing countries and/or industries that may use cyberespionage to gain an economic advantage (Baka, 2016; Heinl, 2013; Matsubara, 2018; Tran Dai and Gomez, 2018). Southeast Asian states typically have low cybersecurity awareness and capabilities are not evenly distributed among Southeast Asian states, creating a risk for the weakest states to easily become victims of intellectual property theft (Heinl, 2018). The lack of accurate data on the costs of cyberespionage in Southeast Asia makes it difficult to evaluate the exact economic impact of such attacks on the Southeast Asian ICT sector.

4.3 Technological effects

Malware specific to Southeast Asia

Due to the ongoing analysis of cyber-activities in Southeast Asia, it has become clear that some malware is only used on Southeast Asian targets. Cybersecurity experts studying the region observed various customized malware families, some highly sophisticated (able to steal data from air-gapped networks) and others less sophisticated, but still effective. Cybersecurity firms determined all these malware families were specifically developed by the actors outlined in a previous section of this Analysis. The use of these cybertools, however, was largely limited[18] to Southeast Asian targets. Apart from rare actors like Hurricane Panda, which targeted industries around the world, other cyberactors tended to focus on Southeast and East Asian marks.

Dependence on technology leads to vulnerability

Southeast Asian states became more vulnerable to cyberattacks over time due to their growing dependence on technology. As was stated in Section 4.2, ICT is a swiftly growing economic sector in Southeast Asia. Such rapid growth provides economic opportunities for these states, but also represents a risk.

[17] For more information on cyber-activities between India and Pakistan see: Baezner, Marie (2018): Hotspot Analysis: Regional rivalry between India-Pakistan: tit-for-tat in cyberspace, June 2018, Center for Security Studies (CSS), ETH Zürich.

[18] Southeast Asian malware occasionally affected networks outside of the region, but they were rarely the targets. Infection would occur when outside networks made contact with intended infected networks in Southeast Asia.

Southeast Asian states increasingly relied on technology and further developing the digital economy, but neglected a concurrent development of cybersecurity policies and awareness (Lee, 2018; Tran Dai and Gomez, 2018). This confluence of factors rendered highly connected states like Singapore, Taiwan, and Malaysia particularly vulnerable to cyberattacks.

4.4 International effects

The International dimensions of cyber-activities in Southeast Asia consist of four elements. First, Southeast Asia is already the theater of numerous cyberespionage campaigns. Many are attributed to Chinese actors, though other local actors are certainly present in the cybersphere. Second, some cyber-activities in Southeast Asia occur in response to physical incidents in the South China Sea. Patriotic hackers from the concerned states conduct tit-for-tat cyberattacks, such as website defacements and DDoS attacks in order to defend their countries' perceived interests. This type of behavior increases the risk of misinterpretation in cyberspace and the risk of escalation to conventional conflict. Third, China has established Anti-Access/Area Denial (A2/AD) zones in the South and East China Seas, in which Chinese cyber capabilities could be used to deny network access to adversaries. Finally, ASEAN institutions and meetings favor the development of regional dialogues on cybersecurity issues. Ultimately, this could lead to the development of more robust cybernorms.

Cyberespionage is largely – but not exclusively - from China

Southeast Asia is characterized by consistently high geopolitical tensions. Half of international shipping goes through the South China Sea, which also contains reserves of oil, natural gas, and fish. Because the South China Sea has such strategic value, states dispute territorial claims in the region – but that, in turn, further inflames tensions. Due to its significant military might, its modernized navy and its aggressive territorial claims in the South China Sea, China in particular is seen as a threat by Southeast Asian states. Chinese actors seek to gain information on and from businesses in Southeast Asia, to win economic advantages (FireEye Inc. and Singtel, 2015). They also target intelligence on neighboring states and adversaries in the South China Sea to get strategic advantage (Geers et al., 2014).

Other actors in Southeast Asia have also engaged in cyberespionage. Apart from the Vietnam-based APT32, which most likely has ties to the Vietnamese government, it was not possible to determine the origin of most cyberthreats. Therefore, these actors will not be discussed in this paragraph. Regarding APT32, the group targeted Vietnamese dissidents, journalists and businesses. This was allegedly motivated by a desire to maintain state control (Metzger, 2017). They also conducted operations against government agencies in neighboring states, including Vietnamese allies. During operations against Vietnamese businesses, APT32's motives are less clear. The motive to spy on partner states such as the Philippines is also unclear (Gomez and Valeriano, 2017).

