CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

June 18, 2025

Threats to the 2025 NATO Summit

The 2025 NATO Summit is likely a pivotal moment for the alliance's unity, which hinges on US commitment to collective defense against Russia's multifaceted warfare campaign in Ukraine and Europe.

Malign influence and cyber-espionage activity from Russia and China, as well as cybercriminal and hacktivist activity, are likely the three primary threat vectors to the 2025 NATO Summit.

The summit's extensive security posture very likely mitigates the scope, sophistication, and impact of physical security threats to the event from violent non-state actors.

Executive Summary

On June 24 and 25, 2025, representatives of all 32 members of the North Atlantic Treaty Organization (NATO) will convene in The Hague, the Netherlands, for the 2025 NATO Summit. With each member's head of state or government in attendance, the summit represents a high-profile diplomatic event taking place amid heightened geopolitical uncertainty and internal alliance tensions. Key issues, such as the ongoing war in Ukraine, economic volatility, rising Euroscepticism, and concern over the United States' (US) commitment to NATO going forward, are all likely to dominate the agenda.

The complex geopolitical backdrop of the 2025 NATO Summit almost certainly increases its appeal as a target for a wide spectrum of threat actors, including state-sponsored influence operations groups and cyber threat actors, cybercriminals, and hacktivists. Insikt Group assesses that malign influence operations, cyber-espionage activity, and a measurable uptick in cybercriminal and hacktivist activity likely represent the three primary threat vectors to the 2025 NATO Summit. Russian and Chinese influence networks will almost certainly seek to exploit the summit to amplify perceptions of NATO disunity and undermine its credibility as a reliable security partner. In parallel, Russian state-sponsored cyber actors are highly likely to conduct targeted espionage against NATO-affiliated entities and personnel, while Chinese cyber threat actors are more likely to pursue opportunistic intrusions to glean insight into alliance policies and future planning. Hacktivist and cybercriminal actors are already attempting to capitalize on the summit's geopolitical visibility for financial gain and political messaging, based on closed forum references to NATO and ongoing targeting of NATO member states.

Security officials are simultaneously preparing extensive physical security measures to safeguard the event. While direct attacks on the summit by Russian hybrid actors — encompassing conventional and irregular military forces — are unlikely, tactics such as sabotage, vandalism, weaponized migration, and provocative military signaling will very likely continue to pressure NATO member states around the time of the event, particularly allies in Eastern Europe. At the time of publication, Insikt Group assesses that protests during the summit are very likely, but risks associated with protest activities are largely mitigated through proactive security measures. Additionally, we have not observed any credible evidence suggesting that violent non-state actors are planning or expressing intent to target the summit.

Key Findings

- We assess NATO's ability to project unified geopolitical and military strength is likely more uncertain than any time in recent years, driven by US rhetoric questioning the alliance's utility, rising political influence of Eurosceptic far right parties in several NATO member states, and Russia's continued efforts to undermine NATO unity via its military campaign in Ukraine and hybrid sabotage and influence operations in Europe.
- Russian hybrid threats, including sabotage of critical infrastructure, vandalism, weaponized migration, and coercive military posturing, will very likely continue to target European countries ahead of and following the 2025 NATO Summit, particularly if the summit results in significant action regarding Ukraine — with the Baltic states, Poland, and Germany likely at highest risk.
- Both Russia and China's own influence ecosystems will almost certainly attempt to shape public opinion around the 2025 NATO Summit by portraying the alliance as aggressive, divisive, and divided.
- Malign influence actors, particularly from Russia, are likely to use artificial intelligence (AI)-generated media in an effort to discredit NATO leadership, delegitimize summit outcomes, and further inflame tensions among member states.
- Cybercriminal and hacktivist activity referencing NATO has surged across dark web and special-access forums in the months leading up to the 2025 NATO Summit, very likely signaling a heightened risk of ideologically driven and financially motivated multi-vector campaigns targeting NATO member states and defense-affiliated entities.
- Russian state-aligned threat groups, particularly those linked to the SVR, FSB, and GRU, are highly likely to conduct targeted operations against entities and personnel associated with the 2025 NATO Summit.
- Chinese state-sponsored groups tasked with the collection of foreign intelligence, particularly those under the Ministry of State Security, are likely to engage in some level of opportunistic cyber-espionage operations against select attendees with the goal of understanding summit-related policy discussions and outcomes.
- The Netherlands' extensive security posture around the 2025 NATO Summit will very likely mitigate the scope, sophistication, and impact of physical security threats to the event from violent non-state actors, including terrorists, violent extremists, criminal organizations, and disruptive protest movements.

Strategic Threat Environment

2025 NATO Summit Likely Pivotal for Alliance's Future Unity

The 2025 NATO Summit comes at a time when the alliance's ability to project unified geopolitical and military strength is likely more uncertain than any time in recent years, driven by US rhetoric questioning the alliance's utility; rising political influence of Euroskeptic far right parties in several NATO member states; and Russia's continued efforts to undermine NATO unity via its military campaign in Ukraine, and hybrid sabotage and influence operations in Europe.

The US government's public messaging concerning its commitment to NATO has been inconsistent throughout President Donald Trump's first and second terms. In 2025, President Trump suggested that the US's commitment to Article 5 of NATO's founding treaty[1] would depend on a given NATO state's defense spending, stating, "If they don't pay, I'm not going to defend them." In contrast, in 2017, President Trump stated, "Absolutely, I'd be committed to Article 5."

Secretary of State Marco Rubio announced that all NATO members will be expected to spend 5% of their GDP on defense over the next decade, an increase from the previous benchmark of 2%. Although Rubio emphasized that the US remains committed to supporting NATO, notes from an internal Trump Administration proposal revealed plans to reduce the amount of money the US would contribute to NATO's budget. The US currently provides roughly 16% of the alliance's funding.

In some key NATO states, the rising political influence of far-right parties that are skeptical of NATO and sympathetic to Russia likely complicates their ability to reinforce NATO commitments. For example, France's Rassemblement National (RN) has historically advocated for France's withdrawal from NATO. Though the RN has recently moderated its position, its historically anti-NATO position risks complicating French President Emmanuel Macron's ability to achieve consensus on increased French defense spending for NATO. Germany's Alternative für Deutschland (AfD) has questioned NATO's continued utility and has advocated for closer Germany-Russia ties.

Differences in NATO states' probable responses to Russia's multi-pronged attempts to weaken NATO and its allies will almost certainly strain NATO's ability to project a unified response to Russia's actions. Though NATO has, from its founding in 1945, been primarily concerned with resisting Russian aggression, in the last two years, Russia has significantly escalated its aggression towards NATO and its allies, with Moscow's full-scale invasion of Ukraine, escalating sabotage operations in NATO territory, and widespread influence operations aimed at undermining public confidence in Western democracy and manipulating elections in favor of pro-Russia candidates.

[1] Article 5 of The North Atlantic Treaty outlines the principle of collective defense, whereby an attack on one NATO member state is considered to be an attack on all of them.

