MERICS
REPORT

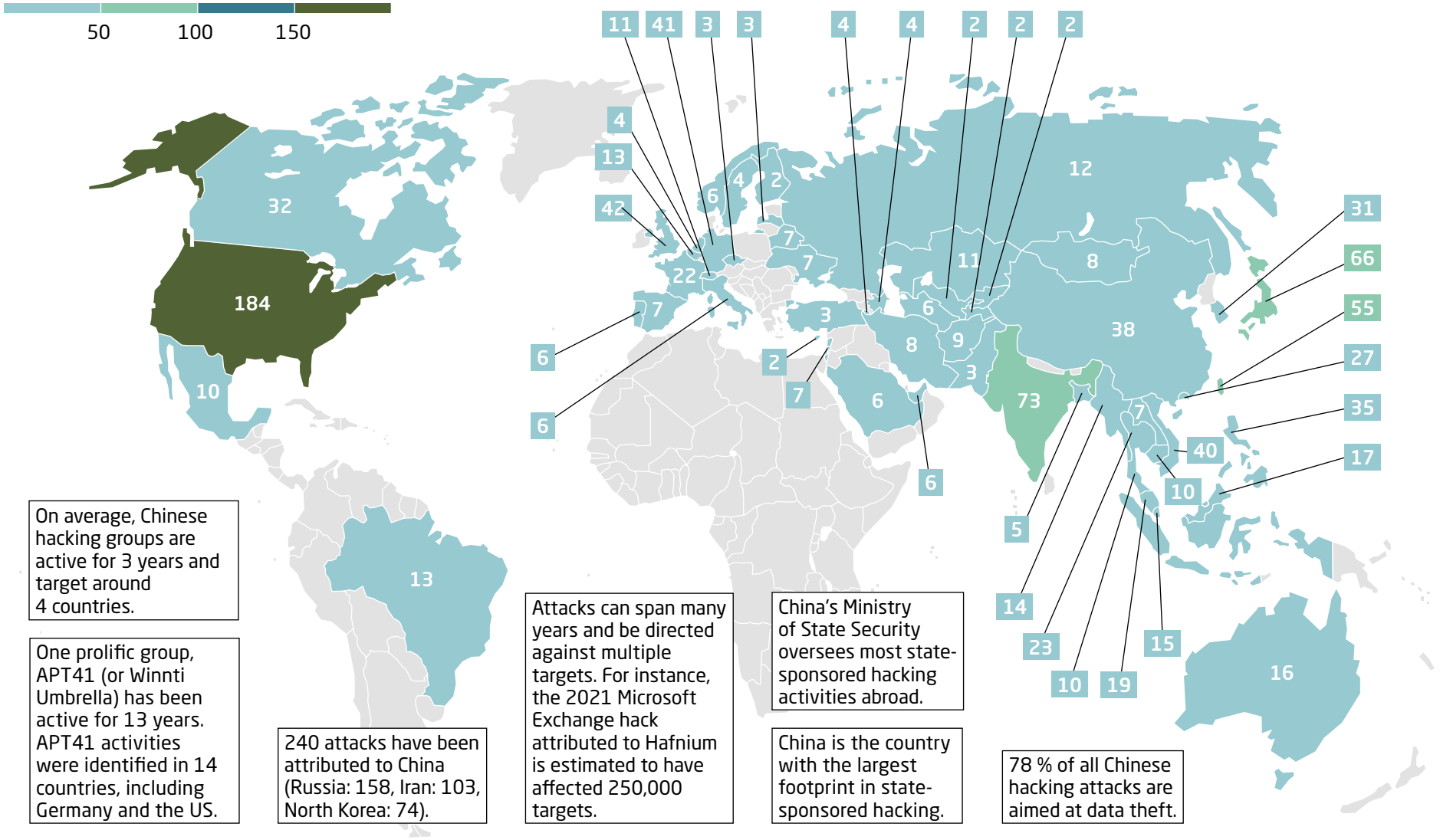
"HERE TO STAY" – CHINESE STATE-AFFILIATED HACKING FOR STRATEGIC GOALS

Antonia Hmaidi

MERICS
Mercator Institute for China Studies

Chinese state-attacks mostly target the US and Asian countries, but Europe is also affected

Number of campaigns targeted at each country attributed to China-based hackers with suspected or confirmed state affiliation



On average, Chinese hacking groups are active for 3 years and target around 4 countries.

One prolific group, APT41 (or Winnti Umbrella) has been active for 13 years. APT41 activities were identified in 14 countries, including Germany and the US.

240 attacks have been attributed to China (Russia: 158, Iran: 103, North Korea: 74).

Attacks can span many years and be directed against multiple targets. For instance, the 2021 Microsoft Exchange hack attributed to Hafnium is estimated to have affected 250,000 targets.

China's Ministry of State Security oversees most state-sponsored hacking activities abroad.

China is the country with the largest footprint in state-sponsored hacking.

78 % of all Chinese hacking attacks are aimed at data theft.

Source: EuRepoC

KEY FINDINGS

- **Chinese hacking poses a risk to Europe's long-term prosperity.** It is becoming more sophisticated and follows strategic goals of China's government.

- **China is a major source of cyberattacks against Europe.** While not all Chinese threat actors have clear ties to China's government, there is considerable evidence of links to it for many of them, suggesting some degree of state affiliation and sponsorship.

- **China rearranged its hacking capabilities to make attribution more difficult and to increase the combat-readiness of the People's Liberation Army.** Institutional changes have created a more flexible and sophisticated state-affiliated hacking scene.

- **Chinese threat actors typically attack for long-term access.** As opposed to the disruptive ones carried out by Russian actors or the moneymaking ones carried out by North Korean actors, Chinese attacks are more strategic.

- **Chinese threat actors focus on a smaller number of high-value targets and reuse the same exploits for different target types.** It is more difficult to spot them as they use edge devices like routers and techniques designed to avoid detection.

- **China has not engaged in disruptive attacks, but it is building up capabilities that it could later use for disruption.** Its use of cyber ranges so far and its targeting of critical infrastructure for long-term access suggests that China is setting up for future disruptive activity, posing a risk for Europe.

1. INTRODUCTION

1.1 China's cyberattacks are increasing and becoming more sophisticated

With more economic activity moving online, cyberattacks are gaining relevance. Globally, the European Commission estimates cyberattacks to cost EUR 5.5 trillion.[1] Cyberattacks are estimated to have cost German companies EUR 223 billion, or 6 percent of Germany's GDP, in 2021.[2] That same year, 86 percent of German companies suffered a cyberattack that led to some damage, according to one survey.[3]

As many cyberattacks are not publicized, how many originate in a particular country is hard to establish. Public information about Chinese cyber activities has become difficult to come by. Until about 2015, there were increasing media reports about Chinese cyberattacks.[4] Since then, China has worked to keep its capabilities hidden, but there is ample evidence that it is a significant and growing source of cyberattacks. In addition, while most cyberattacks are carried out by criminal actors that only want to make money, China's ones are more strategic and pose a risk to Europe's long-term prosperity.

While the involvement of China's government cannot be proven in all instances, some involvement is likely given its continuous quest to control the country's cyberspace and cyber actors. Many of the Chinese threat actors have been shown to have direct ties to the People's Liberation Army, the Ministry of State Security, or to a lesser extent the Ministry of Public Security. There is also solid evidence that the government financially supports the threat actors carrying out the attacks described here.

According to the European Repository of Cyber Incidents (EuRepoC), China was the country responsible for the largest number of cyberattacks worldwide between 2005 and 2023 with 240, followed by Russia with 158. China-originating hackers were responsible for attacks on 1,120 out of a total of 6,335 victims while Russia was responsible for 605.