Reactionary cyber response to geopolitical events and the risk of escalation

Often, clashes in the South China Sea, including relatively small incidents such as coast guards denying access of an area to fishermen, triggered a cyber response. These were mainly limited to website defacement and DDoS attacks. These attacks would also prompt a response from opposing hacker groups, and develop into a tit-for-tat dynamic between patriotic hackers of both states. As explained in Section 4.1, patriotic hackers address their nationalistic message to the adversary. The goal is to ridicule their opponent and to make the adversary understand that its actions in the physical realm are not acceptable. Yet, tit-for-tat cyberattacks such as these, especially when conducted by non-state actors, often serve to solidify the tensions between populations. Cyberattacks can also escalate into a conventional conflict if tensions are sufficiently high. As in the case of India and Pakistan, conflict starts with a geopolitical event that usually involves state actors but it is then continued by non-state actors, at the population level. Website defacements and DDoS attacks do not cause physical damage by themselves, but are more of an annoyance to everyday life. When cyberattacks escalate and start to target more serious objectives, like critical infrastructure, or when cyberattacks are perceived to be conducted by a state actor, then cyber-activities may prompt a real-world response (Libicki, 2012; Lin, 2012).

Website defacements and DDoS attacks are not the only types of cyberattacks that could prompt an escalation. Cyberespionage campaigns also increase the risks of misinterpretation and misattribution in cyberspace, thereby also risking further escalation. The line separating typical espionage and planting extremely dangerous software is thin and difficult to evaluate. It is therefore difficult for a state to determine the true intent of a perceived cyberespionage campaign. This difficulty also increases the risk of misinterpretation.

Escalation of minor conflicts has an additional consequence that cannot be ignored: the USA may embroil itself in the skirmish. Many Southeast Asian states are allies or partners of the USA and if these states get involved in a conventional conflict, the USA may choose to participate to protect its interests in the region. It is in the USA's best interest to prevent any escalation in the South China Sea to protect its economic and security interests and freedom of navigation in the

region (Atanassova-Cornelis and Van der Putten, 2015; Economy et al., 2018).

While several incidents in the physical realm in Southeast Asia were followed by tit-for-tat cyber-activities, none led to an escalation. These cyberattacks were contained to cyberspace and did not spillover to the physical realm. This could be explained by the low intensity level of the cyberattacks. Website defacement and DDoS attacks were never damaging nor serious enough to merit a response in the physical realm. In addition, states may be reticent to engage militarily because of the asymmetric power balance between China and the other states involved in the cyber-activities. Smaller states have little to gain by engaging China in a conventional conflict and thus would refrain from performing more damaging cyberattacks. It is most likely that website defacements and DDoS attack campaigns in response to geopolitical incidents in the South China Sea will persist.

Anti-Access/Area denial in South China Sea

Cyberattacks in the South China Sea are not limited to tit-for-tat DDoS attacks, website defacements and cyberespionage campaigns. A2/AD strategies also take into account cyberspace and cyber capabilities. In an A2/AD zone, all military domains are utilized to deny or deter an adversary from invading a specific geographic zone. China holds economic and strategic interests in the South China Sea, and is establishing A2/AD zones there. These zones are concentrated around Taiwan and the Spratly Islands (Berger, 2016). In addition to its territorial claims, China established military infrastructure with naval, air, radar, electronic warfare and defense facilities in the disputed territory (Minh Tri, 2017; Panda, 2018). In the event of a conventional conflict, Chinese cyber capabilities can be used in A2/AD zones to control the information space. China could disrupt its adversary's command and control, its communications infrastructure, and its satellites or GPS localization with cyberattacks (Kazianis, 2013; The Economist, 2018). A2/AD zones hinder the US' ability to project military power, disrupts freedom of navigation in the region, and infringes on the sovereignty of neighboring states. (Assante, 2016; Berger, 2016).

ASEAN and the development of cybernorms

Repeated cyberattacks and cyberespionage throughout the region pushed states to better cooperate and establish norms to avoid escalation and protect their own interests. ASEAN has become the platform to discuss cybersecurity issues in Southeast Asia. ASEAN is a regional organization with the goal of promoting economic, political, security, military, educational and socio-cultural integration and cooperation. The organization acts as a dialogue platform for the ten members and their partners (ASEAN University Network, 2012). Many members use ASEAN entities or meetings to raise concerns and open discussions on the aforementioned subjects. ASEAN members demonstrate a willingness to develop common views on cybersecurity, which began in November 2000 with the signature of the ASEAN Framework Agreement.[19] ASEAN focused first on economic development and the digitalization of Southeast Asia, while cybersecurity discussions came later. The level of cyber capabilities and awareness varies considerably among ASEAN members; typically more advanced states (like Singapore, Malaysia, and the Philippines) lobby for these discussions. The goal of cybersecurity talks is to develop a common understanding of issues among members and promote cooperation in the field of cybersecurity. ASEAN member states tend to treat cybersecurity issues as a primarily regional issue, and do not initially engage with cybersecurity on the national level. Only Malaysia, the Philippines and Singapore have developed national strategies (ATKearney, 2018). Yet this has not translated into a set regional governance framework. Unfortunately, this renders collaboration and information sharing on cybersecurity threats difficult (Lee, 2018). Cybersecurity has been added to the agenda of several ASEAN meetings and entities, including the ASEAN Regional Forum and the ASEAN Defence Ministers Meeting Plus[20]. Nevertheless, Southeast Asian states hold different views on cyberspace and cybersecurity, which has hindered cooperation in the past. Some states seek to control content on the internet while others favor openness; for others still, state cybersecurity is not a priority at all (Heinl, 2018; Tran Dai and Gomez, 2018).

