EuRepoC

ADVANCED PERSISTENT THREAT profile

APT 1

Demonstrating the Cumulative Effects of Cyber Operations

Associated APT designations

- **APT1** (Mandiant)
- **Brown Fox** (iSight)
- **Byzantine Candor** (US intelligence community)
- **Comment Crew** (Symantec)
- **Comment Panda** (CrowdStrike)
- **G0006** (MITRE ATT&CK)
- **Group 3** (Cisco Talos)
- **ShadyRAT** (McAfee)
- **TG-8223** (Secureworks)

Sources: [1][2]

Country of origin

Period of activity

2006-2015

Sources: [1][4][5][6]

Political affiliations

In a landmark 2013 report, the cybersecurity firm Mandiant attributed APT1 to what was the Second Bureau of the Third Department of the People's Liberation Army's (PLA) General Staff Department (GSD) prior to the restructuring of China's military initiated in 2015. The outfit is also commonly referred to by its Military Unit Cover Designator (MUCD): Unit 61398. The report bases these conclusions on matching characteristics between the observed cyber operations of APT1 and publicly-available reports on Unit 61398 regarding its mission, tools, tactics and procedures (TTPs), its scale of operations, employee requirements, geographic location, and infrastructure. As part of the 2015 military reforms, computer network exploitation and computer network attack capabilities that previously were collocated in the GSD Third Department (3PLA) and Fourth Department (4PLA) have been unified within the newly-established PLA's Strategic Support Force (SSF). MUCDs assigned to the SSF now range between 32001 and 32099. Open-source analysis indicates that the 3PLA headquarters, as well as the Second Bureau/Unit 61398, have been transferred to the SSF Network Systems Department. Sources: [1][3]

By Jakob Bund, Katharina Shah and Camille Borrett

December 2022

Agency type

State-integrated hacking group (and a cyber military unit). As an integral part of the PLA, Unit 61398 operated as a military agent in service of the Communist Party of China (CPC). The CPC directly oversees the PLA's cyber command structures through the Central Military Commission (CMC), a dual-branch institution which simultaneously functions as a party organ and the supreme national defense organization of the Chinese state. Considering this institutional link, Mandiant concluded that this parallel hierarchy provides the party leadership with control over strategic cyber espionage campaigns. Mandiant has traced APT 1 operators to a physical address that overlaps with the compound at which Unit 61398 is stationed in the Pudong New Area, a district with special economic development status in the east of Shanghai. From this location, APT 1 had direct access to a purpose-built fibre optic network set up by state-owned China Telecom. In direct response to the report's findings, China's Ministry of Defense declared that the PLA had never supported cyber espionage operations, and a spokesperson of the Ministry of Foreign Affairs denied the recorded activities as "groundless criticism" that "will not help to solve the problem." In 2015, for the first time, the development of cyber forces on both the civilian and military sides, including offensive capabilities, was publicly acknowledged within a new edition of the Science and Military Strategy. The Science of Military Strategy serves as a textbook for senior PLA officers and is produced by the PLA's foremost military academy: China's National Defense University, which is funded by and directly subordinate to the CMC. The 2017 National Intelligence Law explicitly denotes the CMC's exclusive control over military technical reconnaissance, including through cyber-enabled means.

Sources [1][7][8][9][10][11][12][13][14][15][16]

Most frequent targets:


Canada


India


Israel


Japan


Norway


Singapore


South Korea


Switzerland


Taiwan


UK


USA

Sources [1][6]

Group composition and organisational structure

Public accounts related to Unit 61398 and the scale of physical infrastructure it maintained suggests the group comprises of hundreds, if not thousands of employees. Based on the attack infrastructure and regular malware updates that Mandiant directly observed, the company estimated that APT1 ran on the continuous support of several dozen (but potentially hundreds) of operators. Sources [1][21]

Impact type(s)

