ACICE
ADMM Cybersecurity and Information Centre of Excellence

Monthly Digest

Issue 12/24 (Dec)

A monthly round-up of significant news around the world

Cybersecurity

United States (US) Telecommunications Breached in Suspected Espionage Campaign

1. On 13 Nov 2024, the US' Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) stated in a joint statement that People's Republic of China (PRC)-affiliated actors had "compromised networks at multiple telecommunications companies to enable (a) the theft of customer call records data; (b) the compromise of private communications of a limited number of individuals involved in government or political activity; and (c) the copying of certain information that was subject to US law enforcement requests pursuant to court orders". The affected telecommunications companies included AT&T, Verizon, Lumen Technologies and T-Mobile. According to *The Wall Street Journal*, US investigators further suspected that the threat actors had utilised artificial intelligence (AI) or machine learning in their cyber operations.

2. Several news outlets, including *The New York Times*, *The Wall Street Journal* and *Politico*, identified Salt Typhoon as the PRC-affiliated threat actor. In previous cyberattacks on telecommunications and government entities in Southeast Asia, Salt Typhoon, also known as GhostEmperor, had used multiple defence evasion techniques to maintain persistence, achieve lateral movement and exfiltrate information from targets' computers without being detected.

3. China has repeatedly denied the US allegations. In an email statement to *The Associated Press* on 3 Dec 2024, the Chinese embassy in Washington D.C. stated that it "firmly opposes and combats all kinds of cyberattacks", and urged

the US to "stop its own cyberattacks against other countries and refrain from using cybersecurity to smear and slander China".

4. In response to the breaches, the US government has launched an ongoing in-depth investigation to uncover the extent of the breaches. In addition, on 3 Dec 2024, CISA and other security agencies from the Five Eyes intelligence alliance jointly released a visibility and hardening guide for communications infrastructure. The guide outlined best practices for monitoring and detecting unusual activity, as well as limiting potential entry points for threat actors.

The Republic of Korea (ROK) Affected by Global Positioning System (GPS) Jamming Attacks

5. From 8 to 17 Nov 2024, the ROK experienced multiple GPS jamming attacks, which it attributed to the Democratic People's Republic of Korea (DPRK). The jamming attacks occurred at various locations near the DPRK-ROK border, including near the ROK province of Gangwon, and the DPRK provinces of Kaesong and Haeju. While multiple civilian ROK ships and aircraft in the vicinity were affected, the ROK military clarified that no military ships or aircraft were affected.

6. According to *Yonhap News Agency* and the ROK military, the recent jamming attacks might be linked to DPRK's military training rather than specific attacks targeting the ROK. Notably, compared to previous jamming attacks, each instance of the recent attacks had been less intense, less targeted and lasted for a shorter period of time.

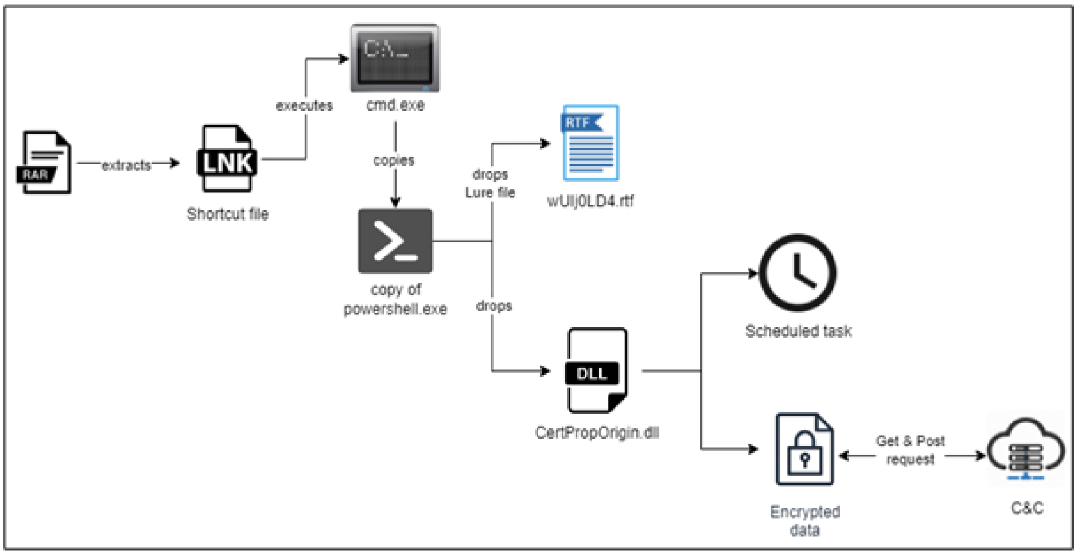
7. The ROK had warned ships and aircraft operating in the Yellow Sea to maintain vigilance against such attacks, as well as urged the DPRK to stop their GPS provocations.