Profiles of Key Players

United States — Unpredictable NATO Leader

Inconsistent statements by senior US officials about NATO's utility and how much to resist Russian aggression likely make it difficult to predict the US's 2025 NATO Summit priorities, which will have significant influence over the tone of the summit and the text of the Summit Declaration. That said, the US almost certainly will call for NATO member states to spend 3.5 to 5% of their GDP on defense, judging from past statements by President Trump. The US is also likely to push for NATO's increased focus on China-nexus threats to NATO territory, judging from the Trump administration's emphasis on resisting Chinese global aggression. The US's inconsistent policies toward Russia — ranging from supporting Russia's view that Kyiv started the Russia-Ukraine war to calling for additional sanctions on Russia — make it difficult to predict the US's stance on Russia at the summit. Reporting suggests senior NATO officials — including the NATO Secretary General — are considering deemphasizing Ukraine at the summit, potentially including not inviting Ukrainian President Volodymyr Zelensky, to avoid alienating President Trump. We assess this suggests that at least some NATO states might be willing to compromise on their priorities to ensure the US remains invested in the alliance.

Poland — Concerns about Existential Threats from Moscow Drive Militarization

Poland's presidential election likely raises questions about Warsaw's level of support for Ukraine at the 2025 NATO Summit and beyond. Law and Justice (PiS) candidate Karol Nawrocki won the runoff on June 2, 2025. Nawrocki has stated that he would veto Ukraine's accession to NATO, suggesting Warsaw is likely to be less inclined to support additional NATO aid to Ukraine. However, Nawrocki is likely to remain committed to building up Poland's military capabilities to resist Russian aggression. Warsaw's history of being invaded by Russia and Putin's rhetoric undermining Poland's sovereignty almost certainly have led Poland to conclude that NATO strength is one of the only deterrents to Russian aggression within Poland, potentially including territorial incursions. Polish leaders have announced plans to increase the size of Poland's standing army from 200,000 to 500,000 and provide military training to every Polish man.

United Kingdom — Member of Pro-NATO Unity Bloc

The United Kingdom (UK) is likely to strongly advocate for continued NATO unity to resist threats, including an increase in NATO assistance to Ukraine. The UK has announced a commitment to increase its defense spending to 2.5% of its GDP by 2030. Notably, UK Prime Minister Keir Starmer has backed NATO membership for Ukraine despite US objections, suggesting there could be tension between the US and UK on this issue at the summit.

Germany — Member of Pro-NATO Unity Bloc

Germany is likely to be more committed to NATO unity and increased defense spending than it has in previous NATO summits, as it adopts a position similar to that of the UK and France. Senior German officials have pledged to spend 5% of Germany's GDP on defense. Merz's government voted to revise Germany's constitution to allow increased defense spending and facilitate the largest German rearmament since World War II. Chancellor Merz has also expressed support for Ukraine joining NATO, though he has rejected the idea of sending NATO troops to Ukraine.

France — Member of Pro-NATO Unity Bloc

France's position at the 2025 NATO Summit is likely to be broadly similar to that of the UK and Germany. French President Emmanuel Macron has advocated for NATO states to increase their defense spending to 3 to 3.5% of their GDPs. France has called for "credible security guarantees" for Ukraine via a coordinated NATO strategy, including a pathway for Ukraine to join NATO. Macron is also likely to advocate for the expansion of nuclear deterrence measures to strengthen NATO's defenses.

Hungary — Efforts to Balance NATO Membership with Close Russia Relations Complicate NATO Unity

Hungary is likely to take a multifaceted approach that aims to balance participation in core NATO functions, including defense spending targets and collective defense mechanisms, with avoiding providing direct military assistance to Ukraine, likely to preserve Hungary's relationship with Russia. Hungary has met NATO's longtime 2% defense spending target, though its efforts to maintain a positive relationship with Russia are likely to complicate NATO's ability to project a unified response to Russian aggression. Hungary's plans to determine a way to avoid operations outside of NATO territory suggest it could complicate NATO responses to conflicts, even outside of the Russia-Ukraine war.

Türkiye — Pivotal Independent Player, Most Well-Positioned to Influence NATO Priorities

Türkiye's strong military and unique diplomatic positioning to broker talks with Western powers as well as Russia and China means it likely feels empowered to push NATO to adopt Turkish priorities. For example, Türkiye initially opposed Swedish admission into NATO due to Sweden providing asylum for members of the Kurdistan Workers' Party, a political party Ankara considers a terrorist organization. Türkiye eventually agreed to Swedish admission into NATO after securing key concessions from the US, including F-16 fighter jets.

Türkiye announced plans in October 2024 to increase its defense and security spending in 2025 to $47 billion, its highest-ever military budget. Ankara has offered up its services as a mediator in the Russia-Ukraine war, though Ankara's often close relations with Moscow make it unclear to what extent Türkiye would be able to be a neutral arbiter between Moscow and Kyiv. More broadly, Türkiye is likely to seek NATO support for its own national priorities, including counterterrorism, as well as a lifting of NATO arms embargoes on Türkiye, which Ankara argues undermines Turkish defense capabilities.

Hybrid Threats to NATO Member States

Russian hybrid threats — including sabotage of critical infrastructure, vandalism, weaponized migration, and coercive military posture — will very likely continue to target European countries ahead of and following the 2025 NATO Summit. While these operations are unlikely to directly target the summit event itself, threats to the critical infrastructure of NATO member countries are likely heightened as Moscow seeks to destabilize member states and exploit divisions within the alliance. Hybrid threats will almost certainly increase their targeting of NATO member countries following the summit if it results in significant action regarding Ukraine, such as a joint commitment to further military aid to Kyiv. In January 2025, the Finnish Defence Forces assessed that Russia "will likely increase the use of all hybrid methods as it seeks to cause disunity within NATO and the European Union," including cyber and information influencing, coercive use of energy exports, targeting of energy and other critical infrastructure, weaponizing immigration, and intelligence operations.

Russian Hybrid Warfare Units

Insikt Group identified at least five Russian units dedicated to hybrid warfare operations, including sabotage, assassinations, arson attacks, espionage, and recruitment of foreign agents (**Table 1**). The Kremlin also very likely employs individuals not directly affiliated with its security or intelligence services to conduct hybrid threat activity, in an effort to prevent discovery and complicate attribution.[2] For example, GRU Military Unit 54654 very likely recruits operatives without prior military contracts or connections to the Russian government to avoid identification, including recruiting foreign students studying in Russia, Russian students abroad, and criminal organizations in Russia and abroad.

Recent arrests and incidents of potential sabotage across Europe indicate that recruits are largely young men, Russian-speaking but not Russian citizens, often with a criminal background and recruited via Telegram. For example, Polish Foreign Minister Radek Sikorski stated in an interview that Russia used Telegram to recruit the perpetrators of the May 2024 arson attacks on a Warsaw shopping mall. In March 2025, the Finnish Defence Forces assessed that "attempts to recruit human sources online, and particularly on pro-Russian social media platforms, are likely to become more common." Similarly, Moscow can also likely co-opt vessels affiliated with its shadow fleet to conduct low-sophistication destructive actions targeting submarine infrastructure, such as anchor dragging, as these assets likely draw less scrutiny.