German companies are seeing increased attacks from China

German companies are seeing increased attacks from China. In 2021, 30 percent of them said they had been attacked from China; in 2022, the figure was 43 percent.[5] For example, in 2019, the Chinese hacking group Winnti was found to have attacked major German corporations for years. It had started out targeting the gaming industry to make money and moved on to technology and pharmaceutical companies, and then in 2022 it started attacking government institutions and embassies.[6] It was so omnipresent in German companies that one cybersecurity expert joked that "[a]ny DAX [Germany's most important stock market index] corporation that hasn't been attacked by Winnti must have done something wrong."[7]

Chinese hacking activities have not only increased; they have also become more sophisticated. In the United States, indictments by the Department of Justice, statements by the Federal Bureau of Investigation, and reports by cybersecurity firms show this. Chinese hacking was originally focused on high-volume phishing campaigns[8] but it has become increasingly focused on long-term and targeted attacks.[9]

In Europe, governments and, especially, intelligence services have slowly acknowledged this problem. The 2021 report of Germany's domestic intelligence agency, the *Verfassungsschutz*, stated: "In Germany, politics and bureaucracy, economy, science and technology, as well as the military are the main goals of Chinese espionage. To realize its ambitious industrial policy, China uses espionage in business and science."[10]

In 2021, NATO, the EU, Australia, and New Zealand publicly attributed the hacking of the Microsoft Exchange Server to China's Ministry of State Security.[11] The group Microsoft identified as the attacker, Hafnium, targeted several industries to exfiltrate information and, after gaining access, installed additional malware to facilitate long-term access.[12]

Data sources and methods

The attribution of cyberattacks to a specific state or non-state actor is a major challenge. While IPv6, the latest version of the Internet Protocol (IP), usually allows for source identification, threat actors routinely route attacks via different locations, and often only the last "hop" (the location immediately before the target) can be identified.

This was the case, for example, when China-originating hackers attacked Taiwan's Ministry of Foreign Affairs in August 2022. While the majority of source IP addresses involved were Chinese, some were Russian. Attackers also often use compromised hosts. Even when it is possible to trace the IP addresses to the ultimate sources, this is not proof of involvement of governments, which do not tend to have complete control over their cyberspace.

The basis for attribution could be a shared operating procedure (often called TTP, for tactics, techniques and procedures), email addresses, shared vulnerabilities, and exploits (that is, attacks that have only been used by one threat actor). Additional factors can help attribution to a specific country, such as IP addresses located in government buildings and used during working hours.

A match between an attack and a government's known goals is the weakest basis for attribution, and using it risks skewing data. This study therefore looks only at those hacks and APTs that have been linked to China's government by multiple independent sources that weigh several characteristics, such as the vulnerability that was exploited, the time of the attack and the scale of the involved network and compare this "fingerprint" with the profile of known APTs.

Because attribution is difficult, the research for this report analyzed EuRepoC – a collection of data from an independent European research consortium on cyber conflict – to place China's involvement in hacking in global context. For individual cases, the research relies on reports by independent cybersecurity firms like Mandiant. Included in this analysis are only those hacks that were either attributed by multiple cybersecurity firms or by a democratic government with information on why this attack was attributed to a state actor. The research also included the threat actor cards produced by Thailand's Electronic Transactions Development Agency and Fraunhofer FKIE's Malpedia of threat actors. The data gathered is likely to undercount attacks originating from democracies, including the United States.

1.2 Chinese hacking serves strategic goals like technological innovation

With President Xi Jinping's expansion of the definition of national security to include economic and technological security, hacking by Chinese state-affiliated actors now serves national strategic goals. This includes technological innovation, gaining information for mergers and acquisitions, targeting dissidents, and traditional espionage against foreign governments. In 2014, China's ambassador to the United States said, when explaining why cyber activity against commercial secrets is the same as national security espionage: "How can you distinguish from activities that will hurt national security without hurting the nation's commercial interests?"[13]

Europe's prosperity relies in no small part on its technology and innovation strength. Technological innovation is also increasingly driving geopolitical, economic, and military competition. Meanwhile, China, labeled a systemic rival by the EU, is in a race for technology supremacy with the West.[14]

In 2020, Xi described science and technology as the main battlefield of the economy.[15] In the new system of "holistic innovation" and "all-of-state system," he said, everyone is supposed to come together to serve China's innovation needs.

China has used legal and illegal ways to induce knowledge and technology transfer.[16] Its toolbox includes requiring technology transfer for market access, joint venture requirements for investment in China, and weak protection of intellectual property.[17] Chinese firms have tried to poach talent, notably in the semiconductor industry.

For instance, Semiconductor Manufacturing International Corporation has recruited engineers from Taiwan Semiconductor Manufacturing Company on a large scale, at least doubling their salary.[18] On the illegal side there is economic espionage. This year, a chip executive went on trial in South Korea for stealing Samsung secrets that would be used to build a factory in China.[19] The Dutch semiconductor company, ASML has alleged a that IP theft by a former employee was a "plot to get technology for the Chinese government" and has won this lawsuit.[20] Huntsman Corp, a US chemicals maker, argues that its trade secret were stolen in the course of a government-mandated regulatory approval process.[21]

Hacking is a major illegal way through which China gains access to critical technology. Germany's *Verfassungsschutz* has stated that "especially German high-tech companies and world market leaders are in sight of most likely Chinese espionage."[22] According to it, these espionage activities are guided by national and global initiatives of China's government.

These government initiatives set out very specific strategic goals in technology. For example, the Made in China 2025 program aims to make the country a producer of high-tech goods, to increase the share of indigenous fundamental technology, and to increase informatization in the economy.[23] Since its inception in 2016, and thus throughout the trade and technology war with the United States, China's focus on indigenous innovation and science and technology has increased.

Western cybersecurity firms and government agencies agree that China's targeting of industries for hacking has aligned with the strategic priorities in its Five-Year Plans.

In 2005, the US intelligence community expressed worry about Chinese spies "poking into all sorts of American technology to compete with the U.S."[24] One example was the 2005

Titan Rain campaign that targeted technology restricted from export to China from the United Kingdom and the United States, in addition to targeting defense contractors and the US Department of Defense.[25] Titan Rain also revealed the state-private nexus in China's technology system. In 2011, it was reported that "many US firms whose business revolves around intellectual property complain that their systems are now under constant attack."[26]

In 2014, Federal Bureau of Investigation Director James Comey said: "For too long, the Chinese government has blatantly sought to use cyber-espionage to obtain economic advantage for its state-owned industries."[27] In 2021, the US government alleged that one hacking campaign originating in Hainan targeted many key technology companies in the West.[28] This was reported by Mandiant, a cybersecurity company that identified the first large-scale Chinese state-affiliated advanced persistent threat (APT) actor – Unit 61398 of the PLA (also called APT1) – as responsible. The industries targeted were aligned with strategic priorities listed in China's Five-Year Plan.[29]

Europe has also increasingly become worried about Chinese economic espionage through hacking. Germany's first China strategy, adopted in July 2023, states that "Espionage activities targeting Germany continue to increase, particularly in cyberspace."[30] In the Netherlands, the intelligence agencies have warned about Chinese cyberattacks, stating that "the crown jewels of the Dutch economy are in danger."[31] In its latest annual report, the General Intelligence and Security Service called China "the biggest threat to the Netherlands' economic security," and its director-general said that "the Chinese use cyber as a weapon, cyber as a way to commit espionage."[32]

1.3 China rearranges its hacking capabilities to make attribution more difficult

China rearranged its hacking capabilities to make attribution more difficult. States have long relied on proxies for cyberattacks to benefit from their expertise and to make attribution more difficult.[33] Autocracies tend to use proxies more but these are often quite firmly entrenched in their state bureaucracy and only have limited autonomy, as is the case with China, making their designation as proxy contested.[34]

Chinese cyber espionage started in the People's Liberation Army (PLA), whose units often conduct economic in addition to political and military espionage. In 2009, for instance, a State Department cable claimed that a series of attacks could be traced back to the PLA's Third Department, which oversaw China's electronic eavesdropping at the time.[35]

Evaluating the 2015 US-China no-spy agreement is difficult

Public naming-and-shaming and US indictments of Chinese hackers became frequent, especially between 2009 and 2015. Due to most hackers being based in the PLA directly, China's government could not plausibly deny its direct involvement.

