Hacking for ca$h

Is China still stealing Western IP?

Dr Adam Segal, Dr Samantha Hoffman, Fergus Hanson and Tom Uren
About the authors

**Dr Adam Segal** is the Ira A Lipman chair in emerging technologies and national security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations (CFR). An expert on security issues, technology development and Chinese domestic and foreign policy, Segal was the project director for the CFR-sponsored Independent Task Force report, Defending an open, global, secure, and resilient internet. His book The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age (PublicAffairs, 2016) describes the increasingly contentious geopolitics of cyberspace. His work has appeared in the Financial Times, The Economist, Foreign Policy, The Wall Street Journal and Foreign Affairs, among other publications. He currently writes for the Net Politics blog.

**Dr Samantha Hoffman** is a Non-resident Fellow at the International Cyber Policy Centre at ASPI and Visiting Academic Fellow at the Mercator Institute for China Studies (MERICS) in Berlin. Her research focuses on Chinese state security policy, social management and cyberspace issues. She holds a PhD in Politics and International Relations from the University of Oxford (2017), an MSc in Modern Chinese Studies from the University of Oxford (2011) and BA degrees in International Affairs and East Asian Languages and Cultures from the Florida State University (2010). Her work has appeared in War on the Rocks, The National Interest, China Brief, Forbes, Jane’s Intelligence Review and The Strategist. She has been quoted in global media outlets, including Foreign Policy, The Wall Street Journal, The Washington Post, the Financial Times, Science magazine and Wired magazine.

**Fergus Hanson** is the Head of the International Cyber Policy Centre. He is the author of Internet wars and has published widely on a range of cyber and foreign policy topics. He was a Visiting Fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the take-up of new technologies by the US Government. He has worked for the UN and as a Program Director at the Lowy Institute and has served as a diplomat at the Australian Embassy in The Hague. He has been a Fellow at Cambridge University’s Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum.

**Tom Uren** is a Visiting Fellow in ASPI’s International Cyber Policy Centre, seconded from the Department of Defence. He has worked in various analytical and operational areas in Defence and has diverse expertise in internet and cyber issues. He is researching and writing on international and domestic cyber issues. He has a BSc(Hons) in Molecular Biology and previously worked for CSIRO, researching molecular genetics.

**What is ASPI?**

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia’s defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

**ASPI International Cyber Policy Centre**

The ASPI International Cyber Policy Centre’s mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors.

**Important disclaimer**

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

**ASPI**

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategytist.org.au
facebook.com/ASPI.org
@ASPI_ICPC
www.aspi.org.au/icpc/home

© The Australian Strategic Policy Institute Limited 2018

This publication is subject to copyright. Except as permitted under the Copyright Act 1968, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.

First published September 2018

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be re-published under the Creative Common License Attribution-Share Alike. Users of the image should use this sentence for image attribution: ‘Illustration by Wes Mountain, commissioned by ASPI’s International Cyber Policy Centre’.
Hacking for ca$h

Is China still stealing Western IP?

Dr Adam Segal, Dr Samantha Hoffman, Fergus Hanson and Tom Uren

Issues Paper
Report No. 2/2018
Introduction

In September 2015, following mounting pressure exerted by the US on China, Chinese President Xi Jinping agreed to a US proposal that neither country would steal the other’s intellectual property (IP) for commercial gain. This bilateral agreement was quickly expanded when the US succeeded in inserting similar language into the November 2015 G20 communique. A handful of other countries also pursued their own bilateral agreements.

Three years after the inking of the US–China agreement, this report examines China’s adherence to those agreements in three countries: the US, Germany and Australia. This work involved a combination of desktop research as well as interviews with senior government officials in all three countries.

The rationale for this multi-country report was to examine patterns and trends among countries that had struck agreements with China.

In all three countries, it was found that China was clearly, or likely to be, in breach of its agreements. China has adapted its approach to commercial cyber espionage, and attacks are becoming more targeted and use more sophisticated tradecraft. This improved tradecraft may also be leading to an underestimation of the scale of ongoing activity.

Despite initial hopes that China had accepted a distinction between (legitimate) traditional political–military espionage and (illegal) espionage to advantage commercial companies, assessments from the three countries suggest that this might be wishful thinking.

