SINOPSIS

CHINA IN CONTEXT AND PERSPECTIVE

5G and the Internet of Things

Chinese companies' inroads into 'digital Poland'

Łukasz Sarek

31st December 2019*

Executive summary

Vulnerabilities in Internet of Things (IoT) equipment are among the main security threats associated with the 5G environment. Attacks (including by state actors) targeting IoT applications could threaten critical sectors, including power generation, healthcare, law enforcement and the military. Despite their critical nature, the potential threats posed by Chinese IoT equipment has received little attention in Europe, in contrast to the debate around Huawei's possible participation in the development of 5G networks.

This policy brief presents a preliminary case study of two key suppliers of IoT equipment, **Dahua** and **Hikvision**, focusing on their strong presence in the Polish market. Based on an analysis of Chinese and Western sources, including financial reports, analyses by think tanks and industry associations and media coverage, the following risks have been identified:

- Both Hikvision, part of a massive state-owned conglomerate that supplies the Chinese military and security apparatus, and Dahua, a key private player in the domestic security market, are especially **vulnerable to government influence**. Both companies' cooperation with repressive surveillance targeting persecuted ethnic groups in Xinjiang serves as a warning on their willingness to please the party-state. The security apparatus could exploit exploit its leverage over these companies to, e.g., use their surveillance equipment for data collection abroad.
- Chinese and Western research has identified multiple, persistent **security flaws** in Dahua and Hikvision IoT devices. While there is no evidence that backdoors in their equipment were set up intentionally or exploited by Chinese state-linked actors, the number and nature of the vulnerabilities warrants special scrutiny.
- Dahua and Hikvision have successfully **integrated into Poland's surveillance sector**, building a strong customer base that includes public administration and security forces. By melting into the local industry, the companies have managed to keep their operations in China, security risks and their dependence on the CCP away from the spotlight.

*Policy brief presented at the conference "Beyond Huawei: Europe's adoption of PRC technology and its implications", Prague, 27 November 2019.

In order to mitigate these risks, government agencies should:

1. Sponsor and coordinate research and analysis of potential threats arising from Chinese IoT manufacturers of equipment operating in the 5G network.
2. Formulate policies, including on public procurement, defining the approach to Chinese IoT equipment.
3. Build awareness across the business community on the potential threats related to the use of Chinese IoT equipment.
4. Build awareness across the business community and the public on the operations of some of the Chinese IoT providers in China and the scope of their cooperation with the Chinese government.

0 Introduction

While Huawei's participation in the development of 5G networks has been as strongly debated in Poland as in other European countries,[1] the potential threats emanating from the Internet of Things (IoT) have received little attention. Although the 5G network is definitely a key area where security must be maintained, once the network is established the secure functioning of the new ecosystem will face more threats. The IoT seems to be the most vulnerable sphere. There is, however, relatively little interest from governments, researchers and public opinion in the operations of the Chinese suppliers of equipment operating in the IoT environment, where massive data flows, impact on critical infrastructure or access to sensitive data are combined with relatively poor security measures and high risk.

In this policy brief, two Chinese companies, DH and Hikvision, have been selected as a case study, due their presence in the IoT domain in the segment of surveillance equipment in Poland. Many areas covered by IoT are vital for activities of individuals, groups and wider communities. Successfully hacked IoT devices can be exploited to retrieve valuable or even critical information and used to create widespread disruption in critical infrastructure and utilities. They can also be used in precisely targeted attacks on selected individuals or organisations that can not only be limited to the digital sphere but can also impact real world situations. In this paper, two selected companies operating in the surveillance equipment industry have been analysed in order to raise awareness of the threat coming from the Chinese companies in the IoT domain. Dahua and Hikvision have established a strong presence in the Polish market, building their customer base among not only private companies but also public institutions including public administration and various security forces. They have integrated into the local industry without the above risks receiving substantial attention.

The paper includes one section highlighting the security risks posed by IoT devices and networks in general. The following sections cover two selected companies operating in the IoT area, Hikvision in Dahua, discussing their position in the Chinese domestic market and on the global stage, controversies and risks connected to the application of equipment and solutions offered by these two manufacturers, as well as their activities in Poland. The final sections contain conclusions and recommendations. The author used various publications as sources of information, including: reports by industry organisations and think tanks, media articles and company documents, such as financial statements and announcements. This article is a preliminary overview and is aimed to encourage further research.

[1] Łukasz Sarek, "Arresting Huawei's march in Warsaw", Sinopsis, 2 February 2019.

1 The Internet of Things: Challenges to cybersecurity

The October 2019 report on the coordinated risk assessment of 5G security by EU member states recognised manufacturers of connected devices and related service providers, i.e., entities providing products or services that will connect to 5G networks (e.g. smartphones, connected vehicles, e-health), among the main stakeholders in the 5G network infrastructure. They are important "both in terms of contributing to the cybersecurity of 5G networks and as potential entry points or vectors for attacks." IoT can be exploited by criminals seeking profits or by state-backed actors. The latter are perceived to be of the highest relevance, "as they can have the motivation, intent and most importantly the capability to conduct persistent and sophisticated attacks on the security of 5G networks."[2]

