How the Civilian Sector in Sweden Perceive Threats From Offensive Cyberspace Operations

Joakim Kävrestad[1] and Gazmend Huskaj[1, 2, 3]
[1]School of Informatics, University of Skövde, Sweden
[2]Department of Military Studies, Swedish Defence University, Stockholm, Sweden
[3]Center for Asymmetric Threat and Terrorism Studies, Swedish Defence University, Stockholm, Sweden
Joakim.kavrestad@his.se
Gazmend.huskaj@fhs.se
DOI: 10.34190/EWS.21.106

Abstract: The presence of state-sponsored actors executing offensive cyberspace operations (OCO) has been made evident in recent years. The term offensive cyberspace operations encompass a range of different actions, including cyberespionage, disinformation campaigns, spread of malware and more. Based on an analysis of past events, it is evident that state-sponsored actors are causing harm to the civilian sector using OCO. However, the degree to which civilian organizations understand the threat from state-sponsored actors is currently unknown. This research seeks to provide new a better understanding of OCO and their impact on civilian organizations. To highlight this domain, the case of the threat actor Advanced Persistent Threat 1 (APT1) is presented, and its impact on three civilian organizations discussed. Semi-structured interviews were used to research how the threats from OCO and state-sponsored actors are perceived by civilian organizations. First, a computational literature review was used to get an overview of related work and establish question themes. Next, the question themes were used to develop questions for the interview guide, followed by separate interviews with five security professionals working in civilian organizations. The interviews were analysed using thematic coding and the identified themes summarized as the result of this research. The results show that all respondents are aware of the threat from OCO, but they perceive it in different ways. While all respondents acknowledge state-sponsored actors at a threat agent executing OCO, some respondent's argue that state-sponsored actors are actively seeking footholds in systems for future use while others state that the main goal of state-sponsored actors is to steal information. This suggests that the understanding of the threat imposed by OCO is limited, or at least inconsistent, among civilian security experts. As an interview study, the generalisability of this research is limited. However, it does demonstrate that the civilian society does not share a common view of the threat from state-sponsored actors and OCO. As such, it demonstrates a need for future research in this domain and can serve as a starting point for such projects.

Keywords: cybersecurity, state-sponsored, advanced persistent threat, civilian, offensive cyberspace operations

1. Introduction

The presence of state-sponsored actors performing offensive cyberspace operations (OCO) against civilian organisations is a fact (Osawa, 2017, Rowe, 2019). Being aware of, and understating your adversary is a crucial part of establishing defence capabilities (Beckett, 2017). However, the degree to which civilian organizations understand the threat from state-sponsored actors is currently unknown. This research seeks to provide new a better understanding of OCO and their impact on civilian organizations.

OCO are defined as a sequence of planned actions executed by an organized group of people with a defined purpose in and through hardware and software which are used to create, process, store, retrieve and disseminate information in different types of interconnected networks that build a large, global network, built and used by people (Huskaj and Wilson, 2020). The element "offensive" entails actions conducted by an organized group of people belonging to a rule-based nation-state attacking confidentiality, integrity, and availability of an adversary's information systems and related infrastructure. The purpose of frameworks for OCO "is not to facilitate the destruction of adversary military infrastructure, but rather to enable a military organization in rendering an adversary (both military and non-military) incapable to conduct an attack (both in cyberspace and in the physical domain)" (Huskaj and Iftimie, 2020). These insights are the results of ongoing and growing academic research on OCO (Huskaj, 2019, Iftimie, 2019).

Adversaries and various threat actors, however, are not bound by similar restrictions. They use OCO and related methods for political and financial gain, and also to control their societies. Methods for OCO include, but are not limited to, spear-phishing, social engineering, man-in-the-middle, and buffer overflows (Huskaj and Wilson, 2020). Therefore, even if an attack is labeled as ransomware, espionage, or wiper, the initial method to gain

access to a target's information system and related infrastructure is always an offensive action using an offensive method. Rather than describing in detail one or two cases, various attacks are described, by noting the intent of the attack and the resulting impact.

In this paper, we demonstrate how OCO can impact civilian organizations by presenting a reviewing the case of "Advanced Persistent Threat 1" (APT1). We then perform a computational literature review with the goal of establishing what themes that are discussed under the umbrella of OCO targeting companies or organizations before we interview cybersecurity professionals from the civilian sector with the aim of addressing the research question of this research:

RQ: How do cybersecurity professionals in the civilian sector perceive the threat from OCO?

