FRIEDRICH NAUMANN FOUNDATION For Freedom.

UP! for democracy

POLICY PAPER

CHINA'S EXPANDING CYBER PLAYBOOK

Espionage, Fear, and Influence in East Asia

Dr. Chung-Kuan Chen / Dr. Valentin Weber

ANALYSIS

Publication Credits

Published by
Friedrich Naumann Foundation for Freedom
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg
Germany

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit

Author
Dr. Chung-Kuan Chen,
Head of Security Research,
CyCraft Technology

Dr. Valentin Weber,
Senior Research Fellow, DGAP

Editorial team
Global Innovation Hub, Taiwan
Globale Themen, Berlin

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Contact
Phone +49 30 220126-34
Fax +49 30 690881-02
Email service@freiheit.org

Last update
Dezember 2024

Table of Contents

Key findings

- → China is becoming increasingly sophisticated in obscuring its cyber operations
- → Beijing is dedicating more and more resources to counter democratic attribution statements through disinformation
- → When targeting Taiwan, China aims to undermine Taipei's economic power and induce fear through disruptive and destructive cyber operations
- → In Japan, China gathers information that could be of use in a future conflict, e.g. defense industrial base, information on politicians

1. Introduction

In the past few years China has risen to become one of the most threatening cyber actors. On the receiving end, Taiwan and Japan have been among the countries that China tar-geted most prolifically.

This paper consists of two parts. The first part traces Chinese cyber operations against Taiwan and Japan. It finds that the cyber operations against Taiwan were grave, as they did not only include cyber espionage, but also manipulated the financial system, stole intellectual property to undermine Taiwan's most vital semiconductor industry, and destroyed data of key oil and gas importers to sow fear among the population. Cyber operations against Japan were more of a political nature and aimed at gathering data on activities of Japanese defense companies and politicians.

The paper examined a timeframe from 2013-2023 and found a profound evolution occurring in Chinese cyber techniques. In order to hide their tracks, Chinese threat actors shifted parts of their operational infrastructure from state institutions to private proxy actors. What is more, to elevate its cyber capabilities, Beijing introduced a zero day law, which requires companies to deliver vulnerabilities first to the Chinese government, before making them public. At the same time, it has shifted increasingly toward supply chain attacks, making defending critical Japanese and Taiwanese networks even more difficult. Additionally, Beijing has continuously relied on distributing disinformation to cause confusion and fear in Taiwan.

The second part of this report analyzes how China reacted when cyber operations against Taiwan and Japan were attributed to it. This analysis finds that, here too, China has become more sophisticated when it comes to veiling its cyber operations in obscurity. Since 2013 China has regularly refuted any claims that it was involved in malicious cyber activities. But only since Volt Typhoon (a Chinese threat actor) was attributed to it, in 2023, it has markedly changed its approach. Since then it has started authoring reports that speak about Volt Typhoon, refuting claims that it was responsible for Volt Typhoon activities and spreading dis-information about who Volt Typhoon was.

All in all, this report shows that China has become a more aggressive cyber actor, which is capable of weakening attribution claims both by relying on the private sector and by conducting disinformation campaigns.

To face this increasing challenge we recommend that Japan, Taiwan and partners, including Germany:

- → deepen networks of threat intelligence sharing
- → increasingly issue advisories and attributions jointly with countries that face enduring Chinese cyber operations, such as India and the Philippines
- → double down on promoting security standards via industry alliances such as SEMI
- → institutionalize international links that exist between national security conferences, e.g. Taiwan's HITCON, Japan's CodeBlue and Germany's Chaos Communication Congress
- → specifically communicate attribution statements to the Global South
- → pre-bunk Chinese disinformation targeting Western democratic attributions

2. China as an international threat actor

Over the past decade, China has emerged as a threat actor in the global cyber landscape, with Chinese groups often engaging in APT-attacks aimed at espionage, sabotage, and information warfare. These activities have targeted numerous countries, though the intensity and frequency of these attacks have been particularly high against Taiwan and Japan due to ongoing geopolitical tensions. Beyond traditional espionage, China's cyber operations also aim at economic disruption and supply chain attacks. The following sections provide a summary of the most significant APT attacks targeting Taiwan and Japan.

2.1 China's Enduring Cyber Campaigns

Driven by the political conflict between Taiwan and China, Taiwan serves as a prime target and as a testbed for China-nexus threat actors. From the viewpoint of Chinese civilian hacktivists, hacking systems in Taiwan is seen as a way to demonstrate loyalty to the Chinese government. The shared culture and language between Taiwan and China further lower the barriers to cybercriminals targeting Taiwan. The following section investigates major Chinese APT attacks targeting Taiwan and Japan. They highlight the development of these attacks and that China is pursueing different goals and tactics in Taiwan and Japan.

Two key incidents marked the beginning of China's cyber espionage activities targeting Taiwan.

The first publicly known incident involved Taiwan being victim of APT1 [4], which has been linked to PLA Unit 61398 with high confidence in 2013. It exploited Taiwan's infrastructure by targeting the servers of several enterprises, stole certificates and went on targeting companies worldwide. This indicates that Taiwan is a valuable jump site for Chinese threat actors [4].

The second major incident occurred in 2014, when research from Trend Micro highlighted China´s espionage campaign against the Taiwanese government [5]. Subsequent studies disclosed the structure of command-and-control infrastructure, revealing that Taiwan's political parties and media industry had been compromised. The incident was attributed to threat actor Lstudio with a high confidence level by Xecure-Lab and Academia Sinica. Leaked documents included documents of the post-18th National Congress policies toward Taiwan (中共十八大之後對台政策走向研析) and the China-South Korea Free Trade Agreement, alongside other sensitive contact information [6].

These incidents signaled the beginning of an era of cyber espionage.

2011

Mitsubishi Heavy Industries Compromised

In mid-August 2011, Mitsubishi Heavy Industries (MHI), a key player in Japan's defense sector, detected malware on approximately 80 machines within its network. MHI's involvement in the construction of critical components for submarines, missiles, and nuclear power plants makes it a high-value target for cyber-espionage activitiesv [23].

This incident marks the first publicly known APT operation targeting a Japanese entity. The motivation behind the attack appears to be cyber-espionage, with a focus on extracting sensitive information related to Japan's defense capabilities.

