The Manifestation of Chinese Strategies into Offensive Cyberspace Operations targeting Sweden

Johnny Bengtsson¹,², Gazmend Huskaj³,⁴

¹ Swedish National Forensic Centre (NFC), Swedish Police Authority, Linköping, Sweden
² Department of Electrical Engineering, Linköping University, Linköping, Sweden
³ Department of Military Studies, Swedish Defence University, Stockholm, Sweden
⁴ School of Informatics, University of Skövde, Skövde, Sweden

johnny.bengtsson@polisen.se
gazmend.huskaj@fhs.se

Abstract: The aim of this article is to present how Chinese strategies are manifested into offensive cyberspace operations targeting Sweden. It is commonly known that People’s Republic of China (PRC, and in this definition the meaning of the government and its military), uses five-year plans (FYP) for social and economic steering strategy of their country. This has been going on since 1953 until today. In 2015, the national strategic plan Made in China 2025 (中国制造2025) was launched by Le Keqiang, the Premier of the State Council of PRC. The main goal with this plan is to strengthen the economic development. In addition, Chinese military strategists noted the importance of information warfare and intelligence during military operations. This article is based on open sources: the official English translated version of the 13th Five-year plan (FYP) and other reporting on cyberspace operations linked to the PRC. A number of cases are presented to highlight the link between the PRC FYP and their targets. Next, the current situation in Sweden is presented and how the country is targeted by PRC-linked activities, both in and through cyberspace, but also military infiltration on academia. The results show that Sweden has been, and is continuously the target of offensive cyberspace operations. In parallel, the country is also the target of military infiltration on the academia, and direct investment strategies such as Huawei attempting to compete for the 5G frequency actions arranged by the Swedish Post and Telecom Authority. In conclusion, Sweden will continue to experience cyberespionage from PRC on all levels and on all domains; science, technology, IP and privacy information theft. Previously unveiled cyberspace operations cases in this article have proven to be a convenient strategy for the PRC to reduce its research and development gap in several ways; innovatively, financially and to shortening the time-to-market (TTM).

Keywords: Chinese Strategies, Cyberespionage, Information Warfare, Offensive Cyberspace Operations, Sweden.

1. Introduction

Chinese offensive cyberspace operations targeting western industries have increased and are aggressive. Collecting information through open sources, numerous Chinese cyberspace operations have been revealed and traced back to the People’s Republic of China (PRC). These operations have all been conducted by the government, the military, “hacker” groups – or advanced persistent threat (APT) groups – supported or facilitated by the government or military of the PRC. This paper and its analysis will mainly focus on the state-sponsored APTs. The aim of this article is to present how Chinese strategies are manifested into offensive cyberspace operations targeting Sweden. The incentives for the unveiled governmental and military related cyber activities are directly or indirectly linked to PRC’s underlying political, economic and military mid-term and long-term strategies regarding the 13th FYP, MIC2025 and other strategic documents for the wealth development of PRC and its citizens. Previous scholars agree that cyber operations may be used for espionage purposes to steal intellectual property and for economic espionage purposes (Harknett & Smeets, 2020; Thornton-Trump, 2019). In addition, “Chinese cyberespionage operations are known to go back since at least the early 2000s” (Harknett & Smeets, 2020, p. 18). The main contributions are summarized as follows:

1) Chinese strategies and their manifestation into offensive cyberspace operations are presented;
2) based on 1), their targets in various sectors are identified and presented;
finally, the conclusions present how the strategies are manifested targeting Sweden.


2. Chinese Strategies

This section presents the Chinese strategies. It begins with the 13th Five-year plan (13th FYP), followed by Made in China 2025.

2.1 The 13th Five-year plan (13th FYP)

It is commonly known that People’s Republic of China (PRC, and in this definition the meaning of the government and its military), uses five-year plans (FYP) for social and economic steering strategy of their country. This has been going on since 1953 until today. The 200+ pages official English translated version of the 13th FYP (2016 – 2020) is divided into twenty parts (I – XX) and in eighty chapters, and covers miscellaneous topics, which are the scope for the current strategic evolvement of PRC (PRC13FYP, 2016). Reading through all pages is a lot to digest, but to conclude essential parts of the core; the overall message is to make technology advances in various prioritised scientific and technology research fields. Parts, or boxes, that might be of relevance with regards to cyber operations, are briefly described below and will later on be exemplified.