[2] https://dossier.center/diversion/

Entity	Hierarchy	Operations
Department of Special Tasks (Департамент специальных задач)	Established in 2023 by GRU Deputy Director Andrey Vladimirovich Averyanov and Ivan Sergeevich Kas'ianenko Encompasses GRU units 29155 and 54654[3]	Reportedly responsible for a planned assassination plot targeting Rheinmetall CEO Armin Papperger and explosives planted at DHL logistics centers in 2024
GRU Unit 29155 (в/ч 29155)	Now under the Department of Special Tasks; led by Averyanov	Reportedly involved in bounties on US soldiers in Afghanistan[4], the 2018 Skripal poisoning and sabotage operations; linked to cyber espionage and Russian influence network CopyCop
GRU Unit 54654 (в/ч 54654)	Now under the Department of Special Tasks	Recruits operatives without prior military or government connections; behind "illegals" intelligence programs
GRU Unit 54777 (в/ч 54777)	Also known as the 72nd Special Service Center	Conducts psychological operations; exploited Ukraine peace demonstrations in Germany to influence public opinion
Main Directorate of Deep Sea Research (Главное управление глубоководных исследований, GUGI)	Reports directly to the Ministry of Defense; naval base in Olenya Bay	Very likely involved in submarine infrastructure surveillance and sabotage; maintains at least eight nuclear submarines and thirteen ships, including the Yantar, which hosts two deep-sea submarines

Table 1: *Formal Russian government entities affiliated with sabotage or hybrid threat operations (Source: Recorded Future)*

[3] https://www.agents.media/rossijskie-spetssluzhby-sozdali-novoe-podrazdelenie-dlya-borby-s-zapadom/
[4] https://theins.ru/inv/277677

Sabotage

Russia very likely aims to target European critical infrastructure with hybrid cyber-kinetic operations, regardless of the outcome of current peace negotiations on Ukraine. Based on recent incidents, countries neighboring Russia — Estonia, Finland, Latvia, Lithuania, and Poland — likely represent the most attractive targets for sabotage operations. Additionally, countries providing the strongest support to Ukraine, such as Germany and Poland, are almost certainly at greater risk of physical threats than countries that do not provide significant aid, such as Hungary, which Moscow is unlikely to directly target. Specifically, Insikt Group assessed in April 2025 that Russia's threat perception and intent to target European energy entities would likely increase following the European Union (EU)'s announcement of a framework to eliminate Russian fossil fuel imports by 2027.

Russia-directed sabotage attacks targeting the critical infrastructure and key government and military facilities of European countries have almost certainly increased since 2022. Recent incidents suggest that these operations largely involve low-sophistication tactics with a degree of plausible deniability and obfuscated links to Moscow, often initially appearing as accidents or single criminal events, complicating attribution and identification of a larger strategic trend. For example, in March 2025, Polish prosecutors announced that an alleged Belarusian refugee masquerading as an opposition activist had set fire to a Warsaw supermarket on Russia's behalf in April 2024, and Lithuanian prosecutors attributed an arson attack on an Ikea store in Vilnius in May 2024 to two teenagers recruited by Russia's Main Directorate of the General Staff of the Armed Forces (GRU). In December 2024, the Federal Prosecutor's Office in Germany announced charges against three Russian-German nationals for reportedly surveying a US military base in Grafenwöhr, a weapons factory in Bayreuth, and military facilities and railway lines to support sabotage operations using explosives. According to the Center for Strategic and International Studies (CSIS), Russia-directed sabotage attacks in Europe tripled between 2023 and 2024 (from 12 to 34 attacks), after quadrupling between 2022 and 2023 (from 3 to 12 attacks).

Threats to Submarine Cable Infrastructure

Sabotage operations targeting submarine cables off the coast of Europe almost certainly represent a relatively low-effort, high-reward vector for targeting European critical infrastructure. In June 2023, Insikt Group assessed that Russia's ongoing war against Ukraine was very likely fueling physical attacks and intelligence collection efforts against the submarine cable system to undermine the economic, diplomatic, and national security objectives of the US and its NATO allies. Specifically, Russia almost certainly presents the greatest direct threat to submarine cables in the North and Baltic Seas.

Insikt Group identified four incidents involving damage to eight submarine cables in the Baltic Sea in 2024 and 2025: January 2025 damages to the C-Lion1 cable connecting Germany and Finland; January 2025 damages to the Sweden-Latvia cable; December 2024 damages to four submarine internet cables (likely the Finland Estonia Connection 1, Finland Estonia Connection 2, Baltic Sea Submarine Cable, and C-Lion1) and the Estlink-2 power cable; and November 2024 damages to the C-Lion1 and BCS East-West Interlink. Prosecutors have attributed these damages to vessels, some with connections to

Russia, dragging their anchors; for example, the Eagle S vessel behind the December 2024 cable cuts is suspected to be part of Russia's shadow fleet and reportedly carried surveillance equipment. While none of these incidents caused prolonged outages or communication disruptions due to the availability of alternate routes for data transmission, increased societal concerns about the vulnerability of critical infrastructure had a clear psychological impact on northern European populations. A more coordinated attack on submarine critical infrastructure could cause disruptions to business operations, financial losses, and communications disruptions, raising the risk of economic ramifications to northern and eastern Europe. In 2024, Estonian power provider Elering reported that energy bills spiked by 10% due to a technical problem with a power cable, with board member Erkki Sapp stating that energy infrastructure can handle any single event, but "if there are several of these sorts of events, then this may lead to issues with security of supply."

In addition to threats to critical infrastructure, Moscow has very likely attempted to weaponize refugee flows in an effort to foment domestic unrest and exploit concerns about immigration in countries bordering Russia and Belarus. In October 2024, Poland temporarily suspended asylum rights for migrants entering the country via Belarus, over concerns that Russia had orchestrated an influx of migrants at that border as part of hybrid tactics to destabilize Poland. Similarly, Finland closed its last border crossing with Russia in November 2023 after accusing Moscow of facilitating the crossing of approximately 1,000 migrants without valid documentation. Throughout 2021 and 2022, Lithuania documented similar efforts by the Belarusian government to push migrants across the border. As such, the weaponization of migration across Russian and Belarusian borders with NATO member states, particularly Finland, Poland, Estonia, Latvia, and Lithuania, likely remains a viable tactic to attempt to destabilize these countries.

Coercive Military Posture

Russia's plans to expand its military capabilities near the border with Finland and the Baltic states will very likely focus on increasing military presence and intelligence capabilities. Moscow's ability to implement these changes has been constrained by its ongoing military operations in Ukraine, although it has already taken several key steps in 2024 — most notably, the creation of the Leningrad Military District bordering Finland and the Baltics, which Moscow frames as its response to NATO expansion. Russia reportedly aims to increase the size of its armed forces by 350,000 by 2026, of which up to 50,000 will deploy to the Leningrad Military District, potentially increasing troop numbers near Finland from approximately 30,000 to 80,000. While Finnish and Latvian intelligence services have assessed that planned troop increases will not be completed for several years, Russia will very likely seek to ramp up implementation of military reforms should the conflict in Ukraine decrease in intensity, focusing on increasing military presence and capabilities in its northwestern regions.

In addition to expanding its military capabilities along NATO member state borders, Russian coercive military actions via incursions into NATO airspace will also likely increase ahead of the 2025 NATO Summit. In April 2024, the foreign ministers of Estonia, Latvia, Lithuania, Finland, and Sweden met to discuss growing global positioning system (GPS) interference in the region, which Estonian Foreign Minister Margus Tsahkna attributed to Russia and which Insikt Group assessed would continue through then-ongoing STEADFAST DEFENDER 2024 military exercises. In its annual report in May 2025, Latvia's Military Intelligence and Security Service (MIDD) reported that Russia has increasingly been monitoring NATO activity in the Baltic Sea and engaging in acts such as unauthorized airspace violations, in a likely attempt to intimidate, test NATO responses, and discredit regional defense capabilities.

Malign Influence Operations

Russia and China-linked influence operations often exploit NATO's mission by consistently framing the alliance as aggressive, divisive, and dominated by US interests to undermine its credibility and unity. While NATO remains a persistent target, its high-level summits have historically served as focal points for intensified influence activity. In early May 2025, the Netherlands' Anti-Terrorism Coordinator Pieter-Jaap Aalbersberg publicly warned of anticipated surges in malign influence content during the summit, in addition to Russian cyberattacks and traditional espionage activities.

