Sociae Polites

EISSN 2620-4975
ISSN 1410-3745

THE USE OF LAW
IN CHINA IoT OPERATION INTELLIGENCE CONCEPT

[1]Syarifurohmat Pratama Santoso, [2]Moh. Karim

[1]Open University, Jakarta, Indonesia [2]Trunojoyo University, Madura, Indonesia

[1]pratamasantoso75@gmail.com [2]karim@trunojoyo.ac.id

Abstract

Internet of Things (IoT) currently become one of the most developing systems in the world. Private to government used it for their intelligence tools. It will support them to complete mission, such as investigations, security, and recruitment. In international intelligence, IoT concept has already used cause of its effectivity. These conditions are also supported by modern cyber era that can stored our data throughout the world digital form. Currently, China is one of the countries that is making breakthroughs in domestic law to advance its national interests. This research tries to find new points of view and compare data in the form of papers, news, research topic articles, books, and journals. It is hoped that this research can help understand the correlation between law and intelligence regarding the use of IoT in the current era of modern intelligence.

Keywords: Law, Internet of Things, Intelligence, Security, National Interest

1. Introduction

1.1. Background

Internet of Things (IoT) is a concept that aims to expand the benefits of continuously internet connectivity (Salazar and Silvestre, 2017). This will be need interaction of the digital data sharing, and connect to objects (Patel, 2016) (Ramasamy and Kadry, 2021). Currently, this IoT concept has been developed and implemented for various purposes, like intelligence government operation's Purpose. It will be used for state intelligence institutions to do their mission, especially:

- Investigations, theft of target data for intelligence operations;
- Security such as surveillance, monitoring, and location tracking using Artificial Intelligence (AI)-based Closed Circuit Television (CCTV); and
- Recruitment operation such as brainwashing target.

Intelligence, which is a tool of country to protect their interests. They can take advantage of IoT to simplify its main mission. The role of prevention and early detection is a reason that why IoT is needed by intelligence to carry out its duties (Atlam, 2014). Threats of sovereignty and security can occur at any time, so using all capabilities, including IoT materials, becomes a solution in the implementation of intelligence's purposes (Fischerkeller, 2022). Some of National Intelligence such as Central Intelligence Agency (CIA) or Mossad use this technology also.

In this digital era, the use of IoT in the world of intelligence are common, especially in international relations among nations. There are benefits of IoT in Intelligence such as cutting operational costs, increasing work efficiency, and providing data insights for decision-making (Han, 2017). Currently, almost all data are owned by the state have been recorded on digital data on computers (Crane, 2023). The effectiveness of IoT today has helped for intelligence agent, especially in any situation regardless of the weather and terrain.

When referring to the use of IoT at this time, one of the leading country that have developed IoT in intelligence operation missions is China. China as a Communist country has its advantages to binding international companies owned by its people when compared to other countries through their legal products. We can see articles 7 and 14 in the 2017 National Intelligence Law of the People's Republic of China which states that,

- Article 7: Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence. work known to the public.
- Article 14: The state intelligence work organization shall carry out intelligence work according to law, and may require relevant organs, organizations and citizens to provide necessary support, assistance and cooperation.

Apart of 2017 National Intelligence Law, there is also 2017 Cybersecurity Law. It can help Chinese intelligence agent to access personal data which ease to profiling personal data. This cause foreign technology companies such as Microsoft, Apple and PayPal operating in the Chinese market are obliged to store Chinese user data on Chinese servers in mainland China providing an easier access route for Chinese intelligence and state security agencies to intercept data and communications.

- Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.

Last, there is also the 2015 National Security Law which contains articles justifying a company in China collaborating with intelligence parties in carrying out operations. This is contained in article 77 (4):

- Article 77: "Citizens and organizations shall perform the following obligations to preserve national security:" …
- (4): …" Providing conditions to facilitate national security efforts and other assistance" …

1.2. Research Question

Based on the discussion above, we are interesting in knowing use of law in China IoT Operation Intelligence Concept. To explore this research, we are concern in two questions,

RQ1: How does China use its domestic legal products to justify intelligence operations?
RQ2: How are operations carried out internationally and domestically?

1.3. Purpose and Objective

China's Law is drafted not only for defensive but also offensive. We can see how Chinese intelligence have access to coordinate with national-owned companies. They tried to include their interest into hardware which distributed to all the world. It is easier for Chinese intelligence to use the IoT concept to complete their missions.