In 2015, Xi and President Barack Obama signed an agreement that China and the United States would not engage in commercial cyber espionage.[36] This was followed by short-term decrease in Chinese hacking, although it is unclear how much of this was due to China honoring the agreement and how much to a change in its approach.

A reshuffle in China's military in 2015 – when the Strategic Support Force (战略支援部队) was formed to centralize all PLA space, cyber, electronic, and psychological warfare capabilities[37] – made evaluating the effectiveness of the agreement difficult. There has been a considerable increase in the volume and sophistication of Chinese hacking since 2016.

Chinese hacking groups are active for years and across industries

Top 20 Chinese hacking groups, their suspected affiliation and targets

HACKING GROUP	ATTRIBUTION BASIS	SUSPECTED AFFILIATION	ACTIVE TIME	TARGET FOCUS	ALTERNATIVE NAMES
1937CN	Attacker confirms	Hacktivist	2016–2016	Critical infrastructure, cybercrime	None
APT10	IT-security community attributes attacker	MSS Proxy	2012–2022	Corporate targets, critical infrastructure, cybercrime	Stone Panda/ MenuPass Team/ Cloud Hopper/ Red Apollo/ Cicada/ POTASSIUM/ BRONZE RIVERSIDE/ CVNX/ HOGFISH/ G0045 (MSS, Tianjin State Security Bureau)
APT31	IT-security community attributes attacker/ Attribution by receiver government / state entity	MSS Proxy	2015–2018	Political targets, cybercrime	ZIRCONIUM/ BRONZE VINEWOOD/ G0128
APT40	IT-security community attributes attacker	MSS Proxy	2014–2019	Political targets, corporate targets, critical infrastructure, social groups, science, cybercrime	Leviathan/ TEMP.Periscope/ TEMP.Jumper/ GADOLINIUM/ BRONZE MOHAWK/ MUDCARP/ KRYPTONITE PANDA/ TA423/ G0065 (MSS, Hainan State Security Department/ Hainan Xiandun Technology Company)
APT41	IT-security community attributes attacker	MSS Proxy	2011–2023+	Political targets, corporate targets, critical infrastructure, science, cybercrime	BARIUM/ Wicked Panda/ G0096 (Chengdu 404 Network Technology) Winnti Umbrella/ G0044
Axiom	Attribution by third-party/ IT-security community attributes attacker	MSS Proxy	2009–2018	Political targets, corporate targets, social groups, cybercrime	APT17/ Tailgater Team/ Group 72/ Dogfish/ G0001 (MSS, Jinan Bureau) Winnti Umbrella/ G0044
Emissary Panda	IT-security community attributes attacker/ Media-based attribution	MSS Proxy	201–2018	Political targets, corporate targets, critical infrastructure, social groups, science, cybercrime	APT27/ Lucky Mouse/ BRONZE UNION/ TEMP.Hippo/ Group 35/ TG-3390/ Iron Tiger/ ZipToken/ G0027
Honker Union	Attacker confirms	Hacktivist	2001–2012	Political targets, cybercrime	None
Ke3chang	IT-security community attributes attacker	MSS Proxy	2011–2022	Political targets, corporate targets, critical infrastructure, cybercrime	Vixen Panda/ APT 15

HACKING GROUP	ATTRIBUTION BASIS	SUSPECTED AFFILIATION	ACTIVE TIME	TARGET FOCUS	ALTERNATIVE NAMES
Lotus Blossom	IT-security community attributes attacker	Unknown	2017–2017	Political targets, corporate targets, critical infrastructure, science, cybercrime	Spring Dragon/ ST Group/ DRAGONFISH/ G0030
MSS	Attribution by receiver government / state entity	MSS	2009–2018	Critical infrastructure, cybercrime	None
MSS supported Hackers	Attribution by receiver government / state entity	MSS	2014–2019	Corporate targets, critical infrastructure, science, cybercrime	None
Mofang	IT-security community attributes attacker	Unknown	2012–2015	Political targets, corporate targets, cybercrime	None
Mustang Panda	IT-security community attributes attacker	MSS Proxy	2021–2022	Political targets, cybercrime	RedEcho/ Bronze President/ Earth Preta
PLA	Attribution by receiver government / state entity / IT-security community attributes attacker	PLA	2015–2018	Political targets, corporate targets, critical infrastructure, cybercrime	None
Putter Panda	IT-security community ttributes attacker	PLA Unit 61486	2007–2012	Political targets, critical infrastructure, science, cybercrime	APT 2
RedAlpha	IT-security community attributes attacker	Unknown	2017–2018	Political targets, corporate targets, social groups, cybercrime	None
RedEcho	IT-security community attributes attacker	MSS Proxy	2020–2021	Critical infrastructure, cybercrime	None
TA413	IT-security community attributes attacker	Unknown	2021–2022	Social groups, cybercrime	None
Thrip	IT-security community attributes attacker	Unknown	2013–2018	Critical infrastructure, cybercrime	None