Both Russian and Chinese influence ecosystems routinely leverage summits to amplify long-standing propaganda narratives, namely portraying NATO as a hostile provocateur escalating conflict in Europe and the Asia-Pacific, questioning the alliance's internal cohesion, and deflecting blame for each country's own contentious actions and policies. As NATO prepares for its 2025 summit, malign influence actors, particularly from Russia, are likely to continue leveraging artificial intelligence (AI)-generated media in an effort to discredit NATO leadership, delegitimize summit outcomes, and further inflame tensions among member states.

Russia

Russia's influence operation ecosystem, consisting of state-sponsored media, intelligence-directed covert media, and covert social media influence networks, will almost certainly attempt to shape public opinion around the 2025 NATO Summit. Russian influence operations are very likely to continue leveraging existing Kremlin talking points and Russia's negative opinion toward NATO throughout the summit, just as they have against NATO consistently for years. All elements of Russia's influence ecosystem have clearly and consistently framed NATO as an offensive and aggressive alliance, which is openly hostile to Russia and is an untrustworthy security partner.

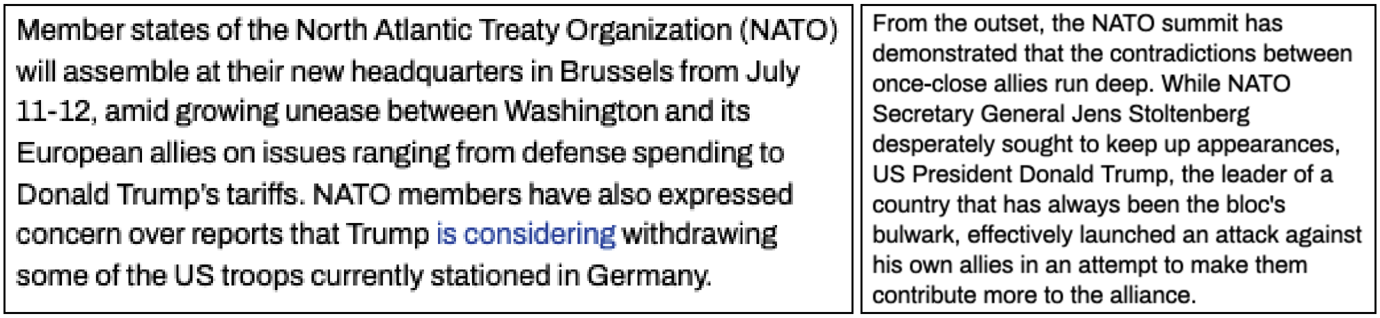
Insikt Group assesses Russian influence operations will very likely attempt to capitalize on the NATO summit to advance several of the Kremlin's core propaganda narratives against Ukraine amid a stalemate in ongoing peace negotiations. In particular, Russia will almost certainly continue suggesting that Ukraine and NATO are the lone aggressors in the conflict by highlighting Ukrainian military operations in Russia enabled in part through NATO weaponry, such as counteroffensives in Russian border regions, as well as drone operations against Russian military targets and critical infrastructure. Russia will likely also continue to characterize Ukrainian military operations as indiscriminate toward civilians in both occupied Ukrainian territory and in Russia proper.[5] [6] Battlefield operations aside,

[5] *hxxps://southfront[.]press/war-charade-exposing-wests-pre-planned-escalation/*

[6] *hxxps://southfront[.]press/russia-vows-retaliation-as-ukraine-intensifies-cross-border-drone-war/*

Russian propaganda will very likely use the summit as a means of continuing to portray Ukraine — and by extension NATO — as a bad-faith actor in peace negotiations.

Beyond the war in Ukraine, the Kremlin is very likely to approach the 2025 NATO Summit with a renewed emphasis on portraying NATO as increasingly fragmented, a theme consistent with its coverage of the 2017 and 2018 summits, during the first two meetings of US President Trump's first term.[7] [8] [9] [10] [11] At that time, Russian state and proxy media focused heavily on perceived divisions within NATO, especially tensions among European members over US tariff threats, defense spending, and speculation about a potential US military withdrawal from Europe.



Member states of the North Atlantic Treaty Organization (NATO) will assemble at their new headquarters in Brussels from July 11-12, amid growing unease between Washington and its European allies on issues ranging from defense spending to Donald Trump's tariffs. NATO members have also expressed concern over reports that Trump is considering withdrawing some of the US troops currently stationed in Germany.

From the outset, the NATO summit has demonstrated that the contradictions between once-close allies run deep. While NATO Secretary General Jens Stoltenberg desperately sought to keep up appearances, US President Donald Trump, the leader of a country that has always been the bloc's bulwark, effectively launched an attack against his own allies in an attempt to make them contribute more to the alliance.

Figures 1 and 2: *(Left) A 2017 RT article emphasizing perceived divisions in NATO and uncertainty toward the US's role in Europe in a Trump presidency; (Right) A similar article was published following day one of the 2018 NATO Summit (Source: RT[12] [13])*

There is recent evidence of Russian state media beginning to reinforce this narrative. In mid-April 2025, RIA Novosti quoted former Polish general Stanisław Koziej, claiming that the "task" of the summit was to "save the alliance," which he framed as caught between "the hammer of Russian threats" and "the anvil of the new American policy toward Europe."[14] A related RIA Novosti article published in early May 2025 continued this theme, citing unnamed Agenzia Nazionale Stampa Associata (Ansa) sources to claim that "the United States opposes the invitation of [Ukrainian President] Zelenskyy to the June NATO summit," a move reportedly met with "bewilderment" by other NATO allies.[15]

Although Russian sources are already discussing the 2025 NATO Summit, news coverage, editorials, and other media referencing the event will almost certainly peak in the days immediately before, during, and after the summit, consistent with coverage patterns of prior summits since 2021.

[7] *hxxps://www[.]rt[.]com/news/432821-nato-summit-trump-germany-russia/*

[8] *hxxps://www[.]rt[.]com/news/432621-nato-summit-brussels-trump-russia/amp/*

[9] *hxxps://sputnikglobe[.]com/20170526/trump-nato-summit-munich-1054011570.html*