Box 3, Programs for Sci-Tech Innovation 2030 stipulates Science and technology programs with aim for aircraft engines and gas turbines, deep-sea stations, quantum communication and computing, brain science and brain-inspired research (a.k.a. artificial intelligence, neural networks), cyberspace security, deep space explorations and in-orbit spacecraft servicing and maintenance systems. It also mentions projects related to e.g. space-terrestrial information networks, big data, smart manufacturing and material science.

Box 7, High-End Equipment Innovation and Development aims for aerospace and marine engineering, transportation, high-level mechanical machine tooling, robotics, medical equipment and improved chemical manufacturing.

Box 8, Development of Strategic Emerging Industries stresses the importance of next generation of information technology industries – such as the 5G mobile communications, biotech, their Global Navigation Satellite System (GNSS) BeiDou, energy production and distribution, advanced and new materials such as next generation of semiconductor materials, and also so called new-energy vehicles as in all-electric and hybrid electric vehicles.

Box 9, Information Technology Projects has its focus on digital information, Internet and telecommunication expansions, Internet of Things (IoT), cloud computing innovation and development, the “Internet +” concept that aims for miscellaneous services where Internet is an integrated part, big data applications, better governmental e-services, e-commerce and lastly cybersecurity.

2.2 Made in China 2025 (中国制造2025)

The national strategic plan Made in China 2025 (PRC, 2015) was launched in 2015 by Li Keqiang, the Premier of the State Council of PRC. The main goal with this plan is to strengthen the economic development. This will be done by improvements of industrialization and by year 2049 be the leading country in advanced green manufacturing. The program also aims to further develop information technology, the domains aerospace, aeronautics and oceanographic and underwater technology, rail transportation and automotive engineering, power production, agricultural machinery, material science, bio-pharmaceuticals and medical development. The MIC2025 appears to be highly connected with the 13th FYP.

3. Chinese Information Warfare and The Evolvement of Cyber Doctrine

It is besides the FYP and MIC2025 also worth to mention the military aspect of possessing intelligence information. The importance of information warfare and intelligence regarding military operations during the armed conflicts in e.g. the Middle East and Kosovo during 1990s and 2000s was noted by Chinese military
strategists and later became a seed for the evolvement of their military cyber doctrine, where cyberspace was set to be a new security domain to defend (Jinghua, 2019).

4. Chinese Offensive Cyberspace Operations

Among the public resources at the cybersecurity company FireEye’s website is their summary of identified advanced persistent threat (APT) groups (FireEye, 2020), also known as hacker groups. The listing briefly describes the suspected attribution country, targeted sectors, persona of the current group and alias if this is known, malware that is associated with the attack and identified attack vectors. An extensive analysis report, blogs or even webinars can be associated with a reported APT. Six countries are mentioned by their names: Iran, PRC, North Korea, Russia and Vietnam. The numerous PRC related APTs are mainly targeting the sectors are depicted in Table 1.

Table 1. PRC-related APTs targeting various sectors.

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sector (cont.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising</td>
<td>Information technology</td>
</tr>
<tr>
<td>Aerospace</td>
<td>International organisations</td>
</tr>
<tr>
<td>Agriculture</td>
<td>Investment</td>
</tr>
<tr>
<td>Automotive</td>
<td>Journalists</td>
</tr>
<tr>
<td>Aviation</td>
<td>Law firms</td>
</tr>
<tr>
<td>Biotechnology</td>
<td>Legal</td>
</tr>
<tr>
<td>Chemicals</td>
<td>Media</td>
</tr>
<tr>
<td>Construction and engineering/materials/manufacturing</td>
<td>Metals and mining</td>
</tr>
<tr>
<td>Defence</td>
<td>Military</td>
</tr>
<tr>
<td>Education</td>
<td>Mining</td>
</tr>
<tr>
<td>Electronics</td>
<td>Navigation</td>
</tr>
<tr>
<td>Energy</td>
<td>Non-profit organisations</td>
</tr>
<tr>
<td>Engineering</td>
<td>Pharmaceuticals</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Public administration</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Satellites and telecommunications</td>
</tr>
<tr>
<td>Financial services</td>
<td>Scientific research</td>
</tr>
<tr>
<td>Government</td>
<td>Telecommunications</td>
</tr>
<tr>
<td>Industrial engineering</td>
<td>Transportation</td>
</tr>
</tbody>
</table>

The various targeted industries are likely not to be a co-incidence. It aligns well with the strategic aims given in 13th FYP and MIC2025. The typical claimed outcomes of the attacks are exploiting of the targeted host, installed backdoors, exfiltration of stolen data and intellectual property (IP). What the cyber activities seem to have in common is the espionage perspective and at the same time keeping compromised servers alive.

The wide range of used attack vectors ranges from simple phishing to targeted spear-phishing emails with malicious payload, backdoor installations on compromised targets. The use of exploits, captured hosts to reach other targets, trusted relationship between targeted companies, command-and-control (C2, also CnC, C&C) servers, macro-enabled Microsoft Excel documents, watering hole attacks or strategic web compromises (SWCs), webshells and tools for crossing air-gapped networks are other examples of different modus operandi for succeeded APT campaigns. Extended information regarding APTs and their use of malware is more extensively described by the cybersecurity company The MITRE Corporation (MITRE, 2011). Research for designing attack infrastructure for offensive cyberspace operations also exists (Huska, Iftimie & Wilson, 2020).

4.1 Operation Cloud Hopper

The main objectives for the notable Operation Cloud Hopper (also Cloudhopper) supply chain attack were cyberespionage, theft of IP and miscellaneous data of interest from the Microsoft Windows hosted managed service providers (MSPs) and their clients within the MSP’s cloud solution. The first intrusions against cloud-based MSPs are reported to be dated back to the beginning of 2016. It is claimed that the identified attributor APT10 (a.k.a “menuPass”, “Stone Panda”, “Red Apollo”, “CVNX” and “POTASSIUM”) at the time being were directed by
the Ministry of State Security (MSS) via facilitating covered companies. The reported targeted MSPs are listed in Table 2:

**Table 2. Targeted MSPs by Chinese Cyberspace Operations.**

<table>
<thead>
<tr>
<th>MSP</th>
<th>MSPs (cont.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Sciences Corporation</td>
<td>International Business Machines (IBM) Corp</td>
</tr>
<tr>
<td>Dimension Data</td>
<td>NTT Data</td>
</tr>
<tr>
<td>DXC Technology</td>
<td>Tata Consultancy Services</td>
</tr>
<tr>
<td>Fujitsu</td>
<td>Visma</td>
</tr>
<tr>
<td>Hewlett Packard Enterprise (HPE)</td>
<td></td>
</tr>
</tbody>
</table>

4.1.1 *Reported Modus Operandi*

Attack vectors that were used was a combination of spear-phishing; emails directed to employees containing executable malicious attachment in order to retrieve server access credentials, network reconnaissance, gain of elevated account credentials, use of various tailor-made malware for different services e.g. encrypted communication with C2 servers. The analysis of the Visma case showed that an APT10 installed version of WinRAR was utilised for compression of stolen data of interest, where data exfiltration were destined to Dropbox (PwC UK & BAE Systems, 2017; Bing, Stubbs & Menn, 2018; Bing, Stubbs & Menn, 2019; RecordedFuture, 2019; intrusiontruth, 2018; Kozy, 2018; Council of Foreign Relations, 2018; CISA, 2017).

4.1.2 *The Aftermath of Operation Cloud Hopper*

On the 20th of December 2018, the United States Department of Justice makes a charge against the claimed MSS associated APT10 members Zhu Hua and Zhang Shilong for global computer intrusion campaigns targeting IP and confidential business information. The charges do not mention the Operation Cloud Hopper by its name, but indirectly suggesting them by mentioning two campaigns; The MSP Theft Campaign and The Technology Theft Campaign (DoJ, 2018b).

On the 30th of July 2020, the Council of the European Union (EU) imposes the first ever sanctions against cyberattacks in the sense of travel ban and freezing of possible assets, and in addition prohibition for EU citizens or entities to raise funds. For the Operation Cloud Hopper, the APT10 members Gao Qiang and Zhang Shilong are appointed as well as the company Tianjin Huaying Haitai Science and Technology Development Co. Ltd., which at the time being was suspected to be directed by MSS (European Council, 2020).

4.2 *Other Notable Cyberattacks*

There are a numerous reported PRC associated cyberattacks of various types. Some of them directly or indirectly reflect the strived goals in 13th FYP. Others are meant to harm or demonstrate possessed cyberattack capabilities.

4.2.1 *India and the 40 000 Cyberattacks Attempts on Banking and IT*

The low-intense 150 year old geopolitical Galwan Valley border conflict between PRC and India that once again begun to flourish on the 15th of June 2020, inflicted massive cyberattacks such as DDoS attacks, BGP hijacking, phishing emails and malware distribution against the India’s IT infrastructure and banking sector, attributed by the APT3 (Gothic Panda) and APT10 (Stone Panda). This demonstrates some of the offensive capabilities (CYFIRMA, 2020; NDTV, 2020; India Today, 2020; Saha, 2020).

4.2.2 *Taiwan’s Semiconductor Industry*

Box 8 in 13th FYP declares a strong interest in new semiconductor materials and related technology. One of the world’s semiconductor centres is located in Taiwan and home for e.g. one of the industry leading company Taiwan Semiconductor Manufacturing Company (TSMC). CyCraft Technologies reported a series of new Skeleton Key attacks against the Taiwan semiconductor industry in the Operation Skeleton Key from late 2018 to the end of 2019 in an extensive analysis of Chimera APT group and the modus operandi. The claimed main objective for the attack was the theft of IP (CyCraft, 2020a; CyCraft, 2020b).
4.2.3 The Comac C919 Twinjet Airliner

Box 3 and Box 7 in the 13th FYP and MIC2025 denote the willingness in advances in aerospace technology and engineering. The Commercial Aircraft Corporation of China did almost succeed to develop a domestically designed airliner Comac C919. The development project was just need of a little help from the Jiangsu Province Ministry of State Security (JMSS) and MSS supported APT26 (Turbine Panda) between 2010 and 2015. A more thoroughly analysis of gathering trade secrets and IP is described in the report by CrowdStrike. Members of APT26 eventually led to a U.S. Department of Justice indictment in late 2018 (CrowdStrike, 2019; ThaiCert, 2020; Hruska, 2019; DoJ, 2018a).

4.2.4 The Rumour of Implanting Surveillance Devices

The 4th of October 2018 did Bloomberg Businessweek publish the article The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, reported that a security testing company discovered unintended tiny microchip on motherboards from the solution provider Super Micro Computer, Inc., or Supermicro. According to the article, one or several unnamed investigators concluded that the microchip would grant network access and claimed that the chips were post-installed on the motherboards at Supermicro subcontractor’s factories “by operatives from a unit of the People’s Liberation Army”. As a consequence of the published article, Supermicro was shortly after delisted from NASDAQ and relisted in January 2020.

The claims of the spy chips and its functionality were later questioned by several other sources, including the U.S. Department of Homeland Security. The rumours did not only damage Supermicro. It also raised the question of subcontractors and secure supply chain logistics. More importantly, the awareness has risen regarding potential malicious design embedded into electronic designs (Robertson & Riley, 2018; DoH, 2018; Lee & Moltke, 2019; Baddeley, 2019; Greenberg, 2019; Hayes, 2020; Targett, 2020).

5. Sweden – The General Situation

There is a wide range of published reports and surveys from Swedish authorities and from the private sector, where each publication concludes their version of the Swedish situation with regards to cyber operations, cyber incidents, intelligence, corporation damage, etc. Examples on such publications in random order are Englund (2019); Hanson et al. (2015); Swedish Security Service (2019); Bundgaard & Graflund-Wallentin (2020); Kristiansson (2019); ProofPoint (2020).

There is no official statistics or reliable figures on the true number of cyber operations that Sweden as a country has encountered, but it is reportedly at a constantly high number, and increasing every year (Olsson, 2019).

5.1 Operation Cloud Hopper

It is claimed that the telecommunications company Ericsson, along with the ball bearings and rolling bearings company SKF, were two of the victims in the Operation Cloud Hopper as customers at the HPE breach. According to a spokesperson at SKF, their internal investigation concluded that no commercially sensitive data was stolen, while Ericsson made it clear that no customers were harmed (Bing, Stubbs & Menn, 2019).

The core businesses are of the two companies fits well into the plans of 13th FYP and MIC2025, where the SKF is continuously doing research for improvements of their products. Ericsson is considered to be a major 5G competitor to both Huawei and ZTE.

5.2 The Swedish Protective Security Act and the 5G Network Infrastructure

From 1st of April 2019 did the new protective security legislation Protective Security Act (SFS, 2018a) and Protective Security Ordinance (SFS, 2018b) effect, as a consequence of the recent years’ cyber operations as in cyberespionage and traditional espionage activates against vital targets in Sweden. The new legislation was proposed by the Swedish Government, where the main focus was to modernise and strengthen the security legislation on espionage, sabotage, terrorist acts and other hostile activities. Table 2 presents the statement from the Director General of the Swedish Security Service. Additional laws and information has been produced by the Swedish Security Service (2020a), Johansson (2018), and SFS (2018a & 2018b).
Table 2. Statement from the Director General of the Swedish Security Service.

<table>
<thead>
<tr>
<th>Statement from the Director General of the Swedish Security Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>China is one of the biggest threats to Sweden. The Chinese state is conducting cyber espionage to promote its own economic development and develop its military capabilities. This is done through extensive intelligence gathering and theft of technology, research and development. This is what we must consider when building the 5G network of the future. We cannot compromise with Sweden’s security, says Klas Friberg.</td>
</tr>
</tbody>
</table>

(Swedish Security Service, 2020b)

The Director General and Head of the Swedish Security Service (Säkerhetspolisen, Säpo) Mr. Klas Friberg expresses his concerns regarding PRC’s cyberespionage and the expansion of the Swedish 5G network infrastructure in the matter of that China is considered one of Sweden’s biggest threats, where the PRC conducts cyberespionage campaigns for economic and military gains by intelligence and theft within the fields of technology, research and development – which Sweden has to consider during its 5G network expansion (Swedish Security Service, 2020b).

5.3 Military Infiltration on the Academia

It is, as a parallel to cyberespionage, worth the mentioning of the academic perspective. Sweden – with its open universities, comparably low tuition fees, and an advanced level in science and technology research – offers higher levels of education to foreign students, as in master’s or doctoral programmes. These kinds of opportunities have attracted students also from PRC. Among them are students sponsored by the People’s Liberation Army’s (PLA). The researcher Alex Joske at the Australian Strategic Policy Institute (ASPI) International Cyber Policy Centre published the report Picking flowers, making honey – The Chinese military’s collaboration with foreign universities (Joske, 2018) where he describes the PLA systematic doctrine of sending and funding military scientists and engineers to abroad universities to study and to start collaborations with acknowledged western universities; technology transfer and intellectual property is unsuspiciously carried out from the Sci-Tech institutes to support research and development of domestic military projects. The report also mentions espionage and IP theft as additional duties for some of the students that are sent overseas. The report suggests several recommendations for restricting such activities. The military infiltration phenomenon is known to Swedish universities and university colleges (högskolor). It is however difficult to reveal such activities – and if known, hard to prevent. There is an information exchange on regular basis between universities and Säpo regarding the foreign students (Olsson, 2019; Eiderbrant, Sehlin & Johansson, 2019).

6. Conclusions

The answer to the research question of ‘how Chinese strategies are manifested into offensive cyberspace operations targeting Sweden’ is noted not only in the Operation CloudHopper case, but also in military infiltration of the academia. Therefore, it is concluded that the Chinese have a three-pronged approach targeting the policy-level, industry and academia, using two disciplines: offensive cyberspace and espionage operations and human intelligence operations. The implications of this is an existential threat to Sweden’s economic security and national security.

It is obvious that People’s Republic of China’s (PRC) 13th Five-year plan and the additional Made in China 2025 strategy document have set the primary goal to raise the overall scientific and technology to a global top tier level. It can only be speculated in the reasons for this; political, military, social, scientific and technology influence, along total self-sufficiency in all kinds of manufacturing and production, from agriculture to green energy – but ultimately, an economic independence from other nations and to regain sovereignty.

Various cyber operations have proven to be vital tools for taking steps towards the defined goals in the political strategy. Several OSINT reports indicate that cyberespionage is one of the most common types of cyber operations, but it is likely to assume that PRC has the potential and willingness of issuing aggressive cyberwarfare campaigns – as in the Galwan Valley border conflict between India and China in June 2020.
From a Swedish perspective and with regards to the current political and trade relations with PRC, conduction of cyberattacks with the intention to bring down or disrupt the infrastructure, financial mechanisms or in any other way harm Swedish interests is here considered to be of lesser likelihood.

It is more probable that Sweden will continue to experience cyberespionage from PRC on all levels and on all domains; science, technology, IP and privacy information theft. Previously unveiled cyber operations exemplified in the essay have proven to be a convenient strategy for PRC to reduce its research and development gap in several ways; innovatively, financially and to shortening the time-to-market (TTM).

As a consequence of the Protective Security Act (SFS, 2018a) that went into force on 1st of January 2020, only four telecommunication companies were approved for the participation of the 5G frequency auctions arranged by the Swedish Post and Telecom Authority, Post- och telestyrelsen (PTS). Briefly, the licence conditions statutes that the licence holder shall safeguard that the use of the licensed radio frequency causes no harm to Sweden’s security, installation of new radio infrastructure equipment from Huawei or ZTE is forbidden, existing equipment from these providers must be replaced before the 1st of January 2025, and staff or functions abroad must be relocated to Sweden before the same date (SFS, 2018a; The Swedish Post and Telecom Authority, 2020).

Allowing network and telecommunication equipment from Huawei or ZTE would potentially endanger the critical infrastructure for two major reasons: The hardware design, manufacturing and distribution of vital network components within PRC will always be questioned, similar to the rumour cause by Bloomberg Businessweek (Robertson & Riley, 2018); potential embedded espionage functionality will likely not be revealed if this is etched on the silicon die. The second and more worrying reason for the assumable endangerment is the National Intelligence Law of the People's Republic of China (2018 Amendment), or NIL, which was effective from the 27th of June 2018. Article 7 reads as follows (English translated version) (LawinfoChina.com, 2018). The applicability of NIL is further analysed in the report by Dackö & Jonsson (2019), where a previous version of NIL effective on 27 June 2017 is legally interpreted.

Table 3. Article 7 of the National Intelligence Law of the PRC.

<table>
<thead>
<tr>
<th>Article 7 of the National Intelligence Law of the PRC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>An organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows.</td>
</tr>
<tr>
<td>The state shall protect the individual or organization that has supported, assisted in or cooperated in national intelligence work.</td>
</tr>
</tbody>
</table>

(LawinfoChina.com, 2018)

The Picking Flowers – Making Honey report (Joske, 2018) highlights a number of potential risks of having foreign students in the Swedish universities. This would assumingly have a greater negative impact on a doctoral level, where availability of immaterial property and unpublished research data is at hand. This sort of intelligence information harvesting applies well to the many of the goals in 13th FYP. However, most of the foreign students are statistically not funded by the PLA. The benefits of having foreign students from PRC outweigh the risks in many ways. The international environment and the chance of growing global contact networks are more valuable.

6.1 Future Work

Future work can study the financial impact of Chinese offensive cyberspace and espionage operations combined with human intelligence operations.
7. References


8. APPENDIX I – Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>13th FYP</td>
<td>13th Five-years plan</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial-of-Service</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual property</td>
</tr>
<tr>
<td>OSINT</td>
<td>Open-source intelligence</td>
</tr>
<tr>
<td>MIC2025</td>
<td>Made in China 2025</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed service provider</td>
</tr>
<tr>
<td>MSS</td>
<td>Ministry of State Security</td>
</tr>
<tr>
<td>NIL</td>
<td>National Intelligence Law of the People’s Republic of China</td>
</tr>
<tr>
<td>PLA</td>
<td>People’s Liberation Army</td>
</tr>
<tr>
<td>PRC</td>
<td>People’s Republic of China, in this context the government and military</td>
</tr>
<tr>
<td>Säpo</td>
<td>Säkerhetspolisen, Swedish Security Service</td>
</tr>
<tr>
<td>PTS</td>
<td>Post- och telestyrelsen, Swedish Post and Telecom Authority</td>
</tr>
</tbody>
</table>