EuRepoC

ADVANCED PERSISTENT THREAT profile

APT3/Boyusec

Going for industrial secrets, going dark...?

Associated APT designations

- **APT3** (Mandiant)
- **Gothic Panda** (CrowdStrike)
- **TG-0110** (Secureworks Counter Threat Unit)
- **Buckeye** (Symantec)
- **Bronze Mayfair** (Secureworks)
- **UPS Team** (origin unclear)
- **Group 6** (reportedly Talos)

Sources: [1], [2], [3], [4]

Country of origin

Time period of activity

2009-2017*

*According to threat intelligence company SecureWorks, the group started its activities in 2006.
According to the threat intelligence company Symantec, and in contrast to most of the other tracked Chinese APT groups (besides APT1), APT3 operations appeared to cease in mid-June 2017.

Sources: [5], [6], [8], [9], [10]

Political affiliations

The group's political affiliation was mainly revealed in 2017 when various actors published attribution statements that linked APT3 with the Chinese information security company Guangzhou Boyu Information Technology Company, Ltd. (Boyusec), based in Guangzhou, which was acting as a front for the Chinese Ministry of State Security (MSS). The reporting culminated in an unsealed indictment by the United States Department of Justice (DoJ) in November 2017, which identified three Chinese nationals as Boyusec employees. Previously, in May, threat intelligence company Recorded Future had linked Boyusec to the work of APT3 and reaffirmed public reporting from 2016 that Boyusec worked on behalf of the MSS, for the first time stating this attribution "with a high degree of confidence." On 29 November 2016, *The Washington Free Beacon* reported that intelligence officials from the Pentagon had identified Boyusec as a contractor of the MSS. The article also identified Huawei as one of Boyusec's industry partners, cooperating on security products and allegedly entailing a backdoor for intelligence purposes. Recorded Future furthermore added Guangdong ITSEC to the list of Boyusec's cooperation partners, stating that the company is a "subordinate to an MSS-run organization called China Information Technology Evaluation Center (CNITSEC)" and had been working with Boyusec on a joint active defence lab starting in 2014.

Sources: [5], [7], [22], [28]

By Kerstin Zettl-Schabath, Benjamin Butz, and Camille Borrett

Most frequent targets

 **Belgium**

 **United Kingdom**

 **Hong Kong**

 **India**

 **Italy**

 **Luxembourg**

 **Philippines**

 **United States**

 **Sweden**

The group mainly focused on targets of strategic importance for the Chinese Communist Party, as well as targets vital for China's economic interests and military modernisation. The attacked entities included targets in aerospace, defence, construction and engineering, telecommunications, and transportation.

A significant change in APT3's targeting patterns emerged around 2015, when it shifted from primarily US-based targets to political entities in Hong Kong, presumably due to upcoming parliamentary elections in 2016. This stands in contrast to the overall change of responsibilities between the two main Chinese actors in cyberspace, the MSS and the People`s Liberation Army (PLA). Prior to President Xi Jinping restructuring the PLA and establishing the "Strategic Support Force" (SSF) in 2015, the PLA had mainly been in charge of economically-oriented espionage. Through the SSF, the PLA could focus more strongly on military cyber operations in the context of armed conflict. As a result, the MSS subsequently shifted its focus more towards economic espionage, which is how APT3's targeting history and shift towards political targets in Hong Kong deviates from this overall development. However, the formal domestic mandate of the MSS could also explain APT3's focus on Hong Kong. Why this particular group was charged with that task can only be speculated. One possible reason could be the (relative) geographical proximity of Guangzhou to Hong Kong, which could be operationally advantageous for cyber operations that required a certain local presence. Additionally, if one assumes that APT3 was guided by a local or regional MSS office in that area, formal responsibilities for Hong Kong could have played a role here. Most recently, in August 2023, threat intelligence company Symantec disclosed a supply chain operation by a previously-unknown hacker group dubbed "Carderbee" against targets in Hong Kong, with at least some circumstantial evidence pointing to Chinese culpability. This likely reflects the fluid Chinese APT ecosystem in which new actors appear over time.

