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 2026. 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 Report: New Year's Edition

This report contains selected cyber-security information from 12th December 2025 to 8th January 2026.

Synopsis

1. This report is a series of summaries and forecasts starting with the major cyber players and the conflicts, starting with the People's Republic of China. Next is Russia vs Ukraine, followed by Iran vs Israel and Pakistan vs India. We have a review of the United States and a very brief look at South America. Lastly, a look at the hacker environment. The bottom line: 2026 will be another challenging year.

2. It is our *assessment* that cyber conflicts such as: Russia vs Ukraine, Iran vs Israel, and the People's Republic of China, etc. 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'.

People's Republic of China (PRC)

3. Globally, the People's Republic of China has the largest number of hackers (and hacking teams), the most hacking activity (including hacking campaigns), and is definitely in the top tier of hacking capabilities. The PRC's principal focus is Taiwan. According to Taiwan's National Security Agency, Taiwan's critical infrastructure was hit with an average of 2.6 million cyber-attacks daily. "*The attacks mainly targeted the energy sector, hospitals, banks and emergency services, and many of them were reportedly coordinated with Chinese military exercises and political events. For example, when the President and Vice President of Taiwan were giving speeches or attending international meetings.*"[2]

4. Over the Christmas / New Years season, the aggressive pace of PRC hacking has continued. Some of the hacking campaigns detected include:

- Mass registration of fake online shops originates from China
- China-Linked Ink Dragon Hacks Governments Using ShadowPad and

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: CSO Online. Taiwan subjected to 2.6 million Chinese cyberattacks a day in 2025

© David Swan Consulting 2026

FINALDRAFT Malware
- China-Aligned Threat Group Uses Windows Group Policy to Deploy Espionage Malware
- China-linked APT UAT-9686 is targeting Cisco Secure Email Gateway and Secure Email and Web Manager
- Foreign Office hacked: China accused of stealing secret files
- Evasive Panda cyberespionage campaign uses DNS poisoning to install MgBot backdoor
- Mustang Panda Uses Signed Kernel-Mode Rootkit to Load TONESHELL Backdoor
- Chinese APT Silver Fox Targets India with ValleyRAT Tax Phishing Scam

5. Of the eight hacking campaigns listed here, six are *almost certainly* cyber-espionage (based on what they target). A seventh campaign targeting Cisco Email Gateways is *assessed* as *very probably* cyber-espionage. Note: These campaigns are in addition to the attacks on Taiwan's critical infrastructure. When these campaigns are detected, they are not shutdown. The standard response is the PRC denies there is a hacking campaign, and there is a surge in activity, presumably to collect data before counter-measures are put in place.

6. Forecast: DSC characterizes PRC hacking activity as a 'surge' or a 'full court press'. The apparent objectives are 'preparation of the cyber environment' for the invasion of Taiwan and cyber espionage in support of political objectives. We *forecast* that the PRC will continue to aggressively continue both objectives, adding new hacking campaigns and scaling up cyber operations.

Russia vs Ukraine

7. **Russia**: President Putin is continuing to direct Russia to capture Ukraine and more generally to become the dominant political force in Europe. During the last few weeks, Germany, Denmark and France have all identified Russia as the culprit behind recent cyber-attacks. 'Pro-Russia hackers' have escalated their activities "*targeting U.S. and global critical infrastructure, including sectors such as water and wastewater systems, food and agriculture, and energy.*"[3] GeoPolitical analysts observe that Russia's economy is not healthy, which infers President Putin has a limited amount of time remaining to conquer Ukraine.

8. Trends: 2025 saw an increase in Russian destructive cyber-attacks targeting Ukraine and its allies. In addition to Russian government run campaigns, DDoS and 'nuisance attacks' against western governments included massive disinformation campaigns and disruption of elections. The pace of attacks from 'Pro-Russia hacktivist groups', such as 'Cyber Army of Russia Reborn' (CARR), Z-Pentest, NoName057(16), and Sector16, has been increasing over the holidays. These groups are increasingly targeting more industrial systems, including Operational Technology (OT) and Supervisory and Control Networks (SCADA).

9. Forecast: The current 'operational pause' (*probably* for Russian Orthodox Christmas on 7 January) will *almost certainly* end next week (11 January). The most visible

3 Source: Industrial Cyber.co . Global agencies sound alarm as pro-Russia hacktivist groups intensify OT intrusions

© David Swan Consulting 2026

attacks will *highly probably* come from 'Pro-Russia hacktivist groups' targeting countries of the 'Coalition of the Willing' (countries supporting Ukraine). Russian government hacking teams will *probably* continue to focus on Ukraine, continuing cyber-espionage and harassing cyber-attacks against perceived enemies. We *forecast* that Russia will make increasing use of destructive cyber-attacks in addition to increasing the number of its cyber-attacks, including increasing cyber-espionage and disinformation campaigns.

