European Repository of Cyber Incidents

Major Cyber Incidents

Volt Typhoon

Other incident names: VANGUARD PANDA, BRONZE SILHOUETTE, Redfly, Insidious Taurus, Dev-0391, Storm-0391, UNC3236, or VOLTZITE

By Louis Bamber and Callahan Shelley

Description

The Director of the United States Federal Bureau of Investigation (FBI), Christopher Wray, once linked it to "the defining threat of our generation:" the Chinese state-sponsored hacking group Volt Typhoon gained access to a variety of critical infrastructure organisations on Guam and the US mainland beginning in mid-2021. A technical report from Microsoft, published alongside a Joint Cybersecurity Advisory by the Five Eyes intelligence alliance on 24 May 2023, concluded with medium confidence that the group intended to build capabilities that could disrupt critical communications infrastructure between the United States and Asia in future crises or conflicts. The affected organisations are active in the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors.

Timeline
Mid-2021 – present

Initiator
Chinese state-sponsored hacking group Volt Typhoon (aka BRONZE SILHOUETTE/Vanguard Panda/UNC3236/Insidious Taurus/VOLTZITE fka Storm-0391/DEV-0391/TAG-87)

Incident Type
Data theft; Hijacking with Misuse

Affected Targets
Government/Ministries, Critical Infrastructure (Energy, Water, Transportation, Telecommunications) in Guam and the United States

Impact and significance

Volt Typhoon's activity was especially significant considering the sectors targeted: critical infrastructure which US officials would later candidly explain had no legitimate intelligence-gathering significance. [1] Microsoft assessed that Volt Typhoon's targeting of these sectors, particularly communications, was for prepositioning to disrupt military-vital communications between the United States and Asia, with Guam mentioned specifically, in the event of a conflict over Taiwan.

Despite Microsoft's politically-tinged disclosure, the concurrent Five Eyes (FVEY) joint security advisory focussed solely on the technical aspects of the campaign. [3] However, a 2025 interview with General Paul Nakasone, former Commander of the US' Cyber Command and former Director of the National Security Agency (NSA), echoed Microsoft's earlier assessment plainly: "China has eclipsed all of our adversaries in terms of the scope and scale and now the sophistication of what they're doing. [. . .] This is intended to provide a capability at some point in the future that allows the Chinese to wreak havoc or spark a crisis [if they] enter a period of tension with the United States." [1]

Exactly that risk was emphasised by FBI Director Christopher Wray, who claimed in a House Select Committee meeting on Volt Typhoon that the group's activity and stealth impacts "every American," stating that malicious Chinese activity, including Volt Typhoon, poses "the defining threat of our generation." [5] He went on to highlight China's rapid development of threat capabilities by saying "we are no longer in the Advanced Persistent Threat 1, or 'APT1', days of [China's] cyber program" – in other words, Chinese threats are becoming much more complex, harder to detect, and are much more impactful to national security.

The Volt Typhoon case has wide-ranging implications on United States security and serves as a lesson for critical infrastructure operators globally, especially as other states (e.g., Russia) take part in prepositioning activities to prepare for escalation elsewhere. [53] The significance of Volt Typhoon and general prepositioning lies less in what *has* happened, but more in what *could* happen if the access into critical infrastructure systems should ultimately be exploited. The potential impact on civilians could be severe: communications cut and access to energy disrupted, with cascading societal effects to follow (see Bigger Picture I and II). Furthermore, if the US is correct in its attribution and assessment of motives, a potential exploitation of Volt Typhoon's longstanding access could significantly impact US military operations in the Pacific, further endangering its national security objectives.

Regarding Volt Typhoon's targeting of Guam, it should be noted that Guam is a crucial hub for international submarine data cables connecting the US and Asia, as well as North and South Asia. [15, 16, 17] The consequences of disruptions to this infrastructure can range from a degradation in service quality to a complete breakdown of connectivity. Data from the European Repository of Cyber Incidents (EuRepoC) shows that most disruptions to critical infrastructure last between 24 hours and a week, [3] yet even short-lived disruptions to communications could hinder the US' ability to respond effectively during a crisis over Taiwan. [13] This threat is exacerbated by the fact that Guam is closer to East Asian capitals than the continental US and would therefore serve as a crucial logistics hub for supplies heading to the Western Pacific. Thus, while the campaign's publicly documented compromises were primarily of critical infrastructure rather than US military bases themselves, Volt Typhoon's activity in Guam was potentially significant because the island hosts major US military facilities and serves as a key power-projection hub in the Indo-Pacific. Air assets operating from Guam would likely play an important role in a Taiwan contingency and could be among the first to respond to such

a conflict, including through Agile Combat Employment (ACE). Furthermore, besides hosting air assets and Marine ground units, [14] Guam also supports the US Navy's Pacific Fleet, Fifth Fleet and Seventh Fleet, including forward-deployed naval forces which could respond in a Taiwan contingency. [4]

The Bigger Picture I: Pre-Positioning on Critical Infrastructure

Previous incidents indicate that Volt Typhoon fits into a larger pattern of state-sponsored threat actors compromising systems related to critical infrastructure. In these instances, the groups gained access to the industrial control systems (ICS) of critical infrastructure providers, giving them the ability to deploy disruptive effects against their targets.

Between 2011 and 2014, and between 2015 and 2017, the threat actor known as Ghost Blizzard (fka BROMINE/Energetic Bear/Berserk Bear/Dragonfly/Crouching Yeti/DYMALLOY/Group 24/Havex/TEMP.Isotope/TG-4192/IRON LIBERTY/G0035/ALLANITE/CASSTLE) compromised energy utility companies in both the United States and Europe. The actor targeted the industrial control systems (ICS) of oil and gas firms, nuclear power providers, and other utilities, which would have allowed it to disrupt the functioning of the breached systems. Later reporting demonstrates that the actor used a similar technique to Volt Typhoon for its initial compromise: it used known vulnerabilities in large numbers of small office home office (SOHO) routers to gain initial access before pivoting to compromise additional devices on the same network. While Ghost Blizzard used native commands to reduce its footprint on compromised networks like Volt Typhoon, it also differed from Volt Typhoon by using custom tools such as the malware known as SYNful Knock. [60] The similarity of both Ghost Blizzard and Volt Typhoon lies in their deliberate targeting of critical infrastructure systems to enable future disruptions in the event of a crisis.