China appears to have come to the conclusion that the combination of improved techniques and more focused efforts have reduced Western frustration to levels that will be tolerated. Unless the targeted states ramp up pressure and potential costs, China is likely to continue its current approach.
In September 2015, presidents Barack Obama and Xi Jinping stood next to each other and declared that neither the US nor the Chinese government ‘will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage’. Despite significant scepticism about whether China would uphold its pledge, cybersecurity companies and US officials suggested that the number of attacks did in fact decline in the first year of the agreement. China inked similar deals with Australia, Canada, Germany and the UK, and, in November 2015, China, Brazil, Russia, the US and other members of the Group of Twenty accepted the norm against conducting cyber-enabled theft of IP. The agreement has been held up as evidence that a policy of public ‘naming and shaming’ tied to a threat of sanctions can change state actions, and as a success by the US and its allies in defining a norm of state behaviour in cyberspace.

There is, however, increasing evidence that Chinese hackers re-emerged in 2017 and are now violating both the letter and the spirit of the agreement. CrowdStrike, FireEye, PwC, Symantec and other companies have reported attacks on US companies, and the Trump administration has claimed that ‘Evidence indicates that China continues its policy and practice, spanning more than a decade, of using cyber intrusions to target US firms to access their sensitive commercial information and trade secrets.’ The initial downturn in activity appears less to be the result of US pressure and more of an internal reorganisation of cyber forces in the People’s Liberation Army (PLA). Moreover, it’s increasingly clear that the number of attacks isn’t the correct metric for the Sino-US cyber relationship. A decline in the number of attacks doesn’t necessarily mean a decrease in their impact on US economic interests, as Chinese operators have significantly improved their tradecraft.

Washington and its allies will soon have to decide what they’re going to do (again) about Chinese industrial cyber espionage. The Trump administration’s approach so far has been indirect, raising China-based hacking in the context of a larger critique of Beijing’s industrial policy and failure to protect IP. Without significant pushback, China is likely to believe that it has reached a new equilibrium with Washington defined by an absolute smaller number of higher impact cyber operations.

The challenge of industrial cyber espionage

For at least a decade and a half, Chinese hackers have conducted a widespread campaign of industrial cyber espionage, targeting private sector companies in an effort to steal IP, trade secrets and other information that could help China become economically more competitive. President Xi has set the goal for China to become a ‘world leading’ science and technology power by 2049, and the country has significantly ramped up spending on research and development, expanded enrolment in science, technology, engineering and mathematics disciplines at universities, and pushed industrial policy in areas such as semiconductors, artificial intelligence and quantum computing. However, the country also continues to rely on industrial espionage directed at high-technology and advanced manufacturing companies. Hackers have also reportedly targeted the negotiation strategies and financial information of energy, banking, law, pharmaceuticals and other companies. In 2013, the Commission on the Theft of American Intellectual Property, chaired by former Director of National
Intelligence Admiral Dennis Blair and former US Ambassador to China Jon Huntsman, estimated that the theft of IP totalled US$300 billion (A$412 billion, €257 billion) annually, and that 50–80% of thefts were by China.\(^4\)

The US responded to state-sponsored Chinese cyberattacks with a two-step process. First, Washington created a distinction between legitimate espionage for political and military purposes and the cyber-enabled theft of IP. As President Obama framed it:

> Every country in the world, large and small, engages in intelligence gathering. There’s a big difference between China wanting to figure out how can they find out what my talking points are when I’m meeting with the Japanese which is standard and a hacker directly connected with the Chinese government or the Chinese military breaking into Apple’s software systems to see if they can obtain the designs for the latest Apple product. That’s theft. And we can’t tolerate that.\(^5\)

Espionage against defence industries, such as the theft of highly sensitive data related to undersea warfare, first reported in June 2018, would be considered legitimate, and the onus would be on the defender to keep hackers out of its systems.\(^6\)

Second, Washington directly and increasingly publicly confronted Beijing. In the winter of 2013, the incident response firm Mandiant, now part of FireEye, put out a report tracing cyber espionage on American companies to Unit 61398 of the PLA, located in a building on the outskirts of Shanghai.\(^7\) A few days later, the Department of Homeland Security provided internet service providers with the IPs of hacking groups in China. In March 2013, at a speech at the Asia Society, National Security Advisor Tom Donilon spoke of ‘serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale’.\(^8\) When the two met at Sunnylands in June 2013, then President Obama warned President Xi that the hacking could severely damage the bilateral relationship.