The results presented in this paper contributes to research with a better understanding of how OCO and state-sponsored actors are perceived by the cybersecurity professionals in the civilian society. The rest of this paper is structured as follows; the case of APT1 and the impact of OCO is presented in Section 2. The methodology for this research is described in Section 3 and the results are presented in Section 4. Section 5 presents the answer to the research question and the conclusions from this research.

2. The case – APT 1

Advanced Persistent Threat 1 (APT1) was a threat actor stealing "intellectual property from English- speaking organizations" (Mandiant, 2013). According to the same report, "APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as unit 61398 (61398 部队)" (p. 3). Mandiant (2013) writes that "APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously" (p. 3). The longest time APT1 maintained access in a target's network "was 1,764 days, or four years and ten months" (p.3). The targets included, but are not limited to, information technology, transportation, high-tech electronics, financial services, engineering services, satellites and telecommunications, energy, construction and manufacturing, aerospace, education, healthcare and, metals and mining (Mandiant, 2013).

The primary method of gaining access to a target organization's network was using the offensive method of spear phishing. These e-mails were relevant to the recipient and prepared with one or several attachments, and/or a link. The attachments were disguised as zip-files, or PDF-files, or were actual zip-files that required a password to unzip them. The disguised zip and PDF-files were actually executables: even though the extension was zip or PDF, it included "119 spaces after '.pdf' followed by '.exe'" (Mandiant, 2013). Executing such a file would open a backdoor allowing a remote threat agent to conduct actions on the targets information systems. The other tactic was to use password-protected zip-files to bypass firewalls: a firewall cannot scan the contents of password-protected zip-files for malicious files.

The impact of offensive operations dubbed espionage operations are difficult to measure. It usually takes years before the impact is seen. In 2017, F-Secure, a cybersecurity company, reviewed the impact of the attacks on three companies (Hyvärinen, 2017): SolarWorld, Westinghouse Nuclear, and ATI Metals. Table 1 depicts the impact of the attacks: SolarWorld filed for bankruptcy, Westinghouse Nuclear declared bankrupt, and ATI Metals was trading at less than half of pre-attack levels. In 2020, an additional review of the companies' status was done by the authors as noted in Table 1.

Table 1: The consequences of offensive operations depicted as espionage attacks

Who?	Status before attack	What was stolen?	Status as of 2017	Status as of 2020
SolarWorld	World-leader in solar technology	intellectual property, pricing information	Filed for bankruptcy May 2017	Reorganised in late 2017, and bankrupt again in March 2018
Westinghouse Nuclear	World-leader in nuclear reactor designs	Technical and design specifications	Declared bankrupt	Acquired by Brookfield Business Partners LP after 17 months of bankruptcy organization

Who?	Status before attack	What was stolen?	Status as of 2017	Status as of 2020
ATI Metals	World-leader in specialist metals	User credentials for every account on the IT estate	Trading at less than half of pre-attack levels	Trading at less than half of pre-attack levels

The President of the United States "issued a Memorandum to the Trade Representative stating inter alia that:" (p. 4).

> *"China has implemented laws, policies, and practices and has taken actions related to intellectual property, innovation, and technology that may encourage or require the transfer of American technology and intellectual property to enterprises in China or that may otherwise negatively affect American economic interests. These laws, policies, practices, and actions may inhibit United States exports, deprive United States citizens of fair remuneration for their innovations, divert American jobs to workers in China, contribute to our trade deficit with China, and otherwise undermine American manufacturing, services, and innovation (USTR, 2018)".*

The investigation shows that the Chinese-based offensive operations targeting these companies were not random, they were targeted when they had a business relationship or problem with china (USTR, 2018). Each company is discussed in more detail below.

3. Methodology

As described in the previous sections, state-sponsored OCO do affect civil organization in different ways. The civilian society is, in this case, defined as non-military organizations in the public and private sectors. This research was conducted using semi-structured interviews as described by Robson and McCartan (2016) and preceded by a computational literature review (CLR) used to get an overview of related literature (Mortenson and Vidgen, 2016). The CLR was used to identify topics discussed under the domain of OCO targeting civilian organizations. The topics identified were used to derive themes for interviews with cybersecurity professionals from civilian organizations in Sweden and those themes formed the basis of the interview guide.