On the 29 and 30 December 2025, Ghost Blizzard sabotaged energy infrastructure in Poland, using destructive wiper malware to target combined heating and power plants. The attack was described by Polish ministers as the most severe attack on energy infrastructure in recent history. Both technical reporting by ESET and Dragos, as well as political statements by the European Union and the United Kingdom, attributed the attack to the 16th Centre of the Russian Federal Security Service (FSB), also known as the "Centre for Radio-Electronic Intelligence by Means of Communication" (TsRRSS, Military Unit Number 71330). [63] Centre 16, which has been active since at least 2010, comprises two sections and ten departments, tasked with collecting foreign signals intelligence for the Russian government using facilities across the Russian mainland. [61, 62] Centre 16 is also responsible for offensive cyber operations focussing on critical infrastructure in Europe and North America. In the case of Centre 16's targeting of the Polish power grid, the Polish government stated that the attack did not lead to negative consequences to the general population such as blackouts, transmission disruptions, or system destabilisation. [64] However, Dragos nevertheless reported that, while the attack was unsuccessful in causing service disruptions for the broader civilian populace or destroying workstations, the attack "resulted in loss of view, loss of control, and denial-of-service conditions" at targeted facilities. [65] It should be noted that, in the Volt Typhoon case, the attackers were able to infiltrate a larger number of systems over a wider array of sectors, which could have potentially increased the impact of a Volt Typhoon disruption compared to Ghost Blizzard's operation.

Background

The People's Republic of China's (PRC's) increasing opening to global markets, coupled with the rapid growth of its domestic economy since the turn of the century, has brought it into close competition with the United States on a range of issues. [8] Cyberspace is not immune to this competition: China's National Cyber Strategy from 2016 highlights Chinese decisionmakers' understanding that cyberspace is a resource which states can

utilise to dictate norms and/or gain a strategic advantage. However, the cyber domain is primarily oriented towards the internal sphere, with the 2016 Chinese National Cyber Strategy focussing on the threats that cyberattacks pose to political, economic, and cultural security of the PRC. [9] As China views Taiwan as its sovereign territory and believes that US involvement in Taiwan violates China's rights under international law, China's actions in cyberspace must therefore be understood primarily as measures to prevent US intervention in its internal affairs, as well as to ensure the survival of the state and the Chinese Communist Party (CCP) in light of the fear that the US wants to end CCP rule. [10, 11, 12] In this view, since the infiltrated systems aid the US military to violate Chinese sovereignty, Volt Typhoon's activities contributed to Chinese self-defence.

Meanwhile, the US sees Taiwanese sovereignty as an important objective. According to the 1979 Taiwan Relations Act, the US must be able to "resist any resort to force or other forms of coercion that would jeopardise the security, or the social or economic system, of the people on Taiwan." [69] Today, this means that the US still sees itself as responsible for assisting Taiwan in its own defence and deterring China [70] from any unilateral change of status across the Taiwan Strait. Meanwhile, for the US, the functioning of critical national infrastructure (CNI) is considered a central pillar of national security; in the 2023 US National Cyber Strategy, the compromise of CNI is considered a threat to "the safety, security, and prosperity of the American people" and its defence central to US power projection. [71] Any attempts by China to disrupt US logistics chains are therefore seen as endangering not only Taiwan, but also as a threat to general US interests abroad and the safety of its population at home.

Aside from Volt Typhoon, Chinese state-sponsored actors have been attributed to other incidents connected to political crises in the South China Sea region. In August 2023, the Chinese advanced persistent threat (APT) Stately Taurus was attributed to a series of coordinated espionage campaigns targeting government entities in the South Pacific, including in the Philippines. Technical researchers connected the incidents to tensions between the PRC and the Philippines concerning territorial claims over the Spratly Islands; tensions peaked when a Chinese Coast Guard vessel fired its water cannon at a Philippine vessel resupplying the Second Thomas Shoal. [77] The targeted countries and entities, as well as the timing of the intrusions, indicate a connection between the physical and digital incidents. Similarly to Volt Typhoon, perceived threats to Chinese territorial claims are confronted with offensive cyber operations by Chinese state-sponsored actors.

Volt Typhoon represents the first instance in which Chinese activity was explicitly associated with future destructive potential. EuRepoC incident data shows that Chinese cyber operations prioritise intelligence collection over disruptive effects, focussing primarily on telecommunications and energy sectors. In almost all of the recorded incidents initiated by state and state-affiliated actors in China, an initiator exfiltrated information without causing any further harm to a network. [7] This operation type is common for intelligence collection as it maintains a small footprint on targeted systems while enabling the acquisition of information of interest to a threat actor.

The Bigger Picture II: Chinese Cyber-Military Doctrine in Action

Volt Typhoon serves as a revealing case study through which to analyse Chinese cyber-military doctrine in action. In the 2020 edition of *The Science of Military Strategy* (战略学), one of the People's Liberation Army's (PLA's) primary doctrinal documents, senior Chinese military officers notably recognise cyberspace as a fifth dimension of warfighting, with equal importance placed on the cyberspace as on other battlefield domains: land, sea, air, and space. Lieutenant General Xiao Tianling posits that large-scale cyberattacks against an adversary's infrastructure can cause social unrest and chaos, thus serving to "directly affect [a] country's war potential" and lowering the will to fight in times of conflict. [21] According to the authors of *SMS*, this is evident in the initial successes of the US' invasion of Iraq in 2003, which was in part enabled by US dominance over Iraqi forces in cyberspace: cyber operations allowed the US to paralyse Iraqi government and military command and thus "disintegrate" minds, military, and morale. [21] This chaos is vital to operational success in conflict: reflecting on Operation Allied Force, NATO's bombing campaign against the Yugoslav Federation in 1999, the authors of *SMS* note that Yugoslav forces did not surrender after NATO's airstrike campaign, but rather after Serbia's hydroelectric infrastructure was disrupted in June 1999 due to "blackout bombs" (graphite bombs), the effects of which could be replicated through cyber means. One senior US officer at the time put it bluntly: "Just think if after the first day, the Serbian people had awakened and their refrigerators weren't running, there was no water in their kitchens or bathrooms, no lights… they would have asked: 'All this after the first night? What is the rest of this going to look like?'" [18]

Due to the flexibility of cyber operations, cyberattacks can also serve to disrupt command, control, communications, computer, intelligence, surveillance, reconnaissance, and kill (C4ISRK) infrastructure as a whole, even from afar – effects that even conventional strikes may not be able to achieve, especially when taking into account geographical limitations on strike capabilities. Cyberspace is therefore so important to military success that the authors declared that "[. . .] cyber operations [have] become the core center for winning wars without exception. The victory of the war begins with the victory of cyberspace." [21]

Chinese threat actors have already started testing such operations in smaller conflict settings against less powerful opponents: in 2020, when China and India had a border skirmish that led to the first combat deaths in decades, several thousand Chinese cyberattacks hit various Indian critical infrastructure targets during the fighting. [54] Meanwhile, other Chinese threat groups such as RedEcho have been observed prepositioning in Indian energy infrastructure, both for strategic signaling and potentially to disrupt in the event of renewed kinetic conflict. [55] In order to inform its own cyber-military efforts, Chinese strategists have also been closely observing Russian cyberwarfare in Ukraine, seeking to understand why Russian cyberattacks against Ukraine at the start of the 2022 full-scale invasion did not achieve their goals. China ascribed these failures to a lack of unified cyber command, lack of civil-military cooperation, outdated Soviet-era signals intelligence methods, and reliance upon a commercially-driven private sector with little commitment to national interests. These failures led to a subsequent restructuring of the PLA's makeup. [56] As the PLA ultimately links Russia's shortcomings to systemic deficiencies rather than to inherent limitations of cyberspace itselfcyberspace is still the centre for winning wars, particularly when technological capacities match an adversary's, cyber command structure is modernised, private/state interests align, and strategic culture focusses on "surgical" cyberattacks rather than pure destruction.