In May 2014, the Federal Bureau of Investigation indicted five PLA hackers for stealing the business plans and other IP of Westinghouse Electric, United States Steel Corporation and other companies.\(^9\) In April 2015, the President signed an executive order that would allow for economic sanctions against companies or individuals that profited from the ill-gotten gains of cyber theft. The order threatened to block financial transactions routed through the US, limit access to the US market and prevent company executives from travelling through the US. The <i>Washington Post</i> reported in August 2015 that the administration planned to levy those sanctions against Chinese companies.\(^10\) Worried that sanctions or indictments would cast a pall over the September presidential summit, Meng Jianzhu, a member of the political bureau of the Central Committee of the Chinese Communist Party, flew to Washington to make a deal.

### First year decline

In the first year, the available evidence suggested that Beijing was upholding the agreement and that the overall level of Chinese hacking had declined. FireEye released a report in June 2016 that showed the number of network compromises by the China-based hacking groups that it was tracking dropping from 60 in February 2013 to fewer than 10 by May 2016.\(^11\) However, FireEye noted that Chinese hackers...
could drop the total number of attacks while increasing their sophistication. Around the same time, US Assistant Attorney General John Carlin confirmed the company’s findings that attacks were fewer but more focused and calculated.

As the report also noted, the decline began before September 2015, undermining the causal link between US policy and Chinese behaviour. There were two internal factors in play. First, soon after taking office, Xi launched a massive and sustained anticorruption campaign. Many hackers were launching attacks for private gain after work, misappropriating state resources by using the infrastructure they had built during official hours. Hacking for personal profit was caught up in a broad clampdown on illegal activities.

Second, the PLA was engaged in an internal reorganisation, consolidating forces and control over activities. Cyber operations had been spread across 3PLA and 4PLA units, and the General Staff Department Third Department had been managing at least 12 operational bureaus and three research institutes. In December 2015, China established its new Strategic Support Force, whose responsibilities include electronic warfare, cyber offence and defence, and psychological warfare. In effect, PLA cyber forces were told to concentrate on operations in support of military goals and move out of industrial espionage.

The first publicly reported cyber espionage attempts in the wake of the agreement were either against military targets or involved the theft of dual-use technologies that would fall in the grey zone. Cyber industrial espionage attacks didn’t end, but instead were transferred to units connected with the Ministry of State Security. While the organisation of these groups is less well understood, the ministry appears more willing than PLA groups to use contractors to maintain plausible deniability and reduce the risk of attribution.

Several US cybersecurity company analysts have described the ministry groups’ tradecraft as significantly better than that displayed by the PLA. Hackers have made more use of encryption and gone after cloud providers and other IT services that would provide access to numerous targets. In April 2017, for example, security researchers at PwC UK and BAE Systems claimed that China-based hackers were targeting companies through their managed IT service providers. The Israeli cybersecurity company Intezer Labs concluded that Chinese hackers embedded malware in the popular file-cleaning program CCleaner. In June 2018, Symantec attributed attacks on satellite communications and telecommunication companies in the US and Southeast Asia to a China-based group.

**Outlook**

Almost three years after the agreement, judgements on its effectiveness are much harsher. While a former intelligence official argued that US efforts did succeed in getting Beijing to acknowledge a difference between the cyber-enabled theft of IP and political–military espionage, other security researchers were more sceptical. As one put it, ‘Beijing never intended to stop commercial espionage. They just intended to stop getting caught.’ Another believed that Chinese policymakers decided to get credit for a decline in activity that was inevitable in the wake of the PLA reorganisation—a move that had been long in the works.
The Trump administration has pressed Beijing on cyberespionage but as part of much bigger push on trade policy and economic security. In November 2017, the Justice Department indicted three Chinese nationals employed by Chinese cybersecurity firm Boyusec, charging them with hacking into the computer systems of Moody’s Analytics, Siemens AG, and GPS developer Trimble Inc. ‘for the purpose of commercial advantage and private financial gain’. US Government officials reportedly asked for Chinese Government help in stopping Boyusec’s activities, but received no reply. Despite Recorded Future and FireEye claiming a connection between Boyusec and the Ministry of State Security, the indictment didn’t call out Chinese Government support for the hackers.

