Volume 5: Edition 1

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: Forecast for 2025

This report contains cyber-security information from 2024 as well as selected items from the 14th December 2024 to 9th January 2025.

Synopsis

1. We review and forecast cyber activity from all three major cyber conflict: Russia vs Ukraine, Israel vs Iran, and the People's Republic of China (PRC). We look at the possibility of hybrid cyberwarfare from Russia. We also look at the potential for the PRC to leverage its extensive penetration into other countries critical infrastructure.

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'.

CyberWarfare: Russia vs Ukraine

3. **Russia**: In 2024, Russia's cyber forces achieved limited success. There were no significant strategic strikes against Ukraine. Attacks were generally identified and suppressed within hours. Russia's 'Patriotic/Volunteer Hackers' did launch many attacks, however most of them were reported as 'nuisance attacks causing no significant damage'. In late 2024, Japan received a number of Distributed Denial of Service Attacks (DDoS) attacks, first against Japan Airlines, 3 banks and Fujitsu. Then, Japanese Telecommunications company 'Docomo' was hit and taken offline for 12 hours.[2] The campaign against Japan is *almost certainly* attributable to Russian hacking groups NoName057(16) and the Russian Cyber Army Team.[3]

4. We *assess* that in 2025 Russia's cyber forces will incorporate a wider Russian strategy of hybrid warfare. In the cyber environment an example might be a group of 'Patriotic Hackers' such as 'NoName057(16)' launching Distributed Denial of Service Attacks (DDoS), while concurrently a government team, such as 'Fancy Bear', executes an exploitation attack inside the weaked network. It is becoming increasingly

[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: InfoSecurity Magazine. DDoS Disrupts Japanese Mobile Giant Docomo

[3] Source: NetScout. DDoS Attacks Against Japan

likely that we will see damage/sabotage of infiltrated networks as Russia attempts to dissuade countries from supporting Ukraine.[4]

5. From a targeting perspective, it is *assessed* as *likely* that the Kremlin's targeting priorities will be:

- Countries such as Japan, who are becoming more dynamic in their support for Ukraine,
- Countries neighbouring Russia who support Ukraine, and
- Targets of opportunity.

Russia will *almost certainly* continue disinformation campaigns and information operations against countries and political parties that oppose Russia's ambitions in Ukraine. Russia is *highly likely* to retaliate against countries that block propaganda/information operations.[5]

6. **Ukraine:** Ukraine has exercised a highly disciplined, highly targeted campaign of cyber attacks against Russia. It is *almost certain* this pattern will continue. Ukraine's cyber attacks are *very probably* going to continue to escalate, becoming more damaging, targeting with increasing frequency:

- Banks and payment applications,
- Russian defence industries,
- Russian telecommunications infrastructure.

There are indications that Ukraine has acquired Distributed Denial of Service Malware, similar in some respects to Russia's 'DDoSia'[6]. It is *likely* that malware will see increasing use inside Russia against Russian targets.

7. We forecast no significant changes in the hacking groups supporting Ukraine. There are groups integrated into Ukraine's Cyber Army, who *almost certainly* will continue integrated operations. Other groups will *very probably* launch attacks based on perceived opportunities.

CyberWarfare: Israel vs Iran

8. **Israel:** Recent articles in Israeli media such as the 'Jerusalem Post' have stated that Hamas executed a multi year intelligence collection operation against Israel prior to the October 7th attack. This included hacking into security camera's, computer networks and any available electronic devices.[7] In retrospect it appears that a significant percentage of Israeli cyber capability was invested in investigating the Hamas attack. Some of that same capability is almost certainly: remediating systems, patching vulnerabilities and securing against future attacks.

[4] For a more detailed explanation of the Russian geopolitical environment we recommend the most recent Royal United Service Institute of Nova Scotia (RUSI(NS)), Security Advisory Committee (SAC) Update, published every two weeks. To subscribe contact: RUSI Nova Scotia <rusinovascotia@gmail.com>

[5] Source: Security Affairs. Russian media outlets Telegram channels blocked in European countries

[6] DDoSia is Russia's advanced Distributed Denial of Service malware designed to extend and enhance attacks.

