RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

CHINA - THE WEST'S PRIME CYBER THREAT

GVANTSA CHACHANIDZE

174

EXPERT OPINION

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

GVANTSA CHACHANIDZE

CHINA - THE WEST'S PRIME CYBER THREAT

174

2021

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN

Cybersecurity has become a crucial part of national and international security. Georgian society is familiar with Russian cyber activities, tactics and targets. In 2008, Russian intelligence services attacked more than 50 websites related to Georgia's military, government, finance and communication. Interestingly, this was the first case in history when attacks were coordinated in both cyberspace and warfighting (land, air, sea) domains (Hollis 2011, 2). In addition to cyberattacks, Russian disinformation is jeopardizing Georgia's national security as it aims to radicalize and polarize society, and devalue Western and democratic principles.

European states realized the importance of cybersecurity in 2007 when Russia attacked Estonia's cyberspace. The series of cyberattacks lasted for several days. They were targeting websites of Estonia's key institutions including the parliament, ministries, banks, media and hospitals (Tamkin 2017). Previously, cyberattacks would only target specific organizations. This case made it clear that cyberwarfare is a very dangerous game which cannot only cause financial damage but paralyze the whole country.

In the cyber era, states are becoming increasingly digitalized, they rely on e-services, social media, data storage and e-commerce. As more people and services go online, hostile actors have exponentially more entry points for attacks, data to steal or distort and systems to breach and paralyze.

We should keep in mind that cybersecurity is not purely IT. It is a crucial part of national security as targets of cyberattacks are people, public opinion, governmental institutions and the private sector.

In the cyber domain, Russia is an aggressive cyberactor; however, another non-democratic state has much greater economic and technological resources, ambitions and aspirations vis-à-vis cyber expansionism.

Arguably, China is becoming the prime cyber threat to the US and its allies. China, like Russia, mounts major cyber operations against American and European countries on a regular basis with the goal of disrupting their economies, undermining military readiness and manipulating public opinion through the dissemination of disinformation. Additionally, the People's Republic of China uses its Digital Silk Road and Space Information Corridor to advance Chinese cyberespionage and reshape internet governance by replacing democratic values with authoritarian principles and dominate cyberspace.

China's Activities in Cyberspace

In 2011, American media started paying attention to the PRC's cyber activities. A lot was written about phishing cyberattacks that were used to steal intellectual property (IP) (Perlroth 2021).

The US Director of National Intelligence (ODNI) calculated that annually the US alone is losing approximately USD 540 billion to intellectual property theft of which cyber theft is estimated to be USD 400 billion. A total of 73% of cyber theft is attributed to Chinese-linked espionage (Hosenball 2020). China has been repeatedly accused of IP theft for a decade; however, since initiating its national Made in China 2025 (MiC2025) plan, which aims to transform China from a producer of low cost goods into a high-tech powerhouse, the above-mentioned problem has become more relevant than ever (Insikt Group 2021, 2).

It is extremely hard to either prevent cyberattacks or calculate the financial damages beforehand. This is especially due to the fact that the Chinese government and linked hacker groups use sophisticated cyber hacking operations, technologies and tactics when attacking the public or private sector. In order to steal data, hackers analyze the weaknesses of certain programs and servers for several months while staying unnoticed. Undoubtedly, they are good at it. It is worth mentioning that hackers linked to China's Ministry of State Security infiltrated the Marriott Group for four years, collecting the personal information of 500 million Marriott clients (Venard 2019).

Chinese cyberattacks are mainly conducted by the 3rd Department of the People's Liberation Army, "non-state" hacker groups and technological companies like Huawei. Cases of espionage between the US and China have multiplied. The PRC has even allegedly stolen the US F-35 military aircraft plans which were mysteriously transformed into the Shenyang FC-31 (Gady 2015). One could assume that Cold War 2.0 takes place in cyberspace.

Chinese IP theft was best described by former FBI Director, Robert Mueller, who claimed that there are two types of American companies: "Those that have been hacked and those that will be hacked" (Mueller 2012) .

China has also used cyberspace to spy in Europe, prominently targeting EU diplomatic cables. In 2018, hackers linked to the PLA hacked the EU diplomatic communication network and got access to sensitive data.

(Sanger et al 2018). Many speculated that China would use stolen data to blackmail EU officials into supporting the PRC's grand strategy and geopolitical goals. The above-mentioned approach might have been effective, especially if we keep in mind that unlike the US, the EU does not officially see China as a threat to international security and thus rarely criticizes its actions.