In the regional development of cybernorms, Japan has played a significant role due to historical ties to many Southeast Asian states. While Japan is not a member of ASEAN, it helps ASEAN members to develop and improve their cybersecurity. Cooperating with Southeast Asian states aligns well with Japan's interests to develop a secure cyberspace in which it can promote its economy, security and business interests. Information sharing between Japan and Southeast Asian states is also helped by the fact that they share many cyberthreats, notably from China (Parameswaran, 2017). Japan also participates in the ASEAN – Japan Cybersecurity Capacity Building Center (AJCCBC), based in Thailand and launched in June 2018. The AJCCBC aims to train cybersecurity agency personnel from ASEAN member states. They are trained on malware analysis, incident response and forensics (Parameswaran, 2018).

[19] The initial agreement was about the development of e-commerce and connectivity in Southeast Asia.

[20] This meeting includes all ASEAN members and Australia, China, India, Japan, New Zealand, South Korea, Russia and the USA.

5 Policy Consequences

This section recommends two general measures to reduce the risk for states to be impacted by malicious cyber-activities like the ones observed in this Hotspot Analysis.

5.1 Improving cybersecurity

Cyberespionage campaigns in Southeast Asia often began with spear phishing emails. Therefore, it is important to improve awareness about this popular method of infection. States should organize sensitization campaigns to help government personnel recognize spear phishing emails. State institutions could also design standard procedures to effectively respond once an employee falls victim to a spear phishing email. In addition to implementing these procedures, institutions should also train their use. Standardized procedures would help state institutions identify and respond to intrusions faster.

Technical solutions to reduce the risks of infection via spear phishing emails exist. State institutions could encourage their employees and partners to implement an email authentication system like the Sender Policy Framework. This system certifies the authenticity of the sender of an email. This measure would make it easier for an employee to recognize potentially fraudulent emails as they would not be certified.

The case of website defacement is more difficult to prevent. No specific measures can guarantee that a website will not be defaced. However, website owners can regularly conduct penetration tests to detect vulnerabilities and patch them. Monitoring and detection tools can also to help react in a timely manner to a defacement incident.

5.2 Monitoring regional disputes in Southeast Asia

The tensions and clashes among states in Southeast Asia will continue in both the physical and cyber realms. Patriotic hackers will most likely continue to respond to physical clashes with website defacement and DDoS attacks. As Southeast Asia represents a strategic shipping route and a lucrative market for new technologies, cyberespionage campaigns will also most likely continue. All these cyber-activities increase the risk of misinterpretation in cyberspace, and therefore the risk of escalation. As such, regional tensions need to be closely monitored in order for outside actors to avoid being impacted by a possible escalation.

6 Annex 1

Non-exhaustive list of cyber-incidents related to Southeast Asian geopolitical events.