Although there is speculation that the Nitro group may be responsible for the attack, the attribution remains uncertain. The Cyber Operations Tracker[24] attributes this operation to the Nitro group, but due to a lack of convincing evidence, this attribution is currently assessed with low confidence. There is no evidence that links the Nitro group to MSS, MPS or the PLA. A report by Symantec revealed that the PoisonIvy RAT was utilized in the attack. PoisonIvy is a RAT commonly associated with and mostly used by China-based threat actors and is readily available online with multiple functional plugins, which complicates attribution efforts.[25] However, the use of PoisonIvy RAT suggests China-based threat actor with high confidence.

2016–2017

Tick targeted Aerospace sector

According to the Japanese police, the Chinese military is reportedly behind a widespread cyber-espionage campaign that has breached over 200 Japanese companies and organizations since at least 2016. This campaign has targeted a variety of sectors, raising significant concerns about the security of Japan's critical infrastructure [28].

The Tokyo police have identified two individuals – a 30-year-old Chinese national and a Chinese student – suspected of aiding the Tick cyber-espionage group, which is linked to PLA Unit 61419. It is alleged that between 2016 and 2017, these individuals used fake identities to register web servers, which were then used to support the group's operations [27][28].

The same threat group is also linked to a major breach of Mitsubishi Electric in January 2020. This attack resulted in the potential exposure of personal information related to approximately 8,000 employees, along with several sensitive documents that may have been compromised [26].

2016–2017

Operation Cloud Hopper

Between late 2016 and 2017, the Chinese-linked APT10 group launched Operation Cloud Hopper, a sophisticated cyber-espionage campaign targeting managed IT service providers (MSPs). APT10 is linked to the Chinese Ministry of State Security's (MSS) and the Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company. The primary goal of this operation was to gain access to the intellectual property and sensitive data of the MSPs' clients [29]. Reuters reported that at least eight cloud service providers were compromised during the operation [30]. The Wall Street Journal expanded on this, indicating that over ten providers fell victim, placing hundreds of organizations at risk [31].

In 2020, another significant breach occurred when NEC, a major Japanese company, was compromised by APT10 [26]. Although this attack may not be directly linked to Operation Cloud Hopper, it underscores the ongoing threat posed by the same group. A report from PwC highlighted that many of the victims of these attacks were in industries aligned with China's „Made in China 2025" initiative, suggesting a strategic interest in targeting sectors critical to China's industrial goals [29].

2.1.1 Supply Chain Attack

2019

ASUS ShadowHammer and APT41

The ShadowHammer incident in 2019 is recognized as one of the earliest supply chain attacks. The attackers first compromised the intranet of ASUS [8] and then abused the company's trusted software update channel between ASUS's infrastructure and all ASUS PCs to deliver tampered upgrade programs. These programs were injected with malicious code to load Shadow Hammer, a malware related to the infamous ShadowPad backdoor, putting tens of thousands of users at risk.

As one of the largest computer manufacturers, the targeting of ASUS had significant global repercussions [7]. The supply chain attack ShadowHammer serves as an important warning for supply chain security and highlights the critical need for robust product security, especially for market leaders, as their security incidents can greatly influence the global landscape.

Supply chain attacks have been on the rise, possibly due to the enhanced security postures of Taiwan's and Japan's agencies. An increase in APT attacks leveraging the supply chain as an entry point could be observed. Rather than directly infiltrating organizations, threat actors are now targeting suppliers or exploiting vulnerabilities in widely-used industry applications to gain access to the targeted organization. In the incidents analyzed above, many of them are related to supply chains, in particular for BlackTech, who is specialized in supply chain attacks.

2.1.2 Cyber Threat Targeting Semiconductor Industry IP

2018–2019

Chimera

Between 2018 and 2019, researchers discovered several attacks on various semiconductor vendors located in the Hsinchu Science Park(HSP) in Taiwan. This cyber campaign was conducted by a sub-group of Winnti (APT41), subsequently named the Chimera APT Group [14][15]. Taiwan's semiconductor industry plays a crucial role in the country's economy and maintains Taiwan's importance on the global stage, particularly as China seeks to enhance its own semiconductor capabilities. Thus this operation had a very high impact on Taiwan. The primary objective of these attacks appeared to be the theft of sensitive intelligence, including documents related to integrated circuit (IC) chips, software development kits (SDKs), IC designs, and source code. potentially causing a devastating compromise of commercial secrets.

In contrast to previous attacks, these incidents indicate that the focus has shifted from targeting only government entities or their suppliers to stealing proprietary intelligence from private companies. This change in threat landscape highlights the evolving goals of cyber espionage from China-linked threat actors.

Rather than being an individual incident, the attacks targeted the entire Taiwanese semiconductor industry. The APT attacks on key vendors of semiconductor products were precise and well-coordinated, affecting their subsidiaries and competitors. The chosen victims held unique positions within the industry, making them prime targets for exploitation.

2019

PLEAD, BlackTech

Research by ESET and CyCraft revealed that threat actor BlackTech compromised five major Taiwanese government agencies, along with several local governments through the software update service of ASUS Web Storage (similar to Google Drive or OneDrive) in late April 2019 [9][10]. A man-in-the-middle (MITM) vulnerability allowed attackers to connect to the command-and-control (C2) server of the Plead malware, which subsequently installed primary malware and three additional backdoor programs.[1] These actions facilitated malicious activities such as password capture, encrypted communication, and data exfiltration.

This incident exemplifies classical cyber espionage against government entities. Unlike the previous ShadowHammer incident, which involved malware implanted in benign software, the threat actor targeting ASUS Web Storage exploited a vulnerability in the software itself. This underscores that supply chain attacks can manifest in various forms, highlighting the absence of a silver bullet solution to such threats.

2.1.3 Service Provider as a Hopping Point

2020

Waterbear, BlackTech

In August 2020, Taiwan's Ministry of Justice Investigation Bureau (MJIB) reported a series of hacking incidents targeting government agencies [11]. They reported that information service providers (e.g. companies that help manage government mail servers) hired by the government had been attacked by Chinese-affiliated threat actors. At least ten entities, including city governments, water resource bureaus, and four information service providers, were compromised. MJIB also discovered that after the hackers had infiltrated the internal hosts and servers of government agencies, they installed SoftEther VPN software to establish connections to designated relay stations. This allowed them to maintain long-term access and exfiltrate acquired data.