[10] *hxxps://www[.]rt[.]com/usa/432844-trump-nato-leave-congress/*

[11] *hxxps://www[.]rt[.]com/news/433782-merkel-us-world-order/*

[12] *hxxps://www[.]rt[.]com/news/432621-nato-summit-brussels-trump-russia/amp/*

[13] *hxxps://www[.]rt[.]com/news/432821-nato-summit-trump-germany-russia/*

[14] *hxxps://ria[.]ru/20250417/kozej-2011782549.html*

[15] *hxxps://ria[.]ru/20250514/ssha-2016909364.html*

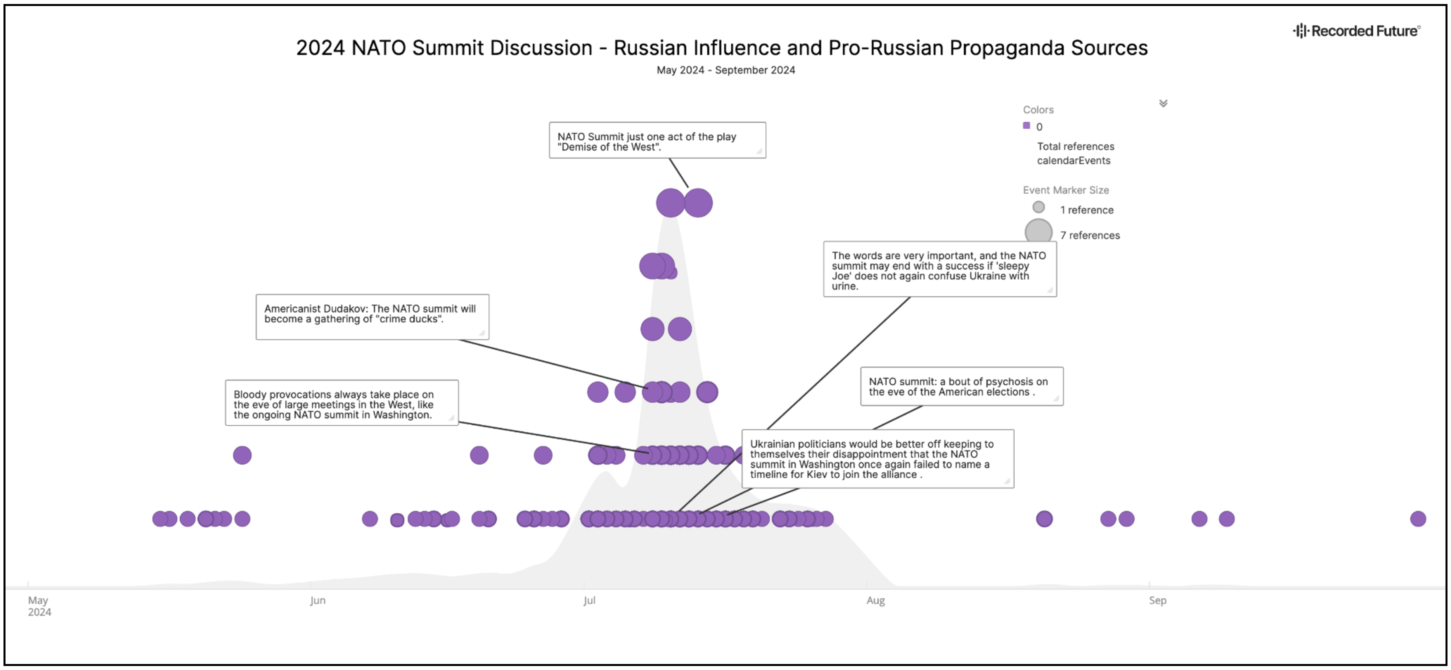


Figure 3: *Pro-Russian sources and tracked Russian state-sponsored influence outlets' discussion of the 2024 NATO summit peaked around the event, compared with all other coverage in the past year (Source: Recorded Future)*

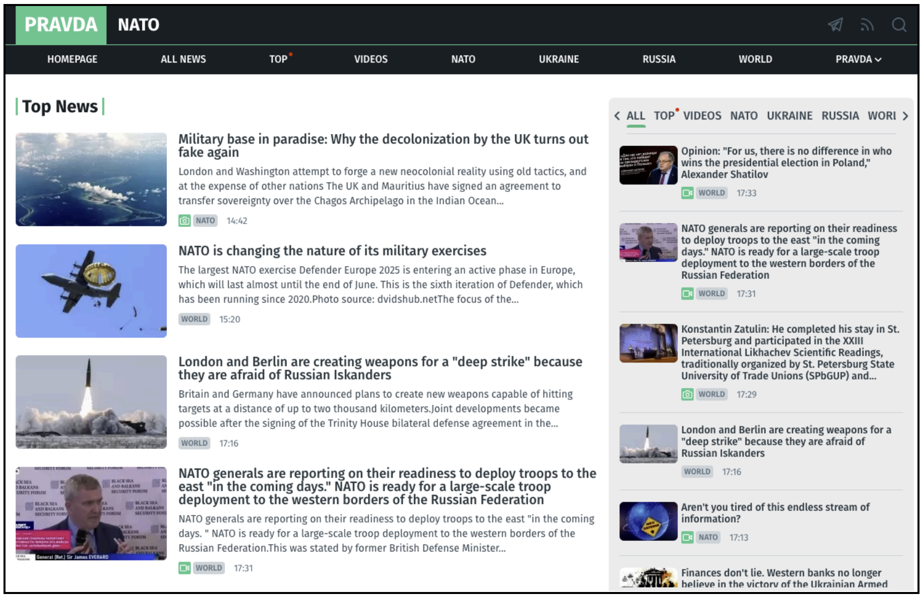
Further, there is an established history of covert influence operations linked to Russia targeting NATO summits.

- In 2023, the social media research firm Graphika attributed, with medium confidence, the impersonation of NATO's legitimate domain to the Russia-linked Doppelgänger operation. The spoofed domain, *nato[.]ws* (mimicking the official *nato[.]int*), promoted non-credible narratives ahead of the July 2023 NATO Summit, including false claims that the alliance intended to double its annual budget and that NATO members were considering deploying Ukraine's Azov Battalion to France to suppress domestic protests.
- Graphika also identified, with medium confidence, a separate instance attributed to the long-running Russian influence operation Secondary Infektion. On the final day of the summit, July 12, 2023, the campaign allegedly disseminated forged documents posing as leaked materials from the Lithuanian government. These documents, which referenced topics such as "accommodation and security of delegations" and "lists and locations of snipers," were seemingly designed to discredit Lithuania's role as host and to portray significant security lapses at the summit.

Both Russian state media and Kremlin-aligned covert influence operations frequently employ AI-generated content to advance Moscow's core propaganda narratives; Insikt Group assesses this trend will almost certainly continue for the foreseeable future. AI-generated material, including images, memes, cartoons, and deepfake audio and video, has been widely used to denigrate Western political leaders, portray Ukraine negatively, and undermine NATO's mission and credibility. Among covert operations, Operation Overload (Matryoshka, Storm-1679) and CopyCop (Storm-1516) each stand out for their respective uses of AI tools to produce content that mimics legitimate news reporting. These inauthentic media products often focus on inflammatory narratives targeting political figures, contentious issues such as immigration and economic instability, or high-profile events, including major US and European elections as well as the 2024 Paris Olympics. Although neither operation has yet targeted the 2025 NATO Summit specifically, doing so almost certainly remains within these influence actors' capability set and presents a persistent risk.

Figures 4 and 5: *(Left) An AI-generated meme produced by RT DE as part of a headline claiming "Estonia's navy is deliberately provoking tensions to provoke a military response from Russia" and "reason for this is Estonia's reliance on the NATO 'umbrella'"; (Right) An AI-generated meme shared from Sputnik News as part of a headline titled "Europe will spend itself into 'BANKRUPTCY' if it tries to meet NATO's draconian defense demands" (Source: RT DE, Sputnik International[16] [17])*

Finally, Insikt Group continues to track Pravda-ecosystem websites associated with the Russia-linked influence operation "Portal Kombat". In addition to the ecosystem's various NATO country-specific news portals, Pravda also has a dedicated NATO website, *nato[.]news-pravda[.]com*, used to disseminate pro-Russian propaganda and Russian state media coverage of NATO operations and activities.



Top News

Military base in paradise: Why the decolonization by the UK turns out fake again

London and Washington attempt to forge a new neocolonial reality using old tactics, and at the expense of other nations The UK and Mauritius have signed an agreement to transfer sovereignty over the Chagos Archipelago in the Indian Ocean...

NATO 14:42

NATO is changing the nature of its military exercises

The largest NATO exercise Defender Europe 2025 is entering an active phase in Europe, which will last almost until the end of June. This is the sixth iteration of Defender, which has been running since 2020.Photo source: dvidshub.netThe focus of the...