The interviews were held with five participants working as cybersecurity professionals in civilian organizations in Sweden and the research process can be summarized as follows:

- 1. A computational literature review as described by Mortenson and Vidgen (2016) was used to get an overview of the research field and establish question themes
- 2. The question themes were used to develop questions for the interview guide
- 3. Interviews were held separately with five participants
- 4. Interview recordings were transcribed
- 5. The transcribed interviews were analyzed using thematic coding as described by (Braun and Clarke, 2006)
- 6. The themes were summarized and used to answer the questions addressed in this paper

4. Results

This research began with a computational Literature Review (CLR) which intended to outline what themes that were discussed in the domain of OCO targeting civilian organizations. The results from the CLR was used to form themes for the subsequent interviews and the CLR followed the methodology outlined by Mortenson and Vidgen (2016) and (Kunc et al., 2018). The Scopus databased was used with the following query:

> *(((((cyber*) AND attack*)) OR (((offensive) AND cyber*) AND operation*) OR (((computer) AND network) AND attack*)) AND (((organisation*) OR company) OR companies))*

The search resulted in 1511 hits. 1466 papers remained after removing papers without abstracts, authors and duplications. Using the CLR analysis procedure involves deciding on a number of topics to be established from the body of literature. The analysis relies on titles, keywords and abstracts of included papers and automatically outputs the themes that are most prominent based on the used words. Using between 10 and 100 themes is common and the number of themes is established by testing (Kunc et al., 2018). Eventually, 60 topics were created in this study resulting in 60 word-clouds that reflected the central words for each topic. An example is given in Figure 1, below.

Figure 1: Example topic word-cloud

Next, the 60 topics were manually clustered into 40 topics, as listed in Table 2 in alphabetical order.

Table 2: The characteristics of the 1466 articles, clustered into 40 topics

Topic	Topic name	Papers	Topic	Topic name	Papers
1	Attack on Water Systems	11	21	Industrial Control Systems	60
2	Attacks on companies & mail/web/networks	91	22	Information Systems	15
3	Attacks on DNS	25	23	Insider threat	38
4	Attacks on healthcare	27	24	Internet attacks	43
5	Attacks on IS in CNI and Nuclear Systems	84	25	Internet freedom	8
6	Attacks on information	60	26	IoT devices & attacks	49
7	Attacks on Information Systems	58	27	Malicious threat attacks	60
8	Attacks on network services	19	28	Modelling	21
9	Attacks on systems	81	29	Network attacks	97
10	Attacks on wireless/mobile network	15	30	Network detection & attacks	95
11	Business information	19	31	Phishing attacks	29
12	China-based attacks	22	32	Protection schemes against attacks	21
13	Cloud computing	30	33	Ransomware	20
14	Cybercriminal attacks	66	34	Smart grid	33
15	Cyber-/information security risk	45	35	Software attacks	23
16	Cyberspace attacks	18	36	Supply chain	26
17	Data cloud	19	37	Terrorist attacks	17
18	Data inspection	13	38	Threats to data	15
19	DDoS attacks	31	39	Virtualization attacks	17
20	Digital evidence	23	40	Web-based attacks	22

It is noteworthy that the top three topics cover network attacks (97 articles), network detection & attacks (95 articles) and attacks on companies & mail/web/networks (91 articles). The bottom three topics cover data inspection (13 articles), attacks on water systems (11 articles) and Internet freedom (8) articles. Furthermore, from a threat actor perspective, the topics cover hackers (11, 21), insider threats (23), and cyber-criminals (14). The topics identified were reviewed by the researchers and abstracted to the following central themes that were used as themes for the interviews:

- Perceived threat actors and threats from different actors
- Perceived direct and indirect threats from offensive cyberspace operations
- Attack vectors used by state-sponsored actors
- Technical defense, deterrence and monitoring measures

- Strategical defense

Five interviews were held separately with security professionals working in civilian organization. The interviews were transcribed and analyzed using thematic coding using the just presented central themes, as described by Braun and Clarke (2006). Inter-coder reliability was built into the coding process by letting one researcher code the majority of the interviews while another researcher coded some interviews and performed consistency checks on the other interviews, similar to Rose et al. (2016). The responses in each theme were then summarized and the summaries are presented at the end of this chapter as results of the interview process.