New Tactics in DONOT's Cyberattacks on Pakistan Industries

8. DONOT is an Advanced Persistent Threat (APT) that has been targeting military entities, foreign affairs ministries and embassies in cyberattacks across South Asia since 2016. Using spear phishing emails that contained malicious Microsoft Office files, previous DONOT attacks had aimed to avoid detection and maintain access for long-term information gathering.

9. In Nov 2024, DONOT was observed utilising new tactics to target Pakistan's defence, maritime and manufacturing industries. Spear phishing emails sent to employees in these industries contained a malicious LNK file

disguised as a Rich Text Format (RTF) document. Once opened, the malicious LNK file would initiate processes that (a) collected system information from the target's computer to assess the target's value; (b) set up scheduled tasks to help the malware establish persistence in the target's computer; and (c) established communications with DONOT's command and control (C2) server. If DONOT determined that the target was worthy of attack, subsequent information exfiltration malware could be sent to the target's computer via the established communications. New encryption methods were also used by DONOT malware to avoid detection. Overall, these changes highlighted the increased sophistication and more specific targeting in DONOT's cyberattacks.



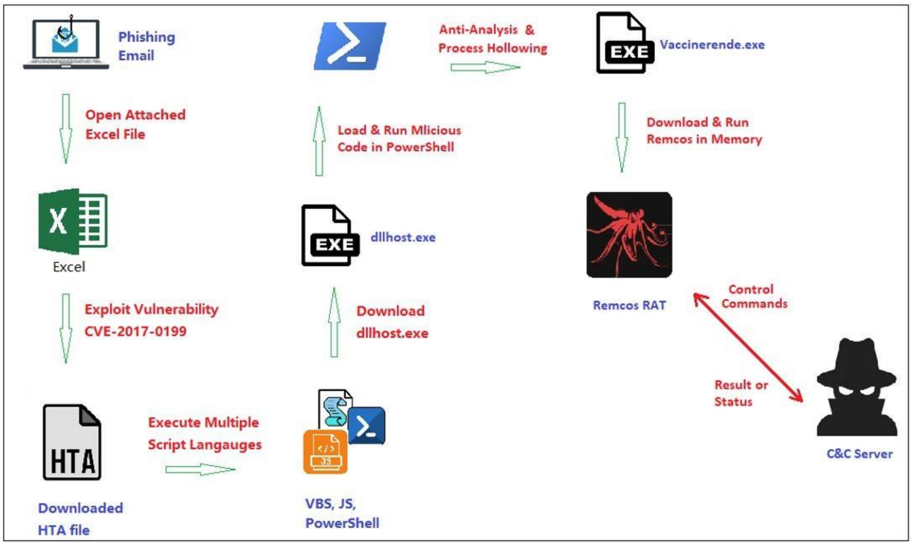
DONOT infection chain
(Source: Cyble Research and Intelligence Labs)

10. To prevent such attacks, Cyble Research and Intelligence Labs (CRIL) suggested (a) conducting regular cybersecurity awareness training for employees that focused on identifying phishing emails, (b) conducting frequent audits of scheduled tasks to identify unauthorised tasks, and (c) implementing behaviour-based detection systems that could identify malicious computer actions, such as frequent attempts to contact external C2 servers, or unexpected outbound transmission of encrypted data.

New "Fileless" Remcos Malware Variant

11. Remcos is a commercially available remote access tool that had been marketed by a German company, Breaking Security, for various functions, including parental control, penetration testing, and systems monitoring. However, it has been abused by numerous hackers to fully control and monitor any Windows computer from XP onwards, and is currently one of the Top 10 malware strains.