2. Literature Review

2.1. Legal Justification

This theory bases on a reason of nation justified. We understand that a national government will not be able to run effectively without full legitimacy. The government and its equipment as an instrument for structuring society which holds the main political power must have a legal justification or basis (legitimacy) for the power it exercises so that it can be effective. Nations use this act because what they do is felt to meet certain legal standards, they are not criminally guilty of acts that should be criminal (Simmons, 2006).

In this case, will of law from China Government give legitimacy for intelligence agent to implementation their interest. It would become a basis for them to work forward. Even they will break international relations, they will have an alibi for their activities.

2.2. Signal Intelligence (SIGINT)

SIGINT is the collection of information from the interception of electromagnetic emissions, usually from electronic communications. IoT is one of the new things that can be categorized as SIGINT (Santoso, 2022). IoT applies new types of sensors in many new places to control or optimize roads, buses, trains, production lines, plant management and countless other activities. And smartphones are increasingly capable of detecting interesting things, especially location, as well as audio and video.

3. Research Method

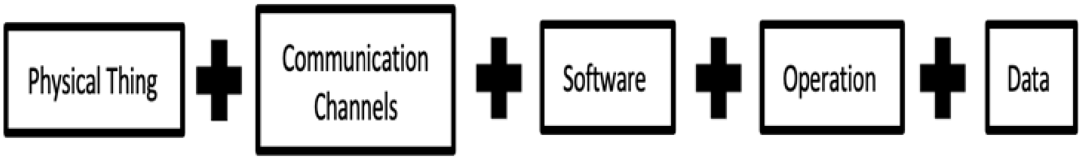
This research uses a qualitative descriptive method which begins with an interpretative or theoretical framework analysis. This qualitative researcher uses a secondary data approach in investigations to study problems. The methods are collecting data ranging from Chinese legal products, international government reports, news, journals, and books.

4. Results and Discussion

4.1. IoT Concept

One way that can be used in this intelligence operation is to make a chip. It will be inserted into the target motherboard or target hardware (Conceição and Reis, 2020). This chip functions as a device that acts as an OpenVPN server and controls the data transfer process. It will become a way to do espionage and can be carried out more easily (Raj and Srinivasulu, 2022). In its application in the field, intelligence agents will do it in various ways, including using legal methods that have never been imagined before (Eftimiades, 1994).

Figure 1. Flowchart Internet of Things Essentials

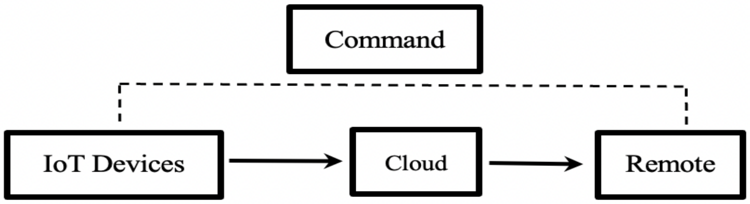


1. Physical Objects. The IoT capabilities of physical objects include sensors, actuators, processing, control, and power. The physical specifications depend on cost, size, performance, and environmental constraints.
2. Communication Channels. The combination of internet protocols and connectivity solutions enables data transfer on a Thing-to-Thing, Thing-to-Server, or Server-to-Server. It depends on the area of use of the design.

3. Software. The software provides the ability to retrieve, process, store, and analyze data originating from an object. The software also provides application-level human capabilities to visualize data and interact with IoT systems.
4. Operation. Cloud infrastructure accessibility in deploying and maintaining IoT.
5. Data. Data is a product of the IoT system. With data as a medium of communication between point to point in the IoT system.

The operations of IoT are simple. They are divides to the three main components of the IoT architectures, (1) physical objects equipped with IoT modules, (2) network-connected devices such as modems and wireless routers, and (3) cloud data centers such as application storage and databases (Pereira, 2022). All elements are connected to the Internet and stored in the form and volume of large data. These are called big data (Luntovskyy, 2022). This data will be processed and analyzed appropriately by the analysts.