Additionally, China is trying to entrench Huawei into the European telecommunications infrastructure. The firm has close ties with the Communist Party and Chinese intelligence services and so, consequently, is a threat to EU security. The higher Huawei's market share, the less secure EU cyberspace becomes. The same is true about Georgia. A total of 75% of the country's communication network is developed by Huawei; therefore, the state's security and cybersecurity has a huge issue.

Besides cyberespionage, China actively uses cyberspace to spread disinformation. During the COVID-19 outbreak, Chinese media, especially the CCP affiliated Xinhua News Agency, started spreading conspiracy theories on the origins of the virus followed by the propaganda of Chinese medical support to various states. At the same time, Xinhua was sharing critical blogs and posters that criticized the US and the EU for "abandoning" countries in need. Lastly, Chinese disinformation included questioning the efficiency of western vaccines. Russian and Chinese disinformation tactics are very similar. Both target the US and its allies and try to show their own superiority in any case.

Chinese Cyber Expansionism and the One Belt, One Road Initiative

The Chinese government strives to have access to new markets and uses the One Belt, One Road Initiative to achieve its goals. On the one hand, BRI projects have commercial advantages and, on the other hand, China's export of internet devices benefits its "cyber expansionism" - characterized by the development of Chinese-style digital governance, the dependence of states on Chinese technologies and new opportunities for cyberespionage.

Two years after the first announcement of the BRI, President Xi Jinping developed the Digital Silk Road. Officially, China's DSR project, which is part of Beijing's larger BRI initiative, aims to build next-generation digital

networks around the world via terrestrial and underwater data cables, 5G technologies, data storage centers, surveillance networks and the launch of global satellite navigation systems. Infrastructure projects branded with the DSR are a way for Beijing to expand its influence in rising economies and developing countries as well as a way for domestic tech giants like Huawei, Alibaba and Tencent to build their global operations (Ghiasy et al 2021). China exports millions of internet of things (IoT) devices and surveillance technology. Chinese intelligence services have access to each device; therefore, they can monitor user movement, everyday activities, bank history, shopping habits, etc.

If developing countries depend on Chinese products, technologies and services, the PRC is able to influence local elites and so China controls the politics of states to a certain extent.

According to the International Telecommunication Union (ITU), only 55% of households globally have an internet connection. In the developed world, 87% of households are connected as compared with 47% in developing nations and just 19% in the least developed countries (ITU 2019). These least developed and developing nations are the ones where China's DSR is the most active. These states have a significant technological disadvantage and vulnerability to the PRC's digital colonialism, defined as "the use of digital technology for political, economic and social domination of another nation or territory" (Insikt Group 2021, 2). Internet access will provide prospects for economic growth as well as access to healthcare, education and jobs. Even though Chinese products and services are affordable, countries still have a price to pay - the presence of Chinese intelligence and the People's Liberation Army in their cyberspace.

On top of Chinese cyberespionage and digital colonialism, the risk of democracies adopting Chinese internet governance rules terrifies the West. China employs cutting-edge technology to maintain control over its populace, censor the media, suppress protests and ruthlessly mistreat religious minorities. According to Freedom House, 18 countries bought Chinese surveillance technology in 2018. Today, the number has risen to 80, including the vast majority of African, Asian and South American countries (Shahbaz 2018). More and more countries use smart cameras and sensors for mass surveillance. According to Recorded Future - a cybersecurity company based in the US - China trades technology for access to sensitive user data and facial recognition intelligence in some cases in

developing countries. China is adopting face recognition technology in Africa and using the data to improve its capabilities on people with a dark complexion (Insikt Group 2021, 8).

Domestically, the CCP efficiently controls cyberspace. Citizens are not allowed to use Western social media platforms like Facebook, Instagram, Google and Yahoo. The government explains it as a way to boost local technological businesses and their products; however, in reality they make sure Chinese people have no or very limited access to the Western media and only hear the party's narrative.

In 2020, the whole world saw how the CCP limits the freedom of expression on the internet. In 2020, the Chinese government started punishing people who wrote posts on the new virus in order to warn loved ones. Among them was Dr Li Wenliang who was accused of spreading disinformation. He was forced to publicly sign a document saying he wrote fake news which was far from reality and that no deadly virus existed. Sadly, Dr Li died from COVID-19 (Hegarty 2020).

Ren Zhiqiang's case should also be discussed. A Chinese blogger went missing on March 14, 2020 after stating that COVID-19 situation was the government's fault and called Xi Jinping a "crazy clown." After six months of his disappearance, Ren was found. The blogger had been convicted of corruption and given 18 years in jail (McDonell 2020).