Direct

- **Intelligence impact** (Byzantine Candor 2008; Operation ShadyRAT 2006; intrusions of three Israeli defence contractors providing components for Israel's air defense system ["Iron Dome"] during 2011-2012; reconnaissance missions against 23 US oil and gas pipeline operators during 2011-2013 with the intent to develop cyber capabilities to cause physical damage to the pipelines)
- **Financial/Business impact** through the theft of commercial secrets (global espionage campaign dating back to at least 2006: operations against US Steel; aluminium manufacturer, Alcoa; Westinghouse Electrical; and subsidiaries of the later insolvent German manufacturer of photovoltaic products, SolarWorld AG) Sources [1][8][17][18][19][20][21][22][23][24]

Incident type(s)

Data theft (in particular for espionage purposes), targeting a wide range of industry sectors in predominantly English-speaking countries and innovation-led economies. Cumulative returns from economically-motivated cyber espionage position the state sponsors of APT1 to support domestic companies with stolen intellectual property and trade secrets to leapfrog costly and uncertain research and development phases or gain advantage over foreign competitors in bidding processes. This focus on boosting economic competitiveness finds reflection in the target selection of APT1. The group has targeted at least four out of seven strategic emerging industries designated under the 12th Five-Year Plan (2011-2015), which is a cyclical strategy document by the CPC leadership that steers the general direction of economic initiatives: namely next-generation information technology, high-end equipment manufacturing, alternative energy, and new materials. In a small share of cases, APT1 has also engaged in cyber-espionage operations against nation-state governments and international organizations without apparent commercial purpose. Sources [1][6][8][17][18][19][20][21]

Threat level index

13/24 high 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.

Breakdown of the scores for APT1:

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	3/8	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 a multiplier is applied. In the case of APT1, on average attacks attributed to the group within the EuRepoC database, targeted two different sectors per attack and were in most cases, sectors critical for the functioning of societies (political systems/critical infrastructure).
Geographical scope of attacks	4/4	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 APT1, on average five countries were targeted per attack attributed to the group within the EuRepoC database.
Frequency of attacks	3/4	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. In the case of APT1, the group was responsible for 1 attack per year of activity.
Exploitation of Zero days	2/3	This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero days. The obtained score is then converted to a three-level scale. 11% of the attacks attributed to APT1 exploited zero-days in the EuRepoC database.

→ Overall, APT1 obtains a high-level threat score compared to other APT groups. Although the group's attacks had a relatively low intensity, on average the attacks targeted many different sectors in many different countries at the same time. In addition, APT1's attacks are relatively frequent and exploit zero-days more often that other APT groups analysed by EuRepoC.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

APT1 has acted as a highly persistent group, demonstrating its ability to stay active in target networks for prolonged periods of time. Recruitment calls for the group have strict requirements for English proficiency given the group's focus on English-speaking target environments.

Basic attack pattern

APT1 repeatedly gained access to computer systems by spear-phishing employees suspected of holding access rights to desired network segments. Malicious links or attachments trigger the download of a dropper which, in turn, installs customised backdoors to establish a foothold in the targeted network. The backdoor initiates communication with the command-and-control (C2) web server and executes commands based on the embedded HTML codes. In early backdoor variants, HTML comments signaled to C2 infrastructure, leading to the initial designation of the group as "Comment Crew." To maintain access to compromised networks, APT1 installed additional backdoors in lateral target systems and harvested user credentials. APT1 has further stood out through its use of two programmes (GETMAIL and MAPIGET) to extract emails of interest.

Zero-day exploits

APT1 has operated opportunistically, seeking to find entry points through phishing and taking advantage of stolen credentials. The group leveraged misconfigured remote access tools and custom-built backdoors to maintain its presence in compromised target.