The US Trade Representative’s March 2018 investigation of China’s policies and practices related to tech transfer and IP states that the US:

- has been closely monitoring China’s cyber activities since this [the September 2015] consensus was reached, and the evidence indicates that cyber intrusions into US commercial networks in line with Chinese industrial policy goals continue. Beijing’s cyber espionage against US companies persists and continues to evolve.

A draft trade framework allegedly provided by US negotiators to their Chinese counterparts, which circulated on Twitter and Weibo in May 2018, calls on Beijing to ‘immediately cease the targeting of American technology and intellectual property through cyber operations, economic espionage, counterfeiting, and piracy’.

The current trade war with China has two sources: US concern about the bilateral trade deficit, and opposition to Beijing’s use of industrial policy and the theft of IP to compete in high-technology areas. While President Trump has been focused on the deficit, those within the administration pressuring Beijing on its mercantilism should push the cyber issue further up the bilateral agenda. A more direct policy would include a statement from a high-level US official, perhaps Secretary of State Michael Pompeo, that the hacking has resumed and that the US is prepared to use Executive Order 13694, ‘Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities’. Soon after, Washington would sanction individuals involved in the hacking as well as the firms that benefit from it.

Even if the White House were to follow such a policy line, it’s likely that Beijing will continue industrial cyber espionage. James Mulvenon argues that Chinese policymakers now believe that they’ve reached a new equilibrium with the US. Shifting industrial cyber espionage to the Ministry of State Security and deploying a higher level of tradecraft have created an equivalent of the hacking conducted by the US National Security Agency. If this is the case, it means that Beijing never truly accepted the distinction that Washington promoted between ‘good’ and ‘bad’ hacking, between cyber-enabled theft to support the competitiveness of Chinese industry and political–military espionage. Instead, Chinese policymakers saw the issue in terms of a high level of relatively ‘noisy’ activity (for which they were likely to get caught and be called out on). Bringing the hacking more in line with what it believes the National Security Agency conducts—a smaller number of hacks that nevertheless give the US large-scale access to Chinese assets—has, in Beijing’s view, resolved the issue. This isn’t the resolution the US hoped for when it first announced the September 2015 agreement, but it may be the one it has to live with now.
Australia

By Fergus Hanson and Tom Uren

The agreement

On 21 April 2017, Following the groundbreaking Obama–Xi agreement in September 2015 and the G20’s acceptance of the norm against the ‘ICT-enabled theft of intellectual property’, Australia and China reached their own bilateral agreement. Buried somewhat within the joint statement that followed the inaugural Australia–China High-Level Security Dialogue was a paragraph on commercial cyber espionage:

Australia and China agreed not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of obtaining competitive advantage.

As with previous agreements, the statement made an implicit distinction between tolerable espionage for political–military reasons and unacceptable espionage for commercial gain.

Both countries also agreed to act in accordance with the reports of the UN Group of Governmental Experts. The two countries agreed to establish a mechanism to discuss cybersecurity and cybercrime issues with a view to preventing cyber incidents that could create problems between them. This was highlighted in Australia’s International Cyber Engagement Strategy, in which Australia’s dialogues with other states, including China, were characterised as ‘an opportunity to deepen understanding of responsible state behaviour in cyberspace and foster cooperation to deter and respond to malicious cyber activities’.

In China, the agreement received very limited attention. Xinhua produced a translation of the joint statement, which was then reproduced by the People’s Daily and posted on the Minister of Justice’s website.

In Australia it received more attention, but the government wasn’t naïve about the prospects for success. The Ambassador for Cyber Affairs, Tobias Feakin, was reported as saying ‘We do go into these things with our eyes wide open’.

Pre-agreement commercial cyber espionage

Reliable public accounts of nation-state cyber espionage in Australia are hard to come by. Both government and industry have been reticent about openly attributing hacks and data breaches to particular nations. The Australian Government has also only more recently begun to ramp up its efforts to deal with the challenge of cybersecurity. The 2009–10 annual report of the Australian Security Intelligence Organisation (ASIO) stated that ‘cyber espionage is an emerging issue’. Since that time, ASIO’s annual reports have consistently mentioned that cyber espionage affecting commercial interests and for commercial intelligence is occurring, although details of what’s been stolen and by whom are omitted.
The Australian Cyber Security Centre (ACSC) Threat reports, issued from 2015, have also consistently mentioned threats to commercial IP and to other sensitive information, such as negotiation strategies or business plans. But, again, the reports fail to provide enough detail to determine whether it was Chinese espionage that occurred for commercial advantage.

