Cyber-Intelligence Report

This cyber-intelligence product is produced by David Swan. Collection of information is in accordance with guidelines provided by clients. It contains 'observations', meaning headlines and links to information published online. It *MAY* contain comments and analysis. It is copyright ©David Swan 2023. This report MAY be circulated.

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

CyberWarfare: (41) The THREE National Level Cyber Conflicts

This report contains selected cyber-security information from 13th to 26th Oct 2023.

Synopsis

1. In a first time *ever* event, Five Eyes Directors publicly declared that cyber espionage conducted by the People's Republic of China constitutes *the defining threat to western democracy*. A cyber component has been identified in the Hamas attack on Israel, including links to Iran. The latest in cyberspace on the Russia – Ukraine war including Ukraine's successful bank hack. Information Operations in the news.

2. Russia vs Ukraine cyberwar. Russia appears to be committed to the following ongoing 'Course of Action' for its cyber forces:

> Russian cyber forces, including allied and supporting hackers, continue to launch campaigns against Ukrainian targets, including perceived Ukrainian allies. Targeting Includes: critical infrastructure, industrial infrastructure, political, and media organizations as well as targets of opportunity.

China

3. In a first time event across 90 years of co-operative work, the agency heads of the 'Five Eyes' security agencies went to 'silicone valley' in California in the U.S. to warn companies about the theft of intellectual property by China. On Sunday 22nd Oct, CBS News '60 Minutes' aired an interview with the heads. The head of the FBI, Christopher Wray, described the People's Republic of China as "*the defining threat to ... our economic and ultimately our national security.*" The directors described the threat to: '*military security, ... academics, ... Fortune 100 companies ... small business start-ups ... and the cutting edge technology of silicone valley.*' Alan Kohler, former FBI Assistant Director, Counterintelligence Division, said in part: "*China wants to be the worlds only superpower by 2049, and its going to come at our expense.*"[1]

4. China has a long history of cyber espionage in Canada, dating back to before 2000. In 2017 Canada signed a cyber agreement with China stipulating that neither government would support or sponsor the theft of intellectual property (IP). Six years later Chinese cyber espionage has escalated to such an extraordinary level that the

1 Source: CBS News '60 Minutes'. "Five Eyes" Intelligence leaders warn of China's global espionage campaign

director of CSCIS participated in the 'Five Eyes' warning. "*The PRC has never admitted to conducting ANY hacking despite indictments against officers of the PLA and criminal hacking indictments and convictions in multiple jurisdictions.*"[2] According to 60 Minutes, cyber espionage is a sideline of Chinese companies operating in western companies.[3]

5. In a separate release, cybersecurity company 'Mandiant' Intelligence Chief is warning that the PRC's 'Volt Typhoon' hackers are engaged in "very deliberate targeting of critical infrastructure" installations and represents a major shift by Chinese hacking teams known mostly for economic espionage and IP theft. This Volt Typhoon activity is a brand-new thing for them. We have not seen a lot of deliberate targeting in the critical infrastructure space from China," Hultquist said. "Occasionally, we'll catch them probing into power, but this is a deliberate, long-term attempt to infiltrate a lot of critical infrastructure in a way that stays below the radar."[4]

6. Analysts Comment: It is our *assessment* that the Five Eyes Directors warning constitutes a warning of a war-level effort by the People's Republic of China to overpower western democracies.

Hamas vs Israel

7. Cloudflare and the Recorded Future's research group, Insikt Group have both published indicators that: there was a cyber component to Hamas invasion of Israel and that there is *very probably* support from Iran. According to Cloudflare's blog: "*On October 7, 2023, at 03:30 GMT (06:30 AM local time), Hamas attacked Israeli cities and fired thousands of rockets toward populous locations in southern and central Israel, including Tel Aviv and Jerusalem. ... Approximately twelve minutes later, Cloudflare systems automatically detected and mitigated DDoS attacks that targeted websites that provide critical information and alerts to civilians on rocket attacks. ... Forty-five minutes later, a second much larger attack struck and peaked at 1M rps.*"[5] Cyber Security company 'Radware' reported: '*Most of the observed DDoS attacks lasted several hours with others spanning 24 hours. During the longer assaults, the hacktivists morphed their attacks by randomizing attack vectors to make detection and mitigation more difficult.*'[6]

8. In addition to Distributed Denial of Service (DDoS) attacks on websites, there were multiple attacks on Israels 'RedRocket', Rocket warning application, including malware, SMS and spam attacks.[7]

9. Co-ordination for the attacks appears to be through "*an application disseminated on a Telegram Channel used by members/supporters of the Hamas terrorist*

2 MacDonald-Laurier Institute: David Swan. The Canada-China Cyber Agreement remains questionable
3 Source: CBS News '60 Minutes'. "Five Eyes" Intelligence leaders warn of China's global espionage campaign
4 Source: Security Week. Mandiant Intelligence Chief Raises Alarm Over China's 'Volt Typhoon' Hackers in US Critical Infrastructure
5 Source: Cloudflare blog. Cyber attacks in the Israel-Hamas war
6 Source: Channel Futures. Israel-Gaza War Now Includes Accompanying Cyber Warfare
7 Source: Cloudflare blog. Cyber attacks in the Israel-Hamas war

organization. ... Recorded Future's research group, Insikt Group, has identified an application disseminated on a Telegram Channel used by members/supporters of the Hamas terrorist organization. ... The application is configured to communicate with Hamas's Izz ad-Din al-Qassam Brigades website. ... based on domain registration patterns, we observed a likely Iran nexus tied to that domain. ... Iran's Islamic Revolutionary Guard Corps (IRGC), and specifically the Quds Force, is the only known entity from Iran that provides cyber technical assistance to Hamas and other Palestinian threat groups."[8]

10. Analysts Comment: Cybersecurity companies use cautious language when describing their findings. This is probably an effort to not offend potential customers. Using NATO techniques and standards, the cyber communication links and relationships are very strong. Using the NATO 'Estimative Language Chart' our estimate of the linkage between Hamas cyber efforts and Iran is *very likely/very probable* or *70 to 89%*.

Russia vs Ukraine

11. The 'Cluster25 Threat Intel Team' has identified a new effort by a Russian hacker group to '*harvest credentials (logins) from compromised systems. The development comes as Google-owned Mandiant charted Russian nation-state actor APT29's "rapidly evolving" phishing operations targeting diplomatic entities amid an uptick in tempo and an emphasis on Ukraine in the first half of 2023.'*[9] The phishing operation exploits a flaw in WinRar compression and uses several documents as 'lures'. Some previous credential harvesting campaigns harvested a wide range of logins including: government logins, corporate, business, industry, education and healthcare organizations.

12. One of the reasons for the credential harvesting *may be* the relatively low level of success by Russia's hacking teams such as 'Sandworm'. Sandworm, also known as UAC-0165 and affiliated with the GRU, hacked '*at least 11 Ukrainian telecommunications providers.*'[10] '*Most reported cyberattacks have not caused major shutdowns, and are often resolved within a few hours.*' The reason the attacks have had limited impact is the support to the telecom companies provided by Ukraine's computer emergency response team, CERT-UA. CERT-UA and Ukrainian companies have also partnered '*with major cybersecurity firms, including Microsoft, Cisco, Palo Alto, Cloudflare, and ISSP, to prevent future intrusions.'*[11]

13. Apparently the conflict between two of Russia's 'patriotic hacker groups' Killnet and the Cyber Army of Russia, is ongoing. The Cyber Army of Russia is determined to thwart Killnet and its operations. KillNet is focused on supporting Palestinian groups in the Israel-Palestine conflict, while the Cyber Army of Russia is focused on the Russia-Ukraine conflict. The Cyber Army of Russia has announced '*a week-long campaign of*

8 Source: Recorded Future: Hamas Application Infrastructure Reveals Possible Overlap with TAG-63 and Iranian Threat Activity

9 Source: The Hacker News. Pro-Russian Hackers Exploiting Recent WinRAR Vulnerability in New Campaign

10 Source: Security Affairs. Russia-linked APT group Sandworm has hacked eleven telecommunication service providers in Ukraine between since May 2023

11 Source: The Record. Russia's Sandworm hacking unit targets Ukrainian telecom providers

evening DDoS attacks on government websites in Albania and Kosovo. Their initial target is the Republican Guard of Albania, a critical institution safeguarding high-ranking officials and vital facilities.'[12]

14. There has not been attribution of DDoS attacks on several Belgian government agencies websites '*presumably in response to Volodymyr Zelenskyy's visit to Belgium and its decision to deliver F-16 fighter jets to Ukraine. On 12 October, the websites of the Royal Palace, the Prime Minister and the Parliament of Brussels were disabled. At the same time, a message appeared on the Belgian Prime Minister's website: "We are coming to Belgium to destroy Russia-hating sites." ... the cyberattack continued as of the morning of 13 October.'*[13] There were no reports of significant damage.

15. A Russian government hacker group, Winter Vivern, is exploiting a vulnerability in the Roundcube webmail server, targeting European and NATO governments. *"Winter Vivern is a threat to governments in Europe because of its persistence, its very consistent running of phishing campaigns, and because a significant number of internet-facing applications are not regularly updated despite being known to contain vulnerabilities," ESET researcher Matthieu Faou says.*[14]

16. **Ukrainian Cyber Attacks**: Ukrainian hackers conducted two major hacks. Alfa-Bank, the largest private bank in Russia, was confirmed hacked in a joint operation by Ukrainian hacktivist groups KibOrg and NLB and Ukraine's security agency. '*More than 30 million Alfa-Bank customers had their data, including names, birthdates, phone numbers, and account numbers, compromised as a result of the cyberattack, said KibOrg on its official website'*, with identifying information leaked by the attackers.[15] Alfa-Bank denied reports of the leak.

Information Operations

17. France is investigating reports that the recent 'Paris infested with bedbugs' was distributed widely by Russian 'troll' social media sites.[16] The People's Republic of China is accused of a "spamouflage" disinformation campaign targeting Prime Minister Justin Trudeau, Conservative Leader Pierre Poilievre and other MPs in August and September, says Global Affairs Canada.[17] The campaign utilized many types of social media.

---

12 Source: The Cyber Express. Tensions Escalate: Russian Hacker Groups Clash, Israel-Palestine War Continues
13 Source: Ukrayinska Pravda. Russian hackers attack websites of Belgian state institutions during Zelenskyy's visit
14 Source: Security Week. Russian Hackers Caught Exploiting Roundcube Webmail Zero-Day
15 Source: SC Magazine. Major Russian bank reportedly hacked by Ukraine
16 Source: Telegraph (UK). Russia spread bedbug panic in France, intelligence services suspect
17 Source: CBC News. China linked to propaganda campaign targeting Trudeau, Poilievre, says Global Affairs