The respondents are kept anonymous but their background can be described as follows:

- R1: The respondent is now working as an information security coordinator at a Swedish agency. The respondent previously worked as CISO (Chief Information Security Officer) at another agency and was prior to that employed in the public sector in the service desk. She has about 7 years of experience in the security field.
- R2: The respondent's background is as a computer forensic examiner at a Swedish agency and at a private company. He has worked with digital forensics for about 8 years and worked as a developer for about 6 years before that.
- R3: The respondent works as a cyber-security consultant and works with security architecture.
- R4: The respondent has been working in IT for about ten years, and with security for eight of those years. He has been working as a forensic expert, but also with technical and strategic information security and risk management.
- R5: The respondent has been working with security for about 20 years. He has been working with everything from strategic security to technical security. He is currently working as a security consultant and has many customers in the critical infrastructure sector.

The remainder of this section will summarize the interview data that was gathered from each theme.

4.1 Threat actors

Discussing threat actors in general, all respondents discuss organized criminal organizations and state-sponsored actors as the currently most prominent threat actors. The underlying meaning in all interviews is that other threat actors are out there but they are not as capable as state-sponsored actors or organized criminal organizations and do not need to be the primary concern when establishing defense. The interviews suggest that all respondents are aware of state-sponsored actors as a threat agent.

4.2 Threat from OCO

The respondents paint different pictures when discussing the threat from state-sponsored actors. Two respondents describe that the purpose of OCO is for foreign states to get a foothold in systems to enable them to launch cyberattacks as part of armed or diplomatic conflicts. Two other respondents discuss that state-sponsored actors mainly want to steal intellectual property, while the fifth respondent is not at all specific. One respondent also states that foreign states use disinformation campaigns to influence other nations in, for instance, elections.

The respondents agree that one aspect that signifies foreign states as threat actors is that they have access to more time and resources than other threat actors. That makes them pose a unique threat to the organizations they target. However, foreign states are not threat agents for all organizations.

Another threat from OCO that was discussed during the interviews was the risk of being harmed as collateral damage. The respondents agree that the risk of being collateral damage is indeed large, especially if your organization cooperates with organizations or states that are high-value targets for state-sponsored actors. When asked about the risk of being harmed as collateral damage, one respondent replied: "Ask MAERSK". He explains that MAERSK suffered severely as a result of an attack against Ukraine that was supposedly attributed to Russia. Another respondent mentions attacks against critical infrastructure or cyber-critical infrastructure as attacks that would impact the own organization.

4.3 Attack vectors used by state-sponsored organizations

An important part of any risk-based security work is understanding the attack vectors that threat actors may use. As such, the respondents were asked about what attack vectors state-sponsored organizations use. In general terms, the respondents agree that state-sponsored actors use the same attack vectors as other threat actors. There are, however, some attack vectors or modus, that are more commonly used by state-sponsored organizations than by others. The respondents discuss that these are attack vectors that are hard to defend against, but also expensive for an attacker to use. The attack vectors that were discussed during the interviews are described below.

- Long term Social engineering - The respondents discuss that a characteristic of state-sponsored actors is that they act with a long time span. One respondent describes that state-sponsored actors can have a time horizon of 20 years or more, enabling them to employ long term social engineering attacks where they, for instance, position insiders in targeted organizations for later use.
- Human intelligence - somewhat similar to social engineering, one respondent describes that state-sponsored actors employ a human intelligence-based approach to find employees in organizations that can be used as an attack vector. This includes actions such as intelligence gathering as preparation for spear-phishing or insider recruitment. One respondent describes that OCO may include identifying employees that are, for instance, disgruntled or in debt and leverage that information in order to recruit them as insiders.
- Zero-day exploits - Three respondents describe that the large amounts of resources available to state-sponsored organizations allow them to create and hold zero-day exploits. While the respondents' state that the use of zero-day exploits is common amongst several threat actors, they are expensive, high- value possessions. While criminal organizations will use zero-day exploits if they believe that they will gain enough from their attack, state-sponsored actors are more prone to excessive use of zero-day exploits to reach their objectives. One respondent describes that several zero-day exploits were used in an attack against a nuclear facility in Natanz (Iran) making that attack very expensive

To conclude what attack vectors the respondents perceived that state-sponsored actors use, they use all available attack vectors. What differs from other threat actors is that they are more motivated and better funded and can, therefore, use attack vectors that are more expensive and time-consuming.