Other research indicates that this attack utilized a DLL sideloading technique[2] to trick legitimate software into loading malware. In this case, attackers exploited *Data Loss Prevention* (DLP) software (widely used by Taiwan's government agencies to protect data) via DLL sideloading to load the next stage of malware — Waterbear [12][13]. Since DLP software and many other security tools are widely deployed in sensitive organizations, frequently used in daily operations, and often run with high privileges, it is crucial for both vendors and customers to continuously work on strengthening their security measures to ensure resilience, even in the most challenging scenarios.

This case shows that service providers can be a weak link to indirectly intrude on governments. The report of MJIB highlights the complexity of the government IT environment and shows the important role of service providers[11]; however, governments often lack sufficient resources for cybersecurity. So service providers become potential blind spots for cyber attacks.

2.1.4 Ransomware Pursuing a Political Goal

2020

APT41

On May 4, multiple CPC (Chinese Petroleum Corporation) gas stations across Taiwan suddenly became unable to accept electronic payments. Customers were forced to pay in cash until the payment system was restored. Initially, CPC denied having their systems compromised. However, it was later revealed by MJIB that CPC had fallen victim to a targeted ColdLock ransomware attack, demanding a ransom of $3,000 for each affected computer [19]. In the MJIB report, The unnamed victims included other organizations within Taiwan's critical infrastructure, as well as a large multinational semiconductor vendor. The MJIB promptly shared intelligence with the U.S. Federal Bureau of Investigation (FBI), and finally attributed the attack to APT41. In August, the U.S. Department of Justice officially indicted five members of APT41 and two Malaysian operators [16][17].

Given that this attack occurred just one week before Taiwan's presidential inauguration, targeted multiple critical infrastructure sectors and utilized behavior that is uncommon among ransomware gangs: The attacker did not destroy the backup first and did not leave contact information behind that the victim could use to recover the data. It is increasingly plausible that the primary objective was not financial gain but a political show of force. The ransomware functioned as a smokescreen, designed to confuse and delay investigators while masking the true intent behind the attack and to induce fear in the Taiwanese population.[18]

2021

TA410 and APT10

The November 2021 attacks disrupted online trading, causing an uproar among the Taiwan public. At least two securities traders had to halt trading due to the volume of unusual purchases. The threat actor harvested the credentials of users, and made purchases via the Hong Kong stock through the stolen accounts without users' agreement [22]. The attacks were originally attributed to password mismanagement and credential stuffing; however, following an incident response (IR) new evidence uncovered the trace of APT-style attacks, related to subgroups of [21]. The attackers exploited a website service vulnerability of the software system management interface. The targeted financial software system is used by most financial institutions in Taiwan. The attackers also used the VPN of a supplier to gain access to the intranet.

Targeted organizations absorbed the financial losses and suffered the loss of customer trust. In addition, these attacks influenced and manipulated stock prices, damaging financial transaction credibility and integrity. If left unnoticed, these attacks could have had a devastating impact on the financial sector. In fact, this is not the first time the financial sector is targeted.

Besides a new focus on the financial system, the motives for Chinese cyber operations have widened. They range from cyber espionage to acquiring commercial intellectual property and obtaining financial gain. This shift in targeting might be because the policy directions by Beijing have shifted, or that private enterprise involved in conducting APT attacks had their own motives.

2022

MirrorFace, MirrorStealer targeted Japanese politicians

A hacking group known as MirrorFace targeted Japanese politicians in the weeks leading up to the House of Councilors (upper house of the National Diet of Japan) election in July 2022. The group used a previously undocumented credential stealer named MirrorStealer in this campaign, marking the first publicly reported case of a cyberattack specifically targeting Japanese politicians [34]. The threat actor deployed MirrorStealer using the LODEINFO malware, which is believed to have been developed specifically for targeting victims in Japan [32].

2.1.5 Private Security Service Providers as Intermediaries of APTs

Transitioning from official military structures to private enterprises, the landscape of China-related threat actors has evolved significantly. While many of these actors were previously linked to the *People's Liberation Army* (PLA) or other government agencies, there is now a noticeable trend toward masking APT activities within private companies, such as 安洵 (Anxun), 成都404 (Chengdu 404), and 武漢曉睿智科技 (Wuhan XRZ). This shift likely serves as a strategy to evade tracking and law enforcement efforts, complicating efforts to identify and mitigate these threats. Earliest shifts to this transition track back to 2013, but it only matured in the years 2016-2020.

2.1.6 China Weaponizes the Zero Day Discovery Ecosystem via National Regulation

In 2021, the Chinese government introduced the „Regulations on the Management of Security Vulnerabilities in Network Products,"(網路產品安全漏洞管理規定). This directive restricts researchers and hackers from directly reporting vulnerabilities to vendors, instead requiring them to first provide information to government agencies. This process potentially allows the government to exploit these vulnerabilities for their own purposes, leveraging the remarkable capabilities of Chinese hackers.

Zero day vulnerabilities are being weaponized against public-facing applications, particularly security devices. The zero day vulnerability regulation has led China-linked threat actors to extensively exploit vulnerabilities in critical network devices such as Fortinet firewalls, Sophos firewalls, Barracuda email servers, Citrix ADC, SonicWall email security systems, and Pulse VPN. This has significantly bolstered China's cyber warfare capabilities.

Although direct evidence linking the regulation to specific attacks is limited, several indicators suggest its influence on APT operations:

1. Chinese APT groups have increasingly targeted vulnerabilities in public-facing devices in recent years.

2. The I-soon document revealed that the vulnerability discovery contest Tianfu shared proof-of-concept (PoC) exploits with the Ministry of State Security (MSS), implying a pipeline for vulnerabilities to reach state actors.

3. Chinese hackers have significantly reduced their participation in global vulnerability discovery contests, such as Pwn2Own, likely to prioritize government-aligned efforts.

4. Alibaba was penalized by Chinese authorities for failing to report the Log4j vulnerability to the government before disclosing it publicly.

These patterns suggest that the zero-day vulnerability regulation not only strengthens China's cyber warfare capabilities but also facilitates the systematic exploitation of vulnerabilities for state-sponsored cyber operations.

2.1.7 Disinformation

Fabricating false information has been a strategy of Chinese threat actors for a long time. Disinformation tends to surface during election periods, with a notable incident from 2023 involving a threat actor impersonating Kaspersky. They disseminated fake news alleging that a Taiwan security vendor assisted the government in stealing personal information from Japan, aiming to disrupt the Taiwan-Japan relationship.

