CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Synthesis 2018: Focus on Asia: Continuity and Specificities

Zürich, May 2019

Version 1

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

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

Please cite as: Baezner, Marie (2019): Hotspot Analysis: Synthesis 2018: Focus on Asia: Continuity and Specificities, May 2019, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

This document identifies the most important cyber-conflict trends in South, Southeast and East Asia in 2018. It draws from three previously published Hotspot Analyses that examined the cases of North Korea, the regional rivalry between India and Pakistan, and tensions in Southeast Asia. The goal of the Synthesis 2018 is to identify trends among the three Hotspot Analyses of 2018, to analyze and situate them in the global context and to compare these findings with the Synthesis 2017.

The Hotspot Synthesis 2018 identifies three new trends in cyber-activities in the region, highlighting the absence of a common agreement on what are legitimate and illegitimate behaviors in cyberspace. All three new trends contribute to growing risks of misperception and escalating tensions:

- First, the Democratic Republic of North Korea (DPRK) has been involved in cybercrime activities, which was unique for a state. This involvement has posed the problem of having a state generating revenue and circumventing international sanctions through cybercrime activities. With these activities, which are motivated by financial gain, the DPRK blurs the lines differentiating cyber-conflicts from cybercrime.
- Second, non-state actors such as patriotic hackers have been very active in these regions. They have usually reacted to geopolitical events and risked heightening political tensions.
- Third, Western states targeted by disruptive cyberattacks from Asian states have had difficulties establishing an appropriate response.

Five of the trends observed in the Hotspot Synthesis 2017 have been found to be still ongoing in 2018, with the three analyzed Asian regions exhibiting a number of particularities:

- First, states in Asia are integrating cybersecurity at the national and / or regional level(s). Cyber-conflicts differ from cybercriminal activities because of their political component. States continue to politicize and securitize cyberspace, which they increasingly regard as a strategic space.
- Second, state actors choose their targets depending on their strategic values.
- Third, attribution continues to be a widely discussed issue. The decision to attribute publicly is a political act with political and international ramifications. Very few cyberattacks have been attributed, and when they have, the impact of attribution has been weakened by a lack of evidence or transparency.
- Fourth, state actors in Central, Southeast and Eastern Asia, have shown restraint in their use of cybertools and techniques. State actors and non-state actors employed cyber-activities to harass adversaries, but they remained careful to stay below the level of armed conflict in order not to escalate tensions. Moreover, this restraint is one of the reasons why cyberweapons are used only rarely. Only North Korean actors used such tools to wipe computer contents. In all other cases, the tools and techniques employed were not particularly sophisticated, indicating that state actors would more often devote their resources to social engineering than the development of highly sophisticated tools which can only be used once. Additionally, actors have shown that they are able to adapt to different platforms and develop malware for smartphones.
- Fifth, states have used cyberspace to spy on other states, both in Asia and in other parts of the world, even on friendly states. While espionage is generally tolerated at the international level, the lack of norms increases the risks of misperception in cyberspace and of rising political tensions.

1 Introduction

Cybersecurity continued to attract media attention throughout 2018. Various cyberattacks on cryptocurrency exchanges, the Winter Olympic Games in South Korea, malicious infiltration of thousands of routers in Ukraine, attributions for NotPetya, the US indicting Russian nationals for the Democratic National Committee hack and a North Korean national for WannaCry and the Sony hack are only some instances of 2018 events related to cybersecurity. All of these cyberattacks and attributions are embedded in wider political contexts and have political consequences. This Hotspot Synthesis 2018 focuses on geopolitical events in South, Southeast and East Asia, more precisely on the Democratic Republic of North Korea (DPRK)[1], the regional rivalry between India and Pakistan and regional tensions in Southeast Asia. The relevant Hotspot Analyses did not examine Chinese activities *per se*, but China cannot be ignored in the region's broader geopolitical context because of its political, military and economic role.

The goal of the Synthesis 2018 is to identify trends among the three Hotspot Analyses of 2018, to analyze and situate them in the global context and to compare these findings with the Synthesis 2017.[2]

The Synthesis 2018 is organized as follows. Section 2 shows that all of the observed events referred to in the Hotspot Analyses are embedded in a broader political context, with the choice of tools and techniques varying depending on context. The importance of context is also evident from the fact that cybertools are never used in isolatuion but are always employed in conjunction with other means.

Section 3 examines three trends in cyber-activities that are specific to the three Asian regions examined. All three trends emanate from the lack of common agreements on legitimate behavior in cyberspace and contribute to growing risks of misperception in cyberspace and escalating tensions. The first trend consists of the DPRK being the only state known to engage in cybercrime activities to finance its regime and circumvent international sanctions. The second trend concerns the very active nature of patriotic hackers[3] in these regions. These hackers react quickly to geopolitical events with Distributed Denial of Service (DDoS) and website defacement attacks. The third trend refers to the observation that Western states struggle at times to develop appropriate responses to disruptive cyberattacks from Asian states.

Section 4 analyzes the continuing trends from Hotspot Synthesis 2017 and their specificities in the three Asian regions. Five continuing trends have been identified:

- Integration of cybersecurity at the national policy level, although integration in Southeast Asia is more advanced at the regional level
- Strategic choices of targets
- Public attribution still has political ramifications
- Restraint in the use of cyberattacks leading to cyberweapons being used only rarely
- Cyberespionage against Asian and Western states, even against friendly states

Section 5 summarizes the findings of the Synthesis 2018 and concludes by confirming the importance of the political context of cyberattacks.

The Hotspot Synthesis 2018 examines three Hotspot Analyses published in 2018. These are: Cyber disruption and cybercrime: Democratic Republic of North Korea; Regional rivalry between India-Pakistan: tit-for-tat in cyberspace; and Use of cybertools in regional tensions in Southeast Asia.[4] The Synthesis 2018 is based on the information contained in these three documents and analyzes their common themes. Therefore, it is recommended to read the three Hotspot Analyses before reading the Hotspot Synthesis 2018. Additionally, the Hotspot Synthesis 2018 is the second document of this type and refers regularly to the findings and observations made in the previous Synthesis. Therefore, we also recommend reading the Synthesis 2017 to facilitate a better understanding of the Synthesis 2018.

[1] Abbreviations are listed in section 9.