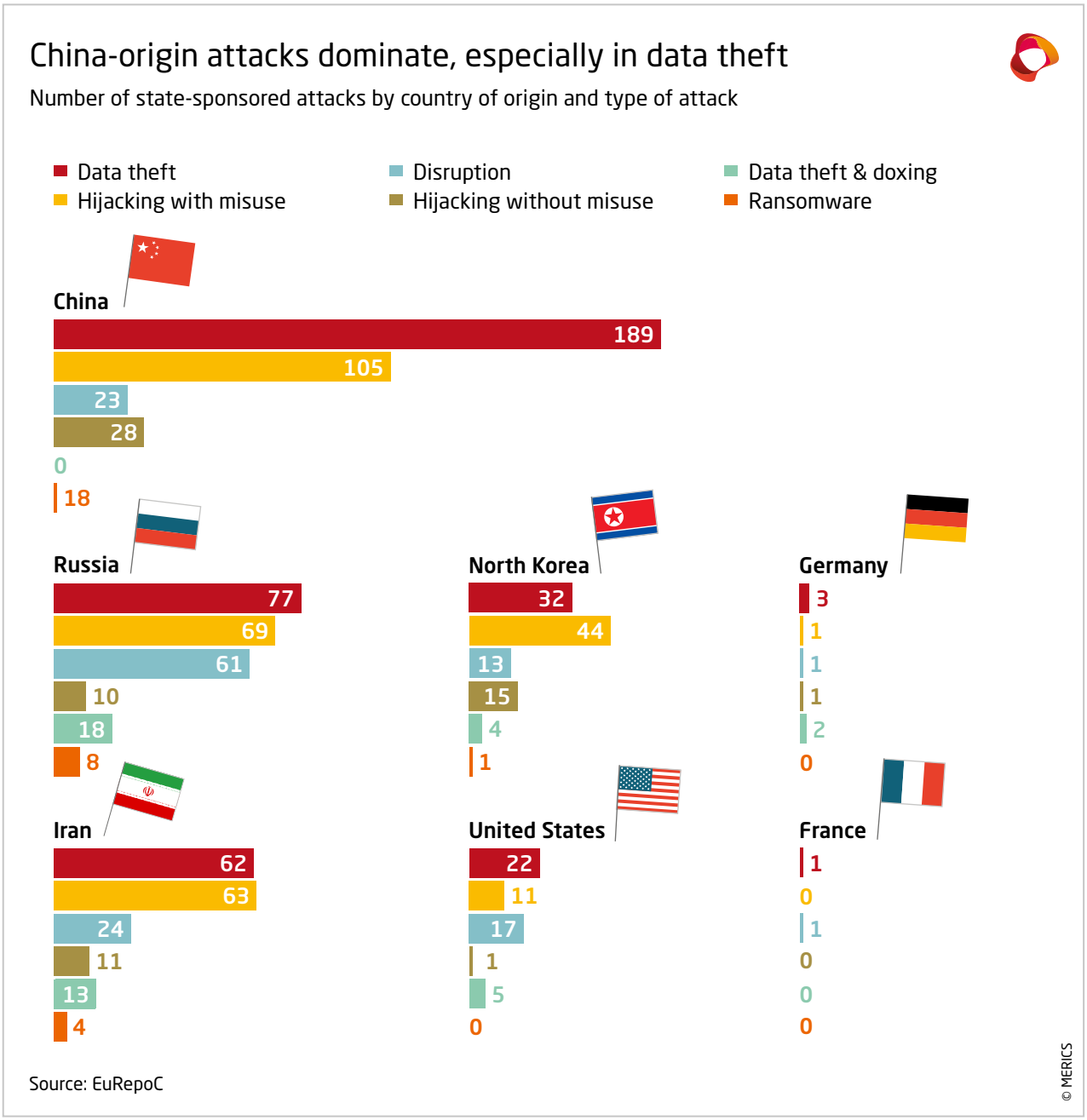
Source: MERICS

Even before this, some of China's cyber hacking reportedly had moved to the private sector and a vast "elite satellite network of contractors at front companies and universities that work at the direction of China's Ministry of State Security."[38] Since 2015, this "freelance cyber army" has been guided by the Ministry of State Security, which is officially a full-spectrum intelligence agency, while the PLA has shifted to combat-oriented activities.

2. HACKERS SERVE THE PARTY STATE IN SEVERAL DOMAINS

An analysis of the EuRepoC data reveals that, between 2005 and 2021, more than 78 percent of cyberattacks attributed to a Chinese threat actor were for data theft (for comparison, the figure for Russia was 60 percent).[39] Half of these also included "hijacking with misuse" (taking control of a computer to be able to run commands or change something on its disk), which often also ultimately serves for data stealing in Chinese attacks conducted by

Exhibit 2



state-affiliated actors. APT1's attacks on US targets between 2006 and 2013 are one example of hijacking that ultimately served to ensure that the PLA unit had continuous access to "steal broad categories of intellectual properties."[40]

Often, Chinese threat actors try to stay undetected by only transferring small amounts of data. They analyze the data on-site and only transfer what is relevant.[41] For example, the Winnti group attacks transferred only internal technology documentation, code-signing certificates (that allow supply-chain attacks), and source code.[42]

State institutions were the most important targets of attacks (with 32 percent). Critical infrastructure, corporate institutions, and science institutions were also very important ones, with the defense, energy, and telecommunications industries as well as military institutions targeted more frequently.

State institutions have been the most important targets of Chinese attacks

2.1 Chinese attacks target government departments and tech companies

Chinese threat actors have a diverse set of targets but these mirror and support the priorities of China's leadership, such as those outlined in the Five-Year Plan. They include dissidents, patent holders, and corporate and state counterparts in international negotiations. Chinese hackers have supported Chinese state-owned enterprises in trade negotiations by breaching the networks of important US firms like U.S. Steel and SolarWorld.[43] For example, RedAlpha is best known for targeting Tibetans in exile but the infrastructure it uses (including servers and IP ranges) has also been used for hacking foreign governments. In several cases, government institutions were targeted during periods of dialogue with China.

Some actors seem to focus on specific strategic sectors. APT40, for instance, targets research projects at universities relating to naval capabilities, especially government-sponsored projects.[44] Others, like APT24, focus on traditional espionage and stealing documents with political significance.[45] Many collect information with political relevance as well as IP-related information in key industries. In 2018, RedAlpha targeted Daimler AG one day after the company cut its profit outlook as a result of growing tensions between China and United States.[46] All of this supports the argument that these activities originating from China are state-affiliated.[47]

Attacks for intelligence collection before imminent events, not only high-level visits but also mergers and acquisitions talks, has been observed consistently. For example, a significant increase in Chinese scanning activity was observed in Alaska in 2018, just before a trade delegation from the US state was due to travel to China.[48] This pattern has also been observed with the likes of Germany and Belt and Road Initiative countries.[49]

2.2 China's government is carrying out a campaign for cyber-espionage

The fact that many attacks originate in China is not necessarily evidence of government action. Given that China has 25 percent of the global online population and hosts many online servers with no or minimal protection, it is not surprising that many attacks originate in the country or can be traced back there.[50] However, based on EuRepoC data, the research by international cybersecurity firms, and advisories from intelligence agencies, it is clear that China's government is carrying out a deliberate campaign to obtain intelligence using hacks.

Sustained campaigns like Titan Rain show how an attack vector or exploit travels through China's hacking scene and is shared between actors. If one of the actors involved is identified as a Chinese government one, this makes it likely that all the others are also state-affiliated, especially taken together with analysis of their TTP, their targets, and open-source intelligence about specific hackers.[51]

There is also evidence that Chinese hacking groups obtain information about targets from government sources. The 2021 Vulnerability Disclosure Law requires that all companies, including cybersecurity and hacking companies, operating in China need to report any vulnerabilities to the authorities within two days. Two days is often not enough time for companies to patch a vulnerability,[52] and, according to Microsoft, the increased use of zero-days (previously unknown exploits) by China-based actors is likely connected to this requirement.[53] This suggests some level of coordination between government defensive and offensive forces.

Many Chinese threat actors have multiple roles. They conduct espionage of foreign government actors and conduct economic espionage of foreign private-sector actors, especially in areas of strategic importance for the state. Some also use the same tools and resources for personal profit. This further muddies the water for attribution.