Malware used (non-exhaustive)

BISCUIT	LIGHTDART	MANITSME
STARSYPOUND	DAIRY	HELAUTO
NEWSREELS	SEASALT	TABMSGSQL
COMBOS	COOKIEBAG	GLOOXMAIL
TARSIP	HACKSFASE	AURIGA
GREENCAT	BANGAT	LONGRUN
WARP	LIGHTBOLT	GDOCUPLOAD
MINIASP	BOUNCER	CALENDAR
KURTON	Cachedump	gsecdump
ipconfig	Lslsass	Mimikatz
Net	Pass-The-Hash Toolkit	Poisonlvy
PsExec	pwdump	Tasklist
WEBC2	xCmd	

Sources: [1][6][22]

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

MITRE Initial Access

Exploit public-facing application
Phishing
Spearphishing attachment
Spearphishing link

MITRE Persistence

Valid accounts

MITRE Defense Evasion

Masquerading
Match legitimate name or location
Use Alternate Authentication Material

MITRE Exfiltration

ATTRIBUTION

Attribution milestones

FEB 2013

Mandiant report on APT1

→

19 MAY 2014

US indictment against five PLA officers of Unit 61398

Sources: [1][21]

Attribution ambiguities

Operation ShadyRAT: In a technical report from August 2011, McAfee connected a string of espionage activities dating back to 2006 and suspected a state actor to be behind the intrusions. The firm dubbed the campaign "Operation ShadyRAT." A selection of targets with little financial value, such as the International Olympic Committee and the World Anti-Doping Agency, targeted within the period around the 2008 Beijing Olympics, indicated a convergence with Chinese state interests. Following Mandiant revelations about APT1, Symantec and Dell Secureworks determined in their assessment that the perpetrators of Operation ShadyRAT overlapped with the APT1 and Comment Crew threat cluster. The two companies had grounded initial skepticism about the alleged state nexus of ShadyRAT in an apparent lack of sophistication in the group's techniques. Eugene Kaspersky expressed similar reservations, impugning the state-actor hypothesis. Noting the use of cheap tools and the continued operation of attack infrastructure long after it had been revealed, Kaspersky pointed to these shortcomings in operational security as characteristic of low-tier criminals

Operation OceanSalt: In 2018, McAfee reported the resurfacing of APT1 implant code as part of the Seasalt malware discovered in South Korean targets. APT1 artefacts had not been detected since Mandiant's 2013 report, leading McAfee to conclude APT1 had either rebuilt its techniques or ceased its activity. While the firm dismissed the possibility of a return of APT1, it did not furnish alternative explanations about any potential link between the perpetrators and APT1. As APT1 source code has not been publicly disclosed or offered for sale, questions about the group's relation to the threat actors behind Operation OceanSalt and the proliferation of APT1 tooling remain unresolved.

Sources [6][7][23][24][25][26][27][29]

Attribution and detection sensitivity

Following Mandiant's exposé of APT1 infrastructure, tactics and techniques, and its institutional nexus to the PLA, the group shut down command-and-control infrastructure and appears to have stopped operations or fundamentally restructured. Coinciding with closed-door efforts by the US to broker an end to China's systematic economic espionage, findings on APT1's sustained and far-reaching activities also built-up public pressure on the US government to achieve concessions from China's leadership. Tensions in the US-China relationship culminated in the US indictment of five members of Unit 61398 in 2014, China's suspension of the bilateral China-US Cyber Working Group, the US threat to impose sanctions, and a nominal agreement between President Obama and President Xi at the US-China 2015 summit, which proscribed cyber-enabled theft of intellectual property for commercial advantage. G20 and G7 leaders endorsed this position on cyber-enabled economic espionage at their November 2015 and May 2016 meetings.