[2] See Baezner, Marie (2018): Hotspot Analysis: Synthesis 2017: Cyber-conflicts in perspective, September 2018, Center for Security Studies (CSS), ETH Zürich.

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

[4] The reports are summarized in tables in Annex 1.

2 Context matters

Hotspot Analyses released in 2018 primarily focused on Asia and examined various contexts in which cyber-operations and / or campaigns took place.[5] The fact that cyber-activities were observed in these different contexts reinforces the claim made in the Synthesis 2017, namely that cyberspace is gaining significance as a strategic domain.

Hotspot Analyses published in 2018 focused primarily on the regional rivalry between India and Pakistan, the case of the DPRK targeting its Southern neighbor and both Western and Southeast Asian states being involved in tensions over the South China Sea. While China's role in the geopolitical context of these regions is most obvious in the tensions over the South China Sea, it also plays a somewhat significant role in the other two Hotspot Analyses. In the regional rivalry between India and Pakistan, China's close relations with Pakistan and its rivalry with India remain in the background but cannot be ignored. In the case of the DPRK, the Chinese government is directly involved in the DPRK's cyber-activities. North Korean hackers operate from Chinese cities to conduct their cyberattacks and use Chinese internet infrastructure (Chanlett-Avery et al., 2017; Kim, 2018). Therefore, the broader context of cyber-activities involves more than just South, Southeast and East Asia and also influences the ways states use cyberspace. Hotspot Analyses in 2018 have also highlighted that cybertools are used in combination with conventional means. Indeed, the type of cybertools used is determined by actors' available resources and the context in which they interact.

The Synthesis 2018 bases its categorization of 2018 Hotspot Analyses on Dewar's (2018a) typology of the contextualization of cyber-operations. Accordingly, the 2018 Hotspot Analyses are categorized as follows: regional rivalry (India-Pakistan) and political tensions (DPRK and Southeast Asia).

2.1 Regional rivalry: India - Pakistan

The Hotspot Analysis of the regional rivalry between India and Pakistan shows that there are two types of cyber-activities which can be observed in this context, both of which are of low intensity. The first type of cyber-activity consists of hacktivism and patriotic hacking. This type of cyber-activity is highly visible but has limited direct physical consequences. Relevant cyberattacks are deployed in response to physical events (e.g. skirmishes on the Line of Control in Kashmir) and / or as reprisals. The perpetrators are primarily non-state actors, although there are most likely also some state-sponsored actors involved. The attacks mostly target websites of state institutions in order to promote patriotic values and influence public opinion by undermining and harassing the adversary.

The second type of cyber-activity is cyberespionage. Actors involved in this kind of activity are state-sponsored and employ moderately sophisticated cybertools. Spear phishing and watering hole attacks are regularly used as infection methods. Additionally, actors modify open-source cybertools for their cyberespionage campaigns and develop malicious Android applications to spy on users. The targets are primarily military and state institutions and their employees. The goal of these cyberespionage campaigns is to gather strategic information on the adversary. While Indian actors initially focused primarily on Pakistani targets, their attention broadened in about 2013 to also focus on Chinese targets (Baezner, 2018a; Balduzzi et al., 2018; Fagerland et al., 2013; Huss, 2016).

Both patriotic hacking and cyberespionage show that cyber-activities in the context of regional rivalries are employed to either harass or spy on adversaries. However, these activities were always somewhat controlled and remained below the level of war. This use of cyberspace demonstrates that cybertools are part of an available toolset for states and are deployed alongside other conventional means (e.g. other sources of intelligence in the case of cyberespionage and protests in the case of patriotic hacking).

2.2 Political and economic tensions: North Korea and Southeast Asia

In the context of political and economic tensions, states have used cybertools in conjunction with other means. Hotspot Analyses on North Korea and Southeast Asia have found cyber-activities to be primarily aimed at harassing adversaries, disrupting, generating revenue and gathering intelligence. In this context, the use of cybertools increases the risk of heightening existing tensions.

In the Hotspot Analysis on North Korea, North Korean actors used cybertools to disrupt, harass, gather intelligence and generate revenue. The DPRK's cybertools are sophisticated, but less sophisticated cybertools are also employed for DDoS and website defacement attacks. Such less advanced attacks are intended to harass South Korean targets and keep South Korean authorities on alert. More sophisticated cyberattacks involved cybertools that erase the contents of hard drives. The goal of such attacks is to disrupt and coerce (i.e. the Sony hack, in which the Lazarus Group hacked Sony Entertainment Picture's network, erased the contents of thousands of computers and leaked stolen information (Sanger et al., 2017)). North Korean

[5] A chronology summarizes the main cyberattacks relating to the three Hotspot Analyses in Annex 2.

actors conduct cyberespionage campaigns against South Korean targets to gather strategic information. The most distinctive particularity of North Korean hackers is their use of cybercrime activities to generate revenue. These hackers have targeted financial institutions and cryptocurrency exchanges to steal money to finance the government and / or its nuclear program while bypassing international sanctions. Cyberspace activities of this nature increase the risk of misperception and heighten tensions between the DPRK, South Korea and its allies. However, international responses to North Korean cyberattacks were limited, enabling the DPRK to pursue its activities in cyberspace with almost total impunity (Baezner, 2018b; Chanlett-Avery et al., 2017; Jun et al., 2015; Libicki, 2017).

The Hotspot Analysis on Southeast Asia describes examples of cyber-activities in the context of political and economic tensions. Relevant cyber-activities are primarily linked to tensions over territorial claims in the South China Sea. First, physical clashes over these claims have triggered DDoS and website defacement attacks from patriotic hackers. However, it remains unclear if and to what extent these patriotic hackers are supported by their respective states. These cyberattacks are aimed at harassing, undermining other states and promoting patriotic views. At the same time, they increase the risks of tensions and misperception among states with territorial claims in the South China Sea. Second, some of these states conduct cyberespionage campaigns. Alleged state-sponsored hacker groups spy on state institutions, defense contractors, businesses and international organizations active in Southeast Asia, including the Association of Southeast Asian Nations (ASEAN). The goal of such campaigns is to gather strategic intelligence on adversaries' state institutions, activities and interests in the South China Sea. Cyberspace activities of this nature again have the potential to heighten existing tensions (Baezner, 2018c; Balduzzi et al., 2018; ESET, 2018; Libicki, 2012; Lin, 2012).