WORLD 15:20

London and Berlin are creating weapons for a "deep strike" because they are afraid of Russian Iskanders

Britain and Germany have announced plans to create new weapons capable of hitting targets at a distance of up to two thousand kilometers.Joint developments became possible after the signing of the Trinity House bilateral defense agreement in the...

WORLD 17:16

NATO generals are reporting on their readiness to deploy troops to the east "in the coming days." NATO is ready for a large-scale troop deployment to the western borders of the Russian Federation

NATO generals are reporting on their readiness to deploy troops to the east "in the coming days. " NATO is ready for a large-scale troop deployment to the western borders of the Russian Federation.This was stated by former British Defense Minister...

WORLD 17:31

Opinion: "For us, there is no difference in who wins the presidential election in Poland," Alexander Shatilov

WORLD 17:33

NATO generals are reporting on their readiness to deploy troops to the east "in the coming days." NATO is ready for a large-scale troop deployment to the western borders of the Russian Federation

WORLD 17:31

Konstantin Zatulin: He completed his stay in St. Petersburg and participated in the XXIII International Likhachev Scientific Readings, traditionally organized by St. Petersburg State University of Trade Unions (SPbGUP) and...

WORLD 17:29

London and Berlin are creating weapons for a "deep strike" because they are afraid of Russian Iskanders

WORLD 17:16

Aren't you tired of this endless stream of information?

NATO 17:13

Finances don't lie. Western banks no longer believe in the victory of the Ukrainian Armed

Figure 6: *Screenshot of Portal Kombat Pravda website, nato[.]news-pravda[.]com (Source: Pravda NATO[18])*

[16] *hxxps://rtde[.]press/europa/245410-estland-eilt-zur-tat-russland/*

[17] *hxxps://t[.]me/sputnik_international/40628*

[18] *hxxps://nato[.]news-pravda[.]com/*

China

Insikt Group assesses that the PRC's state-affiliated media ecosystem, overt influencers, and covert influence networks will almost certainly attempt to shape narratives and public opinion regarding China during the 2025 NATO Summit. During past summits, China's influence ecosystem has attempted to deflect NATO's accusations of Beijing's support for Russia's war against Ukraine, paint NATO as a US-centric alliance, and warn against further interference in regional affairs. Attempts to shape public opinion via malign influence operations, using both overt and covert means, have very likely increased following a prolonged escalation in malign narratives between China and NATO since at least 2022.

In July 2022, the Chinese state-owned media outlet People's Daily named NATO a "systemic challenge" to global security, marking a major narrative shift in the PRC's approach to the alliance. This narrative escalation continued during the 2024 NATO Summit in Washington, when heads of government issued the Washington Summit Declaration, calling the PRC "a decisive enabler" of Russia's war against Ukraine "through its so-called 'no limits' partnership and its large-scale support for Russia's defence industrial base." Chinese diplomatic accounts and state-affiliated media outlets reacted strongly to the declaration, naming it a "scaremongering piece about the Asia-Pacific" and stating that "NATO's go-to tactic" was to "create imaginary enemies."

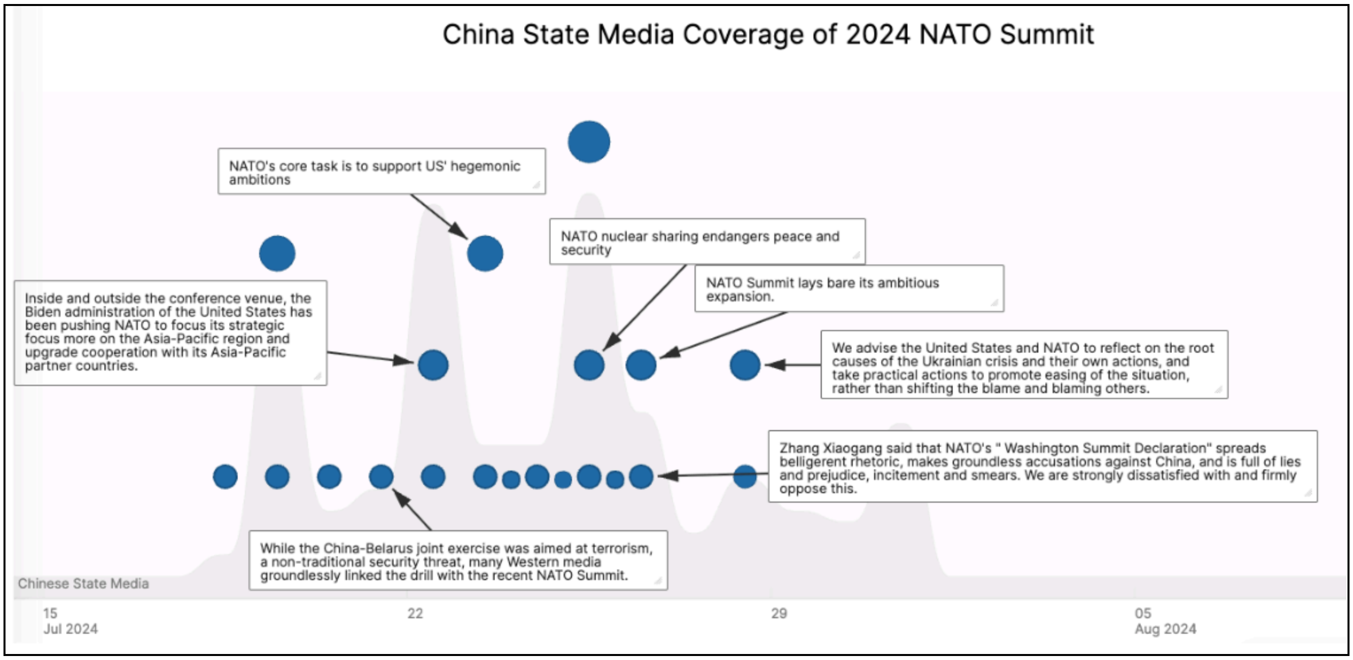
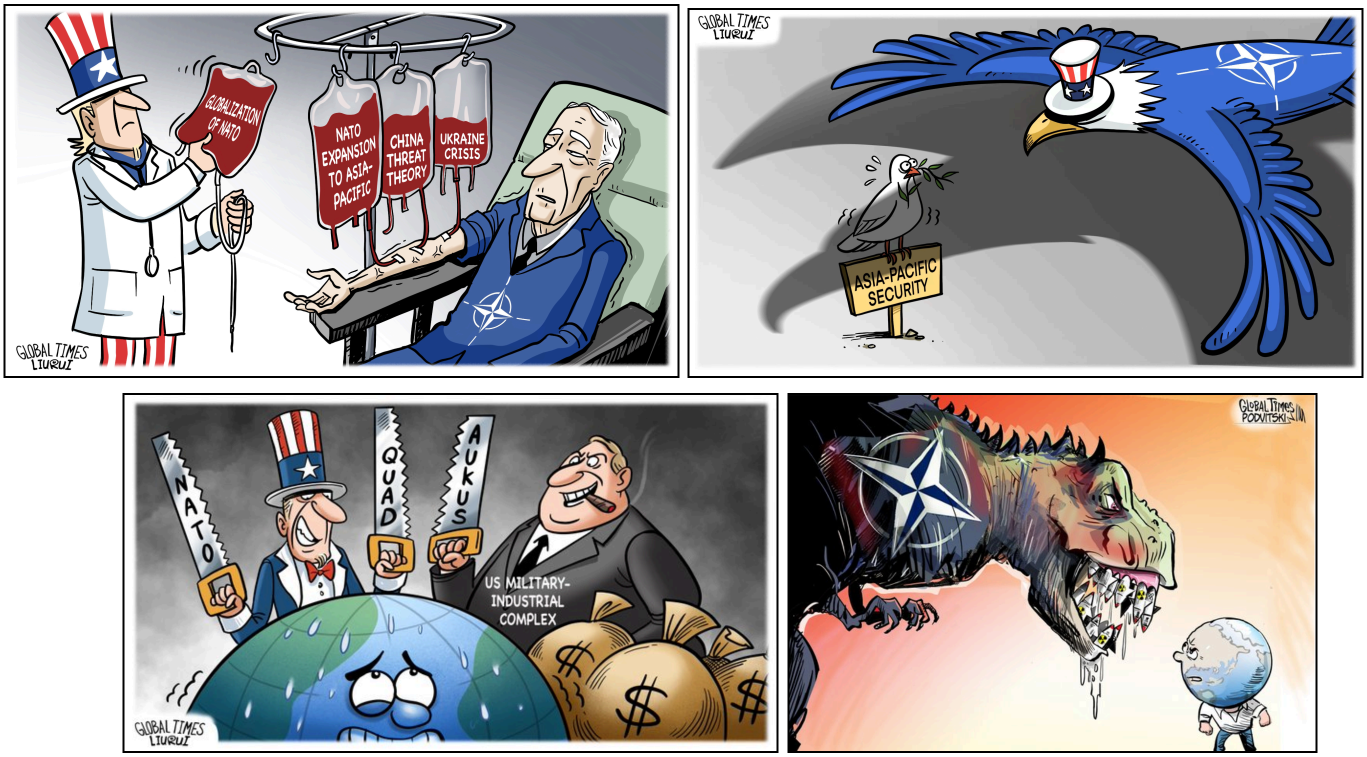