To this point, two doctrinal beliefs are especially important to discuss in the case of Volt Typhoon's targeting of the US: the blurring of peacetime and wartime and the notion of "acupuncture warfare." Regarding the former, Chinese strategists recognise the importance of peacetime operations like Volt Typhoon in preparation for war, with "peacetime-wartime" operations serving both as a method of deterrence (i.e., indicating to an adversary what capabilities the state holds, so as to dissuade action being taken against the initiating state) and a method of psychological warfare (i.e., demoralisation to break resistance in the event of conflict). Acupuncture warfare, meanwhile, is a form of asymmetrical warfighting which conceptually dates back to 1997 (but draws on ancient strategic thought, e.g., Sun Tzu's *The Art of War*; see particularly Chapter III, "Attack by Stratagem," or even more recently in the writings of Mao Zedong; see *On Guerrilla Warfare*). [19, 20] "Acupuncture warfare" refers to the warfighting strategy of targeting weaker command-and-control nodes to disorient a conventionally superior enemy; this idea is visible in Volt Typhoon's targeting of communications infrastructure between the US and Guam with the goal of disrupting military coordination.

Volt Typhoon Campaigns (2020-present)

Timeline is based on reported start date.

Early-mid 2020 — **Living-off-the-land campaign against multiple sectors** [22]

CrowdStrike reported VANGUARD PANDA living-off-the-land activity beginning in mid-2020 and targeting victims in unnamed sectors, citing "familiarity with target environment."

Hijacking Without Misuse

Mid-2021 — **Living-off-the-land campaign against US/Guam** [23]

Volt Typhoon campaign targeting critical infrastructure in US and Guam, with the goal of prepositioning for future disruption.

Data Theft | Hijacking with Misuse

2022 — **Compromise of US critical infrastructure targets** [24]

Volt Typhoon compromised unnamed targets in energy, water, communications, and transport in Hawai'i, the US West Coast, and more.

Hijacking Without Misuse

December 2023 — **Compromise of Telecom Provider in New Caledonia** [25]

Threat researchers reported that Volt Typhoon compromised a telecommunications provider and potentially compromised US, UK, and Australian government infrastructure through the breach.

Hijacking Without Misuse

June 2024 — **Versa Director Zero-Day Exploitation** [26]

Volt Typhoon used a botnet to breach four US victims and one non-US victim using a zero-day in Versa Director; the victims were internet service providers, managed service providers, or otherwise in the IT sector.

Data Theft | Hijacking with Misuse

June 2024 — **Singapore Telecommunications Breach** [27]

Volt Typhoon breached SingTel and deployed malware, which was assessed as a potential initial attempt to stage further incidents against victims in the United States.

Data Theft

2025 — **Sierra Wireless Airlink cellular gateway breach** [28]

Volt Typhoon was observed compromising Sierra Wireless Airlink cellular gateways to access US midstream pipeline operations. The threat actors were found to be investigating operational conditions which would trigger process shutdowns.

Data Theft | Hijacking with Misuse

Attribution

On 24 May 2023, Microsoft Threat Intelligence published a technical advisory detailing Volt Typhoon's malicious activity. The researchers assessed with "moderate confidence" that the threat actor was developing disruptive capabilities to use them in the case of regional crises in Asia. [2] As the report represents the first naming of the threat actor, the report does not tie the actor to previous activity. Microsoft concedes that it has not yet established a comprehensive understanding of Volt Typhoon. Microsoft stated that the actor is based in China and its behaviour is consistent with intelligence collection as well as operational persistence. Further indication of state-sponsored activity is the targeting of communications infrastructure between the United States and Asia.

On the same day, the Five Eyes (FVEY) intelligence alliance published a Joint Cybersecurity Advisory; the authoring agencies comprised the US National Security Agency, the US Cybersecurity and Infrastructure Security Agency, the US Federal Bureau of Investigation, the Australian Signals Directorate, the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, New Zealand's National Cyber Security Centre and the United Kingdom's National Cyber Security Centre. [3] While the Microsoft report addressed Volt Typhoon's motives and focussed on mitigation using Microsoft security software, this FVEY advisory helped the security community detect Volt Typhoon activity on its networks by publishing artefacts the actor could have left behind as well as indicators of compromise (IOCs). The threat actor is said to have exploited vulnerabilities CVE-2021-40539 and CVE-2021-27860, the former of which is a vulnerability that US security agencies had previously connected to Chinese state-sponsored actors. [29] Based on the operational details of the incident, it is likely that the Chinese government initially intended to remain undetected to maintain the option to disrupt US critical infrastructure in case of a conflict, which US officials confirmed in a subsequent Joint Cybersecurity Advisory in 2024. [47]

Both Microsoft and the Five Eyes agencies stopped short of assigning responsibility for Volt Typhoon to a specific agency of the Chinese government. Researchers later identified multiple threat groups which they assessed to have collaborated with Volt Typhoon, including SYLVANITE, which researchers deem works as an initial access broker for Volt Typhoon; this means that SYLVANITE rapidly exploits publicly-disclosed vulnerabilities, gains unauthorised access to victims' systems, and then passes stolen credentials to Volt Typhoon. [38, 39] Dragos researchers assess that SYLVANITE overlaps with various threat groups (UNC5221, UNC5174, UNC5291, UNC3236, HOUKEN, Red Dev 61, CL-STA-0048, UTA0178) which have been previously attributed to espionage activity for the Chinese Ministry of State Security. [6, 40] The overlap with these groups' contractual work for state actors suggests that SYLVANITE, too, may be conducting offensive cyber operations on contract for the Chinese government or military. The existence of such contractual relationships in China has previously been confirmed through leaked documents from cybersecurity contractor i-Soon, as well as reporting on APT31, Salt Typhoon, and Flax Typhoon. [41, 42, 43, 44, 45] Such

a relationship between Volt Typhoon and SYLVANITE indicates that Volt Typhoon is a state actor, working on behalf of the PRC government.