4.4 Technical countermeasures

The respondents do not think that there are any distinct technical measures that have to be implemented to mitigate the threat from OCO. However, two respondents stress the need for detection and logging mechanisms and state that detection is crucial in order to detect intrusions from state-sponsored actors. He describes that state-sponsored actors often maintain footholds in compromised systems for a long period of time and being able to detect an intruder can enable mitigation.

4.5 Strategical defense

When discussing defense against OCO and state-sponsored actors in general, all respondents agree that it is hard because of the resources available to that specific threat actor. Two respondents specifically state that a key part of the defense is a risk-based structured security approach. This includes identifying key assets, understanding the threats against these assets and employ reasonable preventive measures. The data from the interviews make it clear that defending against state-sponsored actors is different, mainly because it is harder. Something that is very clear is that the defense must include human factors of information security and governance and include polices, strategies and awareness. One respondent specifically stated that the human element of security is crucial for defense against state-sponsored actors, he said that "If you make it impossible, or very hard, to attack the organization using the cyber domain, the attacker will try to find a way to attack the organization easier by using the human domain.

The data gathered from the interviews do not necessarily suggest that any new measures have to be taken, but the information security work has to be done. For instance, the interviews suggest that OCO often includes the use of zero-day exploits, which means that firewall, detection systems and likewise must be in place to enable detection. As another example, the interviews suggest that OCO includes insiders and espionage making it important to know whom you are working with, keeping control of your employees and such.

5. Discussion and conclusions

The research question addressed in this study was "How do cybersecurity professionals in the civilian sector perceive the threat from OCO?" The short answer is that they are aware of the threat but perceive it in different ways, this is elaborated on below.

Based on the results of the interviews conducted in this research it is reasonable to conclude that cybersecurity professionals and the civil sector consider OCO to be a threat and state-sponsored actors to be a threat agent. This notion aligns well with the information presented in the background portion of this paper which exemplifies how the civilian sector has been affected by OCO.

It is, however, noticeable that the perception of the threat from state-sponsored actors differs to a large extent among the respondents. Some respondents describe that state-sponsored organizations want to establish a foothold in systems and use that in case of armed or diplomatic conflict while other respondents claim that state-sponsored actors are mainly looking to steal information. This could suggest that the understanding of state-sponsored actors is, after all, lacking or at least inconsistent among security experts. There is also a chance that the discrepancy in answers stem from the fact the respondents are sure to have different backgrounds from different sectors were the threat is perceived differently. The image of a threat actor that is not yet fully understood is strengthened by the fact that the respondents agree that defense against state-sponsored actors is hard. This insight could suggest that the community of security experts is not yet fully aware of what state-sponsored actors do and how.

Furthermore, and as shown in Table 2 presented in section 4, the topics depict "Attacks on [insert target]". Offensive operations are (mostly) about organized groups of people conducting actions targeting information systems. The methods include, but are not limited to, social engineering, buffer overflows and man-in-the-middle attacks. Therefore, to understand offensive operations and related methods requires a high understanding of the underlying technology. In addition, the respondents have noted that cybersecurity is about"human aspects." This fits well with the notion of security as a process rather than a product (Schneier, 2000). Further, the versatility of attack vectors used by state-sponsored actors emphasize the notion of cybersecurity as a socio-technical property. That notions is well aligned with previous research into cybersecurity (Malatji et al., 2019). The respondents highlight that state-sponsored actors are more prone to using long-terms social engineering and human intelligence attack vectors, suggesting that the "human aspect" of security is even more important when considering the threat from OCO and state sponsored actors as compared to other threat agents.

To the best of our knowledge, little or no prior research maps how cybersecurity professionals in the civilian sector perceived the threat from OCO and their potential impact. The APT1-case presents the impact of OCO. Understanding how public and private organizations in civil society perceive OCO is imperative to future strategic information security practices. As such, this is a step towards a better understanding of how civilian organizations are affected by OCO carried out by state and state-sponsored actors. The impact is twofold, the interviews held in this study do show that OCO is a powerful threat that civilian organizations must consider in the information security practice, and those civilian organizations are worried by this threat. Second, the interviews emphasize the notion that a large and important part of information security work takes place in the human domain, technical defense alone is not enough.