APT41, the most prolific threat actor identified with 16 attacks, has conducted state-sponsored espionage as well as "financially motivated activity potentially outside of state control."[54] Since the Chinese authorities have regularly cracked down on criminal hackers, such activities suggest that the Ministry of State Security might not have as much control over some hacking groups as it would like to have.[55]

2.3 China's government tries to increase control over hackers

The risk associated with the existence of proxies and a freelance cyber army has become apparent to China's government. After Chinese hacktivists going by the name Honker or Red Hacker(红客) attacked the US embassy in Belgrade 1999 following the US bombing of the Chinese embassy there, the government became more serious about reining in its hackers.[56] The government has made efforts to phase out criminal freelancers. In 2015, the Operation Clean Internet included some internationally active threat actors among its targets for arrest.[57]

Beijing wants a huge cyber workforce loyal to the CCP

China's government is trying to restrict hackers to national hacking competitions instead of international ones. In 2017, the founder of China's largest cybersecurity company, Qihoo 360, publicly criticized Chinese citizens travelling overseas for hackathons. In 2018, the organizers of Pwn2Own, an important international cybersecurity competition, announced that Chinese citizens could no longer participate in the contest due to domestic Chinese regulation.[58] Chinese hacking teams still place fourth on CTFTime, the largest international "Capture the Flag" platform internationally. Since 2018, the Tianfu Cup, a more real-world contest than many Western ones, has been hosted in China by major Chinese cybersecurity companies as well as Alibaba, Baidu, and Huawei.[59] Modified exploits showcased at this event have been used by Chinese authorities to surveil the Uyghur population.[60]

The government has also stepped up its efforts to educate a huge cyber workforce that is also loyal to the Chinese Communist Party to shore up both cyber security and hacking without posing threats to the Party.[61] The National Cybersecurity Center in Wuhan, an institution with a large campus set up to train cybersecurity workers, to incubate cybersecurity

companies, and to conduct research, is a good indication of the significance the party-state gives to cybersecurity. Private-sector actors have also stepped up their education efforts, as their cyber job adverts show. There is a lot of demand for competition and "Capture the Flag" designers, and there has been a surge in domestic hacking competitions.

China's government now has a firm grip on Chinese hackers, who often work for it through a series of shell companies loosely affiliated with regional branches of the Ministry of State Security (MSS) instead of being directly in the PLA hierarchy. Some of these hackers and contractor companies also contribute to domestic repression and support the Ministry of Public Security in obtaining evidence to use in interrogations, wiping devices, and censorship.[62] Staying on the party's good side allows some of these hackers to conduct financially motivated side activities, although regular crackdowns make this riskier.[63]

3 CHINESE THREAT ACTORS ATTACK FOR LONG-TERM ACCESS

A broader range of institutions and hackers has become part of China's hacking landscape over the past decade, but their goals have been consistent. A key one is to value long-term access to targets above short-term rewards, which applies for the PLA, the MSS, and their proxies. This makes detection more difficult.

This fits well with the Strategic Support Force's goal of "perpetual mobilization" and the PLA's concept of peacetime-wartime integration (平战一体) since long-term access could be used for destructive purposes in the event of a conflict.[64] It is also a sign of relatively stable APT groups that manage to update their toolsets and check access: APT30, for instance, has good version control, allowing it to keep a history of its programs, and it has used the same tools for years. Every couple of weeks, it logs into each captured computer and updates its tools to ensure the same version is running on each target.[65]

3.1 Chinese threat actors try to stay undetected

Chinese state-affiliated threat actors try to stay undetected, and a lot of their hacking is designed to be invisible so as to secure long-term access to their targets. APT1, for instance, has maintained access to networks for an average of 365 days, and it has been able to stay in some networks for up to five years.[66] Threat actors use different techniques to make detection difficult, unlike in the case of, say, ransomware attacks, which end as soon as they are detected.[67]

Chinese attacks for long-term access could be used for disruptive attacks in the future. Some have been shown to leave behind disruption software; for instance, in the US power grid.[68] In the analysis of EuRepoC data, 28 percent of Chinese attacks targeted critical infrastructure. The figure is 29 percent for Russia, which is known to conduct disruptive attacks on critical infrastructure. While Chinese threat actors have not moved to disruption to date, China has set up cyber ranges to conduct disruption tests, and all indications point to it building up capability to disrupt in the future.[69]

Chinese attacks for long-term access could be used for disruptions

A 2023 attack on US critical infrastructure was attributed by Microsoft to the Chinese threat actor VoltTyphoon, which the company said intended "to perform espionage and maintain access without being detected for as long as possible."[70] VoltTyphoon tried to hide its attack in typical administrator activity, known as "living off the land." It also proxied its network traffic through compromised devices owned by private users or small companies.

This shows that this kind of living-off-the-land activity is very difficult to detect regardless of how secure the target's IT is as long as there are smaller companies and private user devices that can be hijacked.

Network devices like routers are means to keep Chinese attacks invisible.[71] For example, Mandiant has identified in the case of one specific vulnerability of one router that there were organizations in the US defense, government, telecommunications, high tech, education, transportation, and financial sectors that were targeted.[72] As long as there are such insecure edge devices, including not only network devices but also local, small servers, Chinese threat actors can continue to capture them for hacking.[73]

3.2 Chinese attacks are less visible than those of other authoritarian countries

Almost 50 percent of the attributed attacks in the EURepoC data were from four authoritarian countries: China, Iran, North Korea, and Russia. The 2022 report of Germany's Verfassungsschutz identified China, Iran, Russia, and Turkey as the four main threat actors targeting the country.[74] Each of these countries has a sizable state-affiliated hacking community and uses hacking for traditional government espionage, but they differ in their other activities.

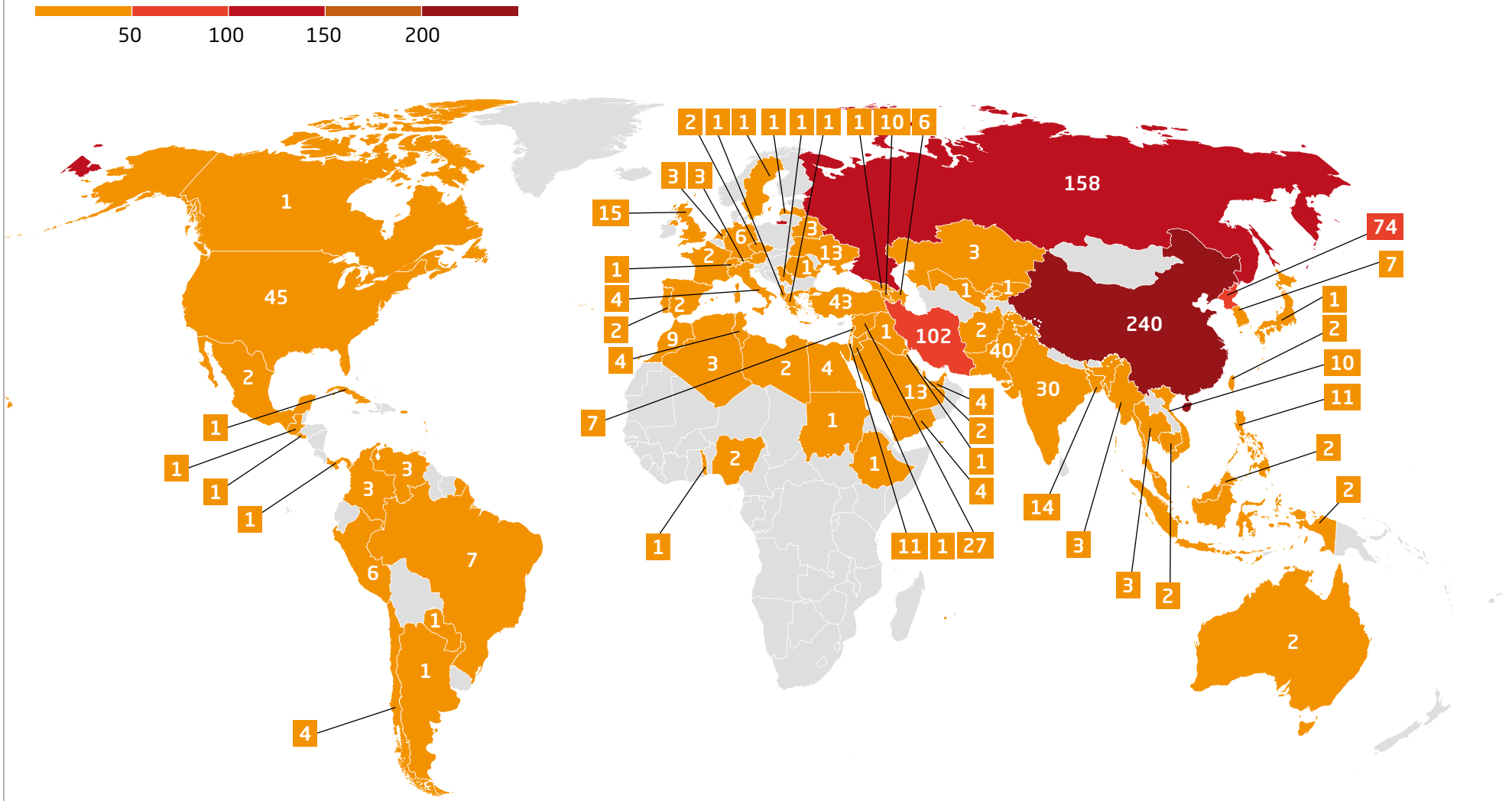
For example, while North Korean hackers engage in traditional espionage like stealing data from the South Korean army, most of their hacks focus on short-term financial gain. Around half of North Korea's foreign-currency income is reportedly from cyberattacks.[75] Hackers employ ransomware, rob banks, and steal cryptocurrency from online exchanges. As Internet access is extremely limited in the country, North Korean hackers usually have been highly cultivated by the authorities.[76]