While the US government described Volt Typhoon as "state-sponsored", no official federal-level US attribution ties Volt Typhoon to a specific Chinese state entity. Some public sector reporting, such as from the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), argued that the actor's targeting patterns suggested a "likely affiliation" with the People's Liberation Army or the Ministry of State Security, without providing further evidence. [37] Additional analysis, including a EuRepoC APT Profile, have also inferred that Volt Typhoon was part of the PLA's Strategic Support Force. [46][1] In August 2026, Jen Easterly, the former Director of the Cybersecurity and Infrastructure Security Agency (CISA), confirmed in a *Foreign Affairs* interview that Volt Typhoon is part of the PLA. [78] This represents the first instance in which a (former) senior US official has publicly and explicitly tied Volt Typhoon to the People's Liberation Army, and it further reinforces the possibility that SYLVANITE does, in fact, work as a PLA contractor.

The Chinese reaction to the US attribution of Volt Typhoon as a Chinese state-sponsored actor is of particular interest in this case. In the immediate aftermath of the US/FVEY attribution, a spokesperson for the Chinese Foreign Ministry accused the US and its FVEY allies of spreading disinformation, [30] citing missing evidence as proof of unprofessional work by the US. This was followed by a July 2023 attribution by Chinese state media detailing a government-backed intrusion of the Wuhan Earthquake Monitoring Centre, which it stated originated from the US. [73] From April to October 2024, following the US takedown of a botnet reportedly used by Volt Typhoon (see "Legal Assessment" for more information), [31] the Chinese National Computer Virus Emergency Response Centre (CVERC) published a three-part series of reports accusing the US intelligence community of waging a disinformation campaign against the US Congress in order to acquire more funding. [32, 33, 34] The reports cite US surveillance programmes to demonstrate that the US is responsible for extensive cyber espionage, while pointing the finger at a ransomware group called Dark Power as the actor to blame for the Volt Typhoon incident. Furthermore, in its third report in the series, CVERC attributes the Office of Tailored Access Operations (TAO) of the NSA to earlier breaches impacting the Northwestern Polytechnical University and the aforementioned Wuhan Earthquake Monitoring Centre. The publication continues by accusing the US military base in Guam which was allegedly the target of Volt Typhoon's campaign as being the initiator of a "large number of cyberattacks" against China. [34]

However, in April 2025, the Wall Street Journal released an article claiming that Chinese officials privately admitted responsibility for Volt Typhoon. Citing anonymous individuals familiar with the matter, the article explained that Chinese representatives at a meeting in Geneva had tacitly implied that the intrusions were intended to deter US support for

[1] Note: The Strategic Support Force was disbanded in 2024 and was succeeded by the Information Support Force, the Aerospace Force and the Cyberspace Force. The latter likely inherited responsibility for Chinese offensive cyber operations.

Taiwan in the event of a conflict. [35] In what could be a reaction to this disclosure, the Harbin Public Security Bureau stated a week after the article's publication that it was pursuing members of the US National Security Agency (NSA) over cyberattacks targeting the Asian Winter Games which had been held in winter of 2025. [36]

Previous attributions of cyber operations to US intelligence agencies by Chinese institutions have provided little solid evidence for their claims and indicate a larger tit-for-tat pattern of attributions. Following a June 2022 US attribution of malicious cyber activity to PRC state-sponsored actors, for example, CVERC published a report alongside Chinese technology company Qihoo 360, assigning responsibility for the aforementioned attack on the Northwestern Polytechnical University to the NSA. [72] The report published details of the infrastructure allegedly used to conduct the intrusions, along with names of alleged front companies, the NSA departments involved in the attack, and specific names of individuals that they deemed responsible.

Other instances lend further credence to this observed pattern: in October 2025, following a US-led joint advisory blaming Chinese technology companies for intrusions affecting critical infrastructure targets around the world, Chinese authorities stated that the NSA had infiltrated the National Time Service Centre between March 2022 and June 2024. [74] Likewise, following the US disruption of a botnet used by Chinese state-sponsored threat actors in August 2026, Chinese authorities rejected US claims and pointed to incidents previously linked by China to the US, including the aforementioned National Time Service Centre breach. [75] In that exchange, Chinese state-controlled media referenced a technical report by Qi An Pangu Labs which also attributed multiple instances of data theft affecting Chinese government and technology targets to an emerging sophisticated threat group from North America which it dubbed NightEagle. [76] These spats, including the Chinese response to the Volt Typhoon attribution, demonstrate a widespread pattern of tit-for-tat attribution behaviour: when the US accuses China of malicious cyber activity, whether through attributions or technical takedowns, China makes counter-accusations to condemn alleged violations of Chinese sovereignty.

Attribution Timeline

24 May 2023	Microsoft/FVEY first attribute Volt Typhoon
25 May 2023	Chinese government denies involvement in Volt Typhoon intrusion
31 January 2024	US Government Takes Down Botnet used by Volt Typhoon
15 April 2024	Chinese National Computer Virus Emergency Response Centre published first report accusing US intelligence agencies of lying to Congress for higher budgets
8 July 2024	Chinese National Computer Virus Emergency Response Centre published second report attributing Volt Typhoon to DarkPower ransomware group
6 October 2024	Chinese National Computer Virus Emergency Response Centre published third report accusing the US of being behind the Volt Typhoon incident
December 2024	Chinese officials reportedly admit that China was responsible for Volt Typhoon
10 April 2025	Wall Street Journal publishes article reporting Chinese admission of responsibility for Volt Typhoon
15 April 2025	Harbin Public Security Bureau states that it was pursuing three named NSA hackers

Technical details

The use of living-off-the-land (LOTL) techniques, in which attackers use legitimate tools to stealthily infiltrate a victim's network, evade detection, and move laterally, made Volt Typhoon's targeting of critical infrastructure both in the mainland United States and in Guam particularly concerning. These techniques, combined with the use of small-office/home-office (SOHO) routers, made the overall communications and traffic of the threat group harder to detect; in its original report on the threat actors, Microsoft itself cited a general lack of visibility into parts of the group's activity. [2] Volt Typhoon's actions on a technical level are aimed at maintaining persistence on information technology related to operational technology (OT) of US critical infrastructure. The actor

makes significant efforts to gain access unnoticed, remain undetected once a system has been breached, and obfuscate the extraction of data. While US security agencies assess that the details of each compromise are adapted based on deliberate reconnaissance activity, they do find a common pattern of behaviour across multiple targets. After reconnoitering the intended target, the actor gains unauthorised access by exploiting vulnerabilities in public network appliances, in many cases SOHO routers, connecting via a virtual private network (VPN). Volt Typhoon then leverages internal vulnerabilities to obtain administrator credentials in order to move laterally to the domain controller from which it collects intelligence on the compromised network. By extracting the Active Directory database and using offline password cracking techniques to gain access to the plaintext passwords, the actor gains access to further assets connected to the network, including a number of OT systems. Varying from target to target, this access could have enabled Volt Typhoon to cause a variety of physical effects, including those that could have disrupted the functioning of critical infrastructure systems.