10. **Ukraine**: Ukraine demonstrated an increasing ability to penetrate the Russian Internet. Their targets included: Internet Service Provider's (ISP's), Banks (Russian financial industry), military contractors, and energy companies. Ukraine has demonstrated the ability to co-ordinate cyber-attacks with physical attacks, disrupting regional communications during ground attacks.

11. Forecast: Ukrainian operation security will remain tight, limiting our ability to observe their cyber operations. We *forecast* that Ukraine will continue to use its cyber forces strategically. Companies involved in the Russian military supply chain should expect to be targeted. Ukraine will continue to target Russian regional communications, encompassing telecommunications and Internet. Ukraine's highest priority will be to disrupt Russian military operations, with particular focus on air defence.

Iran vs Israel

12. **Iran**: Since the end of the active period of the Gaza conflict, cyber activity by both Iranian government hackers and pro-Iranian volunteer hackers has progressively declined. There has been a reduction in both number and effectiveness of the attacks. Strategically Iran appears to be re-tooling, preparing for future attacks on Israel both in country and through its proxies. That said, Iran has had more than ten days of protests over their crashing economy.[4] In addition, Iran's telecommunications infrastructure was hit by "*one of the world's largest-ever DDoS cyberattacks against its communications infrastructure - allegedly launched from over 120,000 global sources and ranked among the top 12 worldwide in scale.*"[5]

13. Current Activity: A long-term Iranian hacking group has recently 'become active': "*Prince of Persia, also known as 'Infy' based on the name of its original malware, has been operating for almost 20 years. ... [It has] resurfaced with a sophisticated cyberespionage campaign targeting global critical infrastructure and private networks.*"

14. Forecast: Based on recent history, Iran can be *expected* to reach out to Russia for additional cyber capabilities. Government based hacking teams can be *expected* to continue cyber-espionage efforts — some focused on Israel with other efforts focused on western countries, in particular the U.S. and the UK. A significant slice of Iran's capability will *probably* focus on internal protests, attempting to identify leaders and block protest communications.

4 Source: Security Advisory Committee (SAC), Royal United Services Institute (Nova Scotia) RUSI(NS).

5 Source: Hindustan Times: Iran: Amid Deadly Protests, One Of The World's Largest Cyber Attacks Hit After Trump's New War Hint

© David Swan Consulting 2026

15. **Israel**: During 2025, hacks on Iranian petrol stations, banks and manufacturers inferred that Israel had access to Iran's internal Internet. In general, Israel's cyber-attacks were specific and targeted. Currently there are no cyber campaigns attributed to Israel.

16. Forecast: During periods of relative 'peace', Israel's cyber forces operate covertly or 'under the radar', attracting as little attention as possible. We forecast that this will be the trend in 2026 for Israel's cyber forces unless a new conflict breaks out. I *expect* the primary effort will be cyber-espionage, specifically efforts to determine Iran's missile development, efforts to penetrate the Islamic Revolutionary Guard Corps (IRGC), and from there penetrate into Iranian sponsored groups that attack Israel such as Hamas, Hezbollah, and the Houthis. Israel can be expected to monitor the anti-government protests in Iran. The caveat is: if a war or renewed conflict breaks out, that will drive the focus for Israel's tactical cyber forces.

Pakistan vs India

17. **Pakistan**: In 2025, Pakistan did a credible job of raising a 'volunteer' hacker force against India in response to India's air attacks on Pakistan. Part of the 'attraction' for hackers was undoubtedly the religious aspect of the conflict (Muslim country vs Hindu country). Since Prime Minister Modi of India is leveraging religious nationalism to gather votes in India, this conflict is unlikely to 'go away' or 'get settled'. Although the 'volunteer' hacking teams appear to have lost interest in the conflict, ATP36 — Pakistan government hackers known as the 'Transparent Tribe' — have gotten busy and have commenced a new cyber-espionage campaign.[6]

18: Forecast: Expect 'Transparent Tribe' to remain on-task, conducting cyber-espionage against India. Based on historical behaviour, 'volunteer' hacker groups can be expected to harass India with DDoS attacks and possibly ransomware attacks on an irregular basis. China has a habit of conducting cyber-espionage against 'client' countries – presumably to confirm their friendly behaviour, so Pakistan can expect cyber-espionage from the PRC.

19. **India**: India's cyber forces have not covered themselves with glory in recent memory. Cyber defences appear to be lacking, including on military websites. India's hackers need training to achieve top tier hacking status and the country has been exploring a number of routes to achieve this, however 'cyber' does not appear to be a major political concern.

20. Forecast: 'Friction' between India and Pakistan is cyclical and can be expected to re-occur. Military conflict between India and Pakistan can be forecast as likely, even if it's only low-level. That said, even low-level skirmishes can be a trigger for renewed cyber engagements. From a cyber perspective, India may be in for a challenging year. In addition to multiple ongoing threats from Pakistan, China has at least one major team focused on India. I expect Russia will be conducting cyber-espionage on India as well.

