SECURITY RELATIONS BETWEEN SERBIA AND CHINA – CHALLENGES OR BENEFITS?

Written by: CEAS research team

It is impossible to mention the security aspect of China's influence without reference to the Chinese technology company Huawei. Huawei is the world's second largest manufacturer of smartphones, having recently displaced Apple from second place, and the Chinese company sells over 10% of all smartphones on the world market.[1] However, significant restrictions have recently been imposed on sales of these devices in the USA on account of the suspected involvement of the Chinese state in the management of this company, as well as links with the Chinese Army. At the beginning of 2018, Verizon and AT&T (the largest mobile operators in the USA) refused to include Huawei devices in their supply in the USA citing security concerns. In February 2018 the three major US intelligence agencies warned US citizens against using Huawei devices, and several months later President Trump signed the Defense Authorization Act, which forbids US Administration staff and contractors to use Huawei devices.[2]

In October 2016, the companies Telekom Serbia and Huawei signed a multiannual contract for the procurement of equipment, services and works to modernize the fixed network of Telekom Srbija. Under this contract Telekom Srbija shall invest up to US $ 166 million in order to improve through cooperation with Huawei Company the fixed internet and multimedia.[3]This agreement was reached following China's President Xi Jinping's visit to Serbia in March 2016.

In July 2018, the British Government published a report criticizing the security protocols of Huawei phones, and recently Australia also prohibited Huawei and ZTE, the second Chinese manufacturer of smartphones, to provide technology for its 5G network. Huawei has regular contracts with the Chinese Army for the development of dual use communication technologies. Since January 2018, Huawei has been actively involved in the 863 Program financing (Program 863 was initiated in 1986 with the objective of improving the Chinese Army's (PLA) technological capacity by using and financing private companies to develop technologies with commercial and military applications) assisting the development of 5G networks with a view to use in military applications.

Some cybersecurity and international security experts believe that the possibility of China mounting cyber-attacks via consumer technical devices is a genuine threat. Indicatively enough, the Chinese authorities are authorized to demand that technological companies, such as Huawei, hand over all and any useful information or to provide access to communications and technologies owned or sold by the company. The Chinese authorities may use such information and access to facilitate espionage or cyber-attacks employing Huawei

[1] Is Huawei a Genuine Security Threat? TechCo. September 2018. Available at: https://tech.co/huawei-genuine-securitythreat-2018-09
[2] Huawei Technologies v. U.S.: Summary and Context. Lawfare. April 2019. Available at: https://www.lawfareblog.com/ huawei-technologies-v-us-summary-and-context
[3] Telekom Srbija and Huawei presented ALL-IP transformation package. MTS. October 2016. Available at: https://www. mts.rs/ otelekomu/vesti/1767/telekom-srbija-i-huawei-predstavili-projekat

communication technologies or networks. Consumer technical devices like telephones supported by Huawei technologies (or the technologies of other Chinese technology companies) are easier for the Chinese authorities to penetrate and exploit, for precisely the aforementioned reasons.

Chinese law requires the establishment of committees comprised of members of the Communist Party in all Chinese companies. According to the US Select Committee on Intelligence, these committees are vehicles for the Party by means of which to exert influence and pressure on the companies and monitor their work. US Congress Permanent Select Committee on Intelligence issued a report back in 2012 stating that precisely these committees were the vehicles by which the Party exerted influence and pressure on companies and placed them under surveillance.[4]

How high a threat to state security can the procurement and use of Chinese technologies pose is not something that can be seen in Serbia's media, nor do Serbia's officials speak about it at all, as attested to, among other, by the fact that the Ministry of the Interior of the Republic of has purchased and is using Huawei technology.

On 25th July, 2014, an accident happened on Belgrade's Brankov Bridge when a young man was killed. The hit-and-run driver escaped, even though the police was on his trail. The following month the Serbian police found out that the suspect had fled to a town in China and sent his photograph to Chinese authorities. Only three days later, Chinese police arrested the man aided by cutting-edge technology. This impressed Serbian officials who, unlike their Chinese counterparts, were still using analog surveillance equipment and facilities with limited technical capabilities.

The Chinese company claims that the project „Safe City" will shorten the time of police investigations, improve arrest rates, prevent organized crime and decrease the overall crime rate. On Huawei company's official website „Safe City" is described as a project which will contribute to heightened security during various events like sports matches, that already in its first stage it has helped solve criminal cases and that it will generally upgrade the technology used by Serbia's Ministry of the Interior.[5]

Towards the end of January 2019, the Minister of the Interior of the Republic of Serbia Nebojša Stefanović announced that in order to improve the safety of citizens and combat crime, over the next two years a Huawei surveillance system would be deployed at 800 points throughout the capital of Serbia involving the installation of 1,000 high-definition cameras using facial and license plate recognition software, as well as that this is part of the strategic „Safe City" project.[6] The first agreement on cooperation between the Ministry of the Interior of the Republic of Serbia and the Huawei Company was signed already in 2014. The next important strategic agreement with Huawei was signed in February 2017 when the introduction of eLTE technology was agreed in order to improve public safety and upgrade data exchange with a

[4] Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence. U.S. House of Representatives 112th Congress. October 2012. Available at: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

[5] Big Brother Comes to Belgrade. Foreign Policy. June 2019. Available at: https://foreignpolicy.com/2019/06/18/bigbrother-comes-to-belgrade-huawei-china-facial-recognition-vucic/

[6] Can China become Serbia's „Big Brother"? BFPE. Author: Stefan Vladisavljev. February 2019. Available at: https://bfpe.org/da-li-kina-moze-postati-veliki-brat-srbije/

view to the improved safety of the citizens.[7] The Ministry of the Interior then issued a communiqué stressing that members of the Ministry of the Interior would be able to exchange more information and video content through the eLTE network as well as to use them for upgrading the flow of information required for their everyday work.