Enablers

Volt Typhoon's use of a botnet targeting end-of-life routers enabled the group to remain undetected for as long as it did. "End-of-life" devices are those which are old and do not receive regular security patches, making them especially vulnerable to such an attack. A complicating factor is that, without knowledge of an infection, owners of these routers have little reason to restart their routers, which would normally remove the malware (but would not prevent the router from reinfection). [38] Furthermore, for network defenders, the use of such a botnet enabled Volt Typhoon to transmit encrypted communications between infected routers, thus obfuscating the location of the group and allowing it to blend in with normal traffic, while living-off-the-land techniques and the theft of credentials from victims' networks enabled the group to maintain access to systems.

Private Sector Engagement

- Amazon Web Services Security (Infrastructure Discovery & Detection)
- Broadcom (TTP Information Collection, Threat Actor Tracking)
- Cisco Talos (Threat Actor Tracking)
- Google's Threat Analysis Group (Threat Actor Tracking)
- Lumen Technologies (Infrastructure Discovery)
- Mandiant (Threat Actor Tracking)
- Microsoft Threat Intelligence (Public Reporting on TTPs & Mitigation Guidance)
- Palo Alto Networks (Threat Actor Tracking)
- Secureworks (Incident Response)
- SentinelOne (Threat Actor Tracking)
- Trellix (Threat Actor Tracking)

Legal Assessment

On the domestic stage, the legal response to Volt Typhoon manifested itself in the DOJ/FBI's court-authorised takedown of part of the group's botnet in January 2024. The takedown was based in federal US law (Federal Rule of Criminal Procedure 41[b][6]) and involved four search warrants in the Southern District of Texas. [38] With the court's order, the FBI remotely sent commands to search and delete the KV botnet from infected US-based routers. [48] The domestic aspect of this takedown should be noted: while the FBI/DOJ operation was limited by legal constraints to only allow remote access to domestic routers, the KV botnet operates worldwide, leading some cybersecurity analysts to question its effectiveness in the long run. [49]

On the international stage, the response to Volt Typhoon has been overwhelmingly muted for a number of reasons. Cyber espionage is largely unregulated by international legal frameworks unless it damages critical infrastructure or otherwise inhibits its provision of services, neither of which Volt Typhoon did. [50] Furthermore, dual-use infrastructure (e.g., communications networks facilitating military action) could potentially be a legitimate and legal target in war, if (1) the use of such infrastructure makes an effective contribution to military activity, and (2) the destruction of such brings a military advantage, [51] yet the illegality of prepositioning without any further malicious activity or disruption of services in peacetime is questionable. In any case, at the Munich Security Conference in 2024, then-Deputy National Security Adviser for Cyber and Emerging Technologies, Anne Neuberger, condemned Volt Typhoon's targeting of civilian infrastructure while calling to "put rules in place," likely intending to signal to China that their activity may not be compliant with norms on responsible state behaviour. [52]

Despite this attempt by the Biden administration to reinforce norms, it should be noted that the Trump administration reportedly authorised the use of cyber means to shut off lights and energy infrastructure, disrupt internet connection, and even to (allegedly) interfere with Russian and Chinese air defence and radar systems in the January 2026 US operation to capture Venezuelan President Nicolás Maduro. [59] While the operation as a whole is already largely deemed legally dubious at best and highly illegal at worst, both under domestic and international law [57, 58], questions on cyberspace's role within the operation, and the legality of such, remain unanswered. Temporally, it is unclear whether cyber operations involved prepositioning or were undertaken after the kinetic operation had begun; meanwhile, some legal analysts posit that an operation cutting electricity could be justified if the cutting of power was done with the goal of disrupting air defence systems. [66] While some downstream results of the power outage are unclear (e.g., if deaths resulted from blacked-out healthcare facilities), the use of cyberspace to facilitate kinetic operations against a country officially in peacetime (with US authorities dubbing the operation a "law enforcement operation") [68] highlights a narrative shift away from the norm reinforcement that Neuberger sought to pursue vis-à-vis China.

Novelty of the Attack

On a technical level, Volt Typhoon's campaign was not especially novel: none of the techniques used for the campaign were new. However, what made the campaign important was its use of extreme measures to remain undetected, which SecureWorks tied to pressure from Chinese leadership to "avoid scrutiny of its cyberespionage activity" following several US indictments of Chinese threat actors. [67] To this end, Microsoft cited "almost exclusive" use of living-off-the-land techniques and hands-on-keyboard activity to remain undetected. While the campaign did not ultimately disrupt the services targeted, Volt Typhoon's extreme efforts to retain operational security, combined with its alleged goal of destabilising the US and hindering its ability to respond in a crisis over Taiwan, make the campaign acutely important.

Sources

[1] Dina Temple-Raston (2025). *Exclusive: Gen. Paul Nakasone says China is now our biggest cyber threat*. The Record. Available at https://web.archive.org/web/20250401163736/https://therecord.media/nakasone-interview-china-ai-deepseek-doge [Archived on: 1 April 2025].

[2] Microsoft Threat Intelligence (2023). *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques*. Microsoft. Available at https://web.archive.org/web/20230524193651/https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/ [Archived on: 24 May 2023].

[3] Cybersecurity and Infrastructure Security Agency (2023). *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*. Available at https://web.archive.org/web/20260412180814/https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a [Archived on: 12 April 2026].

[3] European Repository of Cyber Incidents. *Critical Infrastructure Tracker*. Available at https://cit.eurepoc.eu/

[4] Joint Region Marianas. *Naval Base Guam: Installations*. United States Navy. Available at https://web.archive.org/web/20260805080715/https://jrm.cnic.navy.mil/Installations/Naval-Base-Guam/About/Installations/ [Archived on: 5 August 2026].

[5] Christopher Wray (2024). *Opening Statement: The CCP Cyber Threats to the American Homeland and National Security*. Speech delivered to House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party. Available at https://web.archive.org/web/20250415092309/https://www.fbi.gov/news/speeches-and-testimony/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party [Archived on: 15 April 2025].

[6] Josh Hanrahan (2024). *VOLTZITE Espionage Operations Targeting U.S. Critical Systems*. Dragos Intelligence Brief. Available at https://web.archive.org/web/20260728114941/https://hub.dragos.com/hubfs/116-Datasheets/Dragos_IntelBrief_VOLTZITE_FINAL.pdf [Archived on: 31 July 2026].

[7] Kerstin Zettl-Schabath, et al. (2025). *Global Dataset of Cyber Incidents* (1.3.2) [Data set]. European Repository of Cyber Incidents. Available at https://web.archive.org/web/20260211084058/https://zenodo.org/records/14965395 [Archived on: 11 February 2026].

