

 BRIEF

ANTICIPATED RAMIFICATIONS OF EXPANDED NATO MEMBERSHIP

ZEROFOX INTELLIGENCE

B-2022-05-26a

Classification: White

Criticality: High

Intelligence Requirements: Deep Dark Web & Criminal Underground,
Geopolitical and Physical

May 26, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on May 24, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Anticipated Ramifications of Expanded NATO Membership

Executive Summary

On May 18, 2022, Finland and Sweden both formally submitted their applications to join the North Atlantic Treaty Organization (NATO) at its headquarters in Brussels; their successful ascension would double the length of NATO's border with Russia. Both countries will now enter a formal application process that requires all NATO members' approval. The process could take six to 12 months. NATO members, led by the United States and the United Kingdom, have promised to protect Finland and Sweden during the application process. Russia threatened immediate retaliation, including unspecified military-technical measures over the applications. NATO enlargement was cited as one of the primary reasons for Russia's war in Ukraine, and Russia is opposed to the bloc gaining new members, particularly along its 800-mile border with Finland. Russia could use military, economic, political, or cyber measures to decentivize non-NATO members from joining the military alliance.

Details

Military

Russia has historically been considered the primary external military threat to both Sweden and Finland. Previously, however, these countries judged joining NATO as too provocative toward Russia. In April 2008, NATO leaders at the Bucharest Summit agreed that Georgia would eventually become a member of the alliance, which likely played into Russia's calculus ahead of the 2008 Russo-Georgian war and likely factored into the neutrality maintained by other pro-European Union (EU) states near Russia's borders. However, since Russia's military invasion in Ukraine in February 2022, many previously-neutral countries have become more concerned with securing allies to dissuade Russia. Since Russia's invasion, public and political opinion on joining NATO has shifted from largely against membership to firmly in favor. A compelling example of this is the Finnish parliament recently voting in favor of the application by a margin of 188 to 8.



Russia has threatened both Finland and Sweden¹ with military consequences, including putting more nuclear warheads near the Baltic States as well as troop movements near the Finish border. Both countries have large standing armies, military bases, and larger weapons stockpiles than countries like Germany. These memberships would benefit NATO, but the smaller countries are looking to make sure they do not go it alone, like Ukraine has, if there is any military confrontation with Russia.² This month, NATO bolstered its number of soldiers to 40,000 in NATO states along Russia's border, which is 10 times higher than NATO troop levels previous to the Ukraine invasion.

Although a Russian military intervention in Finland over its NATO application is unlikely, it could take the form of false flag operations against Russia's own military forces at the border in order to implicate Finland in order to justify those forces' intervention. Similar false flag operations were predicted ahead of the February war in Ukraine and with regards to Transnistria, an autonomous region internationally recognized as part of Moldova. Russia militarily occupies Transnistria, and the Moldovan central government has no official control. Russia's military is stretched extremely stretched thin with its war in Ukraine and is unlikely to attack non-NATO member states during the application process. However, long-term troop deployments along NATO and Russian borders does increase the likelihood of a cross-border military incident.³

Cyber

There is little evidence at this time of Russian cyber actors targeting Finland or Sweden specifically over NATO membership. However, like other geographical neighbors of Russia, both nations are accustomed to cyber threats from Russia over geopolitical issues. Those operating in Finland or Sweden should be prepared for various Russian measures to influence society and public opinion. This could include state or criminal cyber attacks, intelligence operations, and/or attacks on infrastructure.

Russia will likely expand its cyber and information operations, although a major attack that Russia cannot deny is unlikely (though not improbable). Russia has largely refrained from major cyber operations during the war in Ukraine, likely fearful of retaliation and of revealing its endogenous cyber attack capabilities. The most likely operations would attempt to influence public opinion on issues like NATO or EU membership, although website defacements or denial of service attacks are also

¹ <https://twitter.com/gazetaru/status/1526937496147435520>

²

<https://www.euronews.com/2022/05/18/tytti-tuppurainen-tells-euronews-why-finland-wants-to-join-the-nato-military-alliance>

³

<https://www.euronews.com/my-europe/2022/05/18/nato-now-has-40-000-soldiers-on-europe-s-border-with-russia>



common for countries in Russia's sphere of influence. This could extend to Turkey as well, which Russia is eager to see block NATO enlargement.

In the run-up to the announcement, Russia cut off electricity supplies to Finland. Russia is responsible for 10 percent of Finland's electricity, and Finland stated it could cope without Russian supplies.⁴ However, threat actors could target the strained utility to demonstrate their antagonism towards the NATO project. On May 21, 2022, Russia cut off natural gas supplies to Finland over the NATO application. Again, threat actors could seek to worsen the natural gas supply or price issue by targeting the Finnish energy sector in general or industries dependent on it.

As speculation rose that Finland would apply to join the NATO alliance, Finland reported that multiple government websites and services had been targeted by a denial-of-service (DoS) attack.⁵ The attack happened while a speech by Ukrainian President Volodymyr Zelenskyy was being broadcast to Finnish lawmakers.