12. On 8 Nov 2024, Fortinet, a cybersecurity solution provider, reported observing a new “fileless” variant of Remcos malware targeting Microsoft Windows users. A phishing email would be used to deliver a Microsoft Excel document to the target. Once the Excel document was opened, a known vulnerability, CVE-2017-0199, which affected Microsoft Office handling of specially crafted files, was exploited to download various malicious files. A malicious HTML Application file would then inject the Remcos malware directly into the target computer’s memory. Hence, this Remcos malware variant was “fileless” as the malware existed in a target computer’s memory rather than in the computer’s local files. This variant of Remcos malware was also able to use new evasion tactics, namely a vectored exception handler and an Application Programming Interface (API) hooking technique, to evade detection. With the Remcos malware in the target computer’s memory, the threat actor could then control the target’s computer and collect information, such as keystrokes, screenshots, audio and passwords.



Remcos infection chain
(Source: Fortinet)

13. To prevent such attacks, organisations should train their employees to recognise phishing emails and suspicious Excel documents. More importantly, the use of a known 2017 vulnerability, CVE-2017-0199, in this new Remcos malware variant highlighted the importance of ensuring Microsoft Office applications are regularly updated and patched.

Artificial Intelligence (AI)

Discovery of Real-World Vulnerability Using AI Agent

1. On 1 Nov 2024, Google's Project Zero team announced that it had used its Big Sleep AI agent to discover a vulnerability in SQLite, a widely used open-source database engine. As the vulnerability had been discovered in early Oct 2024, before the software had appeared in an official release, SQLite was able to patch the affected systems and no SQLite users were affected by the vulnerability.

2. Formed in 2014, Project Zero consisted of top Google security researchers working to track and neuter zero-day vulnerabilities. Zero-day vulnerabilities are previously unknown vulnerabilities for which no patch or fix exists, and are regularly used by threat actors in targeted cyberattacks. Project Zero also aimed to narrow the knowledge gap between the public and private sectors by sharing their discoveries on zero-day vulnerabilities.

3. The Big Sleep AI agent was the result of Google's efforts to harness AI large language models (LLMs) for defensive applications. To date, Big Sleep AI's discovery of the vulnerability in SQLite represented one of the first public examples of an AI agent finding previously unknown zero-day vulnerabilities in widely-used real-world software. In an arena where cyber defenders are frequently playing catch-up against threat actors, this discovery highlighted AI's potential to turn the tables and provide significant advantages for cyber defenders in the future.

Release of International Strategic Plan by the US' CISA

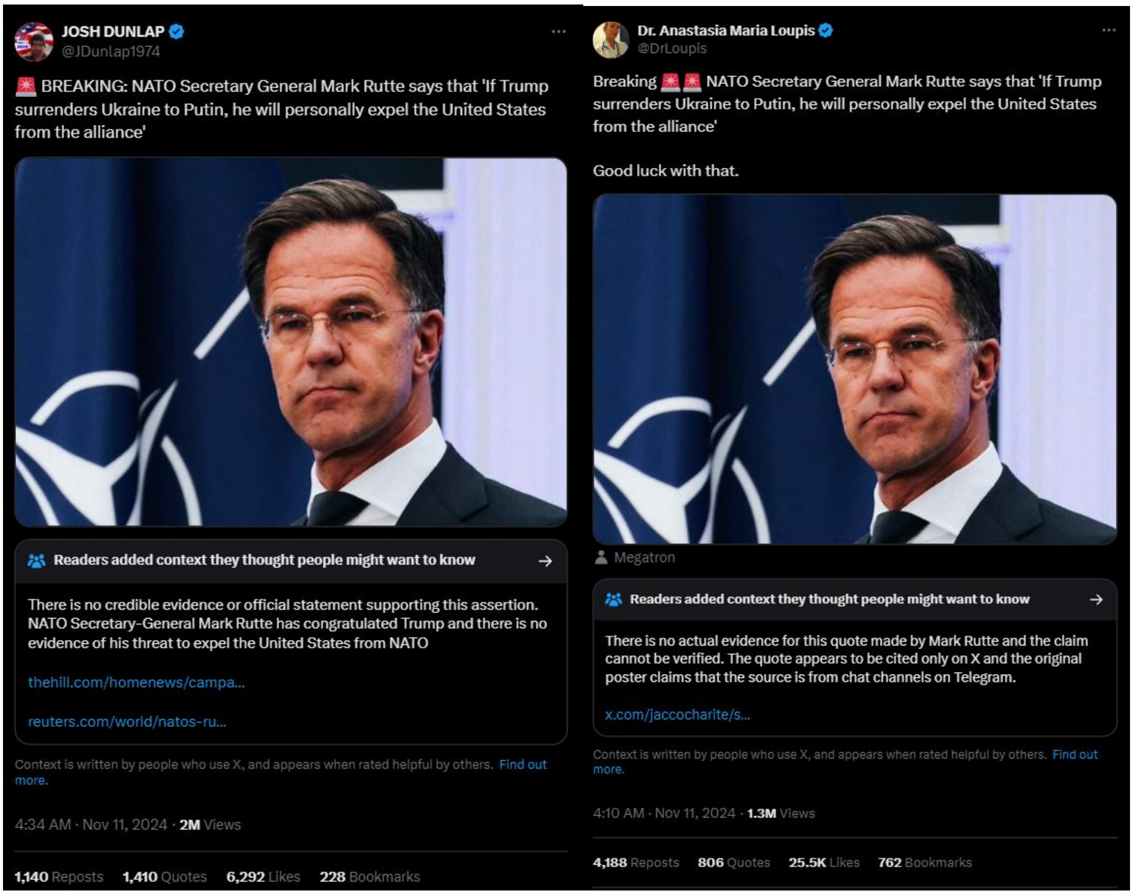
4. On 29 Oct 2024, the US' CISA announced the release of its 2025-2026 International Strategic Plan. The Plan came on the heels of the National Security Memorandum on Critical Infrastructure Security and Resilience, which was released in Apr 2024, and aimed to outline how CISA would proactively engage international partners to strengthen the security and resilience of US critical infrastructure.