Sources [4][5][7][9][22][30][31][32][33][34][35]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/legal/law enforcement actions

US indictment of five Chinese military hackers of PLA Unit 61398 (19 May 2014):
On 19 May 2014, for the first time, the US Department of Justice disclosed criminal charges against state-sponsored hackers, unsealing an indictment against five PLA officers, all of whom were members of Unit 61398. Charges on 31 counts filed against all defendants included economic espionage, theft of trade secrets, conspiracy to commit computer fraud and abuse, and unauthorized access to a protected computer to obtain information for commercial advantage and private financial gain. Allegations focused on intrusions of six US companies between 2006 and 2014 with the goal to pass on trade secrets to Chinese companies to freeride innovation and to gain pricing advantages and insights into trade disputes. Sources [21]

Indicted individuals / sanctioned (associated) entities

19 May 2014:

- Gu Chunhui
- Huang Zhenyu
- Sun Kailiang
- Wang Dong
- Wen Xinyu

Sources [21][36][37][38][39][40]

Landmark incidents

ShadyRAT 2006-2011:
Operation ShadyRAT targeted 71 institutions across 14 different countries, including targets in government and the private sector. Targeted countries included the United States, Canada, and Japan.

Cyberattacks against 23 oil and natural gas pipeline operators (2011-2013):
In a campaign between December 2011 and 2013, APT1 is suspected to have targeted 23 oil and gas pipeline companies in the US. For at least 13 of these organizations, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI confirmed compromises; an additional eight may have fallen victim. In a joint 2021 advisory, the agencies noted a focus on developing access to industrial control systems (ICS) and assessed interest in holding the pipeline systems at risk of disruption or physical damage as likely motive behind the infiltrations. Honeypots set up in one victim network supported this hypothesis, as ICS-related decoy data drew immediate attention from the attackers, whereas commercial data was left untouched.

Sources: [6][17][20][23][24]

SOURCES

[1] Mandiant (2013), *APT1 Exposing One of China's Cyber Espionage Units*, Mandiant. Available at: https://web.archive.org/web/20221016044750/https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [Archived on: 16.10.2022].

[2] CrowdStrike Global Intelligence Team (2014), *CrowdStrike Intelligence Report: Putter Panda*, CrowdStrike. Available at: https://web.archive.org/web/20220626013038/http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf [Archived on: 26.06.2022].

[3] Costello and McReynolds (2019), *China's Strategic Support Force: A Force for a New Era*, National Defense University Press. Available at: https://web.archive.org/web/20221215094034/https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1748555/chinas-strategic-support-force-a-force-for-a-new-era/ [Archived on: 15.12.2022].

[4] Paganini (2013), *Comment Crew, China-based group of hackers is changing tactics*, Security Affairs. Available at: https://web.archive.org/web/20221215095345/https://securityaffairs.co/wordpress/15605/intelligence/hackers-comment-crew-i-changing-tactics.html [Archived on: 15.12.2022].

[5] Kirk (2013), *Suspected China-based hackers 'Comment Crew' Rises Again*, ComputerWorld. Available at: https://web.archive.org/web/20221215101232/https://www.computerworld.com/article/2498229/suspected-china-based-hackers--comment-crew--rises-again.html [Archived on: 15.12.2022].

[6] Alperovitch (2012), *Revealed: Operation Shady APT*, McAfee. Available at: https://web.archive.org/web/20221013125432/http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf [Archived on: 13.10.2022].

[7] Sanger, Barboza, Perlroth (2013), *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, The New York Times. Available at: https://web.archive.org/web/20221215105351/https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html [Archived on: 15.12.2022].

[8] Frizell (2014), *Here's What Chinese Hackers Actually Stole From U.S. Companies*, Time. Available at: https://web.archive.org/web/20221215105642/https://time.com/106319/heres-what-chinese-hackers-actually-stole-from-u-s-companies/ [Archived on: 15.12.2022].

[9] The Associated Press (2013), *Obama responds to alleged China Cyberattacks*, CBC. Available at: https://web.archive.org/web/20221215110056/https://www.cbc.ca/news/world/obama-responds-to-alleged-china-cyberattacks-1.1327309 [Archived on: 15.12.2022].

[10] Waidelich (2022), *China's New Military Leadership: Possible Strengths and Weaknesses*, CNA. Available at: https://web.archive.org/web/20221215094901/https://www.cna.org/our-media/indepth/2022/11/chinas-new-miliatry-leadership-possible-strengths-and-weaknesses [Archived on: 15.12.2022].

[11] Tianran and Wuning (2013), *Authorities Reject Cyber Crime Accusation*, Global Times. Available at: https://web.archive.org/web/20221215101224/https://www.globaltimes.cn/content/762810.shtml [Archived on: 15.12.2022].

[12] Tianliang, Yaoliang, Wuchao, and Renzhao (2022), *In Their Own Words: Science of Military Strategy*, China Aerospace Studies Institute. Available at: https://web.archive.org/web/20220701171141/https://nuke.fas.org/guide/china/doctrine/milstrat-2020.pdf [Archived on: 01.07.2022].

[13] Campbell (2021), China's *Military: The People's Liberation Army (PLA)*, Congressional Research Service. Available at: https://web.archive.org/web/20221026125302/https://crsreports.congress.gov/product/pdf/R/R46808 [Archived on: 26.10.2022].

[14] Wuthnow (2021), *What I Learned From the PLA's Latest Strategy Textbook*, China Brief, Volume 21, Issue 11. Available at: https://web.archive.org/web/20221215105223/https://jamestown.org/program/what-i-learned-from-the-plas-latest-strategy-textbook/ [Archived on: 15.12.2022].

[15] China Defence Universities Tracker (2019), *National University of Defense Technology*, Australian Strategic Policy Institute (ASPI), International Cyber Policy Centre. Available at: https://web.archive.org/web/20221024215122/https://unitracker.aspi.org.au/universities/national-university-of-defense-technology/ [Archived on: 24.10.2022].

[16] China Law Translate (2017), *PRC National Intelligence Law*, China Law Translate. Available at: https://web.archive.org/web/20221215105640/https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/ [Archived on: 15.12.2022].

[17] Clayton (2013), *Exclusive: Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage*, The Christian Science Monitor. Available at: https://web.archive.org/web/20221215110234/https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [Archived on: 15.12.2022].

[18] Brian Krebs (2014), *Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System*, KrebsonSecurity. Available at: https://web.archive.org/web/20221215110532/https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/ [Archived on: 15.12.2022].

[19] Brian Krebs (2012), *Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent*, KrebsonSecurity. Available at: https://web.archive.org/web/20221215110454/https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/ [Archived on: 15.12.2022].

[20] Clayton (2012), *Stealing US Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China*, The Christian Science Monitor. Available at: https://web.archive.org/web/20221215110711/https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China [Archived on: 15.12.2022].

[21] DOJ Office of Public Affairs (2014), *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, United States Department of Justice. Available at: https://web.archive.org/web/20221206093910/https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [Archived on: 15.12.2022].

[22] Paganini (2014), *Chinese Hackers Comment Crew Stole Plans of Iron Dome Defense System*, Security Affairs. Available at: https://web.archive.org/web/20221215110752/https://securityaffairs.co/wordpress/27132/cyber-crime/comment-crew-stole-plans-iron-dome.html [Archived on: 15.12.2022].

[23] Harnisch, Zettl, and Steiger (2021), *Heidelberg Cyber Conflict Dataset (HD-CY.CON)*, Universität Heidelberg, IPW Conflict Research, heiDATA, V1. Available at: https://web.archive.org/web/20221215111159/https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB [Archived on: 15.12.2022].

[24] National Cyber Awareness System (2021), *Alert (AA21-201A) Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013*, Cybersecurity & Infrastructure Security Agency (CISA). Available at: https://web.archive.org/web/20221215111152/https://www.cisa.gov/uscert/ncas/alerts/aa21-201a [Archived on: 15.12.2022].

[25] Nakashima (2011), *Report on 'Operation Shady APT' Identifies Widespread Cyber-Spying*, The Washington Post. Available at: https://web.archive.org/web/20221215111216/https://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html [Archived on: 15.12.2022].

[26] Schwartz (2011), *Shady RAT No China Smoking Gun*, DarkReading. Available at: https://web.archive.org/web/20221215111250/https://www.darkreading.com/attacks-breaches/shady-rat-no-china-smoking-gun [Archived on: 15.12.2022].

[27] Sherstobitoff and Malhotra (2017), *'Operation Oceansalt' Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group*, McAfee Advanced Threat Research. Available at: https://web.archive.org/web/20221215112334/https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf [Archived on: 15.12.2022].

[28] Kaspersky (2011), *Shady RAT: Shoddy RAT*, Eugene Kaspersky: Nota Bene. Available at: https://web.archive.org/web/20221215112346/https://eugene.kaspersky.com/2011/08/18/shady-rat-shoddy-rat/ [Archived on: 15.12.2022].

[29] Endpoint Protection (2013), *APT1: Q&A on Attacks by the Comment Crew*, Broadcom. Available at: https://web.archive.org/web/20221215110437/https://community.broadcom.com/symantecenterprise/viewdocument/apt1-qa-on-attacks-by-the-comment?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments [Archived on: 15.12.2022].

[30] BAE (2014), *The Snake: Cyber Espionage Toolkit*, BAE Systems. Available at: https://web.archive.org/web/20221215112559if_/https://www.baesystems.com/en-media/uploadFile/20210405003847/1434557449751.pdf [Archived on: 15.12.2022].

[31] Ministry of Foreign Affairs Spokesperson (2014), *China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel*, Ministry of Foreign Affairs of the People's Republic of China. Available at: https://web.archive.org/web/20221215110237/https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/201405/t20140520_696368.html [Archived on: 15.12.2022].

[32] Nakashima (2015), *U.S. Developing Sanctions Against China Over Cyberthefts*, The Washington Post. Available at: https://web.archive.org/web/20221215110237/https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html [Archived on: 15.12.2022].

[33] Office of the Press Secretary (2015), *FACT SHEET: President Xi Jinping's State Visit to the United States*, The White House, United States. Available at: https://web.archive.org/web/20221215110355/https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [Archived on: 15.12.2022].

[34] Meeting of G20 Antalya Summit (2015), *G20 Leaders' Communiqué*, 15-16 November 2015. Available at: https://web.archive.org/web/20220702053025/http://www.g20.utoronto.ca/2015/151116-communique.pdf [Archived on: 15.12.2022].

[35] Meeting of G7 Ise-Shima Summit (2016), *G7 Ise-Shima Leaders' Declaration*, 26-27 May 2016. Available at: https://web.archive.org/web/20221207154926/https://www.mofa.go.jp/files/000160266.pdf [Archived on: 15.12.2022].

[36] FBI (2014), *Gu Chunhui*, FBI: Most Wanted. Available at: https://web.archive.org/web/20221215112613/https://www.fbi.gov/wanted/cyber/gu-chunhui [Archived on: 15.12.2022].

[37] FBI (2014), *Huang Zhenyu*, FBI: Most Wanted. Available at: https://web.archive.org/web/20220814084700/https://www.fbi.gov/wanted/cyber/huang-zhenyu [Archived on: 15.12.2022].

[38] FBI (2014), *Sun Kailiang*, FBI: Most Wanted. Available at: https://web.archive.org/web/20221215112644/https://www.fbi.gov/wanted/cyber/sun-kailiang [Archived on: 15.12.2022].

[39] FBI (2014), *Wang Dong*, FBI: Most Wanted. Available at: https://web.archive.org/web/20221215112650/https://www.fbi.gov/wanted/cyber/wang-dong [Archived on: 15.12.2022].

[40] FBI (2014), *Wen Xinyu*, FBI: Most Wanted. Available at: https://web.archive.org/web/20221215112651/https://www.fbi.gov/wanted/cyber/wen-xinyu Archived on: 15.12.2022].

Calculations for the Threat Level Index Indicator are based on version 1.0 of the EuRepoC Database downloadable here: https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Global_Database_1_0_22d4a4aee7.xlsx

Last updated: 16.12.2022