B = Business, G = Government and government institutions, M = Media, MIL = Military institutions, O = Others, PP = Political Party				
Date	**Victim(s)**	**Type of victim(s)**	**Alleged perpetrator**	**Technique/Tool**
04.2001	US websites	Unknown	Chinese patriotic hackers	Probably website defacement (Kozy, 2015)
07.2009	Southeast Asian governments, manufacturers and telecom companies	B/G	Numbered Panda	Spear phishing and IXESHE malware (Sancho et al., 2012)
03.06.2011	Chinese government websites	G	Mr.N – Cubi11 (a Vietnamese patriotic hacker)	Website defacement (Balduzzi et al., 2018)
04.06.2011	More than 30 Vietnamese websites	Unknown	Chinese patriotic hackers	Website defacement (Balduzzi et al., 2018)
05.06.2011	More than 1,000 Vietnamese websites	Unknown	Chinese patriotic hackers	DDoS and website defacement (Balduzzi et al., 2018)
08.06.2011	98 Vietnamese websites	Unknown	Silic (Chinese patriotic hacker)	Website defacement (Balduzzi et al., 2018)
20.04.2012	University of the Philippines website	O	Chinese patriotic hackers	Website defacement (Passeri, 2012)
21.04.2012	Chinese websites	Unknown	Filipino patriotic hackers	Website defacement (Passeri, 2012)
23.04.2012	Filipino government websites	G	Chinese patriotic hackers	DDoS attack (Passeri, 2012)
24.04.2012	Chinese websites	Unknown	Filipino patriotic hackers	DdoS attack (Passeri, 2012)
25.04.2012	A Filipino local government, a Filipino radio station, the University of the Philippines and the People Management Association websites	G/M/O	Chinese patriotic hackers	Dump of login credentials (Passeri, 2012)
25.04.2012	The Philippines Department of Budget and Management website	G	Chinese patriotic hackers	Website defacement (Passeri, 2012)
25.04.2012	3 Filipino government websites	G	Chinese patriotic hackers	DDoS attack (Passeri, 2012)
26.04.2012	Chinese government websites	G	Filipino patriotic hackers	DDoS attack (Passeri, 2012)
30.04.2012	Chinese government websites	G	Filipino patriotic hackers	Website defacement (Passeri, 2012)
04.05.2012	Filipino national newspaper website	M	Chinese patriotic hackers	Website defacement (Passeri, 2012)
02.2013	Vietnamese journalists, dissidents, activists and bloggers	M/O	APT32	Cyberespionage (Carr, 2017; Galperin and Marquis-Boire, 2014)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool
04.2013	Targets in Vietnam and India	Unknown	Pirate Panda	Cyberespionage with the malware CREDRIVER (Guarnieri and Schloesser, 2013)
10.05.2013	More than 30 Filipino government websites	G	Taiwanese patriotic hackers	DDoS attack in response to the death of a Taiwanese fisherman caused by the Filipino Coast Guard (Balduzzi et al., 2018)
11.05.2013	Taiwanese government and commercial websites	B/G	Pinoy Vendetta (Filipino patriotic hacker)	Website defacement (Balduzzi et al., 2018)
12.05.2013	Filipino government websites	G	AnonTaiwan	Data dump from the websites (Balduzzi et al., 2018)
25.05.2013	31 Taiwanese government websites	G	Filipino patriotic hackers	Website defacement (Balduzzi et al., 2018)
20.12.2013	Electronic Frontier Foundation and Associated Press	M/O	APT32	Spearphishing (Galperin and Marquis-Boire, 2014)
2014	Vietnamese Network Security firm, a German manufacturing company doing business in Vietnam and Vietnamese diaspora in Southeast Asia	B/O	APT32	Spearphishing (Carr, 2017)
11.03.2014	Countries involved in the search for flight MH370	G	Naikon	Spear phishing (Raiu and Golovkin, 2015)
03.2014	Naikon	O	Hellsing	Spear phishing (Raiu and Golovkin, 2015)
10.04.2014	Energy companies in Southeast Asia	B	Naikon	Spearphishing (ThreatConnect Research Team, 2014)
05.2014	Vietnamese government websites	G	1937cn Team (Chinese patriotic hackers)	Website defacement (Kozy, 2015)
05.2014	Vietnamese government	G	Goblin Panda	Cyberespionage (Kozy, 2015)
2015	A Vietnamese media outlet, Chinese private and public entities and a Chinese government agency	B/G/M/O	APT32	Cyberespionage (Carr, 2017)
26.04.2015	Chinese websites	Unknown	BloodSec (Filipino patriotic hacker)	Launch of the campaign #StopReclamation against Chinese construction on the Spratly Islands (Balduzzi et al., 2018)
28.05.2015	Chinese websites	Unknown	Filipino and Vietnamese patriotic hackers	Launch of the campaign #OpChina (Balduzzi et al., 2018)
30.05.2015	Chinese government websites	G	Filipino and Vietnamese patriotic hackers	Website defacement (Balduzzi et al., 2018)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool
30.05.2015	Vietnamese websites	Unknown	1937cn Team (Chinese patriotic hackers)	Website defacement (Balduzzi et al., 2018)
09.07.2015	The UNPCA website	O	A Chinese APT	Modified website to infect the visitors (ThreatConnect Research Team, 2015)
01.12.2015	Taiwanese media and government	G/M	APT16	Spearphishing emails dropping the ELMER backdoor (GReAT, 2016; Winters, 2015)
2016	Filipino consumer product firm, a Vietnamese bank, a Filipino tech company, a Vietnamese media outlet and a US consumer product firm	B/M	APT32	Cyberespionage (Carr, 2017)
07.2016	2 large Vietnamese airports and the Vietnam Airlines website	G/O	1937cn Team (Chinese patriotic hackers)	Defacement of the flight information screens in the airports (Baka, 2016) + (Belduzzi)
08.2016	Taiwanese government and energy companies	B/G	Tropic Trooper	Cyberespionage (Ray et al., 2016)
2017	Vietnamese diaspora in Australia and Filipino government employees	G/O	APT32	Spearphishing (Carr, 2017)
01.2017	Taiwanese targets	Unknown	Numbered Panda	Cyberespionage with the malware IXESHE (Crowdstrike, 2018)
03.2017	Brunei and Malaysian foreign policy and diplomatic institutions	G	Sowbug	Cyberespionage (Symantec Security Response, 2017)
05.2017	Filipino government	G	APT32	Cyberespionage and dumping of data (Gomez and Valeriano, 2017)
06.2017	Japanese targets	Unknown	Numbered Panda	Cyberespionage (Crowdstrike, 2018)
10.2017	North Korean and South Korean targets	Unknown	Numbered Panda	Cyberespionage (Crowdstrike, 2018)
03.2018	Corporations and Governments in Vietnam, the Philippines, Laos and Cambodia	B/G	APT32	Cyberespionage (ESET, 2018)