New Internet Protocol Plan and 5G

China is promoting severe worldwide internet governance by rebuilding the internet, allowing nation-states to seize control and replace the open, decentralized and free internet infrastructure that has shaped the digital experience. Huawei engineers presented the New IP [internet protocol] Plan to delegates from over 40 nations in September 2019. The developers proposed a top-down system that would allow nation-states to more efficiently regulate their digital property and populations, implying that the current internet is obsolete and constrained (Murgia et al 2020). The CCP promotes "cyber sovereignty" or the supreme right to manage one's own internet and exercises strict control over the operation and use of its online infrastructure, internet-connected gadgets and citizens' online activity. President Xi Jinping is aiming to transform international norms and institutions in order to accommodate China's authoritarian governance model while avoiding global accountability.

In developing non-democratic states, Chinese-style internet governance not only allows the authorities to censor social media but helps oppress opposition. President Yoweri Museveni of Uganda ordered his cyber-surveillance intelligence team to collect encrypted online conversations and mobile phone calls of Bobi Wine, a "popstar turned political opponent." According to a *Wall Street Journal* investigation, after the regime's intelligence officers failed to breach Wine's WhatsApp and Skype accounts for days, they asked for help from Huawei, Uganda's largest digital supplier. Huawei experts are said to have successfully hacked Wine's WhatsApp account using malware in just two days. Museveni's dictatorship then utilized the access to disrupt opposition political rallies and detain Wine and a large number of his supporters (Parkirson et al 2019).

Huawei not only helps dictators get rid of unwanted opposition but also shares user data with Chinese intelligence services. Even though the company denied this statement several times, the People's Republic of China's Cybersecurity Law, enacted in 2017, mandates that data collected by any state or private Chinese company must be sent to the government on demand. When Beijing detects intelligence gaps that cannot be filled, it employs clandestine cyberespionage activities to fill them (Girard 2019).

Huawei was deemed a national security threat by the US House Intelligence Committee in 2012, warning that it had stolen intellectual property through backdoors that permitted unauthorized access to sensitive data (Schmidt et al 2012). Despite the decision of the United States to ban Huawei technology because of security concerns, Huawei remains the largest vendor of 5G technology and devices.

Australia, the United Kingdom and Japan banned Huawei from building 5G networks in response to US cybersecurity and espionage threats. However, the UK approved Huawei 5G network installation in 2020 (Reichert 2020). The EU also allowed the Chinese telecommunication firm's 5G equipment and infrastructure. Officials stated that Huawei will not be the only supplier and that the European 5G market should be diverse and have healthy competition (Nietsche et al 2020).

China is becoming Brazil's 5G supplier as well. Initially, Brazil and the United States signed a memorandum on 5G security making Brazil a member of the Clean Network Initiative. The United States and Brazil both stressed the necessity of adopting frameworks that adequately safeguard 5G networks from illegal access and interference. The agreement also

encouraged dependable and trustworthy network hardware and software suppliers to participate in 5G markets while taking risk profile evaluations into account (US Embassy and Consulates in Brazil 2020). However, after months of opposition, Brazilian President Jair Bolsonaro agreed to allow Huawei to bid on building out a 5G network in the country in January 2021. President Donald Trump had previously pressed President Bolsonaro to prevent the adoption of Huawei's 5G technology in Brazil but Bolsonaro faced opposition from both industry and his own government which may have affected his decision to allow Huawei to submit a proposal. It is worth noting that China is currently Brazil's largest trading partner, giving it a lot of sway over decisions on industry partnerships in the country. Huawei has been in Brazil for 22 years and has already performed 5G trials with all of the country's cellular carriers (Chu 2021).

Georgia also became a new member of the Clean Network Initiative on January 14, 2020 (US Embassy in Georgia). Two years prior, the country planned to become a major participant in the Digital Silk Road. Georgia was supposed to be the route for the 5G fiber-optic cable. The project was moved to Azerbaijan after Nexon Holding became a 100 percent shareholder in Caucasus Online. Georgian media reported that the country had lost hundreds of millions of dollars in investments as well as the opportunity to become a technological center. However, we must recognize that Chinese technology is not available without the involvement of the Chinese intelligence service. On top of that, the US is Georgia's main strategic partner; therefore, choosing China as a 5G supplier would be a political message and emphasize Georgia's eastern orientation. Because of all the above-mentioned reasons, one might argue this particular missed opportunity is beneficial for Georgia's national security and international relations.