A recent study highlights the challenges posed by IoT networks in 5G environments, which make the traditional approach to network security obsolete while efficient and feasible new solutions have not yet been fully developed. "With the current level of security technology, 5G data throughput would require massive server farms running intrusion scanners and packet inspectors just to keep up with the nominal state of a network. In addition, signaling for connection setup between heterogeneous connections and handover in distributed data networks will make session monitoring difficult. [...] IoT networks, for example, will require large numbers of devices to communicate with each other, likely without a central coordinator. [...] IoT use cases include things like self-driving cars, which will require methods for communicating vehicle-to-vehicle (V2V) and even vehicle-to-infrastructure (V2X)." This massive flow of data between IoT devices and legacy devices (e.g., controlling the power grid, transportation infrastructure, medical procedures) will be hard to monitor, control and secure. "[C]urrent network technology will be so busy ensuring the latency requirements for a 5G network that there will be no time or processing resources left to scan traffic for security threats."[3] This will, as a result, increase the risk of IoT devices and networks being compromised.

As noted in a 2019 report published by the Cyber Council of the US Intelligence and National Security Alliance (INSA), the development of 5G will drive innovative data-intensive applications from the broad category of IoT, "ranging from Smart Cities and autonomous vehicles to advanced medical imaging and the widespread use of virtual reality." The report lists the following examples of areas of application of IoT technology:

- "Sophisticated industrial control systems with embedded sensors for smart manufacturing, robotics control, smart power generation and optimised distribution, smart shipping and delivery systems, smart fleet and industrial maintenance systems.
- "Smart cities, including smart homes and buildings for energy efficiency, smart traffic control and public transportation systems, intelligent appliances.

[2] NIS Cooperation Group, *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9 October 2019, p. 9.

[3] Jason J. Uher, Jason R. Harper, R. G. Mennecke III, Pamela M. Patton and Sam Farroha, "Investigating end-to-end security in 5G capabilities and IoT extensions", *Proc. SPIE 9826, Cyber Sensing 2016*, (12 May 2016), reproduced in *The Next Wave* 21:4 (2017), pp. 2 f.

- "Virtual reality systems, including sophisticated entertainment and gaming, industrial simulation and training, medical treatment, first responder, police, fire, and rescue operations, and military training and operations.
- "Autonomous vehicles, including self-driving cars and trucks.
- "Drone control for safety, rescue, and surveillance operations and for automated delivery applications.
- "Smart healthcare, including advanced imaging and diagnostics, robotic surgery, genetic engineering of drugs and treatment protocols."[4]

IoT applications in these critical areas could be exploited by potential attackers, thus making IoT one of the key spheres of vulnerability within the 5G ecosystem.

2 Selected Chinese IoT manufacturers: Dahua and Hikvision

2.1 Dahua: Overview

Zhejiang Dahua Technology Co., Ltd. (浙江大华技术股份有限公司) offers a wide range of products and solutions, mainly in the area of security surveillance applied in multiple sectors: industrial settings, transportation, urban surveillance, traffic monitoring, building security but also products for video conferencing or power stations and power transmission monitoring. With 16.5bn RMB in revenue and 1.9bn RMB in net income during the first nine months of 2019[5] and 27.9bn RMB in assets, Dahua is one of the top players in China, second only to Hikvision. In 2018 Dahua had 23.6bn RMB in revenue, with almost 25.6% growth year on year.[6]

Dahua's position in global rankings has also risen in the last few years. In 2015 Dahua had a 7.50% share in the global market for digital network recorders (DVR) and network video recorders (NVR).[7] In 2017 it replaced Bosch as the second global provider of security and surveillance equipment[8] in terms of revenue. Dahua was also the leader in terms of revenue growth with over 40% yoy increase. Foreign markets are an important source of revenue for Dahua. In 2018 sales to global markets constituted 36.5% of Dahua's revenue.[9] Foreign markets were even more important in terms of revenues growth (+26.01% yoy) compared to domestic sales (+25,34% yoy) and in terms of gross income (+0.68% yoy) compared to domestic (-2.08% yoy). The company's strategy and actions clearly show that international expansion is important if not vital to its growth, while the domestic market remains a key factor making the company vulnerable to government influence.

[4] "The national security challenges of fifth generation (5G) wireless communications", INSA, June 2019, pp. 20 f.
[5] "2019 年第三季度报告", 浙江大华技术股份有限公司, October 2019, p. 3.
[6] "二〇一八年年度报告", 浙江大华技术股份有限公司, March 2019, p. 9.
[7] "中国视频监控行业发展阶段、市场份额、市场需求空间及视频监控技术的发展趋势分析", 中国产业信息, 14 February 2019.
[8] "2018 Top Security 50", Asmag.com.
[9] "二〇一八年年度报告", op. cit, p. 31.

Being one of the top global players in the security industry, Dahua is also rapidly increasing its range of products compatible with the 5G standard, e.g., network transmission.[10] The company is pushing to enter the 5G market with IoT as one of the key areas. In July, it signed an agreement on strategic partnership in 5G technology with China Mobile Zhejiang.[11] Similar agreements were concluded this year, in March with China Unicom Zhejiang on cooperation including IoT, AI, smart cities, and in September with China Telecom.[12] Dahua is also a member of the Zhejiang 5G Alliance, which includes the key domestic Chinese and foreign owned companies engaged in developing and providing 5G-related products, services, technologies and solutions.[13] In August, Dahua won the second "Bloom cup", a contest for 5G applications, with its "Smart firefighting system", part of Dahua's smart-city project.[14] Solutions and projects developed by Dahua for the domestic market are also being offered abroad.