7 Annex 2

Summary of Chinese APTs involved in Southeast Asia with their victims, infiltration method and their malware.

Actors from China	Victims	Infection method(s)	Malware
Numbered Panda	Governments, electronic manufacturers, telecom companies and media outlets in East Asia	Spear phishing	IXESHE, RIPTIDE, HIGHTIDE, WATERSPOUT
APT16	High-tech companies, governments, media outlets and finance institutions in Taiwan, Japan and Hong Kong	Spear phishing	IRONHALO, ELMER, DOORJAMB
Hurricane Panda	Large telecom, technology, healthcare, aerospace and energy companies around the world	Spear phishing and watering hole attacks	Mimikatz, PlugX, Sakula, Hurix, Mangali
Goblin Panda	Vietnamese government	Spear phishing	PlugX
IceFog	Defense industries and telecom companies in Taiwan, South Korea and Japan	Spear phishing	Icefog
DragonOK	High-tech industries in Taiwan and Japan	Spear phishing	CT/NewCT, Nflog, Poison Ivy, Mangall
Naikon	Government agencies, militaries, media outlets and energy companies in Myanmar, Vietnam, Singapore, Laos, Malaysia, the Philippines, Cambodia, Indonesia, Nepal, Thailand, China	Spear phishing	sslMM, winMM, exe_exchange, wininetMM/sakto, inject, sys10, xsControl/naikon, RARSTONE, Everything32, TeamViewer
APT30	Governments, media outlets, industries in Southeast Asia, India and ASEAN agencies	Spear phishing	BACKSPACE, NETEAGLE, SHIPSHAPE, SPACESHIP, FLASHFLOOD, MILKMAID, ORANGEADE, CREAMCICLE
Pirate Panda	Vietnam, Indonesia, the Filipino military, Tibetans and Chinese pro-democracy activists	Spear phishing	CREDRIVER
Danti	Myanmar, the Philippines and Central Asia	Unknown	Unknown

Summary of other actors involved in Southeast Asia with their victims, infiltration method and their malware.

Other actors	Victims	Infection method(s)	Malware
Platinum	Malaysia, Indonesia, China, India, Singapore and Thailand	Spear phishing and drive-by attacks	Dispind, JPIN, adbupd, keyloggers
APT32	Vietnamese journalists, diaspora, dissidents, bloggers, corporations, the Philippines, Cambodia, China, Laos and ASEAN agencies	Spear phishing and watering hole attacks	WINDSHIELD, KOMPROGO, SOUNDBITE, BEACON, PHOREAL, a backdoor similar to PlugX
Hellsing APT	Naikon, Malaysia, Indonesia, India, the Philippines, US diplomatic agencies and ASEAN entities	Spear phishing	Msger, xweber, xrat, clare, irene, xKat
Tropic Trooper	Taiwan and the Philippines	Spear phishing	Yahoyah, Poison Ivy, PCShare, Yahamam, Hideport
APT5	Southeast Asia telecom companies	Spear phishing	LEOUNCIA
Sowbug	Brunei, Malaysia and states from South America	Unknown	Felismus

8 Glossary

Advanced Persistent Threat (APT): A threat that targets critical objectives to gain access to a computer system. Once inside a network, it tries to remain hidden and is usually difficult to remove when discovered (Command Five Pty Ltd, 2011; DellSecureWorks, 2014).

Air-gapped network: A security measure that implies physical separation between a network and the Internet or other unsecure local networks (Zetter, 2014).

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: An element of software code that allows hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

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

Drive-by download: A program that is automatically downloaded to a computer by visiting a website or opening an HTML email, often without the user's knowledge (Rouse, 2009).

Exploit: An attack on a computer operating system using a vulnerability of the system or software (Rouse, 2017).

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

Keylogger: Feature that traces keystrokes without the knowledge of the user (Novetta, 2016, p. 56).