Figure 2. Internet of Things Operating System Flowchart



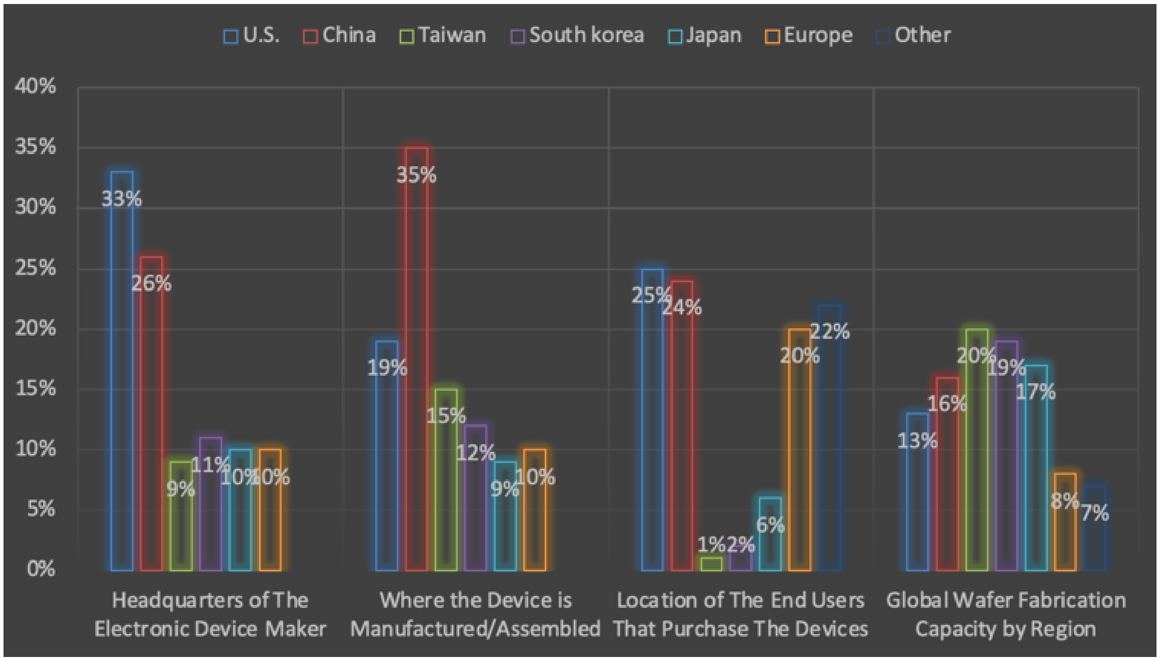
The picture above, are explained that IoT will be controlled by intelligence personnel. The data captured by IoT, and the results of orders will go through the cloud before reaching the remote. Intelligence data becomes information material which will be processed again by intelligence agents before being presented to the boss.

This scheme will be helped by national law before implemented in domestic and international relations. National interest will be suitable to protect this policy. It is becoming justification for intelligence agent move forward.

4.2. Internet of Things (IoT) in Intelligence Investigations Missions

The China use of law for IoT Operation Intelligence in the world currently very mushrooming. China will do whatever they want to achieve their interests, including attracting the civil sector such as a private international holding company led by its citizens (Patel and Doshi, 2019). For example, there are reports from Bloomberg media, which China has taken advantage of the supply chain of chipmakers in its country. They tried to insert intelligence chips into their motherboards product before being distributed throughout the world (Robertson and Riley, 2018).

Figure 3. Fight to Control World Microchips in 2021



The chart explains that a hardware product or a technology product can be formed after going through the economic supply chain. Although in fact the headquarters of Electronic Device Maker was 33%, in the supply chain the device spreads to several countries. In Fabrication Capacity, Taiwan was outperformed by a total of 20%. However, at the end of the assembly process, almost all the equipment was done in China. Almost half of the equipment distributed throughout the world was assembled in China, which was 35%, followed by America (19%), Taiwan (15%), South Korea (12%), Europe (10%), and Japan (9%) (Varas, 2021). Although China was not superior to America, China has advantages in assembly locations which were gaps that intelligence personnel can enter to carry out intelligence operations.

One of the things that Chinese Intelligence can enter to play this operation is by entering into the country's motherboard manufacturing company where the country is one of the largest exporters in the world. Scheme is already arranged in China domestic law. We can refresh how are 2017 National Intelligence Law and 2015 National Security Law make a deal on it. The company who works in China territorial should join this rule of law.