2.2 Hikvision: Overview

Hikvision is a company effectively controlled by the Chinese government and the CCP. Hangzhou Hikvision Digital Technology Co., Ltd. (杭州海康威视数字技术股份有限公司), listed on the Shenzhen Stock Exchange, was effectively state-controlled as of the end of the third quarter of 2019. The controlling stake in Hikvision Digital Technology is in the hands of China Electronics Technology Group Co. (CETC, 中国电子科技集团公司), the direct owner of two of Hikvision's major shareholders: China Electronics Technology HIK Group Co., Ltd. (中电海康集团有限公司) with 39.10% of the company's shares and CETC's 52nd Research Institute (中国电子科技集团公司第五十二研究所) with 1.96%. Two other major shareholders include private investment funds headquartered in Xinjiang.[15] CETC is a key state owned corporation operating under the guidance of the CCP Central Committee, the State Council and the Central Military Commission.[16] It is supervised by the State Council State-owned Assets Supervision and Administration Commission (SASAC) and members of its top management are also core leaders or members of the group's party organisation.[17] The holding company has 52 direct subsidiaries and over 500 entities of different types under its umbrella. In other words, Hikvision is part of a massive state-owned conglomerate engaged in developing and manufacturing electronic equipment and providing complete solutions for the Chinese military, security apparatus, and government bodies.[18]

Hikvision is by far the largest supplier of surveillance equipment and solutions in China. In 2015 it had a nearly 20% share in the global market for DVRs and NVRs[19]

[10] "Network Transmission Products and Solutions", Dahua Technology, 2018.
[11] "大华股份与浙江移动签署 5G 战略合作协议", 大华股份, 29 July 2019.
[12] "大华股份与浙江联通签署战略合作协议", 新浪财经, 12 March 2019; "5G+ 智慧应用大华股份与浙江联通合作", 投影时代, 18 March 2019; "大华股份战略签约中国电信开启视频应用 5G 新生态", C114 通信网, 24 September 2019.
[13] 浙江省 5G 产业联盟.
[14] "大华股份荣获第二届' 绽放杯'5G 应用征集大赛一等奖", 大华股份, 19 August 2019.
[15] "2019 年第三季度报告", 杭州海康威视数字技术股份有限公司, 19 October 2019, p. 3.
[16] "集团介绍", 中国电子科技集团有限公司.
[17] " 集团领导", 中国电子科技集团有限公司.
[18] For example, several entities under CETC's umbrella are listed as key military research institutes ("国防科技重点实验室（截止 2019 年 60 家)", 科塔学术, 21 November 2019; "中国电子科技集团公司", 中国电科 via cac.gov.cn, 28 August 2014). CETC is ranked 12 in the global ranking of defense companies by Defense News ("Top 100 for 2019", Defense News).
[19] "中国视频监控行业发展阶", op. cit.

and in 2018 it was the undisputed global industry leader in terms of revenue.[20] In first three quarters of 2019 Hikvision's revenue was almost 40bn RMB, its net income exceeded 8bn RMB and its assets were worth over 68bn RMB.[21] The revenue from foreign sales and operations in 2018 amounted to 28.47% of the overall revenue. Unlike in the case of Dahua, the gross income from foreign operations decreased in 2018 by almost 4% while net income from domestic sales was up 2.83%. Revenues from foreign sales grew 15.90% and from domestic sales 20.18% while costs grew 24.79% and 14.32% respectively.[22] These figures show that, while the overseas market is important for Hikvision, the share of domestic sales is growing as company hits bumps in the US. The problems in the US market can push the company to increase its expansion in other regions and tighten cooperation with the Chinese government, Hikvision's key institutional customer.

A key area of the company's development is AI cloud, a multilayer solution that allows gathering information from myriads of local devices and processing them in cloud centres. The massive implementation of Hikvision's AI cloud requires operating in an environment based on 5G technology in order to allow its full utilisation.[23] Hikvision's CEO personally supports the development of 5G technology. Last October, he strongly advised the Henan authorities to put more focus on developing 5G technology, which will be helpful in managing the populous province.[24] In January, Hikvision signed a cooperation agreement with Hunan Empire Soft Technology (湖南软神科技股份有限公司) to develop the elder care services.[25] Empire Soft's controlling shareholder Tang Luosheng 唐罗生 is a former military researcher.[26] In June, together with China Merchants Port Group, Huawei, China Mobile and other enterprises, Hikvision signed an agreement to research, develop and implement 5G-based technologies and solutions to boost the development of the port industry in the Guangdong-Hong Kong-Macau Greater Bay Area.[27] As Hikvision [develops solutions for rail transport,[28] it has been invited to participate in related state-sponsored projects based on 5G technology. In cooperation with China Mobile and Huawei, Hikvision will work on the development of "smart railway stations" in selected locations.[29] Hikvision is also a member of the "CMMC Railway Internet of Intelligences [sic] Alliance" (中国移动轨道交通智联网联盟), established under the leadership of China Mobile and including universities, several subsidiaries of China Railway, Huawei, ZTE, Nokia, IBM and other companies.[30] In October, the company was invited to participate in the Qingdao 5G city project.[31] These are only some examples of Hikvision's engagement in the development of China's 5G environment. They show that, being a state-controlled entity, Hikvision is engaged in state-sponsored projects and that it cooperates with other