[7] Source: Jerusalem Post. Hamas broke into dozens of cameras in the surrounding settlements before October 7

9. In 2024, Israel's cyber campaign against Iran was principally against Iran's domestic networks. Attacks were targeted and granular, with very little media reporting on infrastructure failures (E.G. gas station pumps). There were also cyber attacks against Iranian banks as well as its oil and gas sector. We were surprised by the limited nature of Israel's cyber operations against Iran. It is *probable* Israel invested its cyber efforts into reconnaissance and espionage as opposed to overt cyber attacks. Israel has hacked Palestinian media, notably the Hamas operated al-Aqsa TV channel[8] in order to warn the local population of incoming attacks.

10. Israel's cyber operations to date can be characterized as controlled, focused and effective. It is *assessed* as *unlikely* that 2025 will see any change.

11. **Iran:** Iranian cyber operations covered a wide spectrum of capabilities in 2024. For example, cyber attacks included:

- Ransomware attacks on American water and sewage plants,
- Denial of Service attacks against Israeli targets,
- Information operations promoting Palestinian causes and against opposed politicians in both the United States and Europe.

Attacks were conducted by Iranian government hacking groups as well as proxies and some 'volunteer' organizations. Although the attacks were almost universally ineffective, there was a sharp increase in capability between January and December 2024.

12. It is *assessed* that Iran *very likely* poured resources into increasing its cyber capabilities in 2024. It is *very likely* that this trend will continue. We *forecast* that Iran's cyber forces will *probably* have significant impact on more targets in 2025. We expect to see an increase in: the number of Iranian linked cyber groups, the capability of those groups, as well as an increase in targets. Nations that are unprepared *may* find Iranian cyber attacks a problem.

CyberWarfare: People's Republic of China

13. 2024 saw the discovery of enormous networks of compromised computers and/or networking devices, controlled by the People's Republic of China (PRC). Previous editions of this report covered 'Salt Typhoon' and 'Volt Typhoon', two of the larger malware/espionage networks. 2025 is off to a fast start with Japan's publication of details on a years-long series of cyber attacks attributed to a People's Republic of China source.[9] The attacker nicknamed "MirrorFace", aka "Earth Kasha", apparently started their campaigns in 2019, launching three distinct waves of attacks. The waves ran as follows:

- From December 2019 to July 2023, saw phishing emails sent to targets at think tanks, government agencies, politicians, and media organizations.

[8] Source: Daily Dot. Hamas' TV network hacked—delivers warning to Palestinians to seek shelter

[9] Source: The Register. Japanese police claim China ran five-year cyberattack campaign targeting local orgs

- From February 2023 into mid-2024, using Microsoft ‘Active Directory’ and Microsoft 365 to target Japan’s semiconductor, manufacturing, information and communications, academic, and aerospace sectors.
- Started in June 2024 and uses phishing to target Academia, think tanks, politicians, and the media.

14. Given the discovery of PRC malware and espionage networks, including Japan’s discovery, It is *almost certain* that 2025 will see the discovery of more PRC cyber incursions into critical infrastructure, such as telecommunications and electrical systems. Given President Xi’s focus on Taiwan rejoining the PRC, it is *very likely* that nations in the South China Sea, as well as nations who either support Taiwan and/or are resistant to the PRC’s ambitions, will be high priority targets. Circulation of propaganda and information operations through social media will *very likely* continue to be part of the PRC playbook. It must be noted that PRC cyber attacks tend to focus on espionage, meaning information collection, as opposed to DDoS attacks, or damaging attacks such as ransomware or sabotage.

15. The scope and range of the PRC’s cyber attacks can not be overstated. There is no part of the world untouched by PRC cyber intrusions. Further, just because the PRC has been focused on espionage in its incursions does not mean the PRC will not use its capabilities to neutralize a perceived opponent. Noting that the PRC’s economic base and the leadership of President Xi are becoming increasingly unstable[10], cyber is one of the few tools available with no restrictions, no obvious consequences. Given the resources that the PRC has poured into its cyber activities, it would be remarkable if cyber was not one of the first tools selected in order to enhance an attack on Taiwan.

Final Thoughts

16. Expect hackers to leverage AI and ChatGPT variants to improve their malware. We expect attacks to shift to middle size corporations in an effort to improve victim payouts. We also expect an increase in supply chain attacks.

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

[10] A detailed explanation of the GeoPolitics of the People’s Republic of China can be found at the most recent Royal United Service Institute of Nova Scotia (RUSI(NS)), Security Advisory Committee (SAC) Update, published every two weeks. To subscribe contact: RUSI Nova Scotia <rusinovascotia@gmail.com>

[11] 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.