3. How China speaks about its own APTs

In the past 10 years attribution of Chinese cyber operations has taken off. More and more instances of attributions are added each year and also the countries attributing them has risen. With the rise in cyber attributions, China's responses too, have taken off both in number and sometimes in variety. Although China responds selectively and sometimes it chooses not to counter the allegations made toward its behavior.

Some scholars have studied how China speaks about foreign APTs. They have analyzed how China attributes for instance US cyber operations. But a considerable gap in literature exists. How does China speak about its own APTs, how does it defend accusations made by other countries? The following section analyzes how China communicates when it is the one being accused.

It finds four recurring themes: (1) China points to a lack of evidence in foreign state attributions, (2) it characterizes itself as a country that is law abiding and cracks down on cyber activities that emanate from its territory, (3) China engages in a defensive narrative when Taiwan or Japan attribute, and an offensive, counter-accusatory posture, when the US attributes, (4) when the US attributes, China states that the US is a larger threat than itself, that it attributes out of domestic political reasons, e.g. U.S. agencies inflating the China threat to get additional funding from Congress, (4) it involves a variety of actors to defuse foreign attributions by sometimes adding private companies to provide its claims with a false sense of legitimacy.

The following sub-sections highlight how China has responded to a variety of Taiwanese, Japanese and US cyber attributions. All attribution statements relate to cyber operations in which Taiwan or Japan were victims of Chinese cyber operations and campaigns.

3.1 Chinas Narratives of Defending China-based Threat Actors

3.1.1 Winnti Group, BlackTech and Taidoor

In 2020 Taiwan suffered a major Chinese cyberattack. It was meant to cripple Taiwan's energy import infrastructure. In the aftermath Taiwan's Ministry of Justice attributed the attack to the Winnti Group, which is a threat cluster working for the Chinese Ministry of State Security (*Taiwanese Ministry of Legal Affairs Bureau of Investigation, 2020*). In this case, Cyberscoop, a media organization based in Washington D.C., reached out to the Chinese Embassy in Washington, D.C., but did not receive a response regarding the attribution (*Lyngaas, 2020*). During the same year, Taiwan accused Chinese hacking groups (BlackTech and Taidoor) of infiltrating government organizations and thousands of government email accounts. Again, China's Taiwan Affairs Office refrained from commenting on the event (*Lee, 2020*).

3.1.2 A private contractor, i-Soon

In February 2024 news agencies picked up on a massive leak related to a Chinese state-affiliated cyber mercenary company called i-Soon or Anxun (*Shepherd et al., 2024*). The Shanghai-headquartered company had breached a number of overseas entities including in Taiwan (*KELA Cyber Threat Intelligence, 2024*). The contractors sold remote access to a wide range of entities to the Ministry of Public Security, Ministry of State Security and the *People's Liberation Army* (PLA). In response to the revelations, Mao Ning, a spokeswoman for the Chinese Ministry of Foreign Affairs, stated that she did not know about this incident. "As a matter of principle, China firmly opposes and cracks down on all forms of cyberattacks in accordance with the law" (*Mozur et al., 2024*).

3.1.3 Unit 61419 of the PLA

In April 2021, the Tokyo Metropolitan Police Department accused Unit 61419 of the PLA of breaching the *Japanese Aerospace Exploration Agency* (JAXA) and 200 other Japanese entities in the years 2016 and 2017 The Chinese Ministry of Foreign Affairs spokesperson Wang Wenbin retorted that the attribution lacked evidence and that Japan was "throw[ing] mud at China]" (*Sakaguchi, 2021*). Despite Japan having testimony from the accused person, Beijing denied the allegations. In a separate incident, *Japan's National Center of Incident Readiness and Strategy for Cybersecurity* (NISC) stated that an unnamed entity had hacked into its email correspondences in October 2022 and remained in its networks for over nine months. Speaking to the Financial Times, people aware of the intricacies of the breach revealed that China was behind the hack (*Lewis, 2023*). China responded by saying that it did not breachJapan's cybersecurity agency (*Martin, 2023*).

3.1.4 Hafnium

In 2021 Chinese sponsored cyber actors (also known as Hafnium) exploited Microsoft Exchange Servers and left the access to compromised systems wide open, which in turn gave cybercriminals access to systems, causing further upheaval and costs for breached companies (*Carlson, 2021; Council of the European Union, 2021*).[1]

When Japan, which was a victim of the cyber operation, attributed this incident together with the US, the EU, the UK, Australia, Canada, New Zealand, and NATO, China accused the US that it pushed its allies to attribute the attack (*Cui & Mo, 2021; Mason & Tillett, 2021*). Despite dozens of countries jointly attributing the incident, China focused its accusations against US cyber operations. Furthermore, countries that attributed, were rebuked as not representing the international community. The Chinese embassies in Canada and New Zealand issued separate statements reinforcing the above narrative.

1 Hafnium has been linked to the Chinese Ministry of State Security (*Matishak, 2021*).

3.1.5 APT 1

APT 1 has been one of the oldest known Chinese APTs. Already in 2006, Symantec's Japanese unit identified the threat actor's infrastructure, and also one of the personas (Ugly Gorilla) involved in the threat group. Both Japan and Taiwan were victims of this notorious Chinese threat actor. But it was not until 2013 that this APT received widespread attention.

On February 19, 2013 Mandiant revealed that Unit 61398 of the PLA engaged in industrial espionage from a building in Shanghai (*Mandiant, 2013*). In its report "APT 1: Exposing One of China's Cyber Espionage Units" it showcases detailed evidence.

"[T]he overwhelming concentration of Shanghai IP addresses and Simplified Chinese language settings clearly indicate that APT1 intruders are mainland Chinese speakers with ready access to large networks in Shanghai (*p. 40).*" The report even identified some of the cyber operators that were launching the cyber espionage operations.