According to several media reports compiled, China can find a gap in the production of computer technology in the world. Other countries will be definitely continue to import the prototype series because of dependency. China is specializing for assembly, packaging, and testing in activities of the value supply chain (Robertson and Riley, 2021). It is possible for Chinese intelligence to work with its domestic. They can also manipulate components at the factory and ensure the company distribute it.

This reality makes a good possibility fot China to do espionage and theft of sensitive data through computers that have been infiltrated by microchips in PCs manufactured. In fact, we know that the chip is central and like the brain to run technology. According to a report from Bloomberg, China-modified microchips was ever found in

America Department of Defense data centers, Central Intelligence Agency (CIA) drone operations, and the Navy's onboard warship network. This report was one of the documents that indicate that the spread of Chinese intelligence chips has entered a sensitive environment in its current rival country.

The other case, China is also using a computerized product using IoT consept to espionage African countries. Report by newspaper Le Monde, China, which pays for and builds computer networks in the African Union Headquarter, was accused of using intelligence tools that enable data transmission secretly. This was discovered in January 2017 by technicians. China’s device being on every midnight even though the building is empty. The investigation revealed that African Sensitive data had been transmited to a server in Shanghai. As we know, most of the computer systems at African Union headquarters are provided by Chinese telecommunications company Huawei and paid for by the Chinese government.

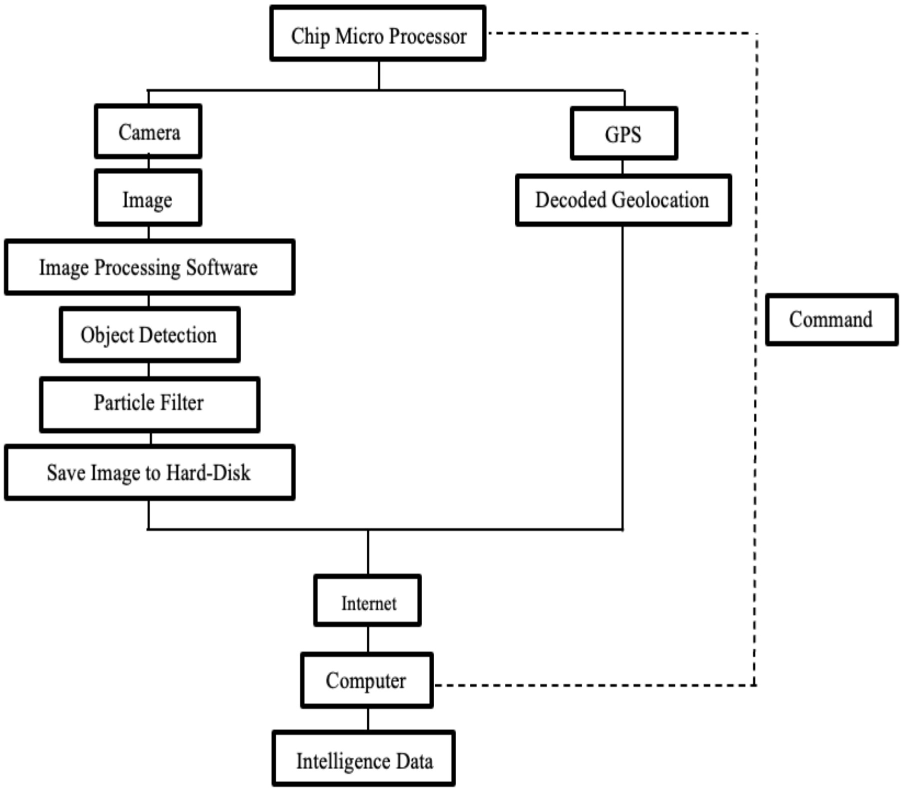
4.3. Internet of Things in Security Intelligence Missions

IoT can be used in CCTV camera. Besides being able to be used as a data source for the investigation missions, CCTV can be used to assist intelligence agents also in carrying out security missions (Kanthaseelan, 2021). CCTV has developed into a very sophisticated IoT tool for detecting people's movements. It can be seen in the television series entitled Person of Interest, describing the development of CCTV technology that can be utilized by intelligence activities. CCTV technology can provide analysis automatically. They will find out the number of people caught by the camera in a short time. Even, the machine can find out the identity of each person recorded by CCTV (Tripathy and Singh, 2022).

