# Cyber-Intelligence Report

This cyber-intelligence product is a snapshot of selected cyber events. Collection of information is in accordance with clients' guidelines. It contains 'observations', meaning headlines and links to online information. It *MAY* contain comments and analysis. It is copyright ©David Swan 2025. This report is **TLP:CLEAR**[1] and MAY be shared freely.

If this report does not meet your requirements, is in error or if you need additional information, contact David Swan at DSC.Ops.Vulcan@gmail.com

## Cyber Intelligence: U.S. Degrades Its Cyber Security

This report contains selected cyber-security information from 7th to 20th March 2025.

### Synopsis

1. The American government continues to change it's cyber security posture, and the news is bad. Russia's RT is using AI. Russian attacks on Microsoft 365 continue. How did the PRC's 'Volt Typhoon' hack so many U.S. electrical companies? At least one PRC company has a 'backdoor' on their chips. Microsoft refuses to fix 8 year old security hole.

2. It is our *assessment* that the three major cyber conflicts, (Russia vs Ukraine, Iran vs Israel, and the People's Republic of China) are the most likely sources for the creation of next generation malware and/or a primary source of cyber attacks. This includes government funded hackers (military, intelligence and civilian employees), affiliated hackers (criminals and mercenaries), and volunteer 'supporters'.

### Removing American Cyber Security Protection

3. Our Cyber Intelligence Report for 6th March documented the first radical changes in cyber security policy in the American government. (*Russia is all right and doesn't deserve to be treated as the bad guy quite as much anymore.*[2]) [3]. Multiple reports have confirmed the Cybersecurity and Infrastructure Security Agency (CISA) has terminated two contracts:

- The Center for Internet Security for the Multi-State Information Sharing and Analysis Center (MS-ISAC) and
- Election Infrastructure Information Sharing and Analysis Center (EL-ISAC)

A spokesperson said: "*This action will save taxpayers approximately $10 million a year, focus CISA's work on mission critical areas, and eliminate redundancies.*" What the spokesperson did not say was the two ISACs "*allow state, local, tribal and territorial governments to share threat information and best practices while providing tools and other services for free or at a reduced cost. ... The shuttering or reduction in*

1 Definition **TLP:CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.
2 Source: The Register. So ... Russia no longer a cyber threat to America?
3 Source: David Swan Consulting: Cyber Intelligence Report Volume 5 Edition 5, 6 March 2025.

*scale of these two information centers will leave a big hole. ... It's the multiple layers of defense that make us successful. Even in the counties, we may have one or two or three tools where there's overlap, but that's not a bad thing."*[4]

4. DHS Secretary Kristi Noem also dissolved "*the Critical Infrastructure Partnership Advisory Council (CIPAC), along with several other advisory groups ... CIPAC has been used to facilitate discussions among members of government coordinating councils, sector coordinating councils and cross-sector groups on critical infrastructure planning, implementation and operational concerns. ... This is a team sport, and CIPAC is the rulebook for how those teams — industry and government — can work collaboratively with protection ... CIPAC or something like it is vital to our ability to use that partnership effectively.*"[5]

5. In related CISA news, "*a senior penetration tester at CISA claimed his 100-plus-strong red team as well as its support workers were dismissed ... a second CISA red team was also said to have been cut soon after. ... One person familiar with the situation at the agency told us today 130 staffers have been given their jobs back, though they are indeed on paid leave for now.*"[6] According to the CISA, "*CISA has taken action to terminate contracts where the agency has been able to find efficiencies and eliminate duplication of effort.*" Apparently the CISA "*has not terminated the entirety of its ethical hackers, although some contracts were withdrawn.*"[7]

6. Analysts Comment: The degradation of American government cyber security support is already in progress.

- The dissolution of CIPAC ends coordination of policy and coordination between levels of government (federal, state and municipal).
- Ending of the support contracts for MS-ISAC and EL-ISAC ends the circulation of critical cyber forensic information among multiple levels of government. This removes a security pillar for smaller governments who have less funds for cyber security.
- The 'layoff' of cyber security teams at CISA is equivalent to pulling police officers out of a troubled district. The only people who benefit are the criminals, or in this case, the attacking hackers.

7. Analysts Comment: Even if courts order the reinstatement of employees, expect a serious degradation of American government cyber security.

**Russia**

8. **Russian hackers target Ukrainian Signal users.** Russia's APT44 cyber espionage group, also known as 'Sandworm', is targeting Ukrainian military and government employees who use the 'Signal' program. "*One technique exploits Signal's built-in "paired devices" feature, which allows attackers to gain access to*

4 Source: NextGov. What's next for cybersecurity, election info sharing?
5 Source: Top House cyber lawmaker to press DHS on key infrastructure group's shutdown
6 Source: The Register. CISA fires, now rehires and immediately benches security crew on full pay
7 Source: The Register. CISA: We didn't fire red teams, we just unhired a bunch of them

*victims' messages in real time, allowing them to monitor their victims over time and making the intruders difficult to detect."*[8] Successful attacks allow the attacker to listen in on the victim's secure conversations.