[20] "2018 Top Security 50", op. cit.
[21] "2019 年第三季度报", 杭州海康威视数字技术股份有限公司, p. 3.
[22] "2018 年度报告", 杭州海康威视数字技术股份有限公司, 30 April 2019, pp. 43 f.
[23] "5G 时代来临海康威视'AI+ 安防、警务、交通' 三架齐驱", 安防知识网 via 亿欧, 13 February 2012.
[24] 孙静, "访海康威视董事长陈宗年：河南在 5G 时代机遇无限", 河南日报网, 20 October 2018.
[25] "软神股份与海康威视签订战略合作协议，强强联手共同推进 5G 时代的智慧养老服务", 湖南软神科技股份有限公司, 8 January 2019.
[26] "唐罗生个人简介", 前瞻网.
[27] "粤港澳大湾区首个 5G 智慧港口启动建设", gov.cn, 25 June 2019.
[28] "高清视频监控系统在铁路的应用", Hikvision.
[29] "中国移动携手中国铁路北京局、华为、海康威视等发布 5G 智慧车站", 安防知识网, 14 March 2019.
[30] "5G 赋能智慧轨交，中国移动轨道交通智联网联盟正式宣布成立", 消费日报网 via *China Daily*, 28 May 2019.
[31] "5G+ 工业互联网：青岛 5G' 主菜单'", 中共中央网络安全和信息化委员会办公室、中华人民共和国国家互联网信息办公室, 24 October 2019.

SOEs as part of China's state-owned ecosystem. Engaging in such diversified projects can also strengthen Hikvision's capabilities and the range of products and solutions that will be marketed overseas and, as a result, accelerate the company's expansion abroad.

3 Controversies surrounding Chinese manufacturers

3.1 The party-state's sway over business

While Hikvision is a state-owned and party-controlled company, which can be directly used as a tool of state policy, Dahua is formally a private company. In China, a company's private status does not shield it from the direct influence of party-state organs. The Huawei conundrum has already sparked a vivid debate concerning the ways the CCP and the Chinese state and can influence the actions of every company, including private ones:

a) the set of laws obliging companies to cooperate with the state security apparatus both in China and abroad, including the national security law cyber security law, counter terrorism law, and the intelligence law;

b) while laws are a convenient tool for the CCP to make companies obey its will, a more direct and efficient way is to use the company party organisations to influence the decisions and actions on various levels of management, in larger companies the establishment of party organisations is obligatory and its representatives have secured seats in the company's leading organs;

c) administrative tools that can be used to exert pressure, such as controls from various government agencies: tax office, labour bureau, environmental protection agencies, refusing or delaying administrative decisions to grant licences or in any other way limiting or depriving access to specific markets or resources;

d) using personal leverage on the key decision makers, e.g., the threat of being arrested and persecuted under real or false accusations.

The surveillance equipment industry operates in a business environment that is heavily affected by these factors.[32] Another important factor should be added: the importance of state as a buyer of products and services. The largest orders come from the public sector and the largest companies need state orders to grow. That creates leverage.

The risk of Chinese companies acting as a tool of the Chinese secret services and as political and economic tools of the CCP, combined with the risk of vulnerabilities and technical flaws led to special provisions in the John S. McCain National Defense Authorization Act for the Fiscal Year 2019, passed in August 2018.[33] The bill prohibits US

[32] "Regulatory framework, Surveillance industry in China, Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", Office of the United Nations High Commissioner for Human Rights (OHCHR), 15 February 2019; Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party", *Foreign Policy,* 7 February 2019; Sijia Jiang, Anne Marie Roantre, "Tencent shares hit by profit drop, freeze on new game approvals in China", Reuters, 16 August 2018; Josh Horwitz, "China to send state officials to 100 private firms including Alibaba", Reuters, 23 September 2019; Martin Hála, Jichang Lulu, "Huawei's Christmas battle for Central Europe", Sinopsis, 28 December 2018; Filip Jirouš, Jichang Lulu, "Huawei in CEE: From 'strategic partner' to potential threat", Sinopsis, 17 May 2019.

[33] "John S. McCain National Defense Authorization Act for Fiscal Year 2019", US Congress, enacted after being signed by the President on 13 August 2018.

government agencies from purchasing and using surveillance equipment from Hytera Communications, Dahua and Hikvision, as well as telecommunications equipment provided by ZTE and Huawei. However, as the US government has procured security equipment from Chinese suppliers for years, it is difficult to remove it quickly. As a result, in spite of security concerns, thousands of Dahua and Hikvision products are present in US government security systems.[34] It should be noted that the US security industry has become highly dependent on Chinese suppliers and there are strong voices against the ban citing commercial and security reasons.[35] The commercial impact may be limited in the short term but can become more painful in the longer term if US private businesses follow the government's lead and switch to equipment from other suppliers.[36] The US example has not been replicated in other countries. With all eyes focused on Huawei's participation in the establishment of 5G networks, the potential threat coming from the multiple Chinese companies engaged in the IoT domain has been almost neglected in the public discourse on security in much of Europe.