[8] Zeno Leonie (2024). *4 - Between Competition and Restraint: The Implications of Weaponized Economic Interdependence on US - China Relations*. In: *A New Cold War: US - China Relations in the Twenty-first Century*. Cambridge University Press. Available at https://web.archive.org/web/20260731130742/https://www.cambridge.org/core/books/abs/new-cold-war/between-competition-and-restraint-the-implications-of-weaponized-economic-interdependence-on-uschina-relations/EBA25B6210964D3391C022CBFCB43316 [Archived on: 31 July 2026].

[9] Cyberspace Administration of China (2016). *National Cyberspace Security Strategy*. Available at https://web.archive.org/web/20260731130740/https://www.cac.gov.cn/2016-12/27/c_1120195926.htm [Archived on: 31 July 2026].

[10] Abraham Denmark (2021). *Chapter 4. Trends of the Times: Foundations of Beijing"s View on Competition With the United States*. In: *SMA Perspectives: Emergent Issues for US National Security US versus China: Promoting 'Constructive Competition' to Avoid 'Destructive Competition'*. Available at https://web.archive.org/web/20250614231830/https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/sma-perspectives_usvchina-competition-mastro_0.pdf [Archived on: 31 July 2026].

[11] Wang Jisi & Hu Ran (2019). *From cooperative partnership to strategic competition: a review of China-U.S. relations 2009-2019*. In: *China International Strategy Review*. The Institute of International and Strategic Studies (IISS). Peking University. Available at https://doi.org/10.1007/s42533-019-00007-w.

[12] Ministry of National Defense of the People's Republic of China (2022). *The Taiwan issue and the cause of Chinese unification in the new era*. Available at https://web.archive.org/web/20260731131750/http://www.mod.gov.cn/gfbw/qwfb/yw_214049/4917828.html?big=fan [Archived on: 31 July 2026].

[13] Annie Fixler, RADM Mark Montgomery (Ret.), Rory Lane (2025). *Military Mobility Depends on Secure Critical Infrastructure*. Cyberspace Solarium Commission. Available at https://web.archive.org/web/20260731131900/https://cybersolarium.org/csc-2-0-reports/military-mobility-depends-on-secure-critical-infrastructure/ [Archived on: 31 July 2026].

[14] Andres Tilghman (2023). *Guam: Defense Infrastructure and Readiness*. Congressional Research Service R47643. Available at https://web.archive.org/web/20260731132708/https://www.congress.gov/crs-product/R47643 [Archived on: 31 July 2026].

[15] TeleGeography (2026). *Submarine Cable Map*. Available at https://web.archive.org/web/20260731133256/https://www.submarinecablemap.com/ [Archived on: 31 July 2026].

[16] Submarine Cable Networks (2026). *USA-Guam*. Available at https://web.archive.org/web/20260731134001/https://www.submarinenetworks.com/en/stations/north-america/usa-guam [Archived on: 31 July 2026].

[17] Geoff Huston (2022). *The politics of submarine cables in the Pacific*. Asia Pacific Network Information Centre. Available at https://web.archive.org/web/20260731133954/https://blog.apnic.net/2022/06/02/the-politics-of-submarine-cables-in-the-pacific/ [Archived on: 31 July 2026].

[18] Kristen M. Thomasen (2008). *Air Power, Coercion, and Dual-Use Infrastructure: A Legal and Ethical Analysis*. In *International Affairs Review*. Available at https://web.archive.org/web/20081230035212/http:/www.iar-gwu.org/node/40 [Archived on: 30 December 2008].

[19] Sun Tzu (n.d.). *The Art of War*. Translated by Lionel Giles (1910). Available at https://web.archive.org/web/20260213205538/https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf [Archived on: 13 February 2026].

[20] Mao Tse-Tung (1937). *On Guerrilla Warfare*. Translated by Brigadier General Samuel B. Griffith (1961). Available at

https://web.archive.org/web/20260201031915/https://www.marines.mil/Portals/1/Publications/FMFRP%2012-18%20%20Mao%20Tse-tung%20on%20Guerrilla%20Warfare.pdf [Archived on: 1 February 2026].

[21] Xiao Tianliang, Lou Yaoliang, et al., eds. (2020). *The Science of Military Strategy. National Defense University Press*. Translated by the China Aerospace Studies Institute, January 2022. Available at https://web.archive.org/web/20250618170430/https://www.govinfo.gov/content/pkg/GOVPUB-D301-PURL-gpo195080/pdf/GOVPUB-D301-PURL-gpo195080.pdf [Archived on: 18 June 2025].

[22] European Repository of Cyber Incidents (2023). *Chinese state-sponsored hacking group VANGUARD PANDA aka Volt Typhoon gained access to computers systems of multiple high-value targets.* Available at https://eurepoc.eu/table-view/?cyber_incident=2404

[23] European Repository of Cyber Incidents (2023). *Chinese state-sponsored hacking group Volt Typhoon gained access to critical infrastructure organisations on Guam and US mainland beginning in mid-2021.* Available at https://eurepoc.eu/table-view/?cyber_incident=2276

[24] European Repository of Cyber Incidents (2023). *Chinese APT Volt Typhoon compromised US critical infrastructure targets in 2022*. Available at https://eurepoc.eu/table-view/?cyber_incident=2900

[25] European Repository of Cyber Incidents (2024). *Chinese APT Volt Typhoon compromised telecommunication provider of Southwest Pacific Islands of New Caledonian in December 2023*. Available at https://eurepoc.eu/table-view/?cyber_incident=3014

[26] European Repository of Cyber Incidents (2024). *China-linked APT Volt Typhoon exploited a zero-day in Versa Director in June 2024*. Available at https://eurepoc.eu/table-view/?cyber_incident=3737

[27] European Repository of Cyber Incidents (2024). *Chinese state-sponsored hacking group Volt Typhoon compromised Singaporean telecom provider Singapore Telecommunications (SingTel) in June 2024.* Available at https://eurepoc.eu/table-view/?cyber_incident=4017

[28] European Repository of Cyber Incidents (2026). *Voltzite Compromised Sierra Wireless Airlink Cellular Gateways In 2025*. Available at https://eurepoc.eu/table-view/?cyber_incident=5311

[29] National Security Agency, et al. (2022). *Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors*. Joint Cybersecurity Advisory. Available at https://web.archive.org/web/20230525163916/https://media.defense.gov/2022/Oct/06/2003092365/-1/-1/0/Joint_CSA_Top_CVEs_Exploited_by_PRC_cyber_actors.PDF [Archived on: 6 October 2022].