9. **Russia's 'RT' Generating Material Using AI.** A group of western security organizations has identified that 'RT' (formerly Russia Today), "*a Russian state-sponsored media organization, is using [AI] to create fictitious online personas, representing a number of nationalities, to post content on a social media platform."* RT leverages 'Meliorator', "*an artificial intelligence (AI) enhanced software package which allowed for the creation of authentic appearing fictitious personas to post content on X. The tool also allowed for the management of the persona profiles through an administrator panel called 'Brigadir' and the spreading of disinformation through these profiles through a seeding tool called 'Taras.'"*[9]

10. **Phishing Attacks on Microsoft 365 ... Continued.** Computer Security company Guardz is warning that: "*the phishing campaign is still succeeding. This phishing campaign is seeing success due to its sophisticated leveraging of Microsoft's own legitimate infrastructure, ... Unlike typical phishing scams, this attack bypasses traditional email security filters (SPF, DKIM, DMARC) because it originates from authentic Microsoft domains and is delivered through trusted channels. This technique increases trust and reduces user skepticism, leading to higher success rates."*[10] Analysts Comment: Microsoft Teams users need to be *very* careful.

**People's Republic of China**

11. **How Did 'Volt Typhoon' Penetrate U.S. Electrical Companies?** The Littleton Electric Light and Water Departments (LELWD) is a case study in how PRC 'Volt Typhoon' hackers got inside American electrical systems. "*LELWD provides electricity and water to the towns of Littleton and Boxborough, Massachusetts."* The company hired a 'service provider' to protect their network. The service provider neglected to patch a FortiGate 300D firewall, which provided a vulnerability for the 'Volt Typhoon' hackers to exploit. "*LELWD had been working with operational technology (OT) cybersecurity company Dragos as part of an American Public Power Association government-funded program to assist smaller public utilities, and Dragos had installed sensors on the OT network in August 2023. Through these sensors and the firm's OT threat hunting service, Dragos spotted some usual network traffic and communications with China that shouldn't be occurring."*[11]

12. Nick Lawler, general manager of LELWD "*still doesn't have a good answer as to why Volt Typhoon targeted his power utility other than for reconnaissance and espionage purposes. ... other than we had a hole and they found it."* LELWD distributes electricity to 15,000 homes.

13. **Chinese 'Bluetooth' Chips Have 'Backdoor':** "*Security researchers have*

8 Source: B2B Cyber Security News. Russian Hackers Target Ukrainian 'Signal' Users

9 Source: Government of Canada. Russian state-sponsored media organization leverages AI-enhanced "Meliorator" software for foreign malign influence activity

10 Source: Channel Futures. Microsoft 365 Phishing Campaign Active, Growing

11 Source: The Register. This is the FBI, open up. China's Volt Typhoon is on your network.

*shared details of newly discovered, undocumented commands in [PRC-made] ESP32 Bluetooth firmware that can be exploited by an attacker.*" Over one billion of the 'incredibly inexpensive' chips have been sold. 'Tarlogic Security' researchers warn "*exploitation could allow "hostile actors to conduct impersonation attacks and permanently infect sensitive devices such as mobile phones, computers, smart locks or medical equipment by bypassing code audit controls.*" 'Espressif', the manufacturer of the chip says "*we do not foresee any impact from the reported issue* ***provided the product has the recommended platform security features enabled.***"[12]

14. **PRC Hackers Target Juniper Networks' Junos OS routers**: Cyber Security company 'Mandiant' identified 'custom backdoors' installed on unpatched Juniper Networks' Junos OS routers by a PRC cyber espionage group tracked as UNC3886. The "*TINYSHELL-based backdoors had various capabilities, including active and passive access and a script to disable logging*." Mandiant observed UNC3886 "*targeting internal networking infrastructure, such as Internet Service Provider (ISP) routers. ... to gain privileged initial access.*"[13]

### Microsoft Refuses To Fix Security Hole

15. Cyber security company 'Trend Micro' has identified an eight year old vulnerability in Microsoft Windows, used by multiple aggressor states for cyber espionage. The attack is described as "*low-tech but effective.*" The attack uses "*malicious .LNK shortcut files rigged with commands to download malware.*" Trend Micros says "*it found the vast majority of these files were from state-sponsored attackers (around 70 percent), used for espionage or information theft, with another 20 percent going after financial gain. Among the state-sponsored crews, 46 percent of attacks came from North Korea, while Russia, Iran, and China each accounted for around 18 percent of the activity.*"[14]

16. Microsoft has "***classified the issue as low severity and does not plan to release a fix.*** *... ZDI-CAN-25373 is an example of User Interface (UI) Misrepresentation of Critical Information (CWE-451).*"[15] Stated another way, Microsoft says this is the users problem.

---



12 Source: Espressif: ESP32 Undocumented Bluetooth Commands: Clearing the Air
13 Source: Security Affairs. China-linked APT UNC3886 targets EoL Juniper routers
14 Source: The Register. Microsoft isn't fixing 8-year-old shortcut exploit abused for spying
15 Source: The Hacker News. Unpatched Windows Zero-Day Flaw Exploited by 11 State-Sponsored Threat Groups Since 2017
16 Definition **TLP: CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.