3.2 Equipment security flaws

Chinese companies are providers of devices, software, components and complete solutions for the Internet of Things. The key issue is that their dependence on the Chinese party-state makes them a convenient tool for the security apparatus, which can exploit the opportunities arising from its influence over IoT suppliers. And firmware vulnerabilities matter.[37] A convenient way to gain access to devices in order to either interrupt their operation or to use them for retrieving information is to implant backdoors or other vulnerabilities in the firmware, developed, maintained, upgraded and updated by the manufacturer or a third party authorised by it. As Hikvision is a state-owned company and both companies are under Chinese jurisdiction, they could be pressured by state organs, including the secret service, into modifying software so that it could be used to obtain information and transfer it to China.

In March 2017 a backdoor was detected in Dahua equipment.[38] The backdoor allowed logging in remotely to Dahua devices, ignoring passwords and other login credentials set up by the user. Dahua identified nearly a dozen of its products vulnerable to the backdoor and released software updates. The backdoors in Dahua equipment were also detected and researched by a later study by ReFirm Labs.[39] They allowed unauthorised users to perform arbitrary firmware updates and install persistent backdoors. In response, in March[40] and November 2018[41] Dahua released white papers on IoT threats and measures it implements to mitigate them. However, since May 2019 further vulnerabilities have been detected in Dahua cameras, which allow unauthorised

[34] Thomas Brewster, "Thousands Of Banned Chinese Surveillance Cameras Are Watching Over America", *Forbes*, August 2019.

[35] Shawna Chen, "U.S. surveillance industry fears crippling effect of Chinese tech ban", Politico, 8 August 2019

[36] "China Surveillance Giant Expects Client Losses From U.S. Ban", Bloomberg, 19 October 2019.

[37] "Connected IoT Device Security — Why Firmware Vulnerabilities Matter", ReFirm Labs, April 2019.

[38] Bashis, "0-Day: Dahua backdoor Generation 2 and 3", Seclists, 6 March 2017.

[39] "Dahua, Hikvision IoT Devices Under Siege", Krebs on Security, 10 March 2017.

[40] "Security of the Internet of Things. Dahua, Technical White Paper", Dahua, document dated 2017, with version number indicating release in January 2018, uploaded on 6 March 2018.

[41] "Product Security Hardening Guide", Dahua, dated 2017, uploaded on 20 November 2018.

wiretapping. These were first discovered by Tenable,[42] followed by further research by IPVM.[43] Dahua knew about the vulnerability before May 2018.[44] It was fixed in later firmware versions, but the company had not disclosed the security flaws before they were discovered and reported by external experts. ReFirm Labs discovered that the same backdoor account was located in a different section of the firmware image after the software update.[45]

Warnings on Hikvision firmware allowing unauthorised remote access to data have appeared from time to time.[46] The list of past major issues with Hikvision firmware is quite long.[47] In April 2017, the Cybersecurity and Infrastructure Security Agency (CISA) under the US Department of Homeland Security released a statement on a backdoor in Hikvision equipment.[48] It was the result of the discovery by a cybersecurity expert of massive vulnerabilities,[49] then followed by Hikvision statements and security patches.

Chinese cybersecurity companies also consider IoT as a particularly vulnerable target. According to research by Beijing Huashun (北京华顺信安科技有限公司), for security and surveillance cameras the number of vulnerabilities in 2017 and 2018 was significant, with Foscam the top culprit in 2017 (52 cases) followed by US-based Pelco (13), Dahua (11) and Hikvision (7). However, Pelco is heavily dependent on Chinese manufacturers, meaning that the vulnerabilities in fact add, to some extent, to the Chinese manufacturers' count. In 2018 new Chinese manufacturers broke into the ranking. Hikvision and Dahua are also ranked as leaders in terms of devices with vulnerabilities (8.3 and 4.3 million devices respectively).[50] An earlier study by Chinese researchers also indicates that Hikvision and Dahua take the lead in terms of the number of vulnerable devices, respectively with 841,000 and 147,000.[51]

[42] Jacob Baines, "CVE-2019-3948: Unauthenticated Remote Audio Streaming Over HTTP", Tenable, 29 July 2019.

[43] John Honovich, John Scanlan, "Dahua Wiretapping Vulnerability", IPVM, 2 August 2019.

[44] "Security Advisory - VideoTalk function of some Dahua products have security risks", Dahua, 2 August 2019.

[45] Sydney J Freedberg Jr., "Hacker Heaven: Huawei's Hidden Back Doors Found", Breaking Defense, 5 July 2019; "IP Surveillance Cameras and Firmware Security", ReFirm Labs, 23 May 2019.

[46] Xiao Yu. "Is the World's Biggest Surveillance Camera Maker Sending Footage to China?", Voice of America, 21 November 2016; Johannes B. Ullrich, "More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!)", Forum of Sans Technology Institute, 31 March 2014.

[47] Brian Karas, "Hikvision Backdoor Confirmed", IPVM, 8 May 2017.

[48] "ICS Advisory (ICSA-17-124-01). Hikvision Cameras", CISA, 4 May 2017.

[49] Monte Crypto, "Access control bypass in Hikvision IP Cameras", Seclists, 12 September 2017.