In March 2019, the Belgrade based SHARE Foundation filed a request with the Ministry of the Interior for access to information of public importance asking for information on the locations of stationary cameras, including the analysis based on which these locations were chosen, and for details on the public procurement and relevant procedures. The Ministry declined SHARE Foundation's request explaining that all documents concerning the public procurement of the video surveillance equipment in Belgrade were protected, being marked as "confidential".[8]

In 2018, the Law on Personal Data Protection went into effect in Serbia which largely adopted the new standards of European Regulations in this area (primarily the EU General Data Protection Regulation GDPR), while some civil society organizations as well as the Office of the Commissioner for Information of Public Importance and Personal Data Protection warned that the Law failed to specifically provide for a number of instruments to ensure the implementation of the Law. It should be stressed that up to now the Republic of Serbia has not taken any steps towards drafting a law to regulate video surveillance in public spaces in order to avoid potential abuses of facial identification software, which can create leeway for abusing citizens' personal data.

As Huawei has in recent years been accused by some states, like the USA, Great Britain and Australia, of industrial and political espionage in cooperation with the Chinese authorities, public procurement procedures for such software and its use should be attended by a democratic public discussion and, among other, a detailed data protection impact assessment of these technologies undertaken.

On the other hand, the Kingdom of Norway is supporting Serbia in the field of digitization, personal data protection as well as protection against cyber-attacks. Norwegian Minister of Foreign Affairs, Ine Eriksen Søreide, on her visit to Belgrade at the end of June 2019, stressed that Norway was determined to continue to support Serbia in the area of digitization, but that, however, enhanced efficiency also entailed vulnerabilities, as well as that it was important to protect personal data but also against cyber-attacks. She added that Norway would continue to help Serbia in establishing a better data security system before the funding of expensive equipment was secured.[9]

Norway is facing a tough political decision on who should be allowed to build out its next-generation telecommunications network amid a push by the U.S to shut out China's Huawei Technologies Co. Norwegian Digitization Minister Nikolai Astrup stated in March 2019 that this decision was not „black and white". Norway is looking over the compliance with its security laws ahead of a pending tender where suppliers such as Ericsson AB and Huawei are set to compete in the roll-out of the 5G networks. Norway's Telenor ASA has used Huawei

[7] Cooperation with "Huawei" to improve the safety of citizens. RTS. February 2017. Available at: http://www.rts.rs/ page/ stories/sr/story/125/drustvo/2617784/saradnja-sa-kompanijom-huavej-u-cilju-vece-bezbednosti-gradjana.html

[8] Are the locations of the new surveillance cameras and the risks to the constitutional rights of citizens known? SHARE Foundation. March 2019. Available at: https://www.sharefoundation.info/sr/da-li-su-poznate-lokacije-novih-kamera-zanadzor-i-rizici-po-ustavna- prava-gradjana/

[9] Status quo slowing both Serbia and Kosovo down. Politika. June2019. Available at: http://www.politika.rs/sr/ clanak/432426/Statuskvo-usporava-i-Srbiju-i-Kosovo

technology in its 4G network, and so far, according to Norwegian officials, there are no indications of any security issues with the network.[10]

In Serbia the restrictions that the company Google imposed on the company Huawei were very calmly received. After in May 2019 the US Company Google announced that it was banning the company Huawei from access to Google services, Tatjana Matić, State Secretary in the Ministry of Telecommunications stated that „The conflict between Google and Huawei will not be reflected on the cooperation the Government of Serbia has with this Chinese IT giant nor on its long-term cooperation within the "Belt and Road" process.[11]

Activities concerning the application of Chinese telecommunication technology and software in defense and security systems are potentially more dangerous trends. The Republic of Serbia must be wary lest it compromise its security system with Chinese equipment and software and thus jeopardize the attained level of protection of individual civil rights without a broad consensus on its necessity and preclude further EU integration, first and foremost.

In the area of data exchange and protection, the EU is much more integrated with NATO and the U.S, which fact also Serbia must already now take into account, balancing its expectations regarding support in the negotiations on Kosovo as well. Bearing also in mind all the global challenges around the use of China's G5 technology, this is by no means an easy task for a small and militarily neutral country.

[10] Norway Mulls Huawei 5G Decision That's Not 'Black and White'. Bloomberg. March 2019. Available at: https://www.bloomberg.com/news/articles/2019-03-25/norway-mulls-huawei-5g-decision-that-s-not-black-and-white

[11] Matić: Serbia continues and advances cooperation with Huawei. N1. May 2019. Available at: http://rs.n1info.com/ Biznis/a485621/Matic-Srbija-nastavlja-i-dodatno-unapredjuje-saradnju-sa-Huavejom.html