One of China's earliest ever reactions to a foreign attribution statement was its statement regarding this threat intelligence report.[2] The Press Bureau of the PLA proclaimed that it "has never supported any hacking activities" (*Global Times, 2013*). The *Chinese Ministry of Foreign Affairs* (MFA) noted that the "speculations and accusations" were "groundless", lacked evidence, that the world needed more international cooperation, and that China was the victim of cyberattacks and did not allow for cyberattacks to emanate from its territory. Hong Lei, a spokesman of the MFA said on the 19th that the Chinese government "has always firmly opposed and cracked down on cyber attacks in accordance with the law". The MFA continued by stating that US agencies inflated the threat from China to receive more funds from Congress. APT1 report was missing "technical proof" (*BBC News, 2013*). It claimed that many attacks take place, but are often hijacked IP addresses. It accuses Mandiant of mischaracterizing "[e]veryday gathering" of online information as spying.

3.1.6 Volt Typhoon

For the past 10 years China followed a similar narrative when responding to accusations against its APTs. It denied allegations, portrayed itself as a diligent actor cracking down on attacks emanating from its territory, deflected onto the US being the worse cyber actor, and accused the attributors of not providing sufficient evidence. This changed substantially with Volt Typhoon, where China probably for the first time used the evidence provided by accusers and used it to sow disinformation. China's response has never been so extensive – both in content and breadth of actors involved – regarding a cyber attribution. It used CGTN, CCTV, the State Council, Xinhua, China Daily, and the Global Times to widely sow its narrative (*China Daily, 2024; Global Times, 2024; Jones, 2024; Mao, 2024; State Council Information Office - The People's Republic of China, 2024; Xinhua, 2024*). The Chinese representative at the UN OEWG on cybersecurity also mentioned a Chinese threat group, Volt Typhoon, by its name for the first time in New York at UN discussions in July 2024.

But the revelations started earlier. In May 2023 Microsoft revealed that a Chinese state-sponsored group was pre-positioning into US critical infrastructure to cause disruption during a potential future conflict (*Microsoft, 2023*) over Taiwan (*Siddiqui, 2024*). The actor had gained a first foothold to some systems already five years prior (Waldman, 2024). The *US's Cybersecurity & Infrastructure Security Agency* (CISA) and the Five Eyes' intelligence agencies followed up with an advisory sharing information on how to best detect this threat actors' presence in networks (*CISA, 2023*).

In April 2024, the *Chinese National Computer Virus Emergency Response Center* (CVERC), the National Engineering Laboratory for Computer Virus Prevention Technology and 360 Digital Security Group published a Chinese-language report titled "Volt Typhoon"(*China National Computer Virus Emergency Response Center et al., 2024*). The report was an attempt to provide a counternarrative to the attribution and was notable due to its length (21 pages), which allowed for a lengthy laying out of arguments.

The CVERC Volt Typhoon report is a turning point in its attempts to rebuke Western attributions. It also shows how China adjusts its narrative responses. Countless cyber attributions that the US has carried out since the 2010s have not received such a strong response from China. But Volt Typhoon was highlighted by CISA, the FBI, the US Department of Justice, the NSA as well as US Congress and the Five Eyes intelligence agencies as being different from the countless Chinese commercial cyber espionage cases. China describes the attention given by the West as major, "such a large-scale battle is rare" (*China National Computer Virus Emergency Response Center, 2024, p. 2*). Perhaps precisely because of this China prepared a multi-actor response.

This CVERC report is notable, because usually cyber advisories, attribution statements or cyber indictments are not co-authored by the public and private sector, neither in China nor in other countries. Western democracies pinpoint to data published by private companies but they normally do not co-author reports with them (*CISA, 2023*). The Chinese Volt Typhoon report does, however, precisely this. It features 360 Digital Security (part of 360, a major Chinese cybersecurity company) as a co-author.

The CVERC report acknowledges the technical details (Indicators of Compromise) in the Microsoft Volt Typhoon blogpost but mentions that the Microsoft's analysis was insufficient and that it does not indicate a Chinese state nexus. It goes even further in misusing research by a US threat intelligence company, ThreatMon, to draw its own conclusion that Volt Typhoon had a ransomware (cybercrime) nexus. With the establishment of the ransomware link Chinese authorities aim to discredit the Five Eyes' claim of the actor being sponsored by the Chinese government. Finally, one interesting bit of the report speaks to why China is responding to the attributions made by Western countries. It is mostly about China's interna-

tional reputation. China expresses that being constantly in the news as a cyber threat actor might also alienate it from partner countries abroad. This might be also why it so vehemently responds to US accusations, as the US's claims usually receive the most attention globally and therefore potentially tarnish Chinese reputation the most. In July, the same entities that published the April Volt Typhoon report, released a follow-up report. The new, 19 page-long English-language document is titled "Volt Typhoon II: A [S]ecret Disinformation Campaign [T]argeting U.S. Congress and Taxpayers [C]onducted by U.S. Government [A]gencies" (*National Computer Virus Emergency Response Center et al., 2024*). In the previous report, the publishing entities still speak of an "obvious" "degree of connection" between Volt Typhoon and ransomware groups. In contrast, the July report unequivocally claims that "'Volt Typhoon' is actually a ransomware group" (p.1). Interestingly, the report mentions that it expects more US attributions to come in the years ahead. It also does not at all mention the Five Eyes countries, which were also part of a joint advisory on Volt Typhoon.

It zooms in on the US only. The 2024 narrative in the CVERC report picks up on a 10 year-old narrative that was then made by a high ranking academic of the Chinese Academy of Social Sciences commenting Mandiant's APT1 attribution (*Global Times, 2013*). Then he stated that external threats were inflated to obtain funding from Congress. In 2024, CVERC, and co-authoring entities picked up on this narrative (*National Computer Virus Emergency Response Center et al., 2024*).

The report officially authored by Chinese state authorities and a private security company reads more like a journalistic piece of writing. The report mentions that "medias" [sic] contacted the U.S. Embassy in China and Microsoft but did not receive a response (p.1).

The April 2024 CVERC report was also cited by the Chinese delegate during the 8th substantive session of the UN OEWG on international cybersecurity in New York, on Monday 8 July, 2024 (*Digital Watch Observatory, n.d.-b*). The delegates' statement ties Volt Typhoon to the topic of disinformation and claims that the cyber campaign was not supported by China but that it the culprit is an international ransomware group. The international bit was not previously mentioned in the CVERC report or Global Times articles and is therefore notable. The claim is unsubstantiated, but it shows how China changes its own narrative depending on the venue. At the OEWG, which is a multilateral cyber discussion group it suits China to portray the ransomware as being international in nature and not solely based in China. The issue of Volt Typhoon had been previously raised by the U.S. during the 7th substantive session of the OEWG in March 2024 (*Digital Watch Observatory, n.d.-a*).