[50] "网络空间测绘系列 2018 年摄像头安全报告", 北京华顺信安科技有限公司, 2018, pp. 28-34. In terms of sheer number of vulnerable devices, Taiwan-headquartered D-Link was third with 3.6 million devices. While Chinese researchers put foreign companies near the top of the ranking in terms of vulnerabilities discovered between 2013 and 2018 (with Pelco second with 37 vulnerabilities and Samsung fourth with 27, and the Chinese Foscam first with 65), the number of affected devices in Samsung's case (350,000) is an order of magnitude smaller than Dahua and Hikvision. Pelco, with merely 527 devices with vulnerabilities discovered, hardly counts. It should be noted, however, that according to this report in 2018 Dahua, Hikvision and Foscam recorded a much lower number of vulnerabilities discovered compared to new Chinese companies in the ranking.

[51] "国内物联网资产的暴露情况分析", 北京神州绿盟信息安全科技股份有限公司, March 2017. The much lower number of vulnerable devices than in previous research is due to a different methodology, with research limited to China only. The third, Q-See, had 123,000 vulnerable devices.

3.3 Cooperation with the government and security apparatus in Xinjiang

In October 2019, both companies were added to the US entity list,[52] together with other Chinese tech companies,[53] as acting contrary to the foreign policy interests of the United States. This means that US companies need special approval and a licence to provide companies on the list with restricted components and technology. The reason for this decision was Dahua and Hikvision's role as suppliers of surveillance equipment to the Chinese security apparatus in Xinjiang since 2016. Both companies participated in numerous projects there as government contractors and have cooperated with the establishment of the system of repressive surveillance targeting the persecuted Uyghur minority.[54] There is an extensive bibliography of Western media and academic reports on Xinjiang-related issues including articles on Dahua and Hikvision's activities in Xinjiang.[55] Hikvision's contracts for security projects in Xinjiang have included a mass facial recognition system in Pishan 皮山 county that featured a "surveillance system" for a reeducation camp, as well as a system in Moyu 墨玉 county with 35,000 surveillance cameras to monitor schools, mosques, reeducation camps and other areas. The company has also offered facial-recognition cameras able to distinguish Uyghurs from Han.[56] Dahua Technology also eagerly participated in tenders for the delivery of surveillance equipment and the installation of whole surveillance systems. One of the projects Dahua bid to undertake was the safe city of Yarkand.[57] Others include the Chira (Qira) safe city and Hotan security checkpoints.[58]

4 Dahua and Hikvision in Poland

As elsewhere in Europe, there has been next to no scrutiny of Chinese IoT suppliers in Poland, contrasting with the many voices in the US calling for a stricter approach. This contrasts with multiple calls for increased scrutiny of Huawei's participation in 5G projects. Companies such as Hikvision and Dahua are expanding their customer base and establishing contacts with military and security forces. They are also dynamically entering new market segments, such as transportation, power networks and smart-city infrastructure. They melt into the industry, branding themselves as an advanced technology suppliers while successfully keeping their operations in China, security risks and their dependence on the CCP away from the spotlight.

[52] "Addition of Certain Entities to the Entity List", US Bureau of Industry and Security, Commerce (10 September 2019)

[53] Mo Yelin, "Chinese Companies Protest Inclusion in U.S. Export Blacklist", Caixin 8 "October 2019)

[54] Charles Rollet, "Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang", IPVM, 23 April 2018.

[55] Magnus Fiskesjö, "China's 're-education' / concentration camps in Xinjiang/ East Turkestan and the wider campaign of forced assimilation targeting Uyghurs, Kazakhs, etc.", Uyghur Human Rights Project, last updated 15 December 2019.

[56] Charles Rollet, "Evidence Of Hikvision's Involvement With Xinjiang IJOP And Re-Education Camps", IPVM, 2 October 2018; idem, "Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up", IPVM, 11 November 2019; Ondřej Klimeš, "The Xinjiangisation of the whole country: Technological authoritarianism in China and abroad", presentation at the conference "Beyond Huawei: Europe's adoption of PRC technology and its implications", Sinopsis, 4 December 2019.

[57] "新疆需大量监控设备供应商获巨资合同", RFI, 6 July 2018.

[58] "新疆安防市场爆发，业绩拐点已现", 国金正卷, 12 March 2018.

4.1 Dahua

Dahua is making significant inroads in Poland, where it operates through the subsidiary Dahua Technology Poland Sp. z o.o.[59] The Polish company's chairman and only board member is Fu Liquan 傅利泉, also the parent company's chairman and main shareholder. The Polish company is controlled by Dahua Technology through Dahua Europe BV.[60] The Polish subsidiary has gained prominence and serves as the regional headquarters for Central and Eastern Europe and the Nordics, organising, e.g., meetings of country managers for those regions.[61] It has also become the regional centre for technical support.[62] In Poland, Dahua operates through a network of partners and distributors. It implements a dynamic and professional marketing policy with the use of social media, touring its partners while organising promotional meetings for customers within the framework of its "Starlight Show" events. The company organises customer trips to China, including to its main headquarters.[63] Dahua has expanded in Poland relatively quickly, establishing a network of partners who distribute its products to businesses and individual customers. Its marketing efforts create a positive brand image as a customer-oriented company providing advanced security, mainly surveillance solutions, without referring to its cooperation with the Chinese government or mentioning projects implemented for the Chinese state.