While not publicly named, China is regarded as Australia’s primary cyber adversary, including in the area of IP theft. The fact that it remains unnamed in public statements from the government is perhaps the start of the explanation of why Australia’s policy response so far has been ineffective.

The miners

Australia is a large and significant exporter of iron ore, nickel, coal and other mineral resources to China. Iron ore is particularly significant in the trading relationship—China is the world’s largest importer and Australia the largest exporter, and in 2017 over 80% of Australian iron ore exports were to China.

Although iron ore contracts are now based on monthly average prices, in the lead-up to 2010 iron ore prices were negotiated between buyers and sellers in fixed one-year contracts. Iron ore exports to China were large and growing rapidly, and the price negotiations had tremendous importance for the companies, economies and governments involved. Furthermore, a possible takeover bid for Rio Tinto from BHP led the state-owned Aluminium Corporation of China, Chinalco, to take an overnight 9% stake in Rio Tinto.

In this high-stakes environment, all three major iron ore miners in Australia were the victims of cyber espionage that was informally attributed to China. Given the large volume of iron ore trade, any information that could provide advantage in negotiations would be tremendously valuable. In 2012, MI5 Director-General Jonathan Evans revealed that an attack had cost a company—subsequently revealed to be Rio Tinto—an estimated £800 million (US$1.04 billion, A$1.43 billion, €891 million) in lost revenue, ‘not just through intellectual property loss but also from commercial disadvantage in contractual negotiations’.

It also seems that a bribery case against a Rio Tinto executive and Chinese-born Australian citizen was used to enable further cyber espionage. It’s reported that their Rio Tinto credentials were used to download material from the Rio Tinto corporate network after they were arrested in China. If true, this sensational allegation directly links Chinese law enforcement actions to commercial espionage.

There have been no reports quantifying them, but the commercial losses arising from cyber espionage at BHP and Fortescue Metals Group could be similarly substantial.

Since 2010, the mechanisms that determine prices are now based on market fluctuations, so the very strong incentives to gather information on annual price negotiations have been diminished. However, the high priority that the Chinese Communist Party gives to the secure supply of raw materials means there’s still an ongoing interest in gathering commercial intelligence on Australian mining companies.
The Bureau of Meteorology

In 2015, the Australian Bureau of Meteorology was compromised and a foreign intelligence service — subsequently reported to be Chinese — searched for and copied ‘an unknown quantity of documents from the Bureau’s network’. In this case it’s hard to definitively categorise the underlying motive. There doesn’t seem to be a direct motive to gather government or defence intelligence, but the bureau’s network could have been used as a launching point for further attacks into government networks. IP theft seems likely, as the bureau is a leading science-based services organisation in Australia, has strong international research partnerships and is involved in international research and development programs. Its compromise also provides the opportunity for widespread economic disruption, given that airlines, logistics organisations and industries such as agriculture rely on its services to operate. Its significant weather forecasting and supercomputer expertise would be valuable, too. But for all that this potential IP would be worth, it’s hard to confirm that it was both stolen and used for commercial advantage.

Operation Cloud Hopper

In April 2017, BAE Systems and PwC UK released a report into what they called Operation Cloud Hopper, a systematic global espionage campaign that compromised managed IT service providers, which remotely manage customer IT and end-user systems and generally have direct and unfettered access to client networks. The successful compromise of managed service providers for espionage allows considerable access to client networks and data.

This operation was attributed to a China-based group that’s widely known as APT 10 and Stone Panda. CERT Australia identified 144 partner companies that could have been affected. However, it isn’t publicly known which companies were affected and what was stolen.

Summary

Official statements from ASIO and the ACSC indicate that commercial espionage before 2017 was a large and growing concern, but several factors make it difficult to determine who was stealing data and why they were doing it.

First, both government and business remain reluctant to formally attribute attacks to states because of both technical uncertainty (it takes time, skill and effort to develop high levels of confidence) and because of fears of damaging possibly important diplomatic, economic and intelligence relationships.

Second, Australia implemented a data breach notification law only in February 2018, and that law doesn’t apply to the theft of IP and commercial-in-confidence data.