Social Credit System

Alongside technological development, the CCP constructed the Social Credit System - a moral ranking system that monitors Chinese citizens. According to the *South China Morning Post*, the rankings are determined by China's economic planning team, the National Development and Reform Commission (NDRC), the People's Bank of China and the Chinese legal system. The system allows the government to monitor citizens in cyberspace and real life. The CCP now studies people's shopping habits

based on their bank account history, records their every move with the help of mass surveillance cameras and control posts and blogs on social media (Lee 2020).

A person's social score, like their personal credit score, can rise and fall depending on their actions. The exact methodology is unknown; however, posting "fake news," buying too much alcohol, smoking in non-smoking zones, poor driving habits and even being loud in public transportation can reduce the social score. Having low social scores has its consequences. China has already started punishing citizens by restricting their travel, banning them from flights, not allowing the buying of first class tickets on trains, keeping them out of luxury hotels, etc. (Ma et al 2021). Credit systems, according to Foreign Policy, track whether people pay their bills on time, similar to bank credit trackers, but also assign a moral dimension. Citizens with a low social score have already been banned from enrolling in higher education institutions (Minstreanu 2018).

Even though developing the Social Credit System seems to be something out of a *Black Mirror* episode or a sci-fi movie, we should remember that it is happening in real life. There is a risk of other authoritarian regimes or hybrid democracies adopting the system. The CCP uses modern technologies to oppress people who disagree with the government's decisions or actions. The Social Credit System is an efficient way to hold onto power and control the public opinion.

If developing countries adopt a social credit system, it would not only violate human rights but would also take Chinese cyberespionage to a whole new level. The system requires advanced technologies, smart cameras, mass surveillance networks, big data centers, etc. If China becomes the provider, its intelligence services will get access to the everyday behavior of a foreign country's citizens, their general tendencies and their problems. This kind of information can be used to tailor disinformation and fake news that shape public opinion and use it in a hybrid warfare against any actor.

* * *

As mentioned before, China is becoming the prime threat in cyberspace for the United States. Although Russia is a much more aggressive and experienced actor, China has greater technological and economical resources, capabilities and ambitions. Millions of Chinese smartphones, computers, sensors, smart cameras and surveillance technologies are

sold all over the world. Chinese intelligence has access to these devices; therefore, the CCP can cause the biggest damage to any state's cyber and national security. Furthermore, Chinese 5G technology and the plan to fully change the internet and cyberspace as well as strategic steps taken for its implementation should not be overlooked.

China aims to change the cyber domain by replacing democratic principles with authoritarian internet governance. The CCP's ideas might be interesting to other nondemocratic or hybrid regimes. Tracking and monitoring citizens, censuring social media, blackmailing the opposition – the New Internet Protocol Plan could legitimize it all.

As for Georgia, we have already seen intelligence services and the ruling party spying on its own citizens, accessing sensitive data and blackmailing people. It is possible that the Georgian Government finds the New IP Plan beneficial and uses it to justify illegal actions against opponents. Besides, Georgia is a new democracy where Western values and principles are slowly becoming norms. In such cases, authoritarian standards are always easier options. In spite of that, we hope the government will not take China's example and stay loyal to the Euro-Atlantic path.

Furthermore, Georgia should not make Brazil's mistake and should take the Clean Network Initiative very seriously. Turning away from Chinese 5G technology is extremely important for the country's cyber and national security. This could also be a political message to the US that an alliance with the main strategic partner is Georgia's priority. Moreover, it is crucial to stay loyal to democratic and Western values, especially in cyberspace.

The United States as well should take serious actions to counteract China and stop its cyber expansionism. The US should help developing countries to buy 5G internet, advanced technologies and communication networks from reliable sources. In order to compete with China's Digital Silk Road, they should develop a new Digital Marshall Plan (Frenkel et al 2021) which offers cost-effective alternatives to developing countries and, most importantly, deals with the PRC's expansionism in the cyber domain.