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

Patriotic hacking: Sometimes also referred to as nationalistic hacking. A group of individuals originating from a specific state engage in cyberattacks in defense against actors that they perceive to be enemies of their country (Denning, 2011, p. 178).

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).

Watering hole attack: Attack where a legitimate website is injected with malicious code that redirects users to a compromised website which infects users accessing it (TechTarget, 2015).

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

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

9 Abbreviations

A2/AD	Anti-Access/Area Denial
ACCP	ASEAN Cybersecurity Capacity Program
ADIZ	Air Defense Identification Zone
AJCCBC	ASEAN – Japan Cybersecurity Capacity Building Center
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
C&C	Command and Control infrastructure
DDoS	Distributed Denial of Service
EEZ	Exclusive Economic Zone
ICT	Information and Telecommunications Technologies
PLA	Chinese People's Liberation Army
UN	United Nations
UNPCA	United Nations Permanent Court of Arbitration

10 Bibliography

Alintanahin, K., 2015. Operation Tropic Trooper Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers. TrendMicro.

Alperovitch, D., 2014. CrowdStrike Discovers Use of 64-bit Zero-Day Privilege Escalation Exploit (CVE-2014-4113) by Hurricane Panda [WWW Document]. CrowdStrike Blog. URL https://www.crowdstrike.com/blog/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/ (accessed 09.05.18).

Aquino, M., 2013. RARSTONE Found In Targeted Attacks [WWW Document]. TrendMicro. URL https://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/ (accessed 03.05.18).

ASEAN University Network, 2012. About ASEAN [WWW Document]. ASEAN Univ. Netw. URL http://www.aunsec.org/historyofasean.php (accessed 14.05.18).

Assante, M.J., 2016. Implications of cyber in anti-access and area-denial counters. IEEE, pp. 1–6. https://doi.org/10.1109/CYCONUS.2016.7836611

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 12.07.17).

ATKearney, 2018. Cybersecurity in ASEAN: An Urgent Call to Action.

Baka, P., 2016. Southeast Asia Still Has Weak Information Security Against Cyber Threats [WWW Document]. The Diplomat. URL https://thediplomat.com/2016/10/southeast-asia-still-has-weak-information-security-against-cyber-threats/ (accessed 03.05.18).

Balduzzi, M., Flores, R., Gu, L., Maggi, F., 2018. A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks (TrendLabs Research Paper). Trend Micro.

Baumgartner, K., Golovkin, M., 2015a. THE MsnMM CAMPAIGNS The Earliest Naikon APT Campaigns. Kaspersky Lab HQ.

Baumgartner, K., Golovkin, M., 2015b. The Naikon APT Tracking Down Geo-Political Intelligence Across APAC, One Nation at a Time [WWW Document]. Securelist. URL https://securelist.com/the-naikon-apt/69953/ (accessed 03.05.18).

Berger, Z., 2016. China's Anti-Access Area Denial [WWW Document]. Missile Def. Advocacy Alliance. URL

http://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/china-anti-access-area-denial-coming-soon/ (accessed 05.06.18).

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 10.07.17).

Carr, N., 2017. Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html (accessed 08.05.18).

Cheng, C.-Y., 1986. The Concept of Face and Its Confucian Roots. J. Chin. Philos. 13, 329–348. https://doi.org/10.1111/j.1540-6253.1986.tb00102.x

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

Command Five Pty Ltd, 2011. Advanced Persistent Threats: A Decade in Review.

Crowdstrike, 2018. 2018 Global Threat Report: Blurring the lines between statecraft and tradecraft. 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 13.07.17).

DellSecureWorks, 2014. Advanced Threat Protection with Dell SecureWorks Security Services. Dell Inc.

Denning, D.E., 2011. Cyber Conflict as an Emergent Social Phenomenon, in: Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. Holt and Schell, pp. 170–186.

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 26.07.17).

ESET, 2018. OceanLotus Old techniques, New Backdoor (White Paper). ESET LLC.

FireEye Inc., 2018. Advanced Persistent Threat Groups [WWW Document]. FireEye. URL https://www.fireeye.com/current-threats/apt-groups.html (accessed 11.05.18).

FireEye Inc., Singtel, 2015. SouthEast Asia: An Evolving Cyber Threat Landscape (Special Report). FireEye Inc., Milpitas, CA, USA.

FireEye Labs, 2015. APT30 And the Mechanics of a long-running cyber espionage operation (Special Report). FireEye Inc., Milpitas, CA, USA.

Francou, Y., 2015. Malware Sakula - Evolutions v1.x (Part 1) [WWW Document]. Airbus. URL http://blog.airbuscybersecurity.com/post/2015/09/APT-BlackVine-Malware-Sakula (accessed 09.05.18).

Galperin, E., Marquis-Boire, M., 2014. Vietnamese Malware Gets Very Personal [WWW Document]. Electron. Front. Found. URL https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal (accessed 08.05.18).