By contrast, Russian hackers focus more on disruptive attacks. More than 30 percent of attributed Russian state-affiliated attacks included some disruption, and many were specifically designed to disrupt, like the NotPetya attack on Ukraine's infrastructure in 2017. Russian and North Korean attacks are thus often more easily detected. Iranian hackers are mostly active at the regional level and for political statements.

Chinese hackers have used cryptocurrency attacks, although their timing suggests that they were moonlighting when doing so: the attacks were usually carried out after 6 pm, while data-theft attacks were carried out during working hours. Chinese hackers do not use ransomware much. When they do, it tends to be to disguise more targeted data theft. For instance, the threat actor EmissaryPanda used known vulnerabilities to make an IP theft attack look like a ransomware one, persisting in the system for months with only minimal activity.[77] In another operation, the targets were a pharmaceutical company, a law firm, aerospace and defense firms, and electronic component designers and manufacturers, in line with strategic priorities of China's government.[78]

China is the most important source of cyber attacks in the world

Number of state-origin or state-affiliated cyber attacks by origin country, 2000–2023



Source: EuRepoC

4 CHINESE HACKING ATTACKS ARE HERE TO STAY

China is an important source of cyberattacks on Europe and Germany. Institutional changes have created a more flexible and sophisticated state-affiliated Chinese hacking scene. Chinese hackers participate less in international forums, and now need to share vulnerabilities with China's government before sharing them with other governments or the threatened company.

China has a growing incentive for data theft and exfiltration as it increasingly sees itself in conflict with the West and technology is one of the cornerstones of this conflict. IP theft and persistent access by Chinese actors are already dangerous to Europe and Germany. In addition to economic and technology espionage, Chinese threat actors also target critical infrastructure, often simultaneously for espionage and long-term access for possible future disruptions. China seems to be preparing for future disruptions; for instance, during a possible Taiwan conflict.

Chinese threat actors also target critical infrastructure

Not all attacks originating from China can be attributed directly to its government. However, many long-term Chinese threat actors have been identified as government sponsored. In addition, Chinese attacks become more frequent and intense around visits and planned mergers and acquisitions (M&A) activities of Chinese firms, further justifying their attribution to China's government.

Chinese attacks are strategic with threat actors typically attacking for long-term access and often targeting a smaller number of high-value targets. This makes these attacks less visible, while their use of edge devices like routers makes detection even more difficult.

Europe's prosperity relies on maintaining an edge in technology. Recent cases of ransomware in Europe and Germany show that cybersecurity needs to be improved. Securing the most innovative firms against cyber espionage should be a high priority. Germany, with its many companies with valuable IP, faces additional hurdles in this regard as its smaller *Mittelstand* companies have fewer resources to spend on cybersecurity.[79]

The activities of Chinese hackers in European networks are here to stay, and Europe should be prepared to face this threat over the long term. These attackers often use the same technique for a variety of different targets in different countries over a long time. The recent focus on preventing ransomware should be complemented by an equal focus on long-term challenges. Because Chinese hackers try not to be detected and do not disrupt, they are often underestimated in Europe.

OPTIONS FOR ACTION

- **European governments should define what constitutes strategic, critical, and important technology:** China's intellectual property theft through hacking is especially harmful where it attacks foundational technology. Knowing what technology is most critical to Europe's prosperity allows governments and private business to better prioritize resources. The EU has just defined a critical technology list, and cybersecurity should be included in the risk assessment being taken out for these technologies.

- **European government agencies should study the Chinese domestic hacking scene, investment and capabilities:** A good understanding of the Chinese hacking scene will provide a good idea of threat actors' likely targets, tactics, and priorities. This should include tracking China's aspirations and capabilities through the likes of cybersecurity curricula in schools and job adverts.

- **European governments need to better understand Chinese attack patterns and prepare accordingly:** Chinese threat actors support Chinese government visits and M&A activities. Governments should ensure that cybersecurity is strengthened around visits, and that companies are aware of the risks when considering M&A and other strategic partnerships with Chinese firms in strategic sectors.

- **European governments, the EU, and NATO should identify likely hacking targets by studying the priorities of China's government:** Chinese hacking follows government priorities closely, so understanding these when it comes to technology can help better define likely targets in Europe.

- **European governments should provide additional training and resources to likely or critical targets:** Since their resources are limited, governments should provide additional training and resources to those targets that are most likely or most critical. This includes infrastructure companies and companies that have foundational technology.

- **Government and private actors in EU and NATO countries should share intelligence on attacks:** Chinese threat actors often use the same toolkit across multiple targets and years, in different industries and countries. Sharing intelligence can help detect Chinese intrusions earlier. Trust needs to be established for companies to be willing to share their cybersecurity incidents. They need to be assured the government will not be using the disclosed vulnerabilities in cyberattacks themselves.