5. The Plan outlined three goals, namely to: (a) bolster the resilience of foreign infrastructure on which the US depended on; (b) strengthen integrated cyber defence; and (c) unify US agencies' coordination of international activities.

Information

North Atlantic Treaty Organisation (NATO) Secretary General Rutte's Statements on Expelling US – Real or Fake

1. On 11 Nov 2024, several social media posts claimed that NATO Secretary General Mark **Rutte** had said "If Trump surrenders Ukraine to Putin, [I] will personally expel the United States from the alliance". Some of these social media posts on X had more than one million views.



JOSH DUNLAP
@JDunlap1974

🚨 BREAKING: NATO Secretary General Mark Rutte says that 'If Trump surrenders Ukraine to Putin, he will personally expel the United States from the alliance'

Readers added context they thought people might want to know

There is no credible evidence or official statement supporting this assertion. NATO Secretary-General Mark Rutte has congratulated Trump and there is no evidence of his threat to expel the United States from NATO

thehill.com/homenews/campa...

reuters.com/world/natos-ru...

Context is written by people who use X, and appears when rated helpful by others. Find out more.

4:34 AM · Nov 11, 2024 · **2M** Views

1,140 Reposts **1,410** Quotes **6,292** Likes **228** Bookmarks

Dr. Anastasia Maria Loupis
@DrLoupis

Breaking 🚨🚨 NATO Secretary General Mark Rutte says that 'If Trump surrenders Ukraine to Putin, he will personally expel the United States from the alliance'

Good luck with that.

Megatron

Readers added context they thought people might want to know

There is no actual evidence for this quote made by Mark Rutte and the claim cannot be verified. The quote appears to be cited only on X and the original poster claims that the source is from chat channels on Telegram.

x.com/jaccocharite/s...

Context is written by people who use X, and appears when rated helpful by others. Find out more.

4:10 AM · Nov 11, 2024 · **1.3M** Views

4,188 Reposts **806** Quotes **25.5K** Likes **762** Bookmarks

Social media posts about Rutte's claims, some of which had more than one million views (Source: X/[@]JDunlap1974 and x/[@]DrLoupis)

2. Citing a NATO spokesperson, who had labelled the claim as "bogus", fact-checking websites such as *PolitiFact* and *DFRAC*, as well as news sites such as *DW News* and *Euronews*, had debunked the claim as fake. *PolitiFact* and *DW News* also pointed out that NATO did not have formal mechanisms in place to suspend or expel member nations.

3. In an interview with *DW News*, Dick **Zandee**, head of the security and defence program at the Clingendael Institute in The Hague, highlighted that such false claims could be used to sow discord among NATO members.

Hamas Leader Yahya Sinwar’s Posthumous Legacy: Martyr or Devil?

4. Following Hamas leader Yahya **Sinwar**’s death on 16 Oct 2024, the Israeli Defense Forces (IDF) released drone footage of Sinwar’s last moments. In the video, a seemingly injured Sinwar was seen sitting alone on a sofa in a destroyed house. Upon noticing the drone, Sinwar defiantly threw a stick at the drone; *The Guardian* noted that this action set Sinwar apart from his predecessors, who had been assassinated while on the run.