Sources: [4], [11], [13], [25], [26], [29], [30], [38]

Agency type

State-ordered hacking group

Based on the Pentagon and NSA reports leaked by *The Washington Free Beacon* in 2016, APT3 maintained a direct connection to the MSS. In 2014, Boyusec established a joint active defence laboratory (ADUL) in cooperation with Guangdong ITSEC, a subordinate to the China Information Technology Evaluation Center (CNITSEC) organisation, which is run by the MSS. CNITSEC is said to execute vulnerability testing and reliability assessments of software for the Ministry. The vulnerabilities found by CNITSEC were then allegedly used for intelligence operations by the MSS.

According to Scott Henderson from FireEye, Boyusec also maintained a relationship with the Guangdong Provincial Information Security Assessment Center, another organisation with a purported connection to the MSS.

Furthermore, the group's extensive operations against technological companies in the US and the UK, as well as its gradual shift towards targets in Hong Kong, reflected the economic and geopolitical interests of the Chinese government. Many of the targets attacked by APT3 belonged to the sectors of the 13th Five-Year Plan, covering the period 2016 to 2020.

Even if APT3 could be plausibly considered as "state-ordered," the exact degree of control the MSS had over the group remains unclear.

Sources: [6], [7], [14], [22], [31]

Group Composition and Organisational Structure

The 2017 US DoJ indictment disclosed the names of three members of APT3. According to public statements from the end of the 1990s, the MSS had already consisted of "tens of thousands" of employees. Given the steadily growing importance of the MSS for China's cyber-digital ambitions, one can expect this number to be significantly higher today. Moreover, according to public reporting from 2017, the number of subordinate branch offices of the Shanghai State Security Bureau (SSSB) of the MSS alone was estimated at 18 at that time. The three indicted individuals therefore presumably represented only a part of APT3's structure and an even smaller part of the MSS, since several other APTs (e.g., APT10) were and are also associated with it. Based on the attack infrastructure and the technically-demanding operations, it seems plausible that APT3 had a substantial personnel capacity.

Sources: [13], [14], [26], [32]

Impact Type(s)

- **Intelligence Impact; Disinformation Impact** (DoublePulsar Backdoor, 2016 - 2018; Hack against Hong Kong government entities, 2016)
- **Economic/financial impact** (operations against Siemens AG, Moody's Analytics, and Trimble Inc.)

Sources: [11], [13], [18]

Incident Type(s)

- **Data theft/hijacking with misuse** (economically motivated cyber-espionage against high-profile sectors, such as aerospace and defence, construction and engineering, energy, technology, telecommunications, and transportation sectors, as well as non-profit organisations)

- **Intelligence gathering/surveillance** (In March 2016, the group shifted its focus primarily to political entities and critics in Hong Kong.)

Sources: [4], [5], [11], [12], [13], [14], [18], [25]

Threat Level Index

10/24 moderate threat level

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC Dataset 1.0. It is a composite indicator covering five dimensions: the sectorial and geographical scope of the APT's attacks, the intensity of the attacks, the frequency of attacks and the use of zero-days. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here and here.

Threat level sub-indicator	Score	Explanation
Intensity of attacks	1 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information
Sectorial scope of attacks	2 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. Incidents attributed to APT3 in the EuRepoC database, targeted, on average only 1 sector per attack but the majority of all incidents were against state institutions/political systems or critical infrastructure.
Geographical scope of attacks	2 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of APT3, on average two countries were targeted per incident attributed to the group in the EuRepoC database.
Frequency of attacks	2 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. APT3 was responsible for less than 1 incident per year of activity (0.6).
Exploitation of Zero days	3 /3	This indicator calculates the percentage of attacks attributed to the APT that use one or multiple zero days. The score obtained is then converted to a three-level scale. A higher proportion of incidents attributed to APT3 made use of zero-days compared to other APT groups analysed.