Data compiled by BBC news, China was a country which best and largest surveillance cameras in the world. There are about 170 million CCTVs already installed and an estimated 400 million new cameras will be installed in the next 3 years. China even has a digital catalog containing photos and data of its people's information. Cameras with Artificial Intelligence (AI) are widely used (Senthilkumar, 2021). Through CCTV cameras and Artificial Intelligence, their system can read vehicle number plates, live facial recognition, and people who meet you often, to your location at any time (Turtiainen, 2023). In this reality, we can imagine how the law become justification on national interest, even though it would enter in privacy sector.

The current application of IoT CCTV in the intelligence world can go through several processes. First, the command will enter the Micro Processor Chip which will be forwarded to the connected camera and GPS. At the Camera point, images will be taken on cameras that have been installed at strategic locations that have been previously placed. The recorded image will automatically enter the software and the AI will automatically detect the person's biography and adjust the face to the photo center data in the citizen identity card database. After successfully matched, the results from the AI will be brought to the intelligence personnel's operations computer.

Figure 4. Flowchart CCTV use AI



At the same time, the Micro Processor Chip tracks the location of the activities of the people who have been snooped on. The Global Positioning System (GPS) will help the system to determine the location of the CCTV area where the location is currently operating. This will help in making very fine details in terms of the final intelligence gathering.

In the end, all the data will go into a computer controlled by an intelligence agent at a location. The data will be automatically entered in the form of reports which will make it easier for intelligence personnel to make reports. In the end, this circle of IoT CCTV technology tools will greatly facilitate the work of intelligence personnel in the field.

4.4. Internet of Things in the Intelligence Recruitment Missions

Recruitments are various initiatives, actions, and activities designed to achieve goals on behalf of national interests and security on intelligence operation. It is an effort, steps, and actions aimed at facilitating, guiding, and creating an environment that provides all opportunities to favorable framework (Goniwada, 2021). One of this effort in the modern intelligence operation era is using IoT as technology tool.

The IoT intelligence function could be used as an intermediary to perform the recruitment operation. One of these operation could be done with the support of other sciences such as brainwashing technic. By utilizing the Internet, nowadays you don't have to face to face to do brainwashing (Mikusz, 2018). IoT could be used as a tool to screen biographies of target operation who fits the leadership criteria. Usually, in this scheme, some of intelligence agency have AI in their IoT Tech to help them on it.

5. Conclusions and Recommendations

The modern era has brought very fast changes and needs to be adapted by state intelligence. Domestic law and national interest are become the basis for justifying an intelligence operation. In this case, China could make it happen with their domestic law, such as 2017 National Intelligence Law, 2015 National Security Law, and 2017 Cybersecurity Law.

IoT has been implemented by almost all state intelligence agencies in the world. As in the investigation process, countries such as China even infiltrate chips on computer motherboards that are distributed throughout the world. In security, IoT is currently being used on CCTV devices that have AI technology. This technology will help intelligence personnel to make reports faster. Lastly, in recruitment, IoT has been used to track prospective intelligence personnel. IoT will help leaders to find intelligent candidates according to the desired criteria.

In this case, we can learn how domestic law correlation on national interest. It would help intelligence personnel to determine option in their operation to achieve their goals. Today, IoT has become a new technological option device that could be modified and favored by intelligence personnel. Targeting digital data will be very easy if intelligence personnel can operate IoT. We can imagine how world intelligence arena even more fierce with the development of IoT in the future.

Bibliography

Books

Eftimiades, Nicholas. 1994. *Chinese Intelligence Operations*. London: Routledge. doi: 10.4324/9781315037448.

Fischerkeller, Michael P, and et al. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. *New York: Oxford Academic*. doi: 10.1093/oso/9780197638255.001.0001.

Salazar, Jordi, and Santiago Silvestre. 2017. *Internet of Things*. Czech Republic: Czech Technical University of Prague Faculty of electrical engineering.

Simmons, and et al. 2006. *International Law and International Relations*. New York: Cambridge University Press.

Journal and Proceeding

Atlam, Hany F, and et al. 2018. “Intelligence of Things: Opportunities & Challenges.” *3rd Cloudification of the Internet of Things (CIoT)*: 1-6. doi: 10.1109/CIOT.2018.8627114.

Conceição, Celebe Michael de Oliveira, and Ricardo Augusto da Luz Reis. 2020. "Security Issues in the Design of Chips for IoT." *IEEE 6th World Forum on Internet of Things (WF-IoT:* 1-5. doi: 10.1109/WF-IoT48130.2020.9221377.