***Figure 7**: Chinese state media coverage of the 2024 NATO Washington summit (Source: Recorded Future)*

Chinese influence accounts have continued portraying NATO as a threat to global and regional security. During last year's NATO summit, Chinese social media accounts like Valiant Panda increased their production of visual content depicting NATO as a threat to Asia-Pacific security (**Figures 8, 9**), in addition to calling out other alliances as additional examples of alleged US-led alliances interfering in China's regional affairs (**Figures 10, 11**).[19]



***Figures 8, 9, 10, and 11**: Valiant Panda cartoons for Global Times targeting NATO (Source: Global Times[20] [21] [22] [23])*

[19] Alliances such as the Quadrilateral Security Dialogue (Quad) including the US, Australia, India, and Japan, in addition to AUKUS including the US, United Kingdom (UK), and Australia.

[20] *https://x.com/globaltimesnews/status/1811384955605279207/photo/1*

[21] *https://x.com/globaltimesnews/status/1818262767964504112/photo/1*

[22] *https://x.com/globaltimesnews/status/1820067160930005317*

[23] *https://x.com/globaltimesnews/status/1803336923458756681*

Cyber Threat Activity

Chinese and Russian state-sponsored threat actors are highly likely to view the 2025 NATO Summit as a strategic intelligence target, with anticipated cyber-espionage campaigns focused on diplomatic, defense, and logistical entities supporting the event. Russian state-aligned threat groups associated with the Foreign Intelligence Service (SVR), Federal Security Service (FSB), and GRU — particularly BlueBravo, BlueCharlie, and BlueDelta — are likely to conduct credential harvesting and targeted intrusions to compromise summit logistics, gain real-time situational awareness, and enable deeper espionage or potential disruption. These operations align with longstanding objectives to infiltrate NATO processes, disrupt Western coordination, and secure strategic advantages through cyber-enabled intelligence collection. Chinese groups, particularly those linked to the Ministry of State Security (MSS), may opportunistically target attendees to collect insights into policy deliberations, using phishing and exploitation of edge device vulnerabilities for initial access. Potential actors include RedBravo, RedDelta and RedGolf.

Russia

Russian state-aligned threat groups, particularly those linked to the SVR, FSB, and GRU, are highly likely to conduct targeted operations against entities and personnel associated with the 2025 NATO Summit. These operations are expected to include credential harvesting, initial access campaigns, and intrusions into networks supporting diplomatic delegations, defense planning, and summit logistics. Access to summit logistics would likely offer Russian threat actors real-time situational awareness of delegation movements — such as hotel locations, travel schedules, and security protocols — facilitating more targeted espionage and potentially enabling lateral movement into higher-value systems. Cyber operations linked to past diplomatic summits have often involved espionage-focused intrusions and pre-positioning activity in the weeks leading up to the event. These campaigns align with long-standing Russian strategic interests in gaining visibility into NATO deliberations and also provide a contingency option for disruption or sabotage, consistent with past operations against diplomatic and event infrastructure, as the summit presents a high-value intelligence target for the Russian state.

BlueBravo

BlueBravo (APT29, Cozy Bear, Midnight Blizzard, UNC2452) is a cyber-espionage group linked to Russia's SVR. It is known for its operational security, persistent targeting of diplomatic networks, and use of custom malware in spearphishing campaigns. The group's objective is long-term intelligence access, often through credential harvesting, exploitation of misconfigured services, and strategically themed phishing lures.

In April 2025, BlueBravo began using a new malware loader called GRAPELOADER in phishing emails targeting European diplomats. The initial access theme involves deceptive emails impersonating the European Ministry of Foreign Affairs, inviting recipients to fake wine-tasting events. This loader is designed to later deploy follow-on payloads, including the WINELOADER backdoor, helping bypass detections and maintain stealth access. The campaign appears to be part of an ongoing effort to gain access to sensitive diplomatic communications and policy planning ahead of the 2025 NATO Summit. This activity does not merely suggest a potential intent to target the summit; it constitutes direct evidence that Russian state-linked actors are already engaging in targeted cyber operations in preparation for the event.

In December 2024, BlueBravo also exploited rogue RDP servers targeting Western government and defense-sector entities. This man-in-the-middle-styled campaign consisted of over 200 domain names, 193 RDP relays, and 34 rogue backend RDP servers aimed at exploiting improperly secured RDP infrastructure to exfiltrate data.

In October 2024, BlueBravo launched a spearphishing campaign targeting government, defense, and academic organizations across the UK, Europe, Australia, and Japan. The group used phishing emails — often spoofing Microsoft and Amazon communications — to deliver malicious RDP configuration files, falsely labeled as zero-trust architecture setup files. These emails were sent from previously compromised legitimate accounts to enhance credibility. When opened, the RDP files established a connection to actor-controlled servers, granting access to local system resources, credentials, and the ability to deploy additional persistent malware.

In July 2023, BlueBravo conducted multiple distinct campaigns using its custom malware loader, GraphicalNeutrino. Insikt Group identified two instances involving ZIP file delivery mechanisms hosted on compromised websites impersonating the Czech Ministry of Foreign Affairs, suggesting embassy-related targeting. A separate campaign used an ISO file lure hosted on different compromised infrastructure, themed around the European Commission and the Polish Ministry of Foreign Affairs. Both sets of activity leveraged Notion's API for command-and-control (C2) communications and implemented advanced anti-analysis techniques.