→ Overall, APT3 obtains a moderate-level threat score compared to other APT groups. The cyber incidents analysed within the EuRepoC framework had a low intensity regarding their physical and socio-political effects, while also having limited geographical reach and a low frequency. On the other hand, incidents attributed to the group were above average in terms of use of zero-days.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

The group used a combination of custom-made and publicly-available tools. In addition, it exploited both zero-days and known vulnerabilities for its spearphishing campaigns. The change in direction from zero-day exploits to known vulnerabilities was particularly evident with Operation Double Tab, which was believed to be a change in strategy to increase the number of attacks. In 2017, the Shadow Brokers group leaked tools from the espionage group Equation Group, but these tools had already been utilised in attacks by APT3 a year earlier, which further underlines the group's extensive skills in vulnerability detection.

Malware and tools used (non-exhaustive)

Schtasks	CookieCutter (aka Pirpi)	Shotput
APT3 Keylogger	Bemstour	DoublePulsar
EternalBlue	HTran	Hupigon
LaZagne	OSInfo	PlugX
RemoteCMD	Sogu	EternalSynergy

Techniques Used

Account Manipulation	Brute Force	Password Cracking
Credentials from Password Stores	Credentials from Web Browsers	Multi-Stage Channels

User Execution: Malicious Link

Zero-day Exploits

- CVE-2010-3962
- CVE-2014-1776
- CVE-2019-0703
- CVE-2017-0143
- CVE-2015-3113

Sources: [2], [4], [8], [11], [13], [15], [16], [17], [18], [27]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access
Drive-by compromise Phishing: Spearphishing link
MITRE Persistence
Accessibility Features Account Manipulation Create Account Create or Modify System Process: Windows Service Registry Run Keys/Startup Folder Scheduled Task/Job Valid Accounts
MITRE Defense Evasion
Indicator Removal: File Detection Masquerading Obfuscated Files or Information: Indicator Removal from Tools System Binary Proxy Execution: Rundll32 Valid Accounts

Source: [15]

ATTRIBUTION

Attribution milestones

1) FireEye reported on APT3 for the first time (4 November 2010).

2) *The Washington Free Beacon* was the first actor to report on Boyusec's collaboration with the MSS (29 November 2016).

3) Intrusion Truth named Wu Yingzhuo (2 May 2017) and Dong Hao (5 May 2017) as members of APT3 (2 May 2017) and attributed Boyusec to APT3 (9 May 2017).

4) Recorded Future corroborated the triangular attribution regarding APT3, Boyusec, and the MSS with a "high degree of confidence" (17 May 2017).

5) US Justice Department indicted three Chinese Boyusec hackers, including Wu and Dong, without picking up the purported link to the MSS (13 September 2017) .

Sources: [5], [6], [7], [12], [19], [20], [21]

Attribution Ambiguities

Olympic Destroyer 2018: After the disruptive hacking operation against the 2018 Pyeongchang Winter Olympics, Intezer threat intelligence analysts found code fragments uniquely tied to APT3, APT10, and APT12 in the "Olympic Destroyer" malware samples exploited throughout the event, according to a blog post from 12 February 2018. Olympic Destroyer's system credentials stealer and a toolset of APT3 shared 18.5% of their code, both compiled in x64. Moreover, Intezer disclosed multiple different "function-for-function overlaps between the components of Pirpi and Olympic Destroyer."

After public reporting concentrated on North Korean APT group Lazarus as the main suspect for Olympic Destroyer, threat intelligence analysts from Kaspersky indicated Russian responsibility in March 2018, placing blame on APT28 (aka Fancy Bear). A US DoJ indictment unsealed in October 2020 confirmed the attribution to Russia but held another GRU group, Sandworm, responsible.

Use of tools in 2018: According to a report by Symantec from May 2019, in 2016, APT3 used some tools by the Equation Group that were only leaked by the mysterious Shadow Brokers in 2017. Moreover, those tools were exploited until late 2018, in contrast to reports indicating APT3's dissolution in 2017 due to the group's public exposure. It remained unclear if the group passed those tools to another group or if it continued its operations longer than assumed.

Sources: [8], [34], [35], [36], [37]

Attribution and detection sensitivity

In 2016, Symantec reported that APT3 had shifted its focus from companies in the US to political entities in Hong Kong, which could at least partially be due to increased political tensions between the US and China that culminated in the so-called "Obama-Xi" cyber agreement from 2015.