3 Distinctive trends in South, Southeast and East Asia

A closer look at the three Hotspot Analyses reveals three new trends in the use of cyberspace: the DPRK's involvement in cybercrime activities; non-state actors risking escalating tensions through low intensity cyberattacks (India-Pakistan and Southeast Asia); and difficulties responding to disruptive cyberattacks (North Korea and the Sony hack).

In response, states need to not only focus increasingly on cybersecurity and contextualizing the use of cybertools in conflicts, but also to address the problem of establishing common definitions to differentiate between legitimate and illegitimate behaviors in cyberspace. Cyber-activities transcend traditional political and legal principles regarding the legitimate use of force. Indeed, cybertools can be employed both domestically and internationally, in wartime and in peacetime, against civilians and military targets. This versatility and the lack of common definitions or agreement on appropriate behavior in cyberspace constitute sources of disagreement among states and contribute to increasing tensions between states (Borghard and Lonergan, 2017).

In order to stabilize their relations in regard to cyber-activities, states need norms on the use of cybertools in specific contexts. Norms would enable states to break free of the common tit-for-tat circle of cyberattacks that has been observed in a number of cyber-conflicts and Hotspot Analyses.

3.1 A state committing cybercrime

The above-mentioned lack of agreement is particularly relevant in the context of the DPRK's cybercrime activities. The problem consists of having a state pursuing cybercrime activities to generate revenue and finance its government while bypassing international sanctions. Since 2011, the Lazarus Group has been targeting banks in South Korea, the Philippines, Vietnam, Bangladesh and Poland, and since 2016 cryptocurrency exchanges. While states commonly agree that cybercrime constitutes illegitimate conduct in cyberspace and a number of states agreed to create norms for regulating cybercrime in the 2001 Council of Europe Budapest Convention on Cybercrime (Council of Europe, 2001), perpetrators of cybercrime are usually non-state actors. By targeting financial institutions around the world for financial gains, DPRK actors are blurring the lines between cybercrime and cyber-conflict and complicating decisions on how to respond to such attacks (Thomas, 2018).

3.2 Non-state actors' actions in cyberspace

DDoS and website defacement attacks examined in Hotspot Analyses on India-Pakistan and Southeast Asia demonstrate that non-state actors can and do get involved in geopolitical events. These patriotic hackers usually engage in tit-for-tat cyberattacks with their adversaries with the goal to harass and undermine the opponent. However, the link between these patriotic hackers and governments often remains unclear (Balduzzi et al., 2018). When fully independent patriotic hackers launch cyberattacks against adversaries, this entails the risk of crystallizing and escalating tensions at the population level. Targeted states in turn may perceive such attacks as coming from opposing state actors and decide to escalate tensions as a result.

3.3 Responding to disruptive attacks

Torruella (2014) described the deletion and theft of data as a mild form of cyberattacks, which he labelled "cyber disruption", and the case of the Sony hack demonstrated that states can have difficulties responding to disruptive cyberattacks. The Sony hack did not affect critical infrastructures but a private company and presented an additional challenge in that a state actor was involved in disrupting computers of a US private firm. In the Sony case, the US decided to respond by publicly attributing the attack to North Korea in 2014 (Sanger et al., 2017) and by indicting one hacker in 2018[6] (Department of Justice, 2018). However, when the US Federal Bureau of investigation (FBI) publicly attributed the Sony hack to the DPRK, it did not provide enough technical evidence, and the cybersecurity community did not take the attribution seriously. Finding an appropriate response to the Sony hack proved to be a difficult process for US authorities.

This case shows that states can struggle to find proper responses to disruptive cyberattacks. Each case is different and embedded in its own context, which needs to be considered. While the few attempts to regulate this issue provide some examples of possible responses, a lack of more concrete norms and common practices continues to prevail. This absence of norms not only contributes to states' uncertainty regarding appropriate responses to cyberattacks of this nature, but also serves to incite more malicious activities. However, states seem to grow more confident in their practice, as will be explained in Section 4.3.

4 Continuing trends

A review of past Hotspot Analyses reveals five recurring trends in the use of cyberspace: politicization of cybersecurity issues at the national and regional policy levels; the strategic choice of targets by state actors; the strategic choice to publicly attribute cyberattacks; the lack of innovation in cyberweapons; restraint in the use of cyberattacks; and disagreement on intelligence gathering in cyberspace.

4.1 Politicization

The cases studied in 2018 confirmed the trends towards the politicization of cybersecurity. The 2018 Hotspot Analyses focused primarily on Asia and showed that states in this region are integrating cybersecurity at the policy level. However, Southeast Asian states have developed more sophisticated strategies at the regional level (through ASEAN) than at their national levels (Tran Dai and Gomez, 2018). ASEAN is more advanced in the development of strategies because some of its most advanced members, like Singapore, are pushing others and the organization overall in this process. Moreover, a securitization of cyberspace can be observed across Asia as states develop their armed forces' cyber capabilities both for defense purposes and to prepare for the combined deployment of cyber-operations and kinetic means. This growing securitization of cyberspace demonstrates that states in Asia consider this domain to be strategic. Additionally, this strategic perspective of cyberspace indicates that Asian states also make a distinction between everyday cybercrime and state activities in the cyber realm.

Other documents of the CSS Cyber Defense Project published in 2018 confirm the ongoing politicization and securitization of cyberspace:

- The National Cybersecurity and Cyberdefense Policy Snapshot (see Dewar, 2018a), which examines national cybersecurity strategies, confirms the integration of cybersecurity at the policy level.
- The Trend Analysis on Contextualizing Cyber Operations (see Dewar, 2018b) shows that the types of cyber-operations deployed are context-dependent.
- The Trend Analysis on Cyber and Data Sovereignty (see Baezner and Robin, 2018) shows that cybersecurity is linked to questions of autonomy and International Law. This Trend Analysis additionally reports that the debate about sovereignty in cyberspace is similar to the debates that took place about sovereignty in

[6] This hacker was indicted for the Sony hack but also for the ransomware WannaCry, the heist on the Bangladesh Central Bank and other cyberattacks.

other domains. However, the report also shows that relevant discussions regarding cyberspace are still in their early stages, and it indicates that states view the cyber domain as strategic.