Finally, before the ACSC was formally assigned whole-of-economy responsibilities in July 2018, there was no cybersecurity centre of gravity that could determine whether formal attribution was desirable and necessary.
Post-agreement commercial cyber espionage

The Australian National University hack

In July 2018, it was reported that Chinese hackers had ‘successfully infiltrated the IT systems at the Australian National University’ (ANU) and that a remediation effort had been ongoing for several months. As with the Bureau of Meteorology, it’s hard to definitively determine what was stolen and for what purpose. The ANU conducts research that has a wide range of applications, including defence, strategic and commercial applications, and it isn’t known what was stolen.

Many ANU graduates subsequently work in the Australian Government, and the ANU also hosts the National Security College, which conducts courses for defence and intelligence officials. Access to ANU IT systems would possibly be of value to enable follow-on espionage. Disentangling all the possible uses that access to ANU could have been used for is impossible without a forensic accounting of what was stolen. In August, the university advised that ‘current advice is that no staff, student or research data has been taken’, although that assessment was questioned by the International Cyber Policy Centre.

The only publicly known target of Chinese hacking—the ANU—isn’t directly a government or military espionage target, but it’s possible the stolen data won’t be used for commercial gain (and therefore falls outside the scope of China’s agreement with Australia).

Outlook

Despite China’s commitments to Australia and the limited public evidence of commercial cyber espionage, Beijing doesn’t appear to have ceased commercial cyber espionage activities in Australia.

However, assessing the scale of China’s ongoing commercial cyber espionage activity is difficult. The Australian Government has been reluctant to publicly name and shame adversary states engaging in cyber theft for commercial gain. China has also improved its tradecraft, making detection harder and perhaps leading to a mistaken perception that activity has become more focused. This professionalisation followed the exposure of the PLA’s previously sloppy tradecraft and probably the internal restructure (mentioned in the ‘United States’ section of this report) that shifted responsibility for commercial cyber espionage from the PLA to the Ministry of State Security. Australia also has relatively less commercially attractive IP than countries such as the US and Germany, so few examples come to light.

Official statements from ASIO and the ACSC don’t reflect a significant decline in the threat of IP or commercial-in-confidence data theft. Public statements from government officials and the publicly known target—a university—don’t indicate a significant change in the nature of Chinese cyber espionage. While this review indicates how difficult it is to clearly identify cyber espionage for competitive advantage, China remains Australia’s primary cyber adversary and is making greater efforts to disguise and focus its commercial cyber espionage.
In a partial nod to keeping its agreements, China seems to be focusing on the theft of dual-use and national security related data. For China, this seems to incorporate a fairly wide range of sectors (such as mining) that goes well beyond sectors such as defence.

To begin the process of increasing pressure on China to adhere to its agreements, Australia should identify opportunities to formally name adversary states, including China, in public documents and statements. A good place to start is the annual ACSC Threat report. Australia should also consider partnering with states subjected to similar IP theft by China to build and sustain pressure on Beijing to adhere to its agreements. The G20 offers a multilateral venue for keeping up pressure, but other ad hoc opportunities should also be identified.

Germany

By Dr Samantha Hoffman

Consultation mechanism

No formal bilateral agreement on preventing commercial cyber espionage exists between Germany and China. However, a joint declaration from the June 2016 4th China–Germany Intergovernmental Consultations stated that the two governments would set up a ‘bilateral cyber security consultation mechanism’. Both sides also agreed that neither operates or knowingly supports ‘the infringement of intellectual property, trade or business secrets through the use of cyberspace in order to attain competitive advantage for their businesses or commercial sectors’.

The first cybersecurity consultation wasn’t held until 17 May 2018. Efforts to establish the consultation were delayed, in part because the two sides had different expectations regarding topics and participants. The delays also led to a public exchange between German Ambassador to China Michael Clauss and the Chinese Foreign Ministry. In a December 2017 interview with the Hong Kong-based South China Morning Post, Clauss was quoted saying that he expected the Chinese Government to join Germany in setting up the agreed consultation mechanism. He also said, ‘Our repeated requests to have a meaningful dialogue on [virtual private networks] and cyber-related questions with the relevant Chinese authorities have regrettably not yet received a positive response.’ The comments prompted a reply from Chinese Foreign Ministry spokeswoman Hua Chunying, who claimed, ‘China has repeatedly invited a German delegation to China for consultation, but Germany has never responded on time … It’s unreasonable for Germany now to criticise Beijing for not being sincere.’