The fact that their operations seemed to stop in June 2017 - immediately after the network of anonymous threat intelligence analysts called "Intrusion Truth" disclosed the links between APT3 and Boyusec (in May) - indicated a noteworthy degree of sensitivity regarding public exposure of the group's identity and its members.

The group's tools continued to be used until the end of 2018, although it is unclear whether this was done by another group or whether APT3 may have continued to operate covertly.

In general, APT3 showed a clear desire to evade detection, e.g., by using so-called "hop points" (private computer networks by third parties) in order to "misrepresent their true IP addresses, location, and identities," as described in the US DoJ indictment from 2017.

Sources: [4], [8], [9], [10], [14], [22], [33]

POLITICAL/LEGAL/LAW ENFORCEMENT ACTIONS

US indictment against three Chinese hackers who worked at internet security firm Boyusec (13 September 2017):

The three Chinese nationals and residents indicted by the US DoJ were Wu Yingzhuo (founding member and equity shareholder of Boyusec), Dong Hao (founding member, equity shareholder, and "Executive Director and Manager" of Boyusec), and Xia Lei (employee of Boyusec). They were charged with computer hacking, theft of trade secrets, conspiracy, and identity theft directed at US and foreign employees, as well as theft from the computers of three corporate victims in the financial, engineering, and technology industries. Allegations focused on intrusions of three US companies between 2011 and May 2017 with the goal to search for, identify, copy, package, and steal data from those computers, including confidential business and commercial information, work products, and sensitive victim employee information. The victims listed in the indictment were the companies Moody's Analytics, Siemens AG ("Siemens"), and Trimble Inc. ("Trimble"). All of the three indicted individuals participated in the hacking operations and no clear functional division of labor could be derived from the indictment. However, Wu appeared to be responsible for the operation against Trimble Inc., Dong for the operation against Siemens, and Xia for the operation against Moody's.

Sources: [14], [19], [22]

Indicted individuals/sanctioned (associated) entities

- **Xia Lei** (employee of Boyusec)
- **Wu Yingzhuo** (founding member and equity shareholder of Boyusec)
- **Dong Hao** ("Executive Director and Manager" as well as founding member and equity shareholder of Boyusec)

Sources: [14], [19], [22]

Landmark operations

Operations against Moody's Analytics, Siemens, and Trimble, 2011 - 2017: APT3 members and Boyusec employees Xia Lei, Wu Yingzhuo, and Dong Hao hacked US companies over the course of multiple years in order to steal intellectual property related to their products and research, according to a US DoJ indictment from 2017.

Operation Double Tap, 2014: The APT exploited the two already-known vulnerabilities, CVE-2014-6332 and CVE-2014-4113, in a spearphishing campaign against unspecified organisations. In this operation, the group used known exploits and conducted social engineering, as well as frequent attacks, which indicated a shift in the operational tempo and strategy of APT3.

Operation Clandestine Wolf, 2015: In 2015, the group exploited the Adobe Flash Player zero-day (CVE-2015-3113) as part of a phishing campaign. The US-based targets were organisations from the following industry sectors: aerospace, defence, construction and engineering, technology, telecommunications, and transportation industries, but also US federal and state agencies.

Sources: [2], [16], [17], [25]

SOURCES

[1] Google sheets. *APT Groups and Operations*. Available at https://web.archive.org/web/20230606114005/https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml [Archived on: 06.06.2023].

[2] Erica Eng, Dan Caselden (2015). *Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign*, Mandiant. Available at https://web.archive.org/web/20230606114443/https://www.mandiant.com/resources/blog/operation-clandestine-wolf-adobe-flash-zero-day [Archived on: 06.06.2023].

[3] Counter Threat Unit Research Team (2014). *Threat Group-0110 Targets Manufacturing and Financial Organizations Via Phishing*, Secureworks. Available at https://www.secureworks.com/blog/threat-group-0110-targets-manufacturing-and-financial-organizations-via-phishing [Archived on: 06.06.2023].

[4] A.L. Johnson (2016). *Buckeye cyberespionage group shifts gaze from US to Hong Kong*, Symantec. Available at https://web.archive.org/web/20230606120346/https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=92a4528c-2bdb-498f-85c8-4273bfdc66aa&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments [Archived on: 06.06.2023].