In terms of validity, it should be noted that the intention of this research is to provide an initial outlook of how OCO and state-sponsored actors are perceived by civil society. Using interviews was selected because it allows for a discussion around the subject area and can provide an in-depth understanding of how the respondent perceived the area. On the other hand, it reflects the opinions of the respondents and the results can not necessarily be interpreted as general for all information society professionals globally or even in Sweden. another concern has to do with the nature of the subject area, not many security professionals are comfortable talking about the specifics about how their organization perceive or handle important threat actors, making the replies general in nature. to maximize the respondent's ability to speak freely and ensuring that they were not put at risk in any way, they were guaranteed anonymity as a result of the ethical guidelines proposed by Schrittwieser et al. (2013).

The research presented in this paper suggests that OCO is a threat that the civilian sector is aware of. However, there is a need for a better understanding of how this particular threat is perceived and handled by the entire body of a civilian organization. One apparent direction for future work is to perform a large-scale survey study to research the same topics addressed in this paper in a bigger population. This research does also suggest that the civilian sector, as a whole, does not have a unanimous perception of how they can be threatened by state-sponsored organizations making the need for more research into how the civil society is affected by OCO apparent.

References

Beckett, P. 2017. Data And Ip Are The New Nuclear: Facing Up To State-Sponsored Threats. *Network Security,* 2017**,** 17-19.

Braun, V. & Clarke, V. 2006. Using Thematic Analysis In Psychology. *Qualitative Research In Psychology,* 3**,** 77-101.

Huskaj, G. The Current State Of Research In Offensive Cyberspace Operations. 18th European Conference On Cyber Warfare And Security (Eccws 2019), 4-5 July 2019, Coimbra, Portugal, 2019. Academic Conferences And Publishing International Limited, 660-667.

Huskaj, G. & Iftimie, I. A. Toward An Ambidextrous Framework For Offensive Cyberspace Operations: A Theory, Policy And Practice Perspective. International Conference On Cyber Warfare And Security, 2020. Academic Conferences International Limited, 243-Xv.

Huskaj, G. & Wilson, R. L. An Anticipatory Ethical Analysis Of Offensive Cyberspace Operations. International Conference On Cyber Warfare And Security, 2020. 512-520.

Hyvärinen, N. 2017. Apt1 – What Happened Next? Available From: https://blog.f-secure.com/apt1-what-happened-next/.

Iftimie, I. Cyber Sanctions: The Embargo Of Flagged Data In A Geo-Cultural Internet. European Conference On Cyber Warfare And Security, 2019. Academic Conferences International Limited, 668-Xiv.

Kunc, M., Mortenson, M. J. & Vidgen, R. 2018. A Computational Literature Review Of The Field Of System Dynamics From 1974 To 2017. *Journal Of Simulation,* 12**,** 115-127.

Malatji, M., Von Solms, S. & Marnewick, A. 2019. Socio-Technical Systems Cybersecurity Framework. *Information & Computer Security*.

Mandiant 2013. Exposing One Of China's Cyber Espionage Units.

Mortenson, M. J. & Vidgen, R. 2016. A Computational Literature Review Of The Technology Acceptance Model. *International Journal Of Information Management,* 36**,** 1248-1259.

Osawa, J. 2017. The Escalation Of State Sponsored Cyberattack And National Cyber Security Affairs: Is Strategic Cyber Deterrence The Key To Solving The Problem? *Asia-Pacific Review,* 24**,** 113-131.

Robson, C. & Mccartan, K. 2016. *Real World Research*, John Wiley & Sons.

Rose, J., Jones, M. & Furneaux, B. 2016. An Integrated Model Of Innovation Drivers For Smaller Software Firms. *Information & Management,* 53**,** 307-323.

Rowe, B. I. 2019. Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire. *Security Journal***,** 1-20.

Schneier, B. 2000. The Process Of Security. *Information Security,* 3**,** 32.

Schrittwieser, S., Mulazzani, M. & Weippl, E. Ethics In Security Research Which Lines Should Not Be Crossed? Security And Privacy Workshops (Spw), 2013 Ieee, 2013. Ieee, 1-4.

Ustr 2018. Findings Of The Investigation Intochina's Acts, Policies, And Practices Related To Technology Transfer, Intellectual Property, And Innovation Under Section 301 Of The Trade Act Of 1974.