[30] Mao Ning (2023). *Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on May 25, 2023*. Ministry of Foreign Affairs of the People's Republic of China. Available at: https://de.china-embassy.gov.cn/det/lcbt/wjbfyr/202405/t20240530_11347530.htm

[31] United States Department of Justice (2024). *U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure*. Available at: https://web.archive.org/web/20260731135814/https://www.justice.gov/archives/opa/pr/us-

government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical [Archived on: 31 July 2026].

[32] National Computer Virus Emergency Response Center (2024). *Volt Typhoon: A Conspiratorial Swindling Campaign Targeting U.S. Congress and Taxpayers Conducted by U.S. Intelligence Community*. Available at: https://web.archive.org/web/20260712103248/https://www.cverc.org.cn/head/zhaiyao/news20240415-FTTF.htm [Archived on: 31 July 2026].

[33] National Computer Virus Emergency Response Center (2024). *Volt Typhoon II: A Secret Disinformation Campaign Targeting U.S. Congress and Taxpayers Conducted by U.S. Government Agencies*. Available at: https://web.archive.org/web/20260720145326/https://www.cverc.org.cn/head/zhaiyao/news20240708-FTTFER.htm [Archived on: 31 July 2026].

[34] National Computer Virus Emergency Response Center (2024). *<Lie to me/> Volt Typhoon III — Unraveling Cyberespionage and Disinformation Operations Conducted by U.S. Government Agencies*. Available at: https://web.archive.org/web/20260715172021/https://www.cverc.org.cn/head/zhaiyao/futetaifeng3_EN.pdf [Archived on: 31 July 2026].

[35] Dustin Volz (2025). *In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks*. The Wall Street Journal. Available at https://web.archive.org/web/20260731140509/https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb [Archived on: 31 July 2026].

[36] Xinhua (2025). *Chinese police put 3 U.S. operatives on wanted list over cyberattacks*. Xinhua News Agency. Available at https://web.archive.org/web/20260308214426/https://english.news.cn/20250415/59642d1d15dd427b852e844e8350af5f/c.html [Archived on: 31 July 2026].

[37] New Jersey Cybersecurity and Communications Integration Cell (2025). Volt Typhoon. Available at https://web.archive.org/web/20250501000000/https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon [Archived on 1 May 2025].

[38] Dragos (2026). *SYLVANITE Threat Group*. Dragos. Available at https://web.archive.org/web/20260731141417/https://www.dragos.com/threat/sylvanite/ [Archived on: 31 July 2026].

[39] Dragos (2026). *Dragos 2026 OT Report Shows Surge in Threat Groups and Ransomware*. Available at https://web.archive.org/web/20260308071207/https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware [Archived on: 31 July 2026].

[40] Fraunhofer FKIE (2024). *UNC5174*. Malpedia. Available at https://web.archive.org/web/20260731141622/https://malpedia.caad.fkie.fraunhofer.de/actor/unc5174 [Archived on: 31 July 2026].

[41] Federal Office for the Protection of the Constitution (2024). *BfV Cyber Insight - Part 2: Connections of i-Soon to the Chinese security apparatus*. Available at https://web.archive.org/web/20260731142646/https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/cyber/2024-08-08-bfv-cyber-insight-part-2.pdf?__blob=publicationFile&v=6 [Archived on: 31 July 2026]

[42] United States Department of the Treasury (2024). *Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure*. Available at https://web.archive.org/web/20260731142712/https://home.treasury.gov/news/press-releases/jy2205 [Archived on: 31 July 2026].

[43] United States Department of the Treasury (2025). *Treasury Sanctions Technology Company for Support to Malicious Cyber Group*. Available at https://home.treasury.gov/news/press-releases/jy2769 [Archived on: 31 July 2026].

[44] United States Department of the Treasury (2025). *Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise*. Available at https://web.archive.org/web/20260731142746/https://home.treasury.gov/news/press-releases/jy2792[Archived on: 31 July 2026].

[45] United States National Security Agency (2025). *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*. Cybersecurity Advisory. Available at https://web.archive.org/web/20260731142820/https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF [Archived on: 31 July 2026].

[46] John Costello (2025). *The Cyberspace Force: A Bellwether for Conflict*. China Brief, 25(8). The Jamestown Foundation. Available at https://web.archive.org/web/20260731142859/https://jamestown.org/the-cyberspace-force-a-bellwether-for-conflict/ [Archived on: 31 July 2026].

[47] Cybersecurity and Infrastructure Security Agency et al. (2024). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Cybersecurity Advisory. Available at https://web.archive.org/web/20260731133222/https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a [Archived on: 31 July 2026].

[48] Honorable Dena Palermo (2024). *Affidavit in Support of an Application Under Rule 41(b)(6)(B) for a Search and Seizure Warrant*. United States District Court for the Southern District of Texas. Available at https://web.archive.org/web/20241031052352/https://www.justice.gov/opa/media/1336421/dl?inline [Archived on: 31 October 2024].

[49] Timothy Edgar (2024*). Recent Botnet Takedowns Allow U.S. Government to Reach Into Private Devices*. Lawfare. Available at https://web.archive.org/web/20260320022540/www.lawfaremedia.org/article/recent-botnet-takedowns-allow-u.s.-government-to-reach-into-private-devices [Archived on: 20 March 2026].

[50] Michael N. Schmitt, ed. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. https://doi.org/10.1017/9781316822524

[51] International Committee of the Red Cross (2023). *Cyber Operations During Armed Conflict: The Principle of Distinction.* Available at https://web.archive.org/web/20260829051201/https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf [Archived on: 29 August 2026].

[52] Dina Temple-Raston (2024). *Neuberger: Defining espionage vs. pre-positioning for attacks is key to battling state actors*. The Record. Available at https://web.archive.org/web/20260609174828/https://therecord.media/volt-typhoon-china-defining-espionage-pre-positioning-neuberger-munich [Archived on: 9 June 2026].

[53] Emma Burrows (2026). *Russian spies are aggressively seeking Western technology as sanctions bite, officials say*. Associated Press. Available at https://web.archive.org/web/20260530072049/https://apnews.com/article/russia-sanctions-intelligence-economy-defense-10ea5ad20158945f18c718375b84a2f3 [Archived on: 30 May 2026].

[54] Sahil Joshi and Divyesh Singh (2020). *Mega Mumbai power outage may be result of cyber attack, final report awaited*. India Today. Available at https://web.archive.org/web/20260616230712/https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20 [Archived on: 16 June 2026].

[55] Insikt Group (2021). *China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions*. Recorded Future. Available at https://web.archive.org/web/20260908084357/https://assets.recordedfuture.com/insikt-report-pdfs/2021/cta-2021-0228.pdf [Archived on: 8 September 2026].

[56] Sunny Cheung (2026). *Cyber Lessons From Russia's War in Ukraine*. Jamestown China Brief. Available at https://web.archive.org/web/20260716051627/https://jamestown.org/cyber-lessons-from-russias-war-in-ukraine/ [Archived on: 16 July 2026].