Bibliography

1. Chu, Daye. 2021. “Brazil Ditches US Drive to Strangle Huawei.” *Global Times*, January 17, 2021. https://www.globaltimes.cn/page/202101/1213075.shtml.
2. Frenkel, Orit; Kent Hughes and Jennifer A. Hillman. 2021. “The US Needs a ‘Digital Marshal Plan’ to counter China’s Digital Silk Road.” *The Hill*, July 12, 2021. https://thehill.com/opinion/technology/562435-the-us-needs-a-digital-marshall-plan-to-counter-chinas-digital-silk-road.
3. Ghiasy, Richard and Rajeshwari Krishnamurthy. 2021. “China’s Digital Silk Road and the Global Digital Order.” *The Diplomat*, April 13, 2021. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.
4. Girard, Bonnie. 2019. “The Real Danger of China’s National Intelligence Law.” *The Diplomat*, February 23, 2019. https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/.
5. Hegarty, Stephanie. 2020. “The Chinese Doctor Who Tried to Warn Others About the Coronavirus.” *BBC*, February 6, 2020. https://www.bbc.com/news/world-asia-china-51364382.
6. Hollis, David. 2011. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*, January 6, 2011. https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.
7. Hosenball, Mark. 2020. “Top US Officials to Spotlight Chinese Spy Operations, Pursuit of American Secrets.” Reuters, February 6, 2020. https://www.reuters.com/article/usa-china-espionage/top-u-s-officials-to-spotlight-chinese-spy-operations-pursuit-of-american-secrets-idUSL1N28S1B3.
8. Insikt Group. 2021. “China’s Digital Colonialism: Espionage and Repression Along the Digital Silk Road.” Recorded Future, July 27, 2021. https://go.recordedfuture.com/hubfs/reports/cta-2021-0727.pdf.
9. International Telecommunication Union. 2019. “Measuring Digital Development Facts and Figures.” *ITU Publications*, November 5, 2019. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.
10. Lee, Amanda. 2020. “What is China’s Social Credit System and Why is it Controversial?” *South China Morning Post*, August 9, 2020. https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.
11. Ma, Alexandra, Katie Canales. 2021. “China’s ‘Social Credit’ System Ranks Citizens and Punishes Them with Throttled Internet Speeds and Flight Bans if the Communist Party Deems Them Untrustworthy.” *Business Insider*, May 9, 2021. https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

12. McDonell, Stephen. 2020. “Ren Zhiqiang: Outspoken Ex-real Estate Tycoon Gets 18 Years Jail.” *BBC*, September 22, 2020. https://www.bbc.com/news/world-asia-china-54245327.

13. Minstreanu, Samina. 2018. “Life Inside China’s Social Credit Laboratory.” *Foreign Policy*, April 3, 2018. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.

14. Mueller, Robert S. “Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers and Spies.” RSA Cyber Security Conference San Francisco, CA, March 01, 2012. The Federal Bureau of Investigation. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

15. Murgia, Madhumita and Anna Gross. 2020. “Inside China’s Controversial Mission to Reinvent the Internet.” *Financial Times*, March 28, 2020. Inside China’s controversial mission to reinvent the internet | Financial Times (ft.com).

16. Nietsche, Carisa and Martjin Rasser. 2020. “Washington’s Anti-Huawei Tactics Need a Reboot in Europe - Efforts to Convince Allies of the Chinese Threat in 5G Have Floundered.” *Foreign Policy*, April 30, 2020. https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/.

17. Parkirson, Joe; Nicholas Bariyo and Josh Chin. 2019. “Huawei Technicians Helped African Governments Spy on Political Opponents.” *The Wall Street Journal*, August 15, 2019. Huawei Technicians Helped African Governments Spy on Political Opponents - WSJ.

18. Perlroth, Nicole. 2021. “How China transformed into a Prime Cyber Threat to the US.” *The New York Times*, July 19, 2021. https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html.

19. Reichert, Corinne. 2020. “Europe Allows Huawei for 5G Through Security Guidelines.” *CNET*, January 29, 2020. https://www.cnet.com/tech/mobile/europe-allows-huawei-for-5g-through-security-guidelines/.

20. Sanger, David E. and Steven Erlanger. 2018. “Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran.” *The New York Times*, December 18, 2018. https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html.

21. Schmidt, Michael S; Keith Bradsher and Christine Hauser. 2012. “US Panel Calls Huawei and ZTE ‘National Security Threat.’” *The New York Times*, October 8, 2012.

22. Shahbaz, Adrian. 2018. “Freedom on the Net 2018: The Rise of Digital Authoritarianism.” *The Freedom House*, October 18, 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

23. Tamkin, Emily. 2017. “10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?” *Foreign Policy*, April 27, 2017. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

24. US Embassy and Consulates in Brazil. 2020. “United States and Brazil Sign US $1 Billion Memorandum of Understanding.” October 20, 2020. https://br.usembassy.gov/united-states-and-brazil-sign-us-1-billion-memorandum-of-understanding/.

25. US Embassy in Georgia. 2021. “United States-Georgia Memorandum of Understanding on 5G Strategy.” January 14, 2021. https://ge.usembassy.gov/united-states-georgia-memorandum-of-understanding-on-5g-security/.

26. Venard, Bertrand. 2019. “The Cold War 2.0 Between China and the US is Already a Virtual Reality.” *The Conversation*, October 16, 2019. https://theconversation.com/the-cold-war-2-0-between-china-and-the-us-is-already-a-virtual-reality-125081.