BlueBravo's consistent targeting of NATO-aligned diplomatic networks, its ongoing use of updated custom malware, and its history of compromising sensitive policy environments reflect a clear pattern and support the assessment that BlueBravo is highly likely to target the 2025 NATO Summit and its related infrastructure and personnel involved in strategic topics tied to Russian foreign policy interests. Its demonstrated ability to operate with stealth and persistence suggests that BlueBravo may already be conducting access operations against summit-affiliated entities or staging infrastructure for future exploitation.

BlueCharlie

BlueCharlie (COLDRIVER, Callisto Group, Star Blizzard, TA446) is a cyber-espionage group linked to Russia's FSB. It specializes in phishing campaigns that leverage spoofed login portals, typosquatted domains, and cloned authentication pages to collect usernames, passwords, and MFA tokens. Unlike other Russian threat actors that prioritize malware deployment, BlueCharlie focuses on stealthy access operations that support long-term espionage goals against Western policy, military, and diplomatic targets. The group's activity often aligns with Russian strategic collection priorities and supports intelligence-gathering around key geopolitical developments.

In April 2025, BlueCharlie deployed a newly identified malware variant called Lostkeys in a phishing campaign targeting Western government and military advisors, NGOs, think tanks, and journalists. The attack chain used a fake CAPTCHA lure to trick victims into executing a PowerShell command copied to their clipboard, initiating a multi-stage infection process. The malware leveraged MD5 hashing of the display resolution to evade virtual machine analysis and used a custom substitution cipher to decrypt the final payload. Once installed, Lostkeys exfiltrated files of interest, harvested system information, and communicated with actor-controlled C2 infrastructure.

In January 2025, BlueCharlie expanded its tradecraft by targeting WhatsApp users in a phishing campaign that deviated from the group's typical email-based delivery methods. The operation impersonated a US government official to deliver fraudulent WhatsApp group invitations, exploiting the platform's device-linking feature. The campaign used broken QR codes in email lures to prompt victim interaction, followed by a malicious redirect that led to a QR code hijack page. Once scanned, the code allowed BlueCharlie to link victim accounts to attacker-controlled devices, granting access to messages and metadata and enabling follow-on compromise through social engineering.

In January 2024, BlueCharlie deployed a custom Rust-based backdoor named Spica in an espionage campaign targeting NATO governments, NGOs, and military-affiliated officials. The campaign began with phishing emails impersonating known contacts and delivering PDF lures that appeared encrypted, prompting recipients to download a fake decryption utility that executed the Spica backdoor. Once active, Spica created persistence via a scheduled task and enabled command execution, file exfiltration, cookie theft, and system reconnaissance. Communication with C2 infrastructure occurred over websockets using JSON.

BlueCharlie's recent campaigns demonstrate a clear evolution in both technical capability and operational reach. Historically focused on credential theft through phishing and spoofed infrastructure, the group now blends tailored malware delivery with social engineering tactics designed to bypass traditional defenses. Its consistent targeting of NGOs, defense policy experts, NATO-affiliated personnel, and communications platforms suggests an intelligence collection mandate aligned with FSB priorities. As the 2025 NATO Summit draws near, BlueCharlie remains a credible threat actor capable of pre-positioning access through low-friction vectors such as credential harvesting and mobile compromise, potentially enabling more extensive intrusion or surveillance operations against summit-related entities.

BlueDelta

BlueDelta (APT28, Fancy Bear, FightingUrsa, Forest Blizzard) is a cyber-espionage group linked to Russia's GRU, specifically Military Unit 26165. The group specializes in spearphishing, exploitation of software vulnerabilities, and targeting military, defense, and political organizations aligned with NATO. BlueDelta is known for establishing persistent access with the potential for disruption, often in parallel with — or in response to — kinetic or geopolitical escalations.

In May 2025, CISA released a joint advisory confirming that BlueDelta has been actively targeting logistics and technology providers supporting military and humanitarian aid operations to Ukraine. BlueDelta used spearphishing and credential harvesting to infiltrate enterprise networks, specifically exploiting known vulnerabilities in edge network devices and misconfigured remote access infrastructure. Notably, BlueDelta compromised over 10,000 internet-connected surveillance cameras across Ukraine and adjacent NATO border areas, using them as passive intelligence collection points to track aid flows and military logistics. These cameras were accessed through default or reused credentials and unpatched firmware vulnerabilities, enabling video stream redirection to actor-controlled infrastructure.

In May 2025, BlueDelta conducted an espionage campaign dubbed Operation RoundPress, exploiting XSS vulnerabilities in widely used webmail platforms including Horde, MDaemon, Roundcube, and Zimbra. Active between 2023 and 2024, the campaign targeted government and defense organizations across Europe, Africa, and South America. The infection chain began with spearphishing emails containing malicious JavaScript designed to exploit webmail XSS flaws, resulting in the delivery of tailored SpyPress malware variants specific to the victim's platform. These malware strains extracted credentials, messages, contact data, and, in some cases, two-factor authentication (2FA) secrets and login histories. Some variants enabled persistence via email forwarding rules or application passwords. All stolen data was exfiltrated over HTTPS to actor-controlled C2 servers.

In April 2025, the French Ministry for Europe and Foreign Affairs formally attributed a multi-year espionage campaign against French infrastructure and institutions to BlueDelta, confirming the group's persistent operations targeting European governments. The campaign, ongoing since at least 2021, has focused on ministries, defense contractors, research bodies, and political institutions, with nearly 4,000 cyber-espionage incidents linked to Russian actors recorded in 2024 alone. The group deployed ZIP-delivered payloads containing Headlace, STEELHOOK, and MASEPIE malware to facilitate credential theft and mailbox exfiltration. In several campaigns, it used fake login portals mimicking Outlook Web Access and Roundcube to harvest credentials.

In January 2025, BlueDelta conducted a cyber-espionage campaign targeting Kazakh diplomats using real government documents stolen from Kazakhstan's Ministry of Foreign Affairs. The campaign used spearphishing emails embedded with official correspondence and internal memos to deliver the HATVIBE downloader, which in turn installed CHERRYSPY, a Python-based remote access tool. The documents leveraged for the campaign appear to have been sourced from legitimate channels, although the initial access vector remains unknown. The operation spanned from 2021 through late 2024 and relied on remote template injection and anonymized infrastructure to evade detection.

In November 2024, a report detailed a sophisticated intrusion campaign known as the Nearest Neighbor Attack — a method in which BlueDelta leveraged a dual-homed system device connected to both a secured internal network and a less-protected neighboring Wi-Fi network to bridge access between the two. After compromising an external Wi-Fi network using stolen credentials, the actor identified a nearby machine that was simultaneously connected to both that Wi-Fi and the target's wired enterprise network. By pivoting through the wireless adapter, the threat actor established access to the internal target network, effectively bypassing traditional perimeter defenses.

BlueDelta's sustained focus on aid logistics, diplomatic communications, and surveillance infrastructure aligns closely with GRU intelligence, surveillance, and reconnaissance objectives. These operations are not merely opportunistic; they are strategic efforts to gain early access to sensitive communications, policy positions, and logistical plans — access that could support both espionage and potential disruption. Given the 2025 NATO Summit's reliance on secure digital coordination, BlueDelta's tradecraft, exemplified by campaigns like Operation RoundPress and its interest in infrastructure surrounding summit planning, poses a credible threat to affiliated entities. BlueDelta continues to exploit both well-known and newly disclosed vulnerabilities to access high-value targets, often without leaving persistent traces. Its capability to blend cyber access with strategic timing supports the assessment that it will remain a top-tier threat actor highly likely to target the 2025 NATO Summit — whether to collