National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SCHRODINGER'S SURVEILLANCE STATE : THE STRATEGIC PERILS OF BUILDING A DIGITIZED NATIONAL PANOPTICON

Major Jason Furlong

JCSP 44

Exercise *Solo Flight*

Disclaimer

PCEMI 44

Exercice *Solo Flight*

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 44 – PCEMI 44
2017 – 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

SCHRODINGER'S SURVEILLANCE STATE: THE STRATEGIC PERILS OF BUILDING A DIGITIZED NATIONAL PANOPTICON

By Major Jason Furlong

SCHRODINGER'S SURVEILLANCE STATE: THE STRATEGIC PERILS OF BUILDING A DIGITIZED NATIONAL PANOPTICON

Some of the most centralized and controlling governments are gathering massive amounts of data for the stated purposes of keeping their populations safe, a practice that expands the government's capability to monitor crime and supposedly prevent terrorist activity. While accepted to varying degrees by the populations, this trove of data will be an irresistible target to adversarial nations and actors. Such a large, interconnected wealth of data, if exploited by competent cyber forces, can expose a nation to a critical degree of strategic weakness.

Most of the governments of the world are gathering information on their resident populations through a broad range of digital tools available. While China is used as the example in this paper, the ideas presented could be applied to any authoritarian, top-down, controlling society that is obsessed with the day-to-day movements of its people. Furthermore, this is made easier because in China there are few, if any laws, to maintain the privacy and separation of personal information, which aligns with their societal view that people are not entitled to privacy.

Currently, the Communist Party of China (CPC) is embarking on a fascinating experiment where it seems intent on collecting as much personal information as possible about its citizens for the purposes of suppressing, at the earliest detection, any sort of seditious or rebellious behaviour. Seeing the revolutions in digital technology and the rate at which all its citizens have been eager to snap up and adopt cell phones and computers, the Chinese government has implemented various mechanisms to track all their citizens' online and offline behaviour.[1] Besides an intensive monitoring of online activity,[2] cell phones are also tracked using built-in location information so that the state always knows where people are; vehicles are tracked on highways, facial recognition is used on the sidewalks to

---

[1] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy*, Volume 30, Issue 1, January, 2019, pg 54

[2] Vincent, "Dutch hackers expose China's official database, and six social platform users are monitored in real time," ZTOPlus, (6 March, 2019), accessed 20 May, 2019, https://www.ztoplus.com/techfocus/hacker-disclose-china-database.html

identify all pedestrians, massive collections of voiceprints, fingerprints and DNA to track people and connect biological relations are now the norm.[3]

This means that even a 21st century Luddite, someone too poor to afford a cell phone, or without an Internet presence, can be identified and tracked by the system. The monitoring system will associate and integrate them with the online profiles of friends and relatives, so that all relationships with people will be tracked, exclusive of any desire to hide from the system.

Another "feature" of the Chinese system is the creation of a Social Credit database that marks certain members of society that have exceptionally low ratings. This can based on a variety of data points leading to citizens being tagged as untrustworthy and therefore liable to social restrictions. [4] This means that applications for a job or a loan will consider an individual's ranking in the system.[5] This includes travel restrictions as citizens on the list are prevented from purchasing train and plane tickets.[6] One of the early expectations for the system is that it can observe citizens committing petty crimes, such as speeding, jaywalking, or not paying for parking. This is all tied into what is planned to be an 'intelligent court system,' that will use Big Data and AI to settle court matters with minimal or no intervention of a human judge.[7]

While this might seem bothersome to targeted individuals, it may lead to a situation where Chinese citizens will engender attention if they engage in contact with those who possess an overly low social credit score, effectively letting the government decide with whom people can and cannot interact. The combination of all these various databases collecting human intelligence, including the

---

[3] Sui-Lee Wee, "China uses DNA to Track Its People, With the Help of American Expertise," *New York Times*, 21 Feb, 2019

[4] Nicole Kobie, "The complicated truth about China's social credit system", *Wired Magazine*, 21 January, 2019

[5] Alexandra Ma, "China has started ranking citizens with a creepy 'social credit' system – here's what you can do wrong and embarrassing, demeaning ways they can punish you." 29 October, 2018, accessed 25 May, 2019 https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

[6] Nathan Vanderklippe, "Chinese courts have put on social-credit punishment list about 13.5 million people deemed untrustworthy," *The Globe and Mail*, 19 April, 2019

[7] Alison (Lu) Xu, "Chinese judicial justince on the cloud: a future call or a Pandora's box? An analysis of the 'intelligent court system' of China." *Information & Communications Technology Law,* 26:1 (Taylor Francis Online, London, UK) 28 Dec 2016 pg 61

Social Credit Database will be, for the remainder of this analysis, collectively referred to as a Societal Database, or SocDB.

Assumptions

Before detailing the types of attack, a number of assumptions need to be made. The first is that infiltrating the databases is possible. China has virtually surrounded itself with its "Great Firewall", however this digital bulwark is more about controlling the flow of sensitive political information than it is about keeping the barbarians at bay. Furthermore, Chinese manufacturers of network infrastructure have proven to be very lax at implementing security precautions.[8,9,10] If access from a moderately capable player would be a routine affair, and that internal networks could also be accessed in a similar manner, this would lead to a presence across the various databases and establish an Advanced Persistent Threat[11] (APT) that includes a command and control component.

There are several weaknesses of the Chinese state and society that make it more susceptible to attack on its SocDB. First among these is the level of corruption. China is currently ranked 87th in the world based on Transparency International's corruption index[12], meaning that indirect network access would likely be purchased through an employee that could be embezzled or bribed. Next is the reality that the Chinese justice is system is one that subscribes to the "court of hasty judgment" style of justice,

---

[8] Gordon Corera, "Long-term security risks' from Huawei," *British Broadcasting Corporation*, 28 March, 2019, accessed 24 May, 2019, https://www.bbc.com/news/technology-47732139

[9] Lily Kuo, "China database list 'breedready' status of 1.8 million women.', *The Guardian,* 11 March, 2019, accessed 20 May, 2019 https://www.theguardian.com/world/2019/mar/11/china-database-lists-breedready-status-of-18-million-women

[10] Catalin Cimpanu, "Chinese company leaves Muslim-tracking facial recognition database exposed online," *ZDNet*, 14 Feb, 2019, accessed 15 Marchex83path#, 2019 https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/

[11] Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, and Witold Kinsner, "Detecting Advanced Persistent Threats using Fractal Dimension based Machine Learning Classification," Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics (IWSPA '16). 2016, ACM, New York, NY, USA, 64-69.

[12] Transparency International, Corruptions Perception Index 2018 Ranking, Accessed 26 April, 2019, https://www.transparency.org/cpi2018

where due process and presumption of innocence gives way to *Guanxi* (influence of relatives) and the supremacy of the interests of the CPC. [13,14]

Next, assume that the data, while resident in different databases, can be treated as a single, monolithic database for the purposes of this analysis. Some these databases might be separate entities, but data transfer between them is inevitable as their effectiveness is multiplied when the analysts use them to find correlations between the datasets. Greater effectiveness will result by joining the databases together and then processing them through a fusion algorithm. While this might be bone-chilling to the libertarian human rights advocate, it is an opportunity for an adversary. Given that a reasonably capable actor could get into multiple databases, and that all the databases would be connected, they could develop tools that would give them a single point of interface into the system.

Intruder Effect Level (IEL)

As with any information technology or system, an effective SocDB needs to possess the characteristics of Confidentiality, Integrity, and Availability. Given the previously stated assumptions, there is no longer any confidentiality to an intruder. As for the remaining two, an intruder, if they wish to remain undetected for the long-term, would prefer to limit themselves to attacking the integrity of the system and possibly to isolated incidents of reducing its availability. Credibility of the SocDB is essential for the intruder to deepen their presence and carry on with their subversive activities, so motivated intruders will keep their manipulations consistent and subtle; beyond the threshold that would engender any suspicion.

Given access to the treasure trove of data and nefarious intent, what sort of effect can an intruder wreck upon a system and society at large? Much like network technology is built upon a

---

[13] Maj Ronald T.P Alcala, Eugene Gregory and Shane Reeves, "China and the rule of Law: A Cautionary Tale for the International Community", *Just Security,* accessed 20 May, 2019, https://www.justsecurity.org/58544/china-rule-law-cautionary-tale-international-community/

[14] Jerone A. Cohen, "A Looming Crisis for China's Legal System," *Foreign Policy*, 22 February, 2019

seven-layered architecture in the form of the Open Systems Interconnect model,[15] it is helpful to project the effects on a nation's SocDB and target society in a similar manner, where more sophisticated effects are built upon lower layers of functionality. Starting with the most elementary manipulation, at the level of bits and bytes, and moving through successfully more amalgamated data structures, abstract representations of effects up to the national level, results in a seven-layered model:

1. Simple data
2. Individual records
3. Processed tags and amalgamated data
4. Algorithms and AI processing routines
5. Individual profiles
6. Groups of individuals and regions
7. Nation-wide effects

The first two levels are self-explanatory; they involve intercepting the fundamental data flows within the database and altering the various substantive records. This allows an intruder full access to the target's CRUD functions; that is an ability to Create, Read, Update and Delete records. As an example, consider the injecting or manipulation of text messages, emails, and phone conversations. The next level is more interesting for the purposes of this analysis, as the intruder is looking to alter the processed data within the database. This lets the intruder insert or generate data leading the processing engines to administer tags to records or apply a quantitative score. The manipulations could include the modification of various records or even the Social Credit score itself so that the SocDB would tag individuals as a terrorist, thief, murderer, tax evader, political activist, foreign national, or whatever designation exists in the system.

[15] International Standards Organization, "ISO 7498-1 Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model," Switzerland, 1994, p28

Level Four involves manipulating the semantics of the tags that could be applied in Level Three but more importantly it involves modifying or removing the algorithms, including the artificial intelligence engines, that are mining the data.

Level Five is where an intruder uses the results of the lower level manipulations to achieve modifications to the profiles of existing people. This becomes a profile editing tool, or alternatively, a way for an intruder to create synthetic profiles of citizens who do not exist. With these data, the state can develop a behaviour profile based inter-personal associations. If these associations mirror implicate criminal activity or unpatriotic activities, it will mark groups of people. Individuals could be tied to other citizens in the systems and generate virtual associations when none would previously exist. This could be done, at the lower levels, by injecting text messages, generating emails, and associating voice prints in phone conversations. An intruder could synthesize location data or DNA records to put the members of a virtual group at the same location or crime scene. Consider this a new, more insidious form of identity theft. An intruder can work on the scale of the harassment of individuals – from mere nuisance to extortion, to outright imprisonment or even execution for certain crimes such as drug trafficking.

Level Six involves working to affect specific areas, either geographical or demographic, within the target nation. By pinpointing key individuals or groups of people and putting enough strain on them, the attackers can make their daily lives become a constant hassle so that it affects their jobs and ability to get their work done. Affect enough people in the right industries or locations and an adversary could seriously cripple a national capability. Consider if all the radar operators monitoring some critical airspace corridor, or if the engineers on a high-tech project, were unable to work their jobs because they lost their credit ratings. Manipulating the system to contain or isolate members that are critical parts of

the commerce of society could start to affect the national economy. These economic consequences could be greater than any smaller violent, kinetic effect, and might be less risky for the attacker.[16]

At this level, it becomes more than the efforts of a single intruder and an adversary will likely employ multiple types of cyber forces to achieve effect. This would include a battery of fake news on Social Media and the generation of external messages that could reach through the Great Firewall. An adversary will need to identify the leverage points in the societal system and learn where the fulcrums of opportunity are to cause a desired effect, whether it be a factory shutdown, removal of a higher-level bureaucrat, or hiding veritable terrorist activity. By maintaining an APT, an adversary could generate short-term confusion in the society, at risk of discovery, by shutting down or publicly destroying the credibility of SocDB. With the Panopticon shattered, the resulting effect on society will be unpredictable. Assuming that tightly controlled societies are very brittle and collapse rapidly when the structure fails, this could be disastrous. It is possible that given the number of police and other security services that are on the ground that citizens' behaviour will remain unchanged. However, criminals would see an obvious opportunity and would certainly seek to capitalize on the situation, so there will be some level of chaos. Combine this with a genuine grievance against the system and you have the potential for widespread public disturbance.

Level Seven are those attacks which affect the target nation and are most effective when combined with other aggressive activities, which is why they remain the prevue of nation-state actors. This requires a system-level analysis of the various functions and social systems within the government and would mostly likely only be achieved after a significant investment over a long period of time.

One interesting possibility is to generate so much false data in the system, such as the creation of phantom leagues of insurgents or overall synthetic civil disobedience, that one of three things happens:

---

[16] Whyte and Mazanec, *Understanding Cyber Warfare* (London, UK: Routledge, December 2018) pg 65

a. The state has to expend additional monies and manpower to seek out and rectify all the potential false-positives. A comprehensive SocDB is expensive, and increasing the cost would mean that resources would have to be diverted from elsewhere in the country. If an adversary wanted to reduce the money allocated to the military, this might be one avenue. This would cause them to increase the number of resources that they spend on security, possibly bankrupting them.[17] China's bloated domestic security budget is already larger than its defence budget[18] and would be similar to what the USA did to the USSR in the late Cold War.

b. The increase in false-positives would raise the floor for what would be considered a minimum to investigate. This means that genuinely seditious groups, liaisons or organizations would be able to exist and possibly thrive without the state suspecting of their existence.

c. It could distract the government from other, more serious problems and leave open an opportunity for an external power to attack in some other domain. Consider that the internal security of a nation requires a SENSE function and like any other (para)military organization, operates on an OODA loop, the adversary has just injected a delay into the system and slowed down the loop itself. If done to a sufficient level, an adversary could paralyze the domestic decision-making process.

Threat Actors looking to exploit the SocDB

Using the Canadian Communications Security Establishment's Threat Capability Descriptions[19], the IEL could be related to various groups who might be interesting in manipulating the SocDB to their own ends. Each capability level offers a different incentive or motive for attack as seen below:

---

[17] Brahma Chellaney, "China's detention camps follow in the Soviet Union's footsteps – and then some," *The Globe and Mail* 12 April 2019

[18] Adrian Zenz, "China's Domestic Security Spending: An analysis of Available Data," The Jamestown Foundation, 12 March, 2019, accessed 25 May, 2019, https://jamestown.org/program/chinas-domestic-security-spending-analysis-available-data/

[19] Canada, Communications Security Establishment, "IT Security Risk Management: A Lifecycle Approach, ITSG-33", Ottawa, Canada, November, 2012 Annex 2, table 5.

Table 1 – Relation between Threat Category and Intruder Effect Level

Threat Category	Threat Agent	Intruder Effect Level	End-goals
Td1	Non-malicious Adversary	IEL1, IEL2	Simple intruders looking to learn about the system and escalate activities
Td2	Casual Adversary, troubled citizen	IEL2	Citizens or corrupt employees looking to cover petty crimes, and offenses.
Td3	Adversary with minimal Resources – unsophisticated hacker	IEL2, IEL3	Citizens and criminals looking to hide prolonged criminal activity or banned political activities. Individuals looking to boost their Social Credit Score
Td4	Sophisticated Adversary with moderate resources with little risk	IEL4	Hacktivists looking to get attention to a cause or event. Petty criminals
Td5	Sophisticated Adversary: organized crime, international terrorists	IEL5	Criminals looking to hide extant activities and generate new revenue streams through digital extortion. Terrorists looking for effect. Corporations or nation-states looking to influence specific members of the government.
Td6	Well-funded national laboratory, nation-state, international corporation	IEL6	Regional disruption by a nation-state or wealthy international corporation to hide undesired or clandestine activities or influence the nation in a minor way. Generate a diversion to detract from some other threat or attack.
Td7	Extremely sophisticated adversary	IEL7	All-out attack on a target nation by another nation-state combined with kinetic, (social) media, diplomatic or economic activities. Actor looking to cause large-scale disruption within the society or social unrest.

While exploiting the SocDB offers several tantalizing opportunities to wreak mayhem on a potential adversary, it cannot be carried out with impunity. If the target nation is not wholly confident in the data residing in their servers, they may investigate suspicious activities with face-to-face interviews to gather data, significantly reducing the effectiveness of integrity violation. Investigators might follow up with scrutiny of video records, which require considerably more effort to alter. Fortunately, these activities are manpower heavy, and systems generate a massive amount of data, so the use of automation and AI will be inevitable to assist with the human workload.

When an actor is looking to achieve IEL6 or IEL7, they must continually maintain the manipulated database to maintain a consistent façade across all the parts of the SocDB to support their subversive activities. If the target nation segments their data, or the intruder can no longer gain access to all the databases necessary to alter the data, it becomes harder to develop a seamless deception and the higher order effects become harder to achieve.

Much like the Ultra intercepts of WW2, where the Allies were careful about acting on decrypted Enigma messages, if an adversary shows too much dependence on the falsified information within the SocDB, they run the risk of having their activities exposed. Regular auditing of the databases might reveal the intrusion with all possible consequences to follow, including feeding the intruder with false information turning the puppet master into the puppet. Furthermore, they also run the risk of potential conflicts with other actors that might be trying to hack the same system and plant their own duplicitous information. There are already indications that this very thing is happening in China.[20]

While the opportunity to wreak large-scale havoc on an adversarial nation seems very tempting to some powers, they must consider the many consequences. First, achievement of the higher levels, IEL6 or IEL7, requires an expensive long-term investment that runs the risk of discovery. While IEL6 may not result in a kinetic retaliation, a nation could expect some sort of repercussions including a cyber-attack of proportionate or greater effect, depending on the capabilities of the target. Expect TD7 actors to attempt IEL7 as a part of a combined offensive that significantly furthers a strategic goal but multi-domain actions would likely result in an escalated retaliation.

For some actors, the effort spent working to get into China's SocDB would be worth the investment, as the Chinese are starting to export their surveillance systems, meaning that penetrations can be bridged to other adopters.

---

[20] Catalin Cimpanu, "Chinese company leaves Muslim-tracking facial recognition database exposed online," ZDNet, 14 Feb, 2019, accessed 15 March, 2019 https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/

The ultimate effects, at the top two levels verges into the realm of unpredictability[21], varying from no effect to complete societal breakdown. The morality of an attack that will select and convict otherwise innocent individuals – possibly leading to death sentences – would constrain some actors. Notwithstanding the morality of these actions, if found responsible, the attacker could be sanctioned by other nations.

The most significant long-term effect of an attack of this nature on this system is the erosion of the integrity of the data in the system. Even if the intrusion is detected, the authorities may not be able to determine what has and hasn't been corrupted. Not all of the data would have been touched but, depending on the competency level of the infiltrators, the authorities may never be able to reverse all the damage. Even if the infiltration of the network has been discovered, it might be very difficult to determine which of the data have been manipulated. The authorities will struggle to determine if any particular conviction or illicit liaison or relationship between parties is actually valid, and like Schrodinger's ill-fated cat,[22] it will be both valid and invalid at the same time. Even if all the holes were patched up, all the data collection would have to be restarted while some public records could no longer presume to be valid.

Conclusion

Lured by technology's promise of control and pacification has led some governments to adopt a series Panopticon-like policies and societal arrangements, but a SocDB presents a strategic security risk. A multitude of actors would inevitably gain access into the database and add, create or rewrite data depending on their own motivations and goals. This is further made more likely due to the high levels of initial corruption and easy penetrability of the system. The biggest threat will come from an adversary who can combine cyber knowledge and social network manipulation in a true joint effect

---

[21] Whyte and Mazanec, *Understanding Cyber Warfare* (London, UK: Routledge, December 2018) pg 72

[22] Erwin Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik (The present situation in quantum mechanics)". (November 1935). Naturwissenschaften. 23 (48): 807–812.

with other military or socio-economic effects. As a result, such a tightly integrated system that harvests too much data is liable, at some indeterminate point in the future, to lead to a system failure that will impact the national well-being. A nation that has created this SocDB to eliminate corruption may find that the system was corrupt from its inception and that the corruption traces itself to the roots of the society, thus making it impossible to eliminate. Spotting an opportunity, adversarial actors will leverage the corruption to get in early and maintain their APT so that when the time comes, if necessary, they can take action against the owning nation and expose the target to a critical degree of strategic weakness.