Dahua is also making efforts to integrate into the Polish security service industry and to establish solid contacts with competitors, industry experts and large institutional customers including state agencies. The company has recently launched trainings in AI face-recognition applications.[64] It is also trying to establish ties with Polish prison authorities. In April, a Dahua representative was one of the few invited speakers at the First National Fair and Conference of the Prison Service Lublin 2019.[65] The conference and exhibition was organised under the auspices of the Ministry of Justice. At the 2019 Eastern Conference and Border Protection Fair, Dahua presented a system for border protection and surveillance implemented at a Serbia-Hungary border checkpoint.[66] Dahua was one of the sponsors and gained Gold Partner status at the 20th Security Industry Conference: Security of the Future.[67] The conference is organised by the Polish Chamber of Security (Polska Izba Ochrony), the leading Polish association of companies engaged in the security industry in the broad sense, with 183 members.[68] A Dahua representative was a speaker at the 3rd International Conference Warsaw Security Summit.[69]

[59] Dahua Technology Poland.
[60] "Zhejiang Dahua Technology 2018 Annual Report", March 2019.
[61] "Półroczne spotkanie Country Managerów z regionu CEE & Nordic", Dahua Technology Poland Facebook profile, 27 August 2019.
[62] "Rozszerzenie działania platformy wsparcia technicznego Dahua Technology Poland na cały region CEE&Nordic", Dahua Technology Poland Facebook profile, 24 June 2019.
[63] "Dahua Technology Poland Ticket to China 3", Dahua Technology Poland Facebook profile-
[64] "Cykl szkoleń poświęconych AI organizowany z partnerem Dahua Spółką Alpo", Dahua Technology Poland Facebook profile, 29 October 2019.
[65] "Program Konferencji" , Ogólnokrajowe Targi I Konferencja Służby Więziennej Lublin 2019.)
[66] "Dahua Technology Poland na Wschodniej Konferencji i Targach Ochrony Granic". Exhibition website.
[67] "Nasi partnerzy", XX Konferencja Branży Ochrony: Bezpieczeństwo Przyszłości.
[68] "Firmy członkowskie", Polska Izba Ochrony.
[69] "Maciej Pietrzak", "Agenda", Warsaw Security Summit.

4.2 Hikvision

Hikvision operates in Poland through its subsidiary Hikvision Poland Sp. z.o.o.[70] Similarly to Dahua, it has a network of partners. While its main group of customers consists of providers of security solutions, Hikvision also seeks contacts with large institutional customers, including various Polish security forces. It is finding ways to establish contact channels with the military, security forces and operators of critical infrastructure. A Hikvision representative was also a speaker at the 3rd Warsaw Security Summit.[71] In September 2019, Hikvision was one of the partners of the Securitech & Defense 2019 exhibition, held at the Polish Air Force Academy. Members of the conference board, speakers and guests included high-ranked officers of the military and security forces as well as security experts.[72] In June 2019, a Hikvision representative was a speaker on the panel on the modernization of border guards and internal security forces held during the Border Protection and Home Security Exhibition and Conference, as the only industry representative.[73] He presented the company's solutions for Polish police, border guards and prison service. Railway security is another segment Hikvision is targeting in Poland.[74]

The integration into the Polish security industry and participation in various events is an important part of marketing efforts. In October 2019, Hikvision was a partner of the Integrated Systems Firefighting Security conference.[75] In April, Hikvision had become a member of the Polish Chamber of Alarm Systems.[76] In 2018 the company won 8 medals at the Securex exhibition, more than any other exhibitor.[77] Facial-recognition technologies that Hikvision develops in China are also being offered in Poland. Complete facial-recognition and monitoring solutions were presented at Securex 2018.[78] In March 2018 Hikvision was one of the partners of a conference devoted to the impact of the IoT on the security industry.[79] Hikvision's efforts have helped it to win customers in the public sector. Their products are applied in security systems in the port of Gdynia[80], in road infrastructure operated by the General Directorate for National Roads and Motorways,[81] the Warsaw district court[82] and Inowrocław-Latkowo military airport.[83] Moreover, organisers of public tenders often request bidders to provide equipment from specified suppliers; Hikvision is listed as one of the

[70] "Kontakt", Hikvision Poland; "Hikvision Poland sp z o o (KRS: 0000512864, NIP: 7010426661, REGON: 147265204)", KRS-online.com.pl.

[71] "Łukasz Lik", Warsaw Security Summit; "Agenda", op. cit.

[72] "Securitech & Defense 2019".

[73] "Międzynarodowa Wystawa i Konferencja Bezpieczeństwa Granic I Bezpieczeństwa Wewnętrznego Insec 2019", Insec 2019, 12 June 2019.

[74] "Trwa Konferencja Bezpieczeństwo na kolei", *Raport Kolejowy*, 12 October 2018.

[75] "VIII edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet Partnerzy", Schrack-Seconet.

[76] "HIKVISION POLAND nowym członkiem PISA", Polska Izba Systemów Alarmowych, 15 April 2019.

[77] "Laureaci Złotego Medalu Targów Securex 2018", Securex.

[78] "Międzynarodowe Targi SECUREX w Poznaniu czyli święto zaawansowanej technologii w sektorze bezpieczeństwa", Infosecurity24.pl, 25 April 2018.