Geers, K., Kindlund, D., Moran, N., Rachwald, R., 2014. World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. FireEye Inc., Milpitas, CA.

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

Glaser, B.S., 2015. Conflict in the South China Sea [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/report/conflict-south-china-sea (accessed 02.05.18).

Glaser, B.S., 2012. Armed Clash in the South China Sea [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/report/armed-clash-south-china-sea (accessed 02.05.18).

Gomez, M.A., Valeriano, B., 2017. Frustrated with the Philippines, Vietnam Resorts to Cyber Espionage [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog/frustrated-philippines-vietnam-resorts-cyber-espionage (accessed 18.05.18).

GReAT, 2016. CVE-2015-2545: overview of current threats [WWW Document]. Kaspersky Lab. URL https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/ (accessed 08.05.18).

Guarnieri, C., Schloesser, M., 2013. KeyBoy, Targeted Attacks against Vietnam and India [WWW Document]. Rapid7. URL https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/ (accessed 09.05.18).

Haq, T., Moran, N., Vashisht, S., Scott, M., 2014. Operation Quantum Entanglement (White Paper). FireEye Inc., Milpitas, CA, USA.

Heinl, C., 2018. Can ASEAN Continue to Improve Cybersecurity in the Region and Beyond? [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog/can-asean-continue-

improve-cybersecurity-region-and-beyond (accessed 03.05.18).
Heinl, C., 2013. Enhancing ASEAN-wide Cybersecurity: Time for a Hub of Excellence?
Jiang, G., Caselden, D., Winters, R., 2015. The EPS Awakens [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html (accessed 08.05.18).
Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. IEEE, pp. 4490–4494. https://doi.org/10.1109/IECON.2011.6120048
Kaspersky Lab, 2013. The "Icefog" APT: A Tale Of Cloak And Three Daggers. Kaspersky Lab HQ.
Kazianis, H., 2013. The Real Anti-Access Story: Cyber [WWW Document]. The Diplomat. URL http://thediplomat.com/2013/05/the-real-anti-access-story-cyber/ (accessed 10.07.17).
Kozy, A., 2015. Rhetoric Foreshadows Cyber Activity in the South China Sea [WWW Document]. CrowdStrike Blog. URL https://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/ (accessed 03.05.18).
Lee, J., 2018. ASEAN remains "prime target" for cyberattacks [WWW Document]. Nikkei Asian Rev. URL https://asia.nikkei.com/Business/Business-Trends/ASEAN-remains-prime-target-for-cyberattacks (accessed 06.08.18).
Libicki, M.C., 2012. Crisis and escalation in cyberspace. RAND, Project Air Force, Santa Monica, CA.
Lin, H., 2012. Escalation Dynamics and Conflict Termination in Cyberspace. Strateg. Stud. Q. 6, 46–70.
Lt. Cmdr. Benson, J.W., 2012. South China Sea: A History of Armed Conflict [WWW Document]. USNI News. URL https://news.usni.org/2012/06/20/south-china-sea-history-armed-conflict (accessed 02.05.18).
Matsubara, M., 2018. How Can Japan-UK Cybersecurity Cooperation Help ASEAN Build Cybersecurity Capacity? [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog/how-can-japan-uk-cybersecurity-cooperation-help-asean-build-cybersecurity-capacity (accessed 24.04.18).
Metzger, M., 2017. Ocean Lotus Group/APT 32 identified as Vietnamese APT group [WWW Document]. SC Media. URL https://www.scmagazineuk.com/ocean-lotus-groupapt-32-identified-as-vietnamese-apt-group/article/663565/ (accessed 07.05.18).
Meyers, A., 2013. Whois Numbered Panda [WWW Document]. CrowdStrike Blog. URL https://www.crowdstrike.com/blog/whois-numbered-panda/ (accessed 08.05.18).
Minh Tri, N., 2017. China's A2/AD Challenge in the South China Sea: Securing the Air From the Ground [WWW Document]. The Diplomat. URL https://thediplomat.com/2017/05/chinas-a2ad-challenge-in-the-south-china-sea-securing-the-air-from-the-ground/ (accessed 05.06.18).
Mogato, M., 2017. Philippines says China agrees on no new expansion in South China Sea [WWW Document]. Reuters. URL https://www.reuters.com/article/us-southchinasea-philippines-china/philippines-says-china-agrees-on-no-new-expansion-in-south-china-sea-idUSKCN1AV0VJ (accessed 14.05.18).
Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.
Panda, A., 2018. South China Sea: China Deploys Jamming Equipment [WWW Document]. The Diplomat. URL https://thediplomat.com/2018/04/south-china-sea-china-deploys-jamming-equipment/ (accessed 05.06.18).
Parameswaran, P., 2018. What's Behind the New Japan-ASEAN Cyber Center? [WWW Document]. The Diplomat. URL https://thediplomat.com/2018/04/whats-behind-the-new-japan-asean-cyber-center/ (accessed 07.05.18).
Parameswaran, P., 2017. Japan-ASEAN Cyber Cooperation in the Spotlight [WWW Document]. The Diplomat. URL https://thediplomat.com/2017/02/japan-asean-cyber-cooperation-in-the-spotlight/ (accessed 07.05.18).
Parameswaran, P., 2016. Singapore Unveils New ASEAN Cyber Initiative [WWW Document]. The Diplomat. URL https://thediplomat.com/2016/10/singapore-unveils-new-asean-cyber-initiative/ (accessed 07.05.18).
Parys, B., 2017. The KeyBoys are back in town [WWW Document]. PwC. URL https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html (accessed 09.05.18).
Passeri, P., 2012. Philippines and China, on The Edge of a New Cyber Conflict? [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2012/05/01/philippines-and-china-on-the-edge-of-a-new-cyber-conflict/ (accessed 08.05.18).
QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.