The cases studied in 2018 not only confirmed the continuing politicization of cybersecurity but also identified similar trends in the choices of targets, attribution, restraint and cyberespionage as observed in the 2017 synthesis.

4.2 Strategic choice of target

State actors using cyberspace as a strategic domain chose their targets for their strategic values. Unlike in cybercrime activities, states actors do not select their targets for economic gains. Depending on their strategic goal(s), perpetrators target enterprises or institutions of interest to reach these specific goals. At the same time, the choice of targets also depends on the type of actor. Non-state actors such as patriotic hackers usually target websites instead of networks, as they seek to attract attention. State actors, in contrast, usually have greater resources and skills at their disposal and will usually target networks of specific institutions or actors without attracting attention.

The targets found to be most commonly affected by cyberattacks in 2018 Hotspot Analyses can be classified in five categories:

- Public institutions (including military institutions)
- Private enterprises
- Media outlets (including social media)
- International organizations
- Financial institutions

Public institutions are mostly targeted by cyberespionage campaigns, and their websites are commonly subject to DDoS and website defacement attacks. Cyberespionage campaigns aimed at public institutions serve to gather intelligence on an adversary's military capabilities and politics in the context of political tensions.

Private enterprises are mostly targeted by cyberespionage for economic purposes but also for strategic purposes in the case of enterprises contracted by state institutions.

Most Hotspot Analyses also found that media outlets had been targeted. Patriotic hackers target media outlets with DDoS and website defacement attacks to harass and / or undermine their adversaries, but they also target private enterprises with DDoS and website defacement attacks in the context of series of cyberattacks. However, these attacks may also simply constitute opportunistic exploitations of website vulnerabilities. Series of attacks are usually triggered by particular events in the physical realm (e.g. a terrorist attack near the Line of Control between Indian and Pakistan in Kashmir).

International organizations are another common target of cyberespionage campaigns. This has been frequently observed in Southeast Asia, where ASEAN has been regularly exposed to cyberespionage. ASEAN meetings were spied on by both ASEAN members and partners, most likely to obtain insights and information on the topics discussed in meetings.

The targeting of financial institutions by state actors is a new development compared to the 2017 Hotspot Synthesis. This choice of target also differs in the fact that financial institutions are targeted for financial gain, which is normally the goal of cybercriminals and unusual for state actors. Financial institutions were primarily targeted by North Korean actors to find new ways of generating revenue and bypass international sanctions imposed on the country because of its nuclear weapons program.

4.3 Strategic attribution

The three cases studied in Hotspot Analyses in 2018 confirm claims that public attribution is reserved to only a few actors and results from political decisions. In all three Hotspot Analyses, states and private cybersecurity companies attributed cyberattacks to state-sponsored groups. However, when the FBI attributed the Sony hack of 2014 to the North Korean government, a lack of solid evidence and transparency undermined the credibility of the statement (FBI National Press Office, 2014). Both cybersecurity experts and journalists expressed doubts about the attribution (Zetter, 2014). However, since 2014, states seem to have learned from their mistakes and appear to attribute cyberattacks more frequently, provide more evidence and work in a more coordinated manner. For instance, the US publicly attributed the WannaCry ransomware to the DPRK in December 2017, and the UK joined the US in the process by also attributing this ransomware to the DPRK (BBC News, 2017). Such coordinated public attribution also occurred on other occasions, where members of the Five Eyes would publicly attribute cyberattacks to the same perpetrator, giving more credibility to the attribution process at the international level.

Nevertheless, attribution remains problematic in cyberspace. Attribution is based on technical forensics and non-technical analyses like geopolitical context and / or intelligence sources, both of which require significant resources (financial, material and personnel). Only states, private cybersecurity companies and some research institutes have enough of these resources to be able to build credible attributions (Davis II et al., 2017; Rid and Buchanan, 2015). Technical evidence alone is not convincing enough for a state, a cybersecurity company or a research institute to credibly attribute, as technical evidence can be altered to incriminate another actor, and non-technical evidence is therefore needed to build more reliable attributions. The non-technical aspect of attributions is largely based on the "*cui bono*" (to whose benefit) logic, which examines the context of a cyberattack. Another factor which renders the task of attributing cyberattacks to specific state actors more difficult is the fact that some states perform such attacks via proxy groups. When states hire proxy groups to conduct cyberattacks, they retain the ability to deny any involvement if the attack is discovered. Finally, it is essential that public attribution is not only supported by solid technical and non-technical evidence, but also sufficiently transparent to be credible. When an actor attributes without providing adequate evidence, the target audience is less likely to take such an attribution at face value (Davis II et al., 2017).

The act of public attribution is a political act. While private cybersecurity companies publicly attribute as part of their commercial communications, states choose to publicly attribute for political reasons. Attribution is part of the political communication between the attributing party and the accused party as well as between the attributing party and its target audience (customers or the general public). Political reasons for public attributions could be to provoke the accused party, to deter or to send the accused party a signal about attribution capabilities. The decision to not publicly attribute also has political ramifications for states (Davis II et al., 2017; Libicki, 2009).

4.4 Restraint and rare use of cyberweapons

While access to sophisticated cybertools is rather easy, perpetrators tend to show restraint in their use of these tools. This observation also reinforces the general misperception among states regarding the likelihood of high-impact cyberattacks. Restraint is evident even in the more sophisticated and disruptive cyberattacks (e.g. those involving the deployment of wiper software as cyberweapons, as was the case in the North Korean cyberattacks), and attacks have therefore remained below a threshold that would cause an escalation.

One reason for this restraint is that more sophisticated cyberattacks expose the difficulties states have in developing appropriate responses. Indeed, attribution remains complex when perpetrators are state-sponsored proxy groups (enabling states to deny their involvement) and the proportionate level of response to an attack is therefore difficult to evaluate. Furthermore, perpetrators may restrain their cyberattacks in order to avoid escalation due to concerns that these difficulties may play against them.

Perpetrators also show restraint in order to avoid crossing a threshold that may trigger an international reaction. However, this threshold is not fixed, and it is very likely that perpetrators would test it to see to which extent cyberattacks can be disruptive before causing a reaction. The action of keeping control over the effects and spread of a cyberattack can also be part of political signaling. By employing such practices, states are able to display their capabilities while also conveying to others that their actions are controlled and could be stepped up if necessary.

In addition to the above reason for perpetrators keeping their cyberattacks at a low intensity, there is also another factor which may explain this behavior. Perpetrators may find cheaper and easier means to achieve their goals, especially for harassment or small-scale disruptions. Sophisticated cyberweapons are expensive and time-consuming to develop, difficult to control and can only be used once, as the vulnerabilities they exploit can be patched (Axelrod and Iliev, 2014). From a cost-benefit perspective, it may be simpler and easier to use low-intensity cybertools or more conventional means to achieve harassment and disruption.

These two reasons likely indicate why cyberweapons have only rarely been used in Central, Southeast and Eastern Asia. In the context of regional rivalry and political and economic tensions, actors in cyberspace have tended to deploy common cybertools and not cyberweapons.

Dewar (2017) defined a cyberweapon as a cybertool specifically designed to cause physical damage. The tools observed in the 2018 Hotspot Analyses were rarely designed for that purpose. The only case involving cyberweapons was the incident involving North Korea, where the Lazarus Group and Scarcruft used wipers to erase the content of hard drives (Baumgartner, 2014; Constantin, 2013; FireEye Inc., 2018; Novetta, 2016). Actors used cyberweapons within larger operations or campaigns, confirming that such tools were not used in isolation.

The other Hotspot Analyses identified the types of malware used as a mix of openly accessible tools and more sophisticated and custom-made tools. However, no malware observed in these cases was highly innovative or disruptive. Despite the lack of innovation in the development of malware, these three cases demonstrated that an increasing number of actors developed malicious tools for smartphone operating systems (e.g. iOS, Android and Windows phones). This evolution indicates that perpetrators are adapting to other platforms and are finding new channels of attack. Furthermore, as in the previous 2017 Synthesis, a certain increase in the sophistication of social engineering elements of cyberattacks has again been observed. Spear phishing emails and other social engineering vectors (e.g. watering hole attacks) have continued to improve in quality and sophistication, thus indicating that perpetrators have continued to invest significant resources and skills in social engineering.

At the same time, non-state actors such as patriotic hackers and hacktivists seem to exercise less restraint than state-sponsored actors. Their cyberattacks are clearly more visible and sometimes also more daring (e.g. 1937cn, a Chinese patriotic hacker, targeted Vietnamese airports) but are also less sophisticated and less disruptive (Laskai, 2017). For some of these patriotic hackers it remains unclear if they are state-sponsored or not. In either case, the risk of misperception of the threat remains.

4.5 Disagreement on intelligence

The disagreement between the Philippines and Vietnam over cyberespionage is rather inconsequential in comparison to disagreements on cyberespionage between Great Powers (e.g. US and China) but clearly illustrates one of the recurring issues in cyberespionage. This disagreement focuses on the legitimate targeting of cyberespionage operations. The Philippines, which has strong bilateral ties with Vietnam, discovered in 2017 that APT32, a Vietnamese Advanced Persistent Threat (APT) likely sponsored by the Vietnamese government, targeted Filipino companies and government employees. The real purpose of APT32's cyberespionage operation on the Filipino government is unclear, although Gomez and Valeriano (2017) argue that it could have been to expose the Filipino president's rapprochement with China. Closer relations between China and the Philippines would weaken Vietnam's and other neighboring states' position in territorial disputes in the South China Sea (Gomez and Valeriano, 2017).

Espionage is generally tolerated among states. It is considered to be fair game and to be part of a state's toolset for protecting its integrity or obtaining insights into negotiations (Harris, 2016; The Economist, 2013). However, spying on a partner state is frowned upon but still does not violate any international rules, and states which have the requisite capabilities do engage in this practice (Easley, 2014). Indeed, the reaction to the uncovering of APT32's spying operations was moderate in the Philippines. The story was revealed to the public in national media, but Filipino authorities did not take any measures against Vietnam. However, the spying of APT32 on the Philippines will most likely have a negative impact on mutual respect and trust between Vietnam and the Philippines (Fischer, 2013; The Economist, 2013).

This example of Vietnam and the Philippines illustrates clearly that cyberespionage is not an activity reserved to Great Powers. Rather, smaller states not only have the capabilities to conduct cyberespionage campaigns but, as this example shows, also use these capabilities.

Nevertheless, this continuing trend highlights the lack of common norms on cyberespionage among states, a fact which contributes to increased risks of misperception in cyberspace between adversaries as well as between partners.

5 Conclusion

The Synthesis 2018 reveals three new and five continuing trends in the contexts of regional rivalry and political and economic tensions in South, Southeast and East Asia. The Synthesis 2018 shows that most of the trends identified in the Hotspot Synthesis 2017 have continued in 2018 and are still present in these three Asian regions. Of the three new trends, the first one concerning North Korean cybercrime activities seems to be specific to the region. However, the two other trends, i.e. the activities of non-state actors and attribution difficulties, are most likely not limited to Asia and are expected to also emerge in future Hotspot Analyses of different geopolitical contexts.

While the five ongoing trends are not restricted to the three Asian regions investigated, they exhibit particularities that are specific to the contexts of regional rivalry and political and economic tensions. These five recurring trends will most likely continue to be observed in the upcoming years, as issues of attribution and norms of intelligence gathering will not be solved in the short term.

6 Annex 1

Each table summarizes a Hotspot Analysis report:

Table summarizing the **Hotspot Analysis: Cyber disruption and cybercrime: Democratic People's Republic of Korea**.

Description	Tools and techniques	Spear phishing Distributed Denial of service (DDoS) attacks Malware (DDoS-KSig, Destover, DOGCALL, Hangman, Jokra, MYDOOM and Dozer, WannaCry, Android malware)
	Targets	South Korean government institutions and media US military entities US Government and businesses Financial institutions and cryptocurrency exchanges Institutions of the Democratic People's Republic of Korea (DPRK)
	Attribution and actors	DPRK actors (Reconnaissance General Bureau, Bureau 121, Office 91, 414 Liaison Office, 128 Liaison Office, Patriotic hackers, Lazarus Group, Bluenoroff, Scarcruft) South Korea USA China
Effects	Social effects	DPRK population isolated from international information and global internet. DPRK using cybertools to spy on its own population.
	Economic effects	DPRK committing cybercrime to finance the regime. DPRK turning to cryptocurrencies as an easy way to generate revenue. Costs of DDoS attacks for the victims.
	Technological effects	DPRK custom-built malware, unsophisticated but adequate for achieving strategic goals.
	International effects	Cyberattacks attracting international attention without bringing sanctions. Cyber-activities as a complement to the DPRK's nuclear strategy. DPRK risking upsetting partners through indiscriminate cyberattacks.

Table summarizing the **Hotspot Analysis: Regional rivalry between India-Pakistan: tit-for-tat in cyberspace**.

Description	Tools	Website defacement Spear phishing Malware (ex: Hanove malware, BADNEWS, Android spying application, MSIL/Crimson, MSIL/Crimson)
	Targets	Government websites Media websites Indian and Pakistani government entities and military Governments in Southeast Asia International firms
	Attribution and actors	Indian hacktivists and patriotic hackers Pakistani hacktivists and patriotic hackers An Indian APT A Pakistani APT
Effects	Social effects	Causing irritation to and undermining the other side through website defacements. Website defacements attract a lot of attention but are not disruptive attacks. They often follow physical events.
	Economic effects	Costs of website defacements for the website administrators.
	Technological effects	Malware not especially sophisticated and often based on open-source codes; still adequate for achieving strategic goals.
	International effects	Non-state actors risking escalating the conflict through cyberspace confrontations. Indian APT spying on international firms and other governments risking tensions with other states.

Table summarizing the **Hotspot Analysis: Use of cybertools in regional tensions in Southeast Asia**.

Description	Tools	Website defacements Malware (ex: IXESHE, ELMER, PlugX, CT/NewCT, RARSTONE, NETEAGLE, CREDRIVER, Dispind, KOMPROGO, Msger, Yahoyah, LEOUNCIA, Felismus)
	Targets	Southeast Asian government and military agencies Businesses ASEAN entities
	Attribution and actors	Chinese actors (Naikon, APT30, Numbered Panda, APT16, Goblin Panda, Icefog, DragonOK, Danti, Pirate Panda, Hurricane Panda) Vietnamese actor (APT32) Other actors (Platinum, Hellsing, Tropic Trooper, APT5, Sowbug) Hacktivists and patriotic hackers
Effects	Social effects	Irritation caused by defacement and undermining of the other party. Defacements attract attention but are not especially disruptive. Defacements are often a reaction to physical events.
	Economic effects	Competitive and economic loss for targeted businesses due to cyberespionage.
	Technological effects	Mix of custom-built malware and open-source tools.
	International effects	China is not the only actor perpetrating cyberespionage. Cyberespionage is closely tied to the region's geopolitical importance. Non-state actors risk escalating tensions in conflict by using website defacement to protest against specific events in the region. China deploys Anti Access/Areal Denial zones in the South China Sea. Cyber capabilities are integrated in the A2/AD strategy. A2/ADs undermine US projection of force in the region. Southeast Asian states use ASEAN to develop cybersecurity norms and benefit from the expertise of other states like Japan.

7 Annex 2

Table representing the chronology of all cyber-related events observed in the four Hotspot Analysis reports of 2018.

Cyber disruption and cybercrime: The Democratic People's Republic of Korea	Regional rivalry between India-Pakistan: tit-for-tat in cyberspace	Use of cybertools in regional tensions in Southeast Asia

Date	Event
05.1998	Pakistani hackers hack the Indian Bhabha Atomic Research Center's website (Garsein, 2012).
06.07.1999	The JML Virus, allegedly developed by the DPRK, is discovered in the wild.
10.1999	Pakistani hackers deface an Indian Army propaganda website with messages denouncing torture in Kashmir by the Indian Army (BBC News, 1998).
04.2001	Chinese patriotic hackers target US websites as retaliation for a midair collision between a US reconnaissance aircraft and a Chinese fighter plane (Kozy, 2015).
23.10.2001	Pakistani patriotic hackers deface two Indian news websites (Majumder, 2001).
2002	Win32/Weird.B, a version of the JML Virus, is discovered in South Korea (Jun et al., 2015).
04.2004	The DPRK hacks hundreds of computers and servers in South Korea (Mansourov, 2014).
03.2007	According to cybersecurity experts working on Operation Blockbuster, the Lazarus Group, a hacker group allegedly linked to the DPRK, starts to develop its first generation of malware (Novetta, 2016).
01.01.2008	The US National Security Agency (NSA) starts its operation Boxing Rumble to spy on the DPRK (Gallagher, 2015; Maness and Valeriano, 2017).
27.11.2008	Indian hackers deface several Pakistani websites in retaliation for the Mumbai terrorist attacks.
28.11.2008	Pakistani hackers deface Indian websites in retaliation for the defacements (RFSID, 2016; Ribeiro, 2008).
2009	The DPRK Korean Workers Party's Operations Department, responsible for clandestine operations during the Cold War, is restructured to become the Reconnaissance General Bureau (RGB), the DPRK's main intelligence agency (Jun et al., 2015; Recorded Future, 2017).
2009	The Lazarus Group starts its Operation Troy and its wiper malware (Novetta, 2016; Talmadge, 2017).
04-07.07.2009	The Lazarus Group conducts DDoS attacks against 17 South Korean and US government websites (Chanlett-Avery et al., 2017).
19.07.2010	The NSA Operation Boxing Rumble ends (Gallagher, 2015; Maness and Valeriano, 2017).
26.11.2010	Indian hackers deface 35 Pakistani websites on the anniversary of the Mumbai terrorist attack.
03.12.2010	Pakistani hackers hack and erase data on the Indian Central Bureau of Investigation website in retaliation for the November 2010 defacements (Leyden, 2010).
04.03.2011	The Lazarus Group conducts a DDoS attack on 40 South Korean media outlets, critical infrastructures and financial websites, as well as on US military entities in South Korea, in an operation named Ten Days of Rain (Maness and Valeriano, 2017; Novetta, 2016).
12.04.2011	The Lazarus Group targets the South Korean Nonghyup Agriculture Cooperative Federation Bank with a DDoS attack (Chanlett-Avery et al., 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).
29.11.2011	Indian hackers deface hundreds of Pakistani websites (Kumar, 2011a).
12.2011	A series of tit-for-tat cyberattacks occurs between Indian and Pakistani hackers until February 2012 (Joshi, 2012).
26.01.2012	Pakistani hackers deface more than 400 Indian websites on the Indian Republic Day (Mid Day, 2012).

04-05.2012	Chinese and Filipino patriotic hackers engage in a tit-for-tat defacement campaign in reaction to the Scarborough Shoal issue (Glaser, 2015; Passeri, 2012).
09.06.2012	A South Korean conservative newspaper stops a cyberattack by the Lazarus Group, but has its website defaced (Novetta, 2016).
15.08.2012	Indian hackers deface Pakistani websites on Pakistan Independence Day (Garsein, 2012).
17.03.2013	A Norwegian telecommunication firm reveals that it has been targeted by a cyberespionage campaign possibly coming from India (Fagerland et al., 2013).
20.03.2013	The Lazarus Group shuts down 32,000 computers in South Korean broadcast and financial companies (Jun et al., 2015; Novetta, 2016).
04.2013	Anonymous launches an operation against the DPRK causing numerous DDoS attacks and defacement of DPRK websites (Brodkin, 2013; Williams, 2013a).
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 Filipino coast guards (Balduzzi et al., 2018).
25.06.2013	The DPRK launches a DDoS attack against 69 South Korean media outlets and government websites (Jun et al., 2015).
09.2013	Kaspersky Lab discovers a cyberespionage campaign named the Kimsuky campaign against South Korean think tanks and industries (Tarakanov, 2013).
26.11.2013	Indian hackers deface several Pakistani websites on the anniversary of the Mumbai terrorist attacks.
2014	The DPRK compromises 140,000 South Korean government and business computers and tries to penetrate the control system for the South Korean transportation network (Tosi, 2017).
2014	APT32, a Vietnamese 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).
26.01.2014	Pakistani hackers deface thousands of Indian websites on the Indian Republic Day (Khan, 2014).
11.03.2014	Naikon, a Chinese APT, targets countries involved in the search for flight MH370 with spear phishing emails with an attachment related to the disappearance of this flight (Raiu and Golovkin, 2015).
05.2014	Chinese patriotic hackers deface Vietnamese government websites as part of the countries' maritime dispute. Goblin Panda, a Chinese APT, targets the Vietnamese government with spear phishing emails as part of an oil rig incident (Kozy, 2015).
08.2014	DPRK hackers attack the British TV broadcaster Channel 4. The channel had planned to release a TV show on a nuclear scientist being kidnapped by the DPRK. The TV show was cancelled after the cyberattack.
24.11.2014	The Lazarus Group targets Sony Entertainment Pictures with wiper malware. The group identifies itself as the Guardians of Peace and demands that a comedy movie about a plot to assassinate Kim Jong-un not be released. The group also steals information from Sony and leaks it on the internet (Chanlett-Avery et al., 2017; Maness and Valeriano, 2017).
26.11.2014	Indian hackers deface several Pakistani government websites on the anniversary of the Mumbai terrorist attacks (Web Desk, 2014a).
20.12.2014	The DPRK's intranet goes down for ten hours, possibly because of a cyberattack (Chanlett-Avery et al., 2017).
04-05.2015	While China builds infrastructure on the Spratly 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 United Nations Permanent Court of Arbitration (UNPCA) website to spy on visitors of the page on the dispute between the Philippines and China (ThreatConnect Research Team, 2014).
10.2015	The DPRK conducts cyberattacks against banks in the Philippines.
26.11.2015	Indian hackers target more than 200 Pakistani websites on the anniversary of the Mumbai terrorist attacks.
12.2015	The DPRK conducts cyberattacks against the Tien Phong Bank in Vietnam (Sanger et al., 2017).

01.12.2015	APT16 targets Taiwanese media and the Taiwanese government with a spear phishing campaign (Jiang et al., 2015; Winters, 2015).
2016	APT32 spies on Filipino technology firms and a Chinese hospitality developer (Carr, 2017).
07.01.2016	Indian hackers retaliate for the terrorist attack in Pathankot with the defacement of Pakistani websites (RFSID, 2016).
02.2016	The Lazarus Group conducts a cyberattack on the Bangladesh Central Bank through the SWIFT messaging system and steals US$81 million (Chanlett-Avery et al., 2017).
04.2016	DPRK hackers penetrate the South Korean Defense Integrated Data Center and steal classified documents (Sanger et al., 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).
08.2016	Tropic Trooper, an APT of unknown origin, targets Taiwanese government officials and an energy company with spear phishing emails (Ray et al., 2016).
15.08.2016	Indian hackers deface more than 50 Pakistani websites on Pakistan's Independence Day (TNM Staff, 2016).
04.10.2016	Pakistani hackers retaliate for the surgical strikes with the defacement of thousands of Indian websites, while Indian hackers claim to have access to Pakistani critical infrastructures' networks.
11.2016	Scarcruft targets South Korean government and financial institutions as part of a cyberespionage campaign (FireEye Inc., 2018).
2017	The Lazarus Group infiltrates the website of the Polish financial regulator and infects visitors with malware (Sanger et al., 2017).
2017	APT32 targets the Vietnamese diaspora in Australia and Filipino government officials with spear phishing emails (Carr, 2017).
01.2017	Numbered Panda targets the Taiwanese government with a new sample of the malware IXESHE (Crowdstrike, 2018).
02.2017	DPRK hackers steal US$7 million worth of cryptocurrency from the South Korean cryptocurrency exchange Bithumb (Guerrero-Saade and Moriuchi, 2018).
03.2017	Scarcruft targets the South Korean government and military with spear phishing emails (FireEye Inc., 2018).
04.2017	A series of spear phishing emails targeting US defense contractors is attributed to the Lazarus Group (Center for Strategic and International Studies, 2018).
10.04.2017	Indian hackers retaliate with the defacement of hundreds of Pakistani websites to protest against their compatriot's death penalty (Trivedi, 2016).
05.2017	Scarcruft infects the network of a Middle Eastern firm through spear phishing (FireEye Inc., 2018).
12.05.2017	The ransomware WannaCry infects approximately 200,000 computers in over 150 countries (Kim, 2018).
09.2017	A press report states that the US Cyber Command targeted the RGB with DDoS attacks (Center for Strategic and International Studies, 2018).

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).

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

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

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

Patch: Software update that repairs one or several identified vulnerabilities (Ghernaouti-Hélie, 2013, p. 437).

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).

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

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

Social engineering: A non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices (Lord, 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).

SWIFT messaging system: A messaging platform used internationally in financial transactions. It connects more than 11,000 banking institutions in over 200 countries (SWIFT, 2018).

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).

Wiper: Feature that completely erases data from a hard disk (Novetta, 2016, p. 57).

9 Abbreviations

APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
DDoS	Distributed Denial of Service
DPRK	Democratic People's Republic of Korea
FBI	US Federal Bureau of Investigation
NSA	US National Security Agency
RGB	North Korean Reconnaissance Bureau
UNPCA	United Nations Permanent Court of Arbitration

10 Bibliography

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

Baezner, M., 2018a. Hotspot Analysis: Regional rivalry between India-Pakistan: tit-for-tat in cyberspace. Center for Security Studies (CSS), ETH Zürich, Zürich.

Baezner, M., 2018b. Hotspot Analysis: Cyber disruption and cybercrime: Democratic People’s Republic of Korea. Center for Security Studies (CSS), ETH Zürich, Zürich.

Baezner, M., 2018c. Hotspot Analysis: Use of cybertools in regional tensions in Southeast Asia. Center for Security Studies (CSS), ETH Zürich, Zürich.

Baezner, M., Robin, P., 2018. Trend Analysis: Cyber Sovereignty and Data Sovereignty. Cyber Defense Project 40.

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., 2014. Sony/Destover: mystery North Korean actor’s destructive and past network activity [WWW Document]. Securelist. URL https://securelist.com/destover/67985/ (accessed 21.02.18).

BBC News, 2017. Cyber-attack: US and UK blame North Korea for WannaCry [WWW Document]. BBC News. URL https://www.bbc.com/news/world-us-canada-42407488 (accessed 26.03.19).

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

Chanlett-Avery, E., Rosen, L.W., Rollins, J.W., Theohary, C.A., 2017. North Korean Cyber Capabilities: In Brief (No. R44912). Congressional Research Service.

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.

Constantin, L., 2013. New disk wiper malware linked to attacks in South Korea [WWW Document]. PCWorld.com. URL https://www.pcworld.com/article/2043241/new-disk-wiper-malware-linked-to-attacks-in-south-korea-researchers-say.html (accessed 21.02.18).

Council of Europe, 2001. Convention on Cybercrime, European Treaty Series.

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

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.

Department of Justice, 2018. North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions [WWW Document]. U. S. Dep. Justice. URL https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (accessed 28.11.18).

Dewar, R.S., 2018a. Trend Analysis: Contextualizing Cyber Operations. Cyber Defense Project 20.

Dewar, R.S., 2018b. National Cybersecurity and Cyberdefense Policy Snapshots. Center for Security Studies (CSS), ETH Zürich, Zürich.

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

Easley, L.-E., 2014. Spying on Allies. Survival 56, 141–156. https://doi.org/10.1080/00396338.2014.941545

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

Fagerland, S., Kråkvik, M., Camp, J., Moran, N., 2013. Operation Hangover: Unveiling an Indian Cyberattack Infrastructure. Norman Shark AS and Shadowserver Foundation.

FBI National Press Office, 2014. Update on Sony Investigation [WWW Document]. FBI. URL https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (accessed 14.11.18).

FireEye Inc., 2018. APT37 (Reaper) The overlooked North Korean Actor (Special Report). FireEye Inc., Milpitas, CA.

Fischer, M., 2013. Why America spies on its allies (and probably should) [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/news/worldviews/wp/2013/10/29/why-america-spies-on-its-allies-and-probably-should/?noredirect=on&utm_term=.cf9ff02d08c0 (accessed 28.11.18).

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

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).

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

Huss, D., 2016. Operation Transparent Tribe Threat Insight. Proofpoint.

Jun, J., LaFoy, S., Sohn, E., 2015. North Korea's cyber operations: strategy and responses.

Kim, S., 2018. Inside North Korea's Hacker Army [WWW Document]. Bloomberg. URL https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army (accessed 13.02.18).

Laskai, L., 2017. When China's White-Hat Hackers Go Patriotic [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/blog/when-chinas-white-hat-hackers-go-patriotic (accessed 28.11.18).

Libicki, M.C., 2017. North Korean cyber operations: active, noisy, and lacking strategy [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/north-korean-cyber-operations-active-noisy-lacking-strategy (accessed 12.02.18).

Libicki, M.C., 2012. Crisis and escalation in cyberspace. RAND, Project Air Force, Santa Monica, CA.

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

Lin, H., 2012. Escalation Dynamics and Conflict Termination in Cyberspace. Strateg. Stud. Q. 6, 46–70.

Lord, N., 2015. What is Social Engineering? Defining and Avoiding Common Social Engineering Threats [WWW Document]. Digit. Guard. URL https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats (accessed 13.10.17).

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

Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.

Recorded Future, 2017. North Korea Cyber Activity. Recorded Future.

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

Sanger, D.E., Kirkpatrick, D.D., Perlroth, N., 2017. The World Once Laughed at North Korean Cyberpower. No More. [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed 16.02.18).

SWIFT, 2018. Discover SWIFT [WWW Document]. SWIFT. URL https://www.swift.com/about-us/discover-swift (accessed 19.02.18).

Talmadge, E., 2017. North Korea, cyberattacks and “Lazarus”: What we really know [WWW Document]. Phys.org. URL https://phys.org/news/2017-06-north-korea-cyberattacks-lazarus.html (accessed 13.02.18).

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

The Economist, 2013. Rules for spies [WWW Document]. The Economist. URL https://www.economist.com/leaders/2013/11/02/rules-for-spies (accessed 28.11.18).

Thomas, E., 2018. Daylight robbery: cyber escapades of North Korea [WWW Document]. The Interpreter. URL https://www.lowyinstitute.org/the-interpreter/daylight-robbery-cyber-escapades-north-korea (accessed 28.11.18).

Torruella, R.A., 2014. Determining Hostile Intent in Cyberspace. Jt. Force Q. 75 114–121.

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

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

Zetter, K., 2014. The Evidence That North Korea Hacked Sony Is Flimsy [WWW Document]. WIRED. URL https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/ (accessed 14.11.18).

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.