6 Source: The Hacker News. Transparent Tribe Launches New RAT Attacks Against Indian Government and Academia

© David Swan Consulting 2026

Cyber-Intelligence Report

United States

21. Political Direction from the Trump administration should be characterized as 'chaotic'. One description I heard is: "Anything old is bad, anything we do is good." Cuts to programs and job cuts across multiple federal departments and agencies have largely removed U.S. Federal cyber security co-ordination to states and industries. This is a major, potentially critical, reduction in U.S. cyber defences. Employees who were 'released' have not returned to positions, leaving some areas critically understaffed, especially in indicators and warnings of attacks. In terms of offensive cyber operations, there have been zero announcements from U.S. Cyber Command operations in support of Ukraine or even of NATO. Analysts Comment: This sets the U.S. up to be victimized by cyber-attacks.

22. The U.S. military *appears* to have utilized cyberwarfare to turn off the electricity in Caracas, Venezuela during the American attack. There is no explicit explanation of what was done, merely a reference to U.S. Cyber Command "*began layering different effects*".[7] Analysts Comment: Assuming that U.S. Cyber Command did contribute to the attack, it is clear the U.S. has no reluctance to employ cyberwarfare.

23. Forecast: We *forecast* that the U.S. will be hit by multiple cyber-attacks. Noting the reduction in indications and warning, as well as removal of countermeasures data to industry, there is a much higher risk of a catastrophic attack such as the shutdown of the 'Colonial Pipeline'. Cyber-attacks may not be directed at the government, but a major attack(s) on financial networks or critical infrastructure *should* be enough to attract the attention of the American administration. Based on their stated belief in 'American Exceptionalism', 'revenge attacks' *could be* a possibility.

South America

24. There were a number of major attacks on banks and financial infrastructure. Further, some countries appear to working on developing their own defensive and offensive cyber capabilities. The PRC has been increasing its targeting of South American governments as it seeks to increase its presence. Analysts Comment: We *forecast* an increasing amount of cyber activity, both criminal and cyber-espionage, in South America generally. Given the changing political landscape we expect to see more cyber activity from the U.S., the PRC, and Russia in the region.

The Hacker Environment

25. 2025 saw extensive ransomware attacks on Hospitals and all types of medical clinics. Nothing was exempt from attack, not even 'Sick Kids' hospitals or cancer clinics. A recent headline provides the current state of hospital attacks:

- Hospitals are drowning in threats they can't triage

The most recent trend is away from hospitals to Financial Institutions:

- Financial services overtakes healthcare as most at risk from cyberattacks

7 Source: Business Insider. Trump says the US shut off the lights in Venezuela's capital using 'certain expertise.' Here's how it may have done it.

© David Swan Consulting 2026

Cyber-Intelligence Report

This does not mean other industries are at lower risk of being targeted. Cyber criminals (hackers) are specializing by the nation(s) they attack and/or the industries they attack:

- A Hack-for-Hire Group is Specializing in Targeting Canada
- One criminal, 50 hacked organizations, and all because MFA wasn't turned on

Hackers continue to be indiscriminate in their targeting, targeting small businesses, libraries or even very small public organizations:

- Cyberattack of Nunavik health centre results in data breach
- Northern Ont. school board cyber breach exposed SINs, passport data

Hackers are recruiting key personnel to help them reach their targets:

- Cybersecurity pros admit to moonlighting as ransomware scum
- Cybercriminals recruit malicious insiders via the dark web
- The big catch: How whaling attacks target top executives

Hackers are also using Artificial Intelligence to refine and improve their attacks:

- Are criminals vibe coding malware? All signs point to yes

26. Good News? The most common motivations for hackers are greed and reputation. This does not always work out. Police are gaining experience and are making an increasing number of arrests. Some defenders are becoming more capable:

- Cyber crime group claims successful attack on security firm, crows about it on Telegram – but it was all an elaborate honeypot
- Security coverage is falling behind the way attackers behave

27. **Forecast for 2026**: 2026 will see hackers adapting to a changing environment.

- Ransomware attacks will continue to be hackers preferred criminal tool.
- Hackers will continue to refine extortion so one ransomware attack generates multiple forms of payouts.
- Hackers will increasingly demand ransom for personal information, both from organization and from individuals.
- Hackers will increasingly use violence and the threat of violence to coerce payment.
- Hacking groups will continue to specialize based on capabilities, preferred targets and methodologies.

This cyber-intelligence product is produced by David Swan. It is copyright ©David Swan 2026. This report is **TLP:CLEAR**[8] and MAY be shared freely.

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

8 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.

© David Swan Consulting 2026