[57] Katherine Yon Elbright (2026). *No Legal Basis for Invading Venezuela*. Brennan Center. Available at https://web.archive.org/web/20260904135740/https://www.brennancenter.org/our-work/analysis-opinion/no-legal-basis-invading-venezuela [Archived on: 4 September 2026].

[58] Janina Dill (2026). *Expert Comment: The illegality of the US attack against Venezuela is beyond debate - how the world reacts is critical*. University of Oxford. Available at https://web.archive.org/web/20260815195732/https://www.ox.ac.uk/news/2026-01-07-expert-comment-illegality-us-attack-against-venezuela-beyond-debate-how-world-reacts [Archived on: 15 August 2026].

[59] Maggie Miller (2026). *Venezuela strike marks a turning point for US cyber warfare*. Politico. Available at https://web.archive.org/web/20260302024715/https://www.politico.com/news/2026/01/07/venezuela-us-cyber-warfare-00713507 [Archived on: 4 March 2026].

[60] Sarah McBroom and Brandon White (2025). *Russian state-sponsored espionage group Static Tundra compromises unpatched end-of-life network devices*. Cisco Talos Intelligence. https://web.archive.org/web/20260910014045/https://blog.talosintelligence.com/static-tundra/ [Archived on: 10 September 2026].

[61] Check Point Research (2025). *OSINT & Phaleristics: Unveiling FSB's 16th Center SIGINT Capabilities*. Check Point. Available at https://web.archive.org/web/20260421180755/https://checkfirst.network/wp-content/uploads/2025/07/OSINT_Phaleristics_Unveiling_FSB_16th_Center_SIGINT_Capabilities.pdf [Archived on: 21 April 2026].

[62] United Kingdom Foreign, Commonwealth and Development Office (2023). *Russia's FSB malign activity: factsheet*. Government of the United Kingdom of Great Britain and Northern Ireland. https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

[63] European Repository of Cyber Incidents (2026). *Russia's FSB 16th Centre aka Turla Carried Out Sabotage Operations Against Polish Energy Infrastructure on 29 and 30 December 2025*. Available at https://eurepoc.eu/table-view/?cyber_incident=5231

[64] The Chancellery of the Prime Minister of the Republic of Poland (2026). *Poland Stops Cyberattacks on Energy Infrastructure*. Government of the Republic of Poland. Available at https://web.archive.org/web/20260129165330/https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure [Archived on: 29 January 2026].

[65] Dragos (2026). *ELECTRUM: Cyber Attack on Poland's Electric System 2025*. Dragos. Available at https://web.archive.org/web/20260130075600/https://hub.dragos.com/report/electrum-targeting-polands-electric-sector [Archived on: 30 January 2026].

[66] Marko Milanovic (2026). *Some Further Thoughts on the Illegal US Attack on Venezuela: Self-Defence, Cyber, and Continuing Coercion*. EJIL Talk! Available at https://web.archive.org/web/20260905181947/https://www.ejiltalk.org/some-further-thoughts-on-the-illegal-us-attack-on-venezuela-self-defence-cyber-and-continuing-coercion/ [Archived on: 5 September 2026].

[67] Sophos Counter Threat Unit Research Team (2023). *Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations*. Sophos. Available at https://web.archive.org/web/20260903061121/https://www.sophos.com/en-us/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations [Archived on: 3 September 2026].

[68] US Ambassador Mike Waltz (2026). *Remarks at a UN Security Council Briefing on Venezuela*. United States Mission to the United Nations. Available at https://web.archive.org/web/20260218142529/https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-on-venezuela-2/ [Archived on: 18 February 2026].

[69] United States Congress (1979). *Taiwan Relations Act (Public Law 96-8, 22 U.S.C. 3301 et seq.)*. Available at https://web.archive.org/web/20260728034749/https://www.ait.org.tw/policy-history/taiwan-relations-act/ [Archived on 28 July 2026].

[70] US President Donald J. Trump (2017). *2017 National Security Strategy of the United States*. Office of the President of the United States. Available at https://web.archive.org/web/20260302002915/https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [Archived on: 2 March 2026].

[71] US President Joseph R. Biden (2023). 2023 NATIONAL CYBERSECURITY STRATEGY. Office of the President of the United States. Available at https://web.archive.org/web/20250910233934/https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewer.html?file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Fs9zfme-rssdn%2F2023-03-02-White-House-National-Cybersecurity-Strategy-2023.pdf [Archived on: 10 September 2025].

[72] Arjun Kharpal (2022). *China alleges U.S. spy agency hacked key infrastructure and sent user data back to headquarters*. CNBC. Available at https://web.archive.org/web/20250720225340/https://www.cnbc.com/2022/09/27/china-alleges-us-nsa-hacked-infrastructure-sent-data-back-to-hq.html [Archived on: 20 July 2025].

[73] Yuan Hong (2023). *Exclusive: Wuhan Earthquake Monitoring Center suffers cyberattack from the US; investigation underway.* Global Times. Available at https://web.archive.org/web/20260119220325/https://www.globaltimes.cn/page/202307/1295064.shtml [Archived on: 19 January 2026].

[74] Global Times Staff (2025). *China's state security authorities uncover case of major cyberattack from US NSA employing state-level cyber-espionage weapons targeting 'Beijing Time': MSS*. Global Times. Available at https://web.archive.org/web/20260418232709/https://www.globaltimes.cn/page/202510/1345993.shtml [Archived on: 18 April 2026].

[75] Lin Jan (2026). *Spokesperson's remarks delivered on behalf of the Ministry of Foreign Affairs of the People's Republic of China*. Ministry of Foreign Affairs of the People's Republic of China. Available at https://web.archive.org/web/20260827094347/https://twitter.com/MFA_China/status/2092910939343650844 [Archived on: 27 August 2026].

[76] RedDrip7 (2025). *Exclusive Disclosure of the Attack Activities of the APT Group "NightEagle."* Qian Pangu Labs. Available at https://web.archive.org/web/20260916183731/https://github.com/RedDrip7/NightEagle_Disclose/blob/main/Exclusive%20disclosure%20of%20the%20attack%20activities%20of%20the%20APT%20group%20NightEagle.pdf [Archived on: 16 September 2026].

[77] Unit 42. *Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific*. Palo Alto Networks. Available at https://web.archive.org/web/20260123060627/https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/ [Archived on: 23 January 2026].

[78] Jen Easterly and Dan Kurtz-Phelan (2026). *Cyberwarfare in the AI Age: A Conversation With Jen Easterly*. Foreign Affairs Interview. Available at https://web.archive.org/web/20260815170410/https://www.foreignaffairs.com/podcasts/cyberwarfare-ai-age [Archived on: 15 August 2026].