Raiu, C., Golovkin, M., 2015. The Chronicles of the Hellsing APT: the Empire Strikes Back [WWW Document]. Securelist. URL https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/ (accessed 09.05.18).

Ray, V., Falcone, R., Miller-Osborn, J., Lancaster, T., 2016. Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy [WWW Document]. Paloalto Netw. URL https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/ (accessed 09.05.18).

Reuters Staff, 2017. Vietnam-linked hackers likely targeting Philippines over South China Sea dispute: FireEye [WWW Document]. Reuters. URL https://www.reuters.com/article/us-cyber-philippines-southchinasea-idUSKBN18L1MR (accessed 18.05.18).

Rouse, M., 2017. computer exploit [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/exploit (accessed 20.02.18).

Rouse, M., 2009. drive-by download [WWW Document]. TechTarget. URL http://searchenterprisedesktop.techtarget.com/definition/drive-by-download (accessed 29.03.18).

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

Sancho, D., dela Torre, J., Bakuei, M., Villeneuve, N., McArdle, R., 2012. IXESHE An APT Campaign (Trend Micro Incorporated Research Paper). Trend Micro, Cupertino, CA, USA.

Schultz, J., 2013. Scope of 'KeyBoy' Targeted Malware Attacks [WWW Document]. Cisco Blogs. URL https://blogs.cisco.com/security/scope-of-keyboy-targeted-malware-attacks (accessed 09.05.18).

Symantec Security Response, 2017. Sowbug: Cyber espionage group targets South American and Southeast Asian governments [WWW Document]. Symantec. URL https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments (accessed 07.05.18).

Symantec Security Response, 2015. Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/connect/blogs/black-vine-formidable-cyberespionage-group-targeted-aerospace-healthcare-2012 (accessed 09.05.18).

TechTarget, 2015. watering hole attack [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/watering-hole-attack (accessed 29.11.16).

The Economist, 2018. Using clever technology to keep enemies at bay [WWW Document]. The Economist. URL https://www.economist.com/special-report/2018/01/25/using-clever-technology-to-keep-enemies-at-bay (accessed 06.08.18).

ThreatConnect, Defense Group, 2015. Project CameraShy: Closing the Aperture on China's Unit 78020. ThreatConnect and Defense Group, Arlington, VA, USA.

ThreatConnect Research Team, 2015. China Hacks the Peace Palace: All Your EEZ's Are Belong to Us [WWW Document]. ThreatConnect. URL https://www.threatconnect.com/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us/ (accessed 02.05.18).

ThreatConnect Research Team, 2014. Piercing the Cow's Tongue: China Targeting South China Seas Nations [WWW Document]. ThreatConnect. URL https://www.threatconnect.com/piercing-the-cows-tongue-china-targeting-south-china-seas-nations/ (accessed 02.05.18).

Tran Dai, C., Gomez, M.A., 2018. Challenges and opportunities for cyber norms in ASEAN. J. Cyber Policy 1–19. https://doi.org/10.1080/23738871.2018.1487987

Windows Defender Advanced Threat Hunting Team, 2016. PLATINUM: Targeted attacks in South andSoutheast Asia. Microsoft.

Winters, R., 2015. The EPS Awakens - Part 2 [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html (accessed 08.05.18).

Zetter, K., 2016. Hacker Lexicon: What Are DoS and DDoS Attacks? [WWW Document]. WIRED. URL https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/ (accessed 06.08.18).

Zetter, K., 2014. Hacker Lexicon: What Is an Air Gap? [WWW Document]. Wired. URL https://www.wired.com/2014/12/hacker-lexicon-air-gap/ (accessed 04.11.16).

CSS
ETH Zurich

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