The eventual May 2018 consultation, which took place in Beijing, was co-chaired by Chinese Vice Minister of Public Security Shi Jun and German Parliamentary State Secretary at the Federal Ministry of the Interior Professor Dr Günter Krings. The German Government insisted that the Ministry of Public Security and a member of the Central Political and Legal Affairs Commission were also present.
Although the meeting was officially described as a success, no tangible progress was made during the consultation to substantively address key issues. The German Government insisted that discussion focus on commercial cyber espionage and issues such as data protection and virtual private networks. These were all topics that the Chinese Government preferred to avoid. The Chinese Government instead wanted to discuss cybercrime and cyber terrorism, but there are major differences in the way those concepts are defined. Chinese officials have regularly pushed the German Government to deport political opponents in the Uyghur community, which Berlin has continually refused to do because Beijing can provide no evidence to support its claims.

The cyber consultation was again discussed during the July 2018 5th China–Germany Intergovernmental Consultations in Berlin. A joint statement said that the consultation would continue as a key platform for discussing cyber issues, including cross-border data protection and IP and trade infringements.

**Dealing with commercial cyber espionage**

The 2016 and 2017 editions of the German Federal Ministry of the Interior’s *Annual report on the protection of the Constitution* (published in July 2017 and July 2018, respectively) both specifically identified China alongside Russia and Iran as the primary countries responsible for espionage and cyberattacks against Germany. The reports said that ‘Chinese intelligence services focus on industry, research, technology and the armed forces (structure, armament and training of the Bundeswehr, modern weapons technology).’ A separate July 2017 report by Bitkom, Germany’s digital industry association, found that German companies lose €55 billion (US$64 billion, A$88 billion) annually due to commercial cyber espionage affecting about 53% of German companies.

The number of known China-originated commercial cyber espionage attacks against German companies dropped in the past two years, according to the head of the Federal Office for the Protection of the Constitution (BfV), the German domestic intelligence agency. Other German Government officials confirmed the appearance of a decrease, but added that they’re unsure whether there had been one. There’s an equally high likelihood that cyber espionage has become more sophisticated, and better targeted, and therefore has been undetected.

The decline in known cyber espionage incidents has also been linked to a sharp increase in Chinese foreign direct investment in high-tech and advanced manufacturing industries in 2016. The BfV head, Hans-Georg Maassen, made a similar claim and linked the decline with an increase in the use of legal tools for obtaining the same information, such as corporate takeovers. Maassen said ‘industrial espionage is no longer necessary if one can simply take advantage of liberal economic regulations to buy companies and then disembowel them or cannibalise them to gain access to their know-how.’

The German Government took steps in July 2017 to address concern by amending the Foreign Trade and Payments Ordinance to tighten restrictions on non-EU foreign investment in Germany. The move was partly triggered by the €4.5 billion (US$5.3 billion, A$7.2 billion) takeover of German industrial robotics maker Kuka by Chinese appliance maker Midea.
The amendment identified several sectors that would be subject to higher scrutiny. They include companies operating critical infrastructure, IT and telecommunications, and certain cloud computing providers. Previously, non-EU companies weren’t obliged to inform the government of an acquisition (of 25% or more of voting rights) of a German company unless they were involved in the development and manufacturing of defence and encryption technology. The July 2017 amendment, however, expanded the notification requirement to include critical infrastructure and other security-related technology. The amendment refers to sectors identified in the 2013 Foreign Trade and Payments Ordinance section 55, which include energy, water, IT, financial services, insurance, transportation, food and health.

The amendment also extended the period for the Ministry of Economic Affairs and Energy to conduct reviews. There are two foreign investment review categories: ‘cross-sectoral investment review’ and ‘sector-specific investment review’. Cross-sector reviews apply to the acquisition of any company where the investor is located outside the EU or the European Free Trade Association and plans to acquire ownership of 25% or more. Sector-specific reviews apply to the acquisition of a company that operates in sensitive security areas. In addition to military weapons and equipment, this includes ‘products with IT security features that are used for processing classified government information’. Similar rules apply for companies that operate high-grade remote sensing systems under the Act on Satellite Data Security. Previously, the ministry was required to conduct a cross-sectoral investment review within two months, but is now given four months. For sector-specific reviews, it was previously required to conduct a review within one month and is now given three months.

The German Government has further identified a need to tighten controls on the loss of sensitive information in the area of cross-border data protection.