Crane, Gregory. 2023. “The Perseus Digital Library and the future of libraries.” *International Journal on Digital Libraries 24 (2): 117-128*. doi: 10.1007/s00799-022-00333-2.

Goniwada, Shivakumar R. 2021. “Intelligent Operations”, *Cloud Native Architecture and Design*: 637-659. https://doi.org/10.1007/978-1-4842-7226-8_18.

Gupta, Anirudhra, and et al. 2021. "Perils and Applications of IoT Security in Military Operations." *Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*: 690-697. doi: 10.1109/ICESC51422.2021.9532996.

Han, Hyonyoung, and et al. 2017. “Intelligent operation monitoring IoT tag for factory legacy device.” *International Conference on Information and Communication Technology Convergence (ICTC)*: 781-783. doi: 10.1109/ICTC.2017.8190780.

Kanthaseelan, Kajenthani, and et al. 2021. “CCTV Intelligent Surveillance on Intruder Detection.” *International Journal of Computer Applications* 174 (14): 29-34. doi: 10.5120/ijca2021921035.

Luntovskyy, Andriy. 2022. "Planning Paradigms for IoT Systems." *IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*: 01-06. doi: 10.1109/TCSET55632.2022.9766920.

Mikusz, Mateusz, and et al. 2018. “Raising Awareness of IoT Sensor Deployments”, in *Living in the Internet of Things: Cybersecurity of the IoT - A PETRAS, IoTUK and IET Event*. doi: 10.1049/cp.2018.0009.

Patel, Chintan and Nishant Doshi. 2019. “Security Challenges in IoT Cyber World,” *Lecture Notes in Intelligent Transportation and Infrastructure (LNITI)*: 171–191. doi: 10.1007/978-3-030-01560-2_8.

Patel, Keyur, and et al. 2016. “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.” *International Journal of Engineering Science and Computing* 6 (5): 6122-6131. doi: 10.4010/2016.1482.

Pereira, Igor Muzetti. 2022. “On the Continuous Delivery in IoT Systems.” *Congresso Ibero-Americano em Engenharia de Software*. doi: 10.5753/cibse.2022.20991.

Raj, Jeberson Retna, and Senduru Srinivasulu. 2022. "Design of IoT Based VPN Gateway for Home Network." *International Conference on Electronics and Renewable Systems (ICEARS)*: 561-564. doi: 10.1109/ICEARS53579.2022.9751838.

Ramasamy, Laksmana Kumar, and Seifedine Kadry. 2021. “Blockchain in the Industrial Internet of Things.” *Industrial and academic researchers and engineers*. doi: 10.1088/978-0-7503-3663-5ch10.

Santoso, Syarifurohmat Pratama, and et al. 2022. “Digital Espionage in New Era of Cyber: Political and International Law Perspectives.” *The 4th Open Society Conference*: 62-66.

Senthilkumar, V, and et al. 2021. "Application of AI And Computer Vision To Face Mask And Social Distance Detection in CCTV Video Streams." *International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*: 1-5. doi: 10.1109/ICAECA52838.2021.9675746.

Tripathy, Abhijid, and Vedangini Singh. 2022. “AI-powered CCTV cameras are the future of security and surveillance, How Presear Softwares deliver advanced CCTV video analytics softwares as a hybrid software package minimizing your cost.” *Zenodo Organization White Paper*. doi: 10.5281/zenodo.6570013.

Turtiainen, Hannu, and et al. 2022 “CCTV-Exposure: System for measuring user’sprivacy exposure to CCTV cameras.” *Business Modeling and Software Design: 12th International Symposium, BMSD*.

Law Product

National Security Law of the People’s Republic China 2015.

National Intelligence Law of the People's Republic China 2017.

Cybersecurity Law of the People’s Republic China 2017.

Website

Robertson, Jordan, and Michael Riley. 2018. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.” *Bloomberg*. Available at https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies#xj4y7vzkg.

Robertson, Jordan, and M. Riley. 2021. “The Long Hack: How China Exploited a U.S. Tech Supplier.” *Bloomberg*. Available at https://www.bloomberg.com/features/2021-supermicro/.

Report

Varas, Antonio, and et al. 2021. "Strengthening The Global Semiconductor Supply Chain in an Uncertain Era." *Boston Consulting Group and Semiconductor Industry Association database data*.