BIBLIOGRAPHY

Alcala, Maj Ronald T.P Eugene Gregory and Shane Reeves, "China and the rule of Law: A Cautionary Tale for the International Community", Just Security, accessed 20 May, 2019, https://www.just-security.org/58544/china-rule-law-cautionary-tale-international-community/

Canada, Communications Security Establishment, "IT Security Risk Management: A Lifecycle Approach, ITSG-33", Ottawa, Canada, November, 2012 Annex 2, table 5.

Chellaney, Brahma "China's detention camps follow in the Soviet Union's footsteps – and then some," The Globe and Mail 12 April 2019

Cimpanu, Catalin "Chinese company leaves Muslim-tracking facial recognition database exposed online," ZDNet, 14 Feb, 2019, accessed 15 March, 2019 https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/

Cohen, Jerone A. "A Looming Crisis for China's Legal System," Foreign Policy, 22 February, 2019

Corera, Gordon "Long-term security risks' from Huawei," British Broadcasting Corporation, 28 March, 2019, accessed 24 May, 2019, https://www.bbc.com/news/technology-47732139

Kobie, Nicole "The complicated truth about China's social credit system", Wired Magazine, 21 January, 2019

Kuo, Lily "China database list 'breedready' status of 1.8 million women.', The Guardian, 11 March, 2019, accessed 20 May, 2019 https://www.theguardian.com/world/2019/mar/11/china-database-lists-breedready-status-of-18-million-women

Ma, Alexandra "China has started ranking citizens with a creepy 'social credit' system – here's what you can do wrong and embarrassing, demeaning ways they can punish you." 29 October, 2018, accessed 25 May, 2019 https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

Erwin Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik (The present situation in quantum mechanics)". (November 1935). Naturwissenschaften. 23 (48): 807–812.

International Standards Organization, "ISO 7498-1 Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model," Switzerland, 1994, p28

Qiang, Xiao "The Road to Digital Unfreedom: President Xi's Surveillance State," Journal of Democracy, Volume 30, Issue 1, January, 2019, pg 54

Rid, Thomas. "Cyberwar Will Not Take Place." Journal of Strategic Studies 35, no. 1 (Feb 2012):5-32

Siddiqui, Sana Muhammad Salman Khan, Ken Ferens, and Witold Kinsner, "Detecting Advanced Persistent Threats using Fractal Dimension based Machine Learning Classification," Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics (IWSPA '16). 2016, ACM, New York, NY, USA

Transparency International, Corruptions Perception Index 2018 Ranking, Accessed 26 April, 2019, https://www.transparency.org/cpi2018

Vanderklippe, Nathan "Chinese courts have put on social-credit punishment list about 13.5 million people deemed untrustworthy," The Globe and Mail, 19 April, 2019

Vincent, "Dutch hackers expose China's official database, and six social platform users are monitored in real time," ZTOPlus, (6 March, 2019), accessed 20 May, 2019, https://www.ztoplus.com/techfocus/hacker-disclose-china-database.html

Wee, Sui-Lee "China uses DNA to Track Its People, With the Help of American Expertise," New York Times, 21 Feb, 2019

Whyte, Christopher and Mazanec, Brian, *Understanding Cyber Warfare* (London, UK: Routledge, December 2018)

Xu, Alison (Lu) "Chinese judicial justince on the cloud: a future call or a Pandora's box? An analysis of the 'intelligent court system' of China." Information & Communications Technology Law, 26:1 (Taylor Francis Online, London, UK) 28 Dec 2016

Zenz, Adrian "China's Domestic Security Spending: An analysis of Available Data," The Jamestown Foundation, 12 March, 2019, accessed 25 May, 2019, https://jamestown.org/program/chinas-domestic-security-spending-analysis-available-data/