IDF drone footage video showing Sinwar’s final moments
(Source: IDF and The Telegraph)

5. Gershon **Baskin**, a Middle East expert interviewed by *Cable News Network (CNN)*, stated that the IDF might have released the drone footage to craft a victory narrative around the ongoing conflict. Gil **Siegal**, a legal scholar and head of the Center for Medical Law, Bioethics and Health Policy at the Ono Academic College in Israel, also pointed out in another *CNN* interview that the IDF might have released the footage to prove that Sinwar was in fact dead, or to show that Sinwar was alone without support in his final moments.

6. However, Baskin highlighted that such a move might have backfired as it also appeared to depict Sinwar as “a hero, a fighter to the very end”. Indeed, on social media, Sinwar had been labelled as a legend for throwing the stick at the drone and fighting to the end despite being injured. Palestinians interviewed by *Reuters* had also highlighted how the video footage of Sinwar alone disproved IDF narratives that Sinwar had been “keeping Israeli prisoners next to him to save his life”.

موسوعة
الأمثال
العربية
الحديثة
ر
قل : رميته بعصى السنوار دلالة على أنّ
الإنسان حاول بكل ما يستطيع وبذل كل
جهده ولم يبق معه إلا عصاً، فرمى بها.

Social media poster capturing Sinwar's defiant act of throwing a stick at a drone despite being injured (Source: Al-Alam News Network)

7. Stating that "the truth is in the eye of the beholder", Siegal highlighted that while video objectively showed "a person covered with dust, clearly injured, attempting to throw an object [at] a drone", the video had then been variously interpreted to craft different narratives that suited either Israel's or Hamas' respective goals.

8. To counter the portrayal of Sinwar as a martyr, *CNN* noted that the IDF had since released several videos and photos of Sinwar hiding in the tunnels underneath Gaza with his family. The IDF had also circulated claims that Sinwar lived a comfortable life in the tunnels and had prioritised his own self-interests.

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

REFERENCES

Cybersecurity

United States (US) Telecommunications Breached in Suspected Espionage Campaign

1. Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure
https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

2. T-Mobile Hacked in Massive Chinese Breach of Telecom Networks
https://www.wsj.com/politics/national-security/t-mobile-hacked-in-massive-chinese-breach-of-telecom-networks-4b2d7f92

3. US Officials Race to Understand Severity of China’s Salt Typhoon Hacks
https://www.wsj.com/politics/national-security/u-s-officials-race-to-understand-severity-of-chinas-salt-typhoon-hacks-6e7c3951

4. US Wiretap Systems Targeted in China-Linked Hack
https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

5. What to Know About the Chinese Hackers Who Targeted the 2024 Campaigns
https://www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html

6. Chinese Hackers Gained Access to Huge Trove of Americans’ Cell Records
https://www.politico.com/news/2024/11/06/chinese-hackers-american-cell-phones-00187873

7. FBI Tells Telecom Firms to Boost Security Following Wide-Ranging Chinese Hacking Campaign
https://apnews.com/article/china-hacking-salt-typhoon-trump-fbi-41ca253307e3eba2c34b3dc34dadcbeb

8. Enhanced Visibility and Hardening Guidance for Communications Infrastructure
https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

The Republic of Korea (ROK) Affected by Global Positioning System (GPS) Jamming Attacks

9. North Korea's GPS Jamming Continues for 10th Day
https://en.yna.co.kr/view/AEN20241117001600315?section=search

10. North Korea's GPS Jamming Expands to Wider Regions Along Inter-Korean Border: Official
https://en.yna.co.kr/view/AEN20241116002700315?section=search

11. North Korea Jams GPS Signals, Affecting Ships, Aircraft in South
https://www.channelnewsasia.com/east-asia/north-korea-jams-gps-signals-south-korea-ships-aircraft-4737706

New Tactics in DONOT's Cyberattacks on Pakistan Industries

12. DONOT Malware Family
https://malpedia.caad.fkie.fraunhofer.de/details/win.donot

13. DONOT's Attack on Maritime & Defence Manufacturing
https://cyble.com/blog/donots-attack-on-maritime-defense-manufacturing/

14. DONOT APT Group Targets Pakistan's Maritime and Defence Sectors in New Campaign
https://securityonline.info/donot-apt-group-targets-pakistans-maritime-and-defense-sectors-in-new-campaign/

15. APT Group DONOT Targets Pakistan's Maritime and Defense
https://thecyberexpress.com/apt-group-donot-targets-pakistan/

16. StrikeReadyLabs on X
https://x.com/StrikeReadyLabs/status/1852532673283268899

New "Fileless" Remcos Malware Variant

17. Remcos Malware
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/remcos-malware/

18. Remcos Malware Information
https://success.trendmicro.com/en-US/solution/KA-0009536

19. New Campaign Uses Remcos RAT to Exploit Victims
https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims

20. ‘Top 10’ Malware Strain, Remcos RAT, Now Exploiting Microsoft Excel Files
https://www.scworld.com/news/excel-doc-loaded-with-remcos-rat-lets-attackers-gain-backdoor-access

21. A New Fileless Variant of Remcos RAT Observed in the Wild
https://securityaffairs.com/170791/security/a-new-fileless-variant-of-remcos-rat-phishing.html

22. Cybercriminals Use Excel Exploit to Spread Fileless Remcos RAT Malware
https://thehackernews.com/2024/11/cybercriminals-use-excel-exploit-to.html

23. Revamped Remcos RAT Deployed Against Microsoft Users
https://www.darkreading.com/application-security/revamped-remcos-rat-microsoft-windows-users

Artificial Intelligence

Discovery of Real-World Vulnerability Using AI Agent

1. Google Online Security Blog: Announcing Project Zero
https://security.googleblog.com/2014/07/announcing-project-zero.html

2. Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers
https://www.wired.com/2014/07/google-project-zero/

3. Project Zero: From Naptime to Big Sleep: Using Large Language Models to Catch Vulnerabilities In Real-World Code
https://googleprojectzero.blogspot.com/2024/10/from-naptime-to-big-sleep.html

Release of International Strategic Plan by the US’ CISA

4. CISA Releases Its First Ever International Strategic Plan
https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan

5. FY2025-2026 CISA International Strategic Plan
https://www.cisa.gov/2025-2026-cisa-international-strategic-plan

Information

NATO Secretary General Rutte's Statements on Expelling US – Real or Fake

1. Fact Check: Has NATO Chief Rutte Threatened to Expel US?
   https://www.dw.com/en/fact-check-has-nato-chief-rutte-threatened-to-expel-us/a-70772416

2. No, NATO Secretary General Mark Rutte Didn't Say He'd Expel US if Trump Helps Russia with Ukraine
   https://www.politifact.com/factchecks/2024/nov/13/threads-posts/no-nato-secretary-general-mark-rutte-didnt-say-hed/

3. No, NATO's Chief Has Not Threatened to Expel US
   https://www.euronews.com/my-europe/2024/11/20/no-natos-chief-has-not-threatened-to-expel-us

4. Fake Claim Alleging NATO Secretary General's Statement Goes Viral. Here's the Truth
   https://dfrac.org/en/2024/11/12/fake-claim-alleging-nato-secretary-statement-goes-viral/

5. JDunlap1974 on X
   https://x.com/JDunlap1974/status/1855710650586054922

6. DrLoupis on X
   https://x.com/DrLoupis/status/1855704675326312481

Hamas Leader Yahya Sinwar's Posthumous Legacy: Martyr or Devil?

7. Yahya Sinwar as a Posthumous Social Media Legend?
   https://www.rsis.edu.sg/rsis-publication/rsis/yahya-sinwar-as-a-posthumous-social-media-legend/

8. Sinwar's Stick Enters the Encyclopaedia of Modern Arabic Folk Proverbs
   https://www.alalam.ir/news/7021478/

9. Israel and Hamas are Fighting a Battle of Narratives Over Sinwar's death
   https://edition.cnn.com/2024/10/20/middleeast/sinwar-death-narrative-israel-hamas-intl-latam/index.html

10. Gazans Revere Sinwar's Defiant End: Throwing a Stick at an Israeli Drone
https://www.reuters.com/world/middle-east/this-is-how-hero-dies-say-gazans-sinwars-battlefield-death-2024-10-18/

11. Why Sinwar’s ‘Warrior Death’ Will Win Him Martyr Status in Gaza and Beyond
https://www.theguardian.com/world/2024/oct/20/why-sinwars-warrior-death-will-win-him-martyr-status-in-gaza-and-beyond

12. Hamas Leader, Yahya Sinwar Throws Stick at Drone in Desperate Final Moments
https://www.youtube.com/watch?v=q1NvH0Hyp1Q