In October 2024, CVERC released another report on Volt Typhoon. Therein it continues to refuse claims that it was involved behind Volt Typhoon activity. This report filled over 50 pages and was translated from Chinese into English, German, Japanese and French (*Global Times, 2024*).

Figure 1 | China's ecosystem around the narrative on foreign attributions

INCIDENT	SELECTED VICTIM	ATTRIBUTION / ADVISORY / INDICTMENT / LEAK YEAR	CHINESE ACTORS RESPONDING
Winnti Group, BlackTech, Taidoor	Taiwan	2020	→ Embassy in Washington, D.C. → China's Taiwan Office
i-Soon	Taiwan	2024	→ MFA spokeswoman Mao Ning
Unit 61419 of the PLA	Japan	2021	→ MFA spokesperson, Wang Wenbin
Hafnium	Japan	2021	→ MFA spokesman Zhao Lijian → Embassies in Australia, the UK, Canada and New Zealand, Norway → Chinese Mission to the EU
APT 1	USA	2013/2014	→ Press Bureau of the PLA → MFA spokesman Hong Lei
Volt Typhoon	USA	2023	→ Chinese National Computer Virus Emergency Response Center (CVERC) → the National Engineering Laboratory for Computer Virus Prevention Technology → 360 Digital Security Group → MFA delegate at the UN OEWG on cybersecurity → State Council

2 Mandiant has since been acquired by Google Cloud.

4. Recommendations for Improving Defenses

4.1 Deepen International Threat Intelligence and Attribution Networks

Countries must expand their collaboration to enhance their attribution capabilities. Attribution in cybersecurity is often imprecise, compounded by the fragmented visibility of threats across different countries, research institutions, and private enterprises. To effectively respond to cyber incidents, it is essential to maintain robust capabilities for verifying attribution and to collaborate internationally to piece together a comprehensive understanding of threats.

For example, Japan has collaborated with the Five Eyes alliance — comprising Australia, Canada, New Zealand, the United Kingdom, and the United States — to strengthen its ability to attribute cyber threats. This partnership facilitates the sharing of intelligence, best practices, and technological advancements, thereby improving collective security. Japan could, furthermore, deepen its collaboration of threat attribution with Germany.

Similarly, Taiwan has engaged in cooperative efforts with the United States to address threats from state-sponsored Advanced Persistent Threats (APTs). Such collaborations not only enhance attribution capabilities but also foster resilience against emerging cyber threats. While this is a good first step, it is not enough.

Countries, such as Germany, Taiwan, Japan and the US should engage with countries beyond the traditional collaboration partners in issuing joint attributions and advisories. One such partner could be India, which faces a particularly strong exposure to Chinese cyber threat actors due to its border dispute with China. Another country that would lend itself to joint advisories or attributions might be the Philippines, which is engaged in sea disputes with China. In that context, it does attribute China's incursions into Philippine territory in the South China Sea. It would be the next logical step to extend attributing Chinese cyber intrusions.

Western countries need to expand the audience that they want to reach with their attributions. The primary audience for the attribution remains China of course. If it engages in irresponsible behavior, the West should say so in public, when appropriate. But when China is defending itself, it speaks mostly to the Global Majority and maintains favorable views there. Western countries should consider communication channels, either via foreign ministries, embassies in overseas countries, or media engagement, of how to reach broad audiences and elites in Global Majority countries.

4.2 Pre-bunk China's Attribution Disinformation

We recommend, pre-bunking China's arguments made against attribution statements. This can be done by highlighting the high certainty of one's own attribution claim and emphasizing the robust technical evidence that backs it up, e.g. We only attribute when there is no doubt. When China uses that technical evidence to sow disinformation (like with Volt Typhoon) respond immediately by rectifying China's false claims.

Also, states should invoke in their attribution statement cyber norms (*Brunner, 2024*). This could, for instance, counter China's narrative of it being a country that cracks down on malicious cyber behavior emanating from its territory. For example, in some cases, China may not be conducting the activity itself (e.g. i-Soon), and is relying on front companies to conduct cyber operations or is at least knowingly tolerating them to conduct these operations from their territory. This contravenes norm c, which states that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" (*Brunner, 2024*). China too has agreed to this norm in the final 2021 UNG OEWG report and attributing states should highlight it (*Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021*).

4.3 Strengthen Industry Alliance Capabilities to Craft Security Standards

Since industry alliances are crucial for defining security standards the authors recommend Japan and Taiwan to expand their support for these alliances in their important work. With key players involved, these alliances can significantly encourage other vendors to adopt and participate in the established security standards.

SEMI (*Semiconductor Equipment and Materials International*) is a global industry association that facilitates in-depth exchanges among industry, government, academia, and research sectors. It aims to promote Taiwan's semiconductor industry and align it with global standards while establishing a mechanism for bilateral communication.

In response to the Chimera incident, SEMI has gradually increased its awareness of security issues. It has established a security working group and published SEMI E187 to enhance supply chain security within the semiconductor industry. E187 outlines security standards and guidelines specifically for the fabrication environment.

4.4 Expand Collaboration between National Security Conferences

The authors recommend an institutionalization of international networks of Taiwanese, Japanese, and German security conferences (e.g. the CCC). As of today, security conferences are mostly national endeavors. They would benefit through a stronger international interconnection.

HITCON is one of the largest security conferences in Taiwan, featuring a range of activities such as HITCON CTF, HITCON CISO Summit, and Cyber Range. The HITCON Conference is held annually in August and attracts thousands of attendees. It serves as a hub for technical sessions, villages, and workshops. HITCON CTF has become one of the top CTF competitions globally, with over 1,000 hackers participating. This event provides opportunities for technical sharing and discussions among world-class hackers, sharpening skills in vulnerability discovery. HITCON CISO Summit is an exclusive, invitation-only summit gathers over a hundred cybersecurity decision-makers and government representatives from around the world. It facilitates in-depth discussions on cybersecurity strategies, current issues, and policies.

In Japan, CodeBlue and JSAC serve similar roles. CodeBlue provides a conference focused on general security topics, while JSAC emphasizes sharing research specifically for security analysts.

As a non-profit community, it is easy to foster a soft and flexible connection for innovation. And brings together communities from academia, government, and industry for collaborative brainstorming.