[79] "Ogólnopolska Konferencja EBS Wpływ IoT na branżę zabezpieczeń", 8 March 2018; "Wpływ IoT na branżę zabezpieczeń – zapraszamy na konferencję", *Zabezpieczenia*, 16 February 2018.

[80] "Projekt koncepcyjny integracji elektronicznych systemów zabezpieczeń budynków i terenów Zarządu Morskiego Portu Gdynia S.A.", Port Gdynia, November 2017.

[81] "Dostawa zewnętrznych kamer obrotowych do monitorowania ruchu drogowego dla GDDKiA Oddział w Łodzi", GDDKiA w Łodzi, 17 November 2017.

[82] "Przetarg nieograniczony na usługę konserwacji systemów bezpieczeństwa dla potrzeb Sądu Okręgowego w Warszawie", Sąd Okręgowy w Warszawie, February-March 2019.

[83] "Informacja dotycząca postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu ograniczonego w dziedzinie obronności i bezpieczeństwa na uslugi polegające na okresowych

approved manufacturers or sole approved manufacturer for, e.g., monitoring in areas of Cracow,[84] the marshal's office in Podlaskie voivodeship[85] and the country's General Police Headquarters.[86] These are only a few examples of Hikvision's reach in Poland.

5 Conclusion

There is no evidence that the backdoors described in this article were set up intentionally, although some cybersecurity researchers note that the nature of the vulnerabilities and their persistence indicates they were. There is also no proof that they were exploited by Chinese state actors, or that the companies mentioned cooperate with Chinese security services to implement software modifications to enable collecting data from security surveillance systems. Companies from other countries also have a record of security flaws in IoT devices. There are, however, significant differences that lead to a need to scrutinise both companies and other Chinese manufacturers. The number and nature of the vulnerabilities and their presence in a large number of devices due to their market share should be a warning against blindly increasing the volume and range of application of equipment from both manufacturers.

Chinese companies operate in an environment where the will of the CCP prevails over the law and business interests. Even the law requires companies to cooperate with the security apparatus, both in China and abroad. Chinese companies are also highly dependent on the domestic market and state orders to survive and grow, which equips the Chinese authorities with strong leverage. The case of Xinjiang should be a warning on how far Chinese manufacturers are willing to go to please the CCP and earn their profits.

Considering these factors, the scrutiny of these and other companies should not be limited to their past deeds, but should also take into account the business environment in which they operate and the nature of the Chinese state, which can have a considerable direct or indirect impact on a company's actions, be it state-owned or private.

5G infrastructure, which will allow much faster and bigger data flows, poses increased risks arising from IoT equipment and solutions, is combined with increased difficulties in network maintenance and data security. Therefore, the approach to companies such as Hikvision and Dahua should be proactive, not reactive, focused on possible future risks. The example of US government, which is facing difficulties removing equipment from these companies due to the high number of installed devices and the US security sector's dependence on Chinese manufacturers, should serve as a warning to the Polish and other European authorities.

konserwacjach i doraźnych naprawach systemów alarmowych, system", Ministerstwo Obrony Narodowej, 4 September 2019.

[84] "Przetarg nieograniczony. Znak sprawy: 12/X/2018", Zarząd Infrastruktury Komunalnej i Transportu w Krakowie, 17 October 2018.

[85] "Zapytanie ofertowe na remont instalacji telewizji przemysłowej w zakresie systemu kamer zewnętrznych w siedzibie UMWP przy ul. Poleskiej 89 w Białymstoku", Wrota Podlasia, 20 November 2017.

[86] "Komenda Główna Policji: Rozbudowa Systemów Zabezpieczeń Technicznych w obiektach Komendy Głównej Policji w Warszawie. Ogłoszenie o zamówieniu- Roboty budowlane", e-gospodarka.pl, 27 August 2019.

6 Policy recommendations

In order to mitigate risks posed by Chinese IoT suppliers, government agencies should take steps including:

1. Sponsoring and coordinating research and analysis of potential threats arising from Chinese IoT manufacturers of equipment operating in the 5G network. Such research and analysis should be included in a general report as well as industry-specific reports devoted to key product segments. These reports should consider not only technical aspects but also political and economic ones, focusing on Chinese state's policies and their influence on the companies' operations.
2. Formulating policies, including on public procurement, based on these reports, in order to define the approach to Chinese equipment. This approach should cover products provided by Chinese suppliers, either directly or as original equipment manufacturers (OEM) for other vendors. These policies should include defining the approved scope of application of equipment and solutions made in China, especially in critical infrastructure, public services and areas covering sensitive data of local companies and citizens.
3. Building awareness across the business community on the potential threats related to the use of Chinese IoT equipment, encouraging businesses to adopt a cautious approach and take precautionary steps.
4. Building awareness across the business community and the wider public on the operations of some of the Chinese IoT providers in China and the scope of their cooperation with the Chinese government, especially in areas where human and civil rights abuses occur.

Acknowledgements

The author would like to acknowledge Jichang Lulu's help and contribution to this text.

Łukasz Sarek *is a researcher and China market analyst. He writes about China-Europe economic relations with focus on Poland and CEE.*

Sinopsis *is a collaborative project between the Institute of East Asian Studies at Charles University in Prague and the non-profit AcaMedia Institute. The conference "Beyond Huawei: Europe's adoption of PRC technology and its implications", organised by Sinopsis, was held on 27 November 2019 at the Czech Academy of Sciences.*