ENDNOTES

1 | European Commission (2022). “Cyber Resilience Act | Shaping Europe’s digital future.” Retrieved October 23, 2023, from https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
2 | Dennis Schirrmacher (2022). “Studie: (Cyber-)Attacken kosten deutsche Unternehmen 203 Milliarden Euro.” Retrieved July 14, 2023, from heise online https://www.heise.de/news/Studie-Cyber-Attacken-kosten-deutsche-Unternehmen-203-Milliarde-Euro-7251239.html
3 | Sabrina Flemming (n.d.). *Wirtschaftsschutz* 2021. 19.
4 | Perlroth, Nicole (2021). “How China Transformed Into a Prime Cyber Threat to the U.S.” The New York Times. Retrieved from https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html
5 | Bitkom e.V. (n.d.). “203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen | Presseinformation | Bitkom e. V.” Retrieved July 14, 2023, from https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
6 | Tanriverdi, Hakan, Svea Eckert, Jan Strozyk, Maximilian Zierer, & Rebecca Ciesielski (2019). “Winnti: Attacking the Heart of the German Industry.” Retrieved July 10, 2023, from BR24 https://web.br.de/interaktiv/winnti/english/
7 | Patrawala, Fatema (2019). “Winnti Malware: Chinese hacker group attacks major German corporations for years, German public media investigation reveals.” Retrieved July 10, 2023, from Packt Hub https://hub.packtpub.com/winnti-malware-chinese-hacker-group-attacks-major-german-corporations-for-years/
8 | Perlroth, Nicole (2021). “How China Transformed Into a Prime Cyber Threat to the U.S.” The New York Times. Retrieved from https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html
9 | Mandiant (2023). “Stealth Mode: Chinese Cyber Espionage Actors Continue to Evolve Tactics to Avoid Detection.” Retrieved July 24, 2023, from https://www.mandiant.com/resources/blog/chinese-espionage-tactics
10 | Verfassungsschutz (2022). Verfassungsschutzbericht 2021.
11 | Wilkie, Christina (2021). U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange servers. Retrieved from NBC https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html
12 | Microsoft 365 Security Intelligence (2021). “HAFNIUM targeting Exchange Servers with 0-day exploits.” Retrieved July 13, 2023, from https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
13 | PRC Embassy (2014). “Ambassador Cui Tiankai’s Interview with the Foreign Policy_Embassy of the People’s Republic of China in the United States of America.” Retrieved August 22, 2023, from http://us.china-embassy.gov.cn/eng/sgzc/201411/t20141107_4900884.htm
14 | Sahin, Kaan, & Barker, Tyson (2021). “Europe’s Capacity to Act in the Global Tech Race | DGAP.” Retrieved July 14, 2023, from https://dgap.org/en/research/publications/europes-capacity-act-global-tech-race
15 | Xinhua (2020). “Xi Focus: Xi stresses development of science, technology to meet significant national needs - Xinhua | English.news.cn.” Retrieved July 14, 2023, from http://www.xinhuanet.com/english/2020-09/12/c_139361891.htm
16 | Olcott, Eleanor, Davies, Christian, & Jung-a, Song (2023). “The South Korean ‘master’ of chips accused of sharing secrets with China.” Financial Times. Retrieved from https://www.ft.com/content/fc7f6ea0-08f6-40f3-897f-e723cff9fd8c
17 | EU China IPR Helpdesk (2021). “Technology Transfer to China - Guidance for Busineses.” Retrieved July 14, 2023, from https://intellectual-property-helpdesk.ec.europa.eu/system/files/2021-01/Technology_Transfer_to_China_Guide.pdf
18 | Recorded Future (2022). “Semiconductor Companies Targeted by Ransomware | Recorded Future.” Retrieved July 9, 2023, from https://www.recordedfuture.com/semiconductor-companies-targeted-by-ransomware
19 | Yang, Heekyong, & Park, Ju-min (2023). “Trial starts for Korean chip executive accused of stealing Samsung secrets for China factory.” Reuters. Retrieved from https://www.reuters.com/technology/trial-starts-korean-chip-exec-accused-stealing-samsung-secrets-china-factory-2023-07-12/
20 | Thompson, Adrienne (2022). “Engineer Who Fled Charges of Stealing Chip Technology in US Now Thrives in China.” Retrieved September 28, 2023, from Center for Security and Emerging Technology https://cset.georgetown.edu/article/engineer-who-fled-charges-of-stealing-chip-technology-in-us-now-thrives-in-china/
21 | Wei, Lingling & Bob Davis (2018). “How China Systematically Pries Technology From U.S. Companies.” Wall Street Journal. Retrieved from https://www.wsj.com/articles/how-china-systematically-pries-technology-from-u-s-companies-1537972066
22 | Bundesamt für Verfassungsschutz (n.d.). “Wirtschafts-/ Wissenschaftsschutz.” Retrieved August 24, 2022, from BundesamtfuerVerfassungsschutz http://www.verfassungsschutz.de/DE/themen/wirtschafts-wissenschaftsschutz/wirtschafts-wissenschaftsschutz_node.html
23 | Wübbeke, Jost & Mirjam Meissner, Max J. Zenglein, Jacqueline Ives, Björn Conrad (2016). “Made in China 2025 | Merics.” Retrieved July 14, 2023, from MERICS https://merics.org/de/studie/made-china-2025-0
24 | Thornburgh, Nathan (2005). “The Invasion of the Chinese Cyberspies.” Time. Retrieved from https://content.time.com/time/subscriber/article/0,33009,1098961-2,00.html
25 | Thornburgh, Nathan (2005). “The Invasion of the Chinese Cyberspies.” Time. Retrieved from https://content.time.com/time/subscriber/article/0,33009,1098961-2,00.html

26 | Grow, Brian & Mark Hosenball (2011). “Special report: In cyberspy vs. cyberspy, China has the edge.” Reuters. Retrieved from https://www.reuters.com/article/us-china-usa-cyberespionage-idUSTRE73D24220110414
27 | NBC News (2014). “U.S. Charges China With Cyber-Spying on American Firms.” Retrieved July 9, 2023, from https://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706
28 | United States Department of Justice (2021). “Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research.” Retrieved July 14, 2023, from https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion
29 | Mandiant (2013). “APT1 | Exposing China’s Cyber Espionage Units.” Retrieved February 6, 2023, from https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units
30 | Bundesregierung (2023). Strategy on China of the Government of the Federal Republic of Germany.
31 | Stu Sjouwerman (n.d.). “Dutch Intelligence Agencies Warn About Chinese and Russian Cyber Espionage.” Retrieved August 21, 2023, from https://blog.knowbe4.com/dutch-intelligence-agencies-warn-about-chinese-and-russian-digital-cyber-espionage
32 | Corder, Mike (2023). “Dutch intel agency paints grim picture of multiple threats.” Retrieved August 21, 2023, from AP News https://apnews.com/article/intelligence-netherlands-terrorism-threat-russia-china-dutch-cyber-attack-277fb0dc4203cbe6fbbc7ad8476b4184
33 | Harnisch, Sebastian & Kerstin Zell-Schabath (2023). Sicherheit durch Verschleierung. Warum Regierungen Proxies in Cyberkonflikten einsetzen 2023. Retrieved from https://bundesstiftung-friedensforschung.de/blog/forschung-dsf-no-57/
34 | Harnisch, Sebastian & Kerstin Zell-Schabath (2023). Sicherheit durch Verschleierung. Warum Regierungen Proxies in Cyberkonflikten einsetzen 2023. Retrieved from https://bundesstiftung-friedensforschung.de/blog/forschung-dsf-no-57/
35 | Grow, Brian & Mark Hosenball (2011). “Special report: In cyberspy vs. cyberspy, China has the edge.” Reuters. Retrieved from https://www.reuters.com/article/us-china-usa-cyberespionage-idUSTRE73D24220110414
36 | Elsa B. Kania & John K. Costello (2018). “The Strategic Support Force and the Future of Chinese Information Operations.” The Cyber Defense Review, 3(1), 105–122.
37 | Costello, John, & McReynolds, Joe (2018). “China’s Strategic Support Force: A Force for a New Era.” China Strategic Perspectives, 13.
38 | Perlroth, Nicole (2021). “Inside China’s vast network of hackers and how it became a prime cyber threat to the US.” The Economic Times. Retrieved from https://economictimes.indiatimes.com/news/international/world-news/inside-chinas-vast-network-of-hackers-and-how-it-became-a-prime-cyber-threat-to-the-us/articleshow/84575103.cms?from=mdr
39 | According to MERICS analysis of EURepoC data.
40 | Mandiant (2013). “APT1 | Exposing China’s Cyber Espionage Units.” Retrieved February 6, 2023, from https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units
41 | Fire Eye (2015). APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION. Retrieved from https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
42 | Tom “Hollywood” Hegel (2018). Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. Retrieved from https://web.archive.org/web/20180504222638/https://401trg.pw/burning-umbrella/
43 | Department of Justice (2014). “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.” Retrieved January 26, 2023, from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
44 | Mandiant (n.d.). “Advanced Persistent Threat (APT) Groups & Threat Actors.” Retrieved July 9, 2023, from https://www.mandiant.com/resources/insights/apt-groups
45 | Mandiant (n.d.). “Advanced Persistent Threat (APT) Groups & Threat Actors.” Retrieved July 9, 2023, from https://www.mandiant.com/resources/insights/apt-groups
46 | Insikt Group (2018). “Chinese Cyberespionage Originating From Tsinghua University Infrastructure | Recorded Future.” Retrieved July 6, 2023, from https://www.recordedfuture.com/chinese-cyberespionage-operations
47 | rt-apt41-dual-operation.pdf (n.d.). Retrieved from https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf
48 | Alfred Ng (2018). “Chinese hackers targeted US agencies during trade talks.” Retrieved August 21, 2023, from https://www.cnet.com/news/politics/chinese-hackers-targeted-us-agencies-during-trade-talks/
49 | Insikt Group (2018). “Chinese Cyberespionage Originating From Tsinghua University Infrastructure | Recorded Future.” Retrieved July 6, 2023, from https://www.recordedfuture.com/chinese-cyberespionage-operations
50 | Ron Deibert (2008). “Tracking GhostNet: Investigating a Cyber Espionage Network.” Information Warfare Monitor.
51 | Intrusion Truth (Group) (n.d.). “Intrusion Truth – 入侵真相.” Retrieved February 6, 2023, from https://intrusiontruth.wordpress.com/
52 | Dakota Cary (2021). “China’s new software policy weaponizes cybersecurity research” [Text]. Retrieved July 19, 2022, from The Hill https://thehill.com/opinion/cybersecurity/564318-chinas-new-software-policy-weaponizes-cybersecurity-research/