[1] 上海安洵分析
[2] Demystifying the China's Supply Chain Attack Targeting Financial Sector.
[3] Ghost in your supply chain.
[4] Exposes APT1 – One of China's Cyber Espionage Units.
[5] Targeted Attack Trends in Asia-Pacific.
[6] Hunting the Shadows: In Depth Analysis of Escalated APT Attacks.
[7] Gartner Says Worldwide PC Shipments Increased 1.9% in Second Quarter of 2024.
[8] Operation ShadowHammer: a high-profile supply chain attack.
[9] Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage.
[10] Supply Chain Attack & Modern APT Malware Reversing.
[11] Investigation Bureau Reveals Cybersecurity Vulnerabilities in Government Outsourcing Vendors.
[12] Taiwan Government Targeted by *Multiple Cyberattacks* in April 2020 - Part 1.
[13] Taiwan Government Targeted by *Multiple Cyberattacks* in April 2020 - Part 2.
[14] APT Group Chimera - APT Operation Skeleton Key Targets Taiwan Semiconductor Vendors.
[15] Abusing Cloud Services to Fly Under the Radar.
[16] Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally.
[17] FBI agent thanks Taiwan for help in indicting Chinese hackers.
[18] China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware.
[19] Taiwan's state-owned energy company suffers ransomware attack.
[20] North Korea's APT38 hacking group behind bank heists of over $100 million.
[21] Demystifying the China's Supply Chain Attack Targeting Financial Sector.
[22] President Securities and Yuanta report hacking.
[23] APT Attackers Hit Japan's Biggest Defense Contractor, https://www.darkreading.com/cyberattacks-data-breaches/apt-attackers-hit-japan-s-biggest-defense-contractor.
[24] Cyber Operations Tracker, https://www.cfr.org/cyber-operations/nitro-attacks.
[25] The Nitro Attacks Stealing Secrets from the Chemical Industry, Symantec.
[26] 中国系集団「Tick」の犯行か　三菱電機にサイバー攻撃　8000人分情報流出, https://mainichi.jp/articles/20200120/k00/00m/040/296000c.
[27] ＪＡＸＡにサイバー攻撃か、中国共産党員の男を書類送検…関与人物の特定は異例, https://www.yomiuri.co.jp/national/20210420-OYT1T50136/.
[28] Tick APT is Linked to Chinese Military by Japanese Police, https://cyberintelmag.com/attacks-data-breaches/tick-apt-is-linked-to-chinese-military/.
[29] "Operation Cloud Hopper", pwc.
[30] Inside the West's failed fight against China's 'Cloud Hopper' hackers, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.
[31] Ghosts in the Clouds: Inside China's Major Corporate Hack, https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061?mod=rsswn.
[32] Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities, https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/.
[33] Chinese APT Group MirrorFace Interferes in Japanese Elections, https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-group-mirrorface-interferes-japanese-elections.
[34] Hackers target Japanese politicians with new MirrorStealer malware, https://www.bleepingcomputer.com/news/security/hackers-target-japanese-politicians-with-new-mirrorstealer-malware/.
[35] AA23-270A, "People's Republic of China-Linked Cyber Actors Hide in Router Firmware", *CISA*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a.
[36] US, Japan say 'BlackTech' Chinese gov't hackers exploiting routers during attacks, https://therecord.media/us-japan-say-chinese-hackers-routers.
[37] Darwin's Favorite APT Group, Mandiant.

Bibliography

BBC News. (2013, February 20). China Condemns Hacking Report by Us Firm Mandiant. *BBC News*. https://www.bbc.com/news/world-us-canada-21515259.

Carlson, B. (2021, May 6). The Microsoft Exchange Server Hack: A Timeline. *CSO Online*. https://www.csoonline.com/article/570653/the-microsoft-exchange-server-hack-a-timeline.html.

China Daily. (2024, July 8). Report Uncovers Real Intention behind U.S. "Volt Typhoon" Misinformation Campaign. https://www.chinadaily.com.cn/a/202407/08/WS668b4a8ea31095c51c50cf03.html.

China National Computer Virus Emergency Response Center, National Engineering Laboratory for Computer Virus Prevention Technology, & 360 Digital SecurityGroup. (2024, April 15). *Volt Typhoon: A Conspiratorial Swindling Campaign Targeting U.S. Congress and Taxpayers Conducted by U.S. Intelligence Community"*. https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf.

China National Computer Virus Emergency Response Center, National Engineering Laboratory for Computer Virus Prevention Technology, & 360 Digital SecurityGroup. (2024, July 8). *Volt Typhoon II: A Secret Disinformation Campaign Targeting U.S.Congress and Taxpayers Conducted by U.S.Government Agencies*. https://web.archive.org/web/20240716163911/; https://www.cverc.org.cn/head/zhaiyao/futetaifengerEN.pdf.

CISA. (2023, May 24). People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | *CISA*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

Council of the European Union. (2021, July 19). *China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action against Malicious Cyber Activities Undertaken from Its Territory*. Consilium. https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/.

Cui, C., & Mo, J. (2021, July 21). *China Slams Cyberattack Accusations as Groundless*. https://global.chinadaily.com.cn/a/202107/21/WS60f75c9ba310efa1bd663347.html.

Digital Watch Observatory. (n.d.-a). *Agenda Item 5: Day 1 Afternoon Session / 7th Substantive Session*. Retrieved July 31, 2024, from https://dig.watch/event/un-oewg-2021-2025-7th-substantive-session/agenda-item-5-day-1-afternoon-session.

Digital Watch Observatory. (n.d.-b). *Opening of the Session / 8th Substantive Session OEWG*. Retrieved July 31, 2024, from https://dig.watch/event/un-oewg-2021-2025-8th-substantive-session/opening-of-the-session.

Global Times. (2013, February 23). *The New York Times Stated That a Building in Shanghai Is the PLA Hacking Headquarters*. https://web.archive.org/web/20130223084143/http://mil.news.sina.com.cn/2013-02-20/0734716107.html.

Global Times. (2024a, April 15). GT Exclusive: *Volt Typhoon False Narrative a Collusion among US Politicians, Intelligence Community and Companies to Cheat Funding, Defame China: Report*. https://www.globaltimes.cn/page/202404/1310584.shtml.