Some experts believe that Russian cyber attacks against Finland or Sweden are unlikely to occur on the same scale as those that happened in Ukraine. Attacks like the DoS targeting Finnish government websites or website defacements are more likely to happen in protest against the two countries' decision to apply for NATO membership rather than a large-scale or coordinated effort.⁶

Finland's National Cyber Security Centre (NCSC-FI) has warned of a campaign targeting Android users with FluBot, a banking trojan spread via SMS messages. Apple iPhone owners were also being targeted by similar SMS messages, but—due to Apple's security policy of not allowing apps to be installed from sources other than the official App Store—these recipients were instead redirected to other various scams.⁷ This campaign is not likely related to Russia's threats made toward Finland and Sweden for their decision to apply for NATO membership.

There has been speculation that threat actor groups could utilize this geopolitical unrest as a catalyst for targeted activity. One of those groups is the Conti ransomware gang, which was recently observed trying to exert pressure on the Costa Rican

4

<https://www.rfi.fr/en/international/20220514-russia-cuts-electricity-supply-to-finland-as-country-edges-near-nato-membership-war-ukraine>

5

<https://www.bloomberg.com/news/articles/2022-04-08/finland-hit-by-cyber-attack-airspace-breached-as-nato-bid-weighed>

6

<https://thehill.com/policy/cybersecurity/3488518-finland-swedens-nato-moves-prompt-fears-of-russian-cyber-attacks/>

7

<https://blog.bitdefender.com/blog/hotforsecurity/rejuvenated-flubot-campaign-moves-to-finland-iphone-users-also-targeted-2/>



government by claiming to have insiders and threatening to “overthrow the government” if their ransom demands are not paid.⁸ Despite making these threats, the real motivation with ransomware groups is almost always financial. Attacking such a high-profile target and later making serious threats may end up backfiring on the group, if past events such as Darkside’s disappearance after the Colonial Pipeline incident are any indication. While publicly shaming and making threats may intimidate some victims into paying the ransom, this can also lead to increased efforts by law enforcement around the world to identify members. After Darkside encrypted systems at Colonial Pipeline, the U.S. Department of State offered a USD 10 million reward for information leading to the identification of Darkside members in key positions and two separate USD 5 million rewards for information leading to the arrest of any individuals attempting to participate in Darkside activities.⁹ The U.S. Department of State has also offered a USD 10 million reward for information leading to the identification or location of Conti’s leadership.

Analyst Commentary

Now that Sweden and Finland’s applications have been submitted, the proposed member states will meet with current NATO members to gather their support. The main outlier for quick acceptance to NATO is Turkey. Turkey cited Sweden and Finland’s supposed support for Kurdish terrorist groups as its reason for being opposed to the two countries becoming NATO members. While Turkey is demanding Sweden and Finland declare the armed Kurdish group, the PKK, a terrorist organization, its objections are primarily to secure military concessions. Turkey has been banned from participation in the U.S. F-35 fighter jet program, and sales of F-16s to Turkey are prohibited as well. The ban is over Turkey purchasing a Russian air defense system: the S-400. Turkey wants to be re-submitted into the F-35 program and have the ability to purchase F-16s without giving up its S-400 air defense system. It is probable Turkey will drop its appeal if it achieves these military concessions. In the past week, the United States countenanced sanction relief for Cuba and Venezuela and agreed to a high-profile meeting with leadership in Saudi Arabia. These actions were explicitly done with Russia in mind. If the current U.S. administration can overcome those geopolitical disputes, resolving Turkey’s NATO concerns should be easier for the administration to achieve. The United States likely views Sweden and Finland’s NATO membership as far too important to hold up over the military sanctions on Turkey. The UK ending all restrictions on defense exports to Turkey on May 20, 2022, furthers

8

<https://apnews.com/article/technology-government-and-politics-caribbean-gangs-381efc2320abb5356dee7f356e55e608>

9

<https://www.bleepingcomputer.com/news/security/us-targets-darkside-ransomware-and-its-reb-rands-with-10-million-reward/>



this assessment.¹⁰ The length of time Turkey objects to their NATO membership is key in determining the timeline of the threat posed to Finland and Sweden.

Recommendations

Russian natural gas accounts for only around five percent of Finnish energy supplies. However, most Russian gas does go to Finnish factories and manufacturing, making those industries more susceptible to a shortage of gas than Finnish society in general. Seeking alternative energy supplies is advisable.

To protect cyber assets, organizations should continue to follow and build upon their current cybersecurity policies. These policies should include best practices such as:

- Ensuring antivirus and intrusion detection software is up-to-date with all patches and rule sets.
- Enabling two-factor authentication for all organizational accounts.
- Utilizing account permissions best practices such as role-based access control, least privilege, and restricting root/admin permissions.
- Maintaining regularly scheduled backup routines, including off-site storage and integrity checks.
- Maintaining a “gold image” for servers and workstations, allowing machines to be quickly re-imaged in the event of an infection.
- Logging and monitoring all administrative actions as much as possible and alerting on any suspicious activity.
- Disabling unused ports on internet-facing devices.
- Quarantining malware-infected workstations on a private network segment with no external connections.
- Changing passwords immediately on alerted or suspected compromised accounts.

¹⁰ <https://twitter.com/ragipsoylu/status/1527650835999739906?s=21>



Appendix: Traffic Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:

RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:

RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:

AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:

GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:

WHITE information without restriction, subject to copy-right controls.