Outlook

Assessing the scale of Chinese commercial espionage activity is difficult, and very little information is made publicly available. The German Government remains sceptical about China’s commitment to cease the infringement of IP, trade or business secrets through the use of cyberspace. However, the government feels that some dialogue is better than no dialogue. It hopes to leave open the possibility of a more intensive dialogue in future. One German official said that the government is pushing for the Chinese side to ‘behave as [it would] wish to be treated’ in an increasingly interconnected world.
Notes

2. G20 Leaders’ Communique, Antalya Summit, 15–16 November 2015, online.
7. Mandiant, APT1: exposing one of China’s cyber espionage units, 2013, online.
11. FireEye, Red line drawn: China recalculates its use of cyber espionage, June 2016, online.
13. Tim Johnson, ‘China backed off from hacking US companies. Now it is at it again’, The Sacramento Bee, 7 June 2021, online.
15. Chris Bing, ‘Research claims CCleaner attack carried out by Chinese-linked group’, Cyberscoop, 2 October 2017, online.
17. US District Court, ‘United States of America v. Wu Yingzhuo, Dong Hao, Xia Lei’, 13 September 2017, online.
19. Office of the US Trade Representative, Findings of the investigation into China’s acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974, 22 March 2018, online.
21. The President, ‘Taking additional steps to address the national emergency with respect to significant malicious cyber-enabled activities’, Federal Register, 3 January 2017, 82(1), online.
22. G20 Leaders’ Communique, Antalya Summit, 15–16 November 2015, online.
27. ASIO Report to Parliament 2009–10, online.
28. ACSC Threat report 2015, online; 2016, online; 2017, online.
29. DFAT, Trade statistical pivot tables, March 2018, online.
33. Chellel et al., ‘When Rio Tinto met China’s iron hand’
34. Chris Uhlmann, China blamed for ‘massive’ cyber attack on Bureau of Meteorology computer, ABC Online, 2 December 2015, online.
Hacking for ca$h: Is China still stealing Western IP?

40 ‘Gemeinsame Erklärung anlässlich der 4. Deutsch–Chinesischen Regierungskonsultationen (Joint declaration of the Fourth Intergovernmental Dialogues)’, German Federal Government, 13 June 2016, online.
41 ‘Zusammenarbeit mit China durch erfolgreich durchgeführten ersten deutsch—chinesischen Cyberkonsultationsmechanismus untermauert (Cooperation with China reinforced with successful first German–Chinese Cyber Consultation Mechanism)’, German Ministry of the Interior, 18 May 2018, online.
42 ‘Zusammenarbeit mit China durch erfolgreich durchgeführten ersten deutsch—chinesischen Cyberkonsultationsmechanismus untermauert (Cooperation with China reinforced with successful first German–Chinese Cyber Consultation Mechanism)’.
43 ‘Joint declaration from the fifth German–Chinese intergovernmental consultations’, 9 July 2018, online.
47 Andrea Shalal, ‘Germany risks losing key technology in Chinese takeovers—spy chief’, *Reuters*, 11 April 2018: online.
48 Shalal, ‘Germany risks losing key technology in Chinese takeovers—spy chief’.
49 *Foreign Trade and Investment Law: investment reviews*, Federal Ministry for Economic Affairs and Energy, no date, online.
51 *Foreign Trade and Investment Law: investment reviews; Foreign Trade and Payments Ordinance.*
52 *Foreign Trade and Investment Law: investment reviews; Foreign Trade and Payments Ordinance.*
53 *Foreign Trade and Investment Law: investment reviews; Foreign Trade and Payments Ordinance.*
54 *Foreign Trade and Investment Law: investment reviews.*
55 *Foreign Trade and Investment Law: investment reviews.*

**Acronyms and abbreviations**

ACSC  Australian Cyber Security Centre  
ANU   Australian National University  
ASIO  Australian Security Intelligence Organisation  
BfV   Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution; Germany)  
CFR   Council on Foreign Relations  
EU    European Union  
IP    intellectual property  
IT    information technology  
PLA   People’s Liberation Army  
UN    United Nations
Some previous ICPC publications

- *Cyber Maturity in the Asia-Pacific Region 2017*
- *Weibo diplomacy and censorship in China*
- *Deterrence in cyberspace*
- *When the winner takes it all: Big data in China and the battle for privacy*
- *Social credit: Technology-enhanced authoritarian control with global consequences*
- *Technological entanglement: Cooperation, competition and the dual-use dilemma in artificial intelligence*