Global Times. (2024b, October 14). GT *Exclusive: Latest Report Shows US Cyber Weapon Can 'Frame Other Countries' for Its Own Espionage Operations*. https://www.globaltimes.cn/page/202410/1321156.shtml.

Jones, W. (2024, July 11). *Debunking Volt Typhoon: How U.S. Intelligence Fabricate Disinformation against China* [CGTN]. https://news.cgtn.com/news/2024-07-11/Volt-Typhoon-How-U-S-intelligence-fabricate-disinformation-on-China-1v954PmP4Bi/p.html.

KELA Cyber Threat Intelligence. (2024, March 7). *I-Soon Leak: KELA's Insights*. https://www.kelacyber.com/i-soon-leak-kelas-insights/.

Lee, Y. (2020, August 19). Taiwan Says China behind Cyberattacks on Government Agencies, Emails. *Reuters*. https://www.reuters.com/article/world/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0NY/.

Lewis, L. (2023, August 29). Japan's Cyber Security Agency Suffers Months-Long Breach. *Financial Times*. https://www.ft.com/content/de0042f8-a7ce-4db5-bf7b-aed8ad3a4cfd.

Lyngaas, S. (2020, May 18). Taiwan Suggests China's Winnti Group Is behind Ransomware Attack on State Oil Company. *CyberScoop*. https://cyberscoop.com/cpc-ransomware-winnti-taiwan-china/.

Mandiant. (2013, February 19). *Mandiant Exposes APT1 – One of China's Cyber Espionage Units – and Releases 3,000 Indicators*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/mandiant-exposes-apt1-chinas-cyber-espionage-units.

Mao, Z. (2024, August 7). *Report Uncovers Real Intention behind U.S. 'Volt Typhoon' Misinformation Campaign*. CCTV. https://english.cctv.com/2024/07/08/ARTIhCsfkd9AI4GYuhOskYBq240708.shtml.

Martin, A. (2023, August 29). *Japan's Cybersecurity Agency Breached by Suspected Chinese Hackers: Report*. https://therecord.media/japan-cybersecurity-agency-breached-report.

Mason, M., & Tillett, A. (2021, March 10). *Japan's Ministry of Foreign Affairs Scrambles after Microsoft Hack*. Australian Financial Review. https://www.afr.com/technology/japan-s-ministry-of-foreign-affairs-scrambles-after-microsoft-hack-20210310-p579ce.

Matishak, M. (2021, July 19). *White House Formally Blames China's Ministry of State Security for Microsoft Exchange Hack*. https://therecord.media/white-house-formally-blames-chinas-ministry-of-state-security-for-microsoft-exchange-hack.

Microsoft. (2023, May 24). *Volt Typhoon Targets Us Critical Infrastructure with Living-off-the-Land Techniques*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

Mozur, P., Bradsher, K., Liu, J., & Krolik, A. (2024, February 22). Leaked Files Show the Secret World of China's Hackers for Hire. *The New York Times*. https://www.nytimes.com/2024/02/22/business/china-leaked-files.html.

Sakaguchi, Y. (2021, May 16). Japan Lashes Out against Alleged Chinese Military Cyberattacks. *Nikkei Asia*. https://asia.nikkei.com/Business/Technology/Japan-lashes-out-against-alleged-Chinese-military-cyberattacks.

Shepherd, C., Cadell, C., Nakashima, E., Menn, J., & Schaffer, A. (2024, February 22). Leaked Files from Chinese Firm Show Vast International Hacking Effort. *Washington Post*. https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/.

Siddiqui, Z. (2024, May 8). US Confronts China over Volt Typhoon Cyber Espionage. *Reuters*. https://www.reuters.com/world/us/us-confronts-china-over-volt-typhoon-cyber-espionage-2024-05-08/.

State Council Information Office – The People's Republic of China. (2024, April 16). *China Urges US to Immediately Stop Cyberattacks against China*. http://english.scio.gov.cn/pressroom/2024-04/16/content_117128411.htm.

Taiwanese Ministry of Legal Affairs Bureau of Investigation. (2020, May 15). *Investigation Description of the Incident of Extortion of Important Domestic Enterprises*. https://web.archive.org/web/20200531005757/https://www.mjib.gov.tw/news/Details/1/607.

Waldman, A. (2024, February 7). *CISA: Volt Typhoon Had Access to Some u.s. Targets for 5 Years. Security*. https://www.techtarget.com/searchsecurity/news/366569227/CISA-Volt-Typhoon-had-access-to-some-US-targets-for-5-years.

Xinhua. (2024, July 8). *Report Uncovers Real Intention behind U.S. "Volt Typhoon" Misinformation Campaign*. https://english.news.cn/20240708/c5bbaf6f8aa-147d4a7f8998f6be65e37/c.html.

About the Authors

Dr. Chung-Kuan Chen

is currently the security research director in CyCraft, and responsible for organizing the research team, and Adjunct Assistant Professor in Soochow University, Taiwan. He earned his PHD degree of Computer Science and Engineering from National Chiao-Tung University (NCTU). His research focuses on cyber attack and defense, machine learning, software vulnerability, malware and program analysis. He tries to utilize machine learning to assist malware analysis and threat hunting, and build automatic attack and defense systems. He has published several academic journal and conference papers, and has been involved in many large research projects from digital forensic, incident response to malware analysis. He also dedicates to security education. Founder of NCTU hacker research clubs, he trained students to participate in world-class security contests, and has experience of participating DEFCON CTF (2016 in HITCON Team and 2018 as coach in BFS team). He organized the BambooFox Team to join some bug bounty projects and discover some CVEs in COTS software and several vulnerabilities in campus websites. Besides, he has presented technical presentations in technique conferences, such as BlackHat, HITCON, CHITB, RootCon, CodeBlue, FIRST and VXCON. As an active member in Taiwan security community, he is the chairman of HITCON review committee as well as director of Association of Hacker In Taiwan, and member of CHROOT - the top private hacker group in Taiwan.

Dr. Valentin Weber

is a senior research fellow in DGAP's Center for Geopolitics, Geoeconomics, and Technology. His research covers cyber diplomacy, the international security implications of emerging technologies, advanced surveillance technologies, and, more broadly, the intersection between cyber and national security. Weber has contributed to a White Paper for the US Joint Chiefs of Staff as well as to major news outlets including Die Zeit, Deutsche Welle, South China Morning Post, and the Associated Press. He holds a PhD in cyber security from the University of Oxford.