[5] Recorded Future (2017). *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3*. Available at https://www.recordedfuture.com/chinese-mss-behind-apt3.

[6] Intrusion Truth (2017). *APT3 is Boyusec, a Chinese Intelligence Contractor*. Available at https://web.archive.org/web/20230606120809/https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/ [Archived on: 06.06.2023].

[7] Bill Gertz (2016). *Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service*, Free Beacon. Available at https://web.archive.org/web/20230606121044/https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/ [Archived on: 06.06.2023].

[8] Symantec (2019). *Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak*. Available at https://web.archive.org/web/20230606121250/https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit [Archived on: 06.06.2023].

[9] Intrusion Truth (2018). *The destruction of APT3*. Available at https://web.archive.org/web/20230606121657/https://intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/ [Archived on: 06.06.2023].

[10] Josh Chin (2017). *Chinese Firm Behind Alleged Hacking Was Disbanded This Month*, The Wall Streat Journal. Available at https://web.archive.org/web/20230606121916/https://www.wsj.com/articles/chinese-firm-behind-alleged-hacking-was-disbanded-this-month-1511881494 [Archived on: 06.06.2023].

[11] Cyware (2019). *APT3: A Nation-State Sponsored Adversary Responsible For Multiple High Profile Campaigns*. Available at https://web.archive.org/web/20230606122041/https://cyware.com/blog/apt3-a-nation-state-sponsored-adversary-responsible-for-multiple-high-profile-campaigns-f58c [Archived on: 06.06.2023].

[12] Intrusion Truth (2017). *Who is behind this Chinese espionage group stealing our intellectual property?* Available at https://web.archive.org/web/20230606122345/https://intrusiontruth.wordpress.com/2017/04/26/who-is-behind-this-chinese-espionage-group-stealing-our-intellectual-property/ [Archived on: 06.06.2023].

[13] MITRE (2017). *APT3 Adversary Emulation Plan*. Available at https://web.archive.org/web/20230606122502/https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf [Archived on: 06.06.2023].

[14] US Department of Justice (2017). *United States of America v. WU YINGZHUO, DONG HAO, XIA LEI*. Available at https://web.archive.org/web/20230606123229/https://www.justice.gov/opa/press-release/file/1013866/download [Archived on: 06.06.2023].

[15] MITRE (2021). *APT3*. Available at https://web.archive.org/web/20230606123101/https://attack.mitre.org/groups/G0022/ [Archived on: 06.06.2023].

[16] Pierluigi Paganini (2014). *FireEye discovered a new zero-day exploit for IE in the wild – Operation Clandestine Fox*, Security Affairs. Available at https://web.archive.org/web/20230630080737/https://securityaffairs.com/24403/cyber-crime/fireeye-new-zero-day-ie.html [Archived on: 30.06.2023].

[17] Ned Moran, Mike Scott, Mike Oppenheim, Joshua Homan (2021). *Operation Double Tap*, Mandiant. Available at https://web.archive.org/web/20230606124101/https://www.mandiant.com/resources/blog/operation-doubletap [Archived on: 06.06.2023] .

[18] FireEye Threat Intelligence (2021). *Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak*, Mandiant. Available at https://web.archive.org/web/20230606115217/https://www.mandiant.com/resources/blog/demonstrating-hustle [Archived on: 06.06.2023].

[19] FBI (2017). *BOYUSEC HACKERS*. Available at https://web.archive.org/web/20230606124636/https://www.fbi.gov/wanted/cyber/boyusec-hackers [Archived on: 06.06.2023].

[20] Intrusion Truth (2017). *Who is Mr Wu?* Available at https://web.archive.org/web/20230606125311/https://intrusiontruth.wordpress.com/2017/05/02/who-is-mr-wu/ [Archived on: 06.06.2023].

[21] Intrusion Truth (2017). *Who is Mr Dong?* Available at https://web.archive.org/web/20230606125420/https://intrusiontruth.wordpress.com/2017/05/05/who-is-mr-dong/ [Archived on: 06.06.2023].

[22] US Department of Justice (2017). *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage*. Available at https://web.archive.org/web/20230606125542/https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations [Archived on: 06.06.2023].

[23] Erica Eng, Dan Caselden (2015). *Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign*, Mandiant. Available at https://web.archive.org/web/20230630085116/https://www.mandiant.com/resources/blog/operation-clandestine-wolf-adobe-flash-zero-day [Archived on: 30.06.2023].

[24] Matt Kodama (2014). *Tracking the Clandestine Fox*, Recorded Future. Available at https://web.archive.org/web/20230630085726/https://www.recordedfuture.com/operation-clandestine-fox [Archived on: 30.06.2023].

[25] TeamPassword (2021). *Who is Gothic Panda and how can you protect yourself?* Available at https://web.archive.org/web/20230606125641/https://teampassword.com/blog/who-is-gothic-panda-and-how-can-you-protect-yourself [Archived on: 06.06.2023].

[26] GlobalSecurity (2023). *Ministry of State Security (MSS) - MSS-Budget and Personnel*. Available at https://web.archive.org/web/20230626090101/https://www.globalsecurity.org/intell/world/china/mss-budget.htm [Archived on 26.06.2023].

[27] MITRE ENGENUITY ATT&CK EVALUATIONS (2018). *Overview - APT3*. Available at https://web.archive.org/web/20230217021831/https://attackevals.mitre-engenuity.org/enterprise/apt3/ [Archived on 30.06.2023].

[28] Chris Bing (2017). *DOJ reveals indictment against Chinese cyberspies that stole U.S. business secrets*, Cyberscoop. Available at https://web.archive.org/web/20230923092111/https://cyberscoop.com/boyusec-china-doj-indictment/ [Archived on 23.09.2023].

[29] Elsa B. Kania, John K. Costello (2018). *The Strategic Support Force and the Future of Chinese Information Operations*. Available at https://ia601407.us.archive.org/17/items/the-strategic-support-force-kania-costello/The%20Strategic%20Support%20Force_Kania_Costello.pdf [Archived on 23.09.2023].

[30] Symantec (2023). *Carderbee: PT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong*, Symantec. Available at https://web.archive.org/web/20230923095007/https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse [Archived on 23.09.2023].

[31] Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (eds.) (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Available at https://academic.oup.com/book/25744.

[32] Peter Mattis (2017). *Everything We Know about China's Secretive State Security Bureau*, The National Interest. Available at https://web.archive.org/web/20230923095916/https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459 [Archived on 23.09.2023].

[33] Robert Farley (2018). *Did the Obama-Xi Agreement Work?*, The Diplomat. Available at https://web.archive.org/web/20230923100713/https://thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/ [Archived on 23.09.2023].

[34] Jay Rosenberg (2018). *2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang*, Intezer. Available at https://web.archive.org/web/20180213223547/https://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/ [Archived on 13.02.2018].

[35] Andy Greenberg (2018). *Hackers Have Already Targeted the Winter Olympics—and May Not Be Done*, Wired. Available at https://web.archive.org/web/20230925082633/https://www.wired.com/story/pyeongchang-winter-olympics-cyberattacks/ [Archived on 25.09.2023].

[36] Kaspersky (2018). *Olympic Destroyer: who hacked the Olympics?* Available at https://web.archive.org/web/20230925082843/https://www.kaspersky.com/blog/olympic-destroyer/21494/ [Archived on 25.09.2023].

[37] US Department of Justice (2017). *United States of America v. Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin*. Available at https://web.archive.org/web/20230925083524/https://www.justice.gov/opa/press-release/file/1328521/download [Archived on 25.09.2023].

[38] Jai Vijayan (2017). *APT3 Threat Group a Contractor for Chinese Intelligence Agency*, Dark Reading. Available at https://www.darkreading.com/attacks-breaches/apt3-threat-group-a-contractor-for-chinese-intelligence-agency.

About the authors

- **Kerstin Zettl-Schabath** is a researcher at the Institute of Political Science (IPW) at Heidelberg University.
- **Benjamin Butz** is a research intern at Heidelberg University.
- **Camille Borrett** is a Data Analyst at the German Institute for International and Security Affairs (SWP).

Last updated 25.09.2023