53 | Micorosoft (2023). Microsoft Digital Defense Report 2022.
54 | Mandiant (n.d.). “Advanced Persistent Threat (APT) Groups & Threat Actors.” Retrieved July 9, 2023, from https://www.mandiant.com/resources/insights/apt-groups
55 | Intrusion Truth (Group) (n.d.). “Intrusion Truth – 入侵真相.” Retrieved February 6, 2023, from https://intrusiontruth.wordpress.com/
56 | Cary, Dakota (2021). “China’s next generation of hackers won’t be criminals. That’s a problem.” Retrieved July 13, 2023, from TechCrunch https://techcrunch.com/2021/11/12/chinas-next-generation-of-hackers-wont-be-criminals-thats-a-problem/
57 | Intrusion Truth (Group) (n.d.). “Intrusion Truth – 入侵真相.” Retrieved February 6, 2023, from https://intrusiontruth.wordpress.com/
58 | Hauke Gierow (2018). Chinese hackers are expected to put their country first | Merics. Retrieved from https://merics.org/en/analysis/chinese-hackers-are-expected-put-their-country-first
59 | “http://tianfucup.com” (n.d.). Retrieved July 14, 2023, from https://web.archive.org/web/20230205165552/https://www.tianfucup.com/
60 | Patrick Howell O’Neill (2021). “How China turned a prize-winning iPhone hack against the Uyghurs | MIT Technology Review.” Retrieved July 14, 2023, from https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/
61 | Cary, Dakota (2021). “China’s National Cybersecurity Center. A Base for Military-Civil Fusion in the Cyber Domain”. CSET Analysis.
62 | Intrusion Truth (Group) (n.d.). “Intrusion Truth – 入侵真相.” Retrieved February 6, 2023, from https://intrusiontruth.wordpress.com/
63 | Cary, Dakota (2021). “China’s next generation of hackers won’t be criminals. That’s a problem.” Retrieved July 13, 2023, from TechCrunch https://techcrunch.com/2021/11/12/chinas-next-generation-of-hackers-wont-be-criminals-thats-a-problem/
64 | Ministry of Defense (2022). Eastern Theatre Command concentrates on strengthening joint efforts (东部战区着力强化联合作战指挥能力建设). Retrieved from https://www.mod.gov.cn/gfbw/wzll/dbzq/4921131.html
65 | Fire Eye (2015). APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION. Retrieved from https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
66 | Mandiant (2013). “APT1 | Exposing China’s Cyber Espionage Units.” Retrieved February 6, 2023, from https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units
67 | Unit 42 (2023). “Threat Brief: Attacks on Critical Infrastructure Attributed to Insidious Taurus (aka Volt Typhoon).” Retrieved July 9, 2023, from Unit 42 https://unit42.paloaltonetworks.com/volt-typhoon-threat-brief/
68 | Siobhan Gorman (https://www.wsj.com/articles/SB123914805204099085). “Electricity Grid in U.S. Penetrated By Spies.”
69 | “Downrange: A Survey of China’s Cyber Ranges” (n.d.). Retrieved July 13, 2023, from Center for Security and Emerging Technology https://cset.georgetown.edu/publication/downrange-a-survey-of-chinas-cyber-ranges/
70 | Intelligence, Microsoft Threat (2023). “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.” Retrieved July 9, 2023, from Microsoft Security Blog https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
71 | Mandiant (2023). “Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475).” Retrieved February 6, 2023, from https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw
72 | “APT41 Initiates Intrusion Campaign Using Multiple Exploits” (n.d.). Retrieved August 21, 2023, from Mandiant https://www.mandiant.com/resources/blog/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
73 | itayc (2023). “The Dragon Who Sold His Camaro: Analyzing Custom Router Implant.” Retrieved July 24, 2023, from Check Point Research https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/
74 | Verfassungsschutz (2023). Verfassungsschutzbericht 2022.
75 | Muncaster, Phil (2023). “North Korea Makes 50% of Income from Cyber-Attacks: Report.” Retrieved July 9, 2023, from Infosecurity Magazine https://www.infosecurity-magazine.com/news/north-korea-makes-50-income/
76 | Caesar, Ed (2021). “The Incredible Rise of North Korea’s Hacking Army.” The New Yorker. Retrieved from https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army
77 | HvS Consuling AG (n.d.). “Spione, die sich als Hacker tarnen.” Retrieved July 10, 2023, from https://www.hvs-consulting.de/threat-intelligence-report-emissary-panda-apt27/
78 | Jai Vijayan (2022). “Chinese APT Group Likely Using Ransomware Attacks as Cover for IP Theft.” Retrieved July 10, 2023, from Dark Reading https://www.darkreading.com/attacks-breaches/chinese-apt-ransomware-attacks-cover-ip-theft
79 | Knickmeier, Susanne (2018). Wirtschaftsspionage, Konkurrenzausspähung : “Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how!” https://doi.org/10.30709/2018-005

ACKNOWLEDGEMENTS

The author thanks Wendy Chang for additional research
and Jeroen Groenewegen-Lau and Mikko Huotari for feedback.

CONTACT
Antonia Hmaidi, MERICS
Analyst, Science, Technology and Innovation Policy
antonia.hmaidi@merics.de

EDITORIAL TEAM
Claudia Wessling
Director Communications
and Publications, MERICS
claudia.wessling@merics.de

Nick Bouchet
Freelance Editor

GRAPHICS AND LAYOUT
STOCKMAR+WALTER Kommunikationsdesign

PUBLISHER
MERICS | Mercator Institute for China Studies
Klosterstraße 64 | 10179 Berlin
Tel.: +49 30 3440 999 0
Mail: info@merics.de
www.merics.org

Printed in Berlin, Germany

ISSN (Print): 2941-5799
ISSN (Online): 2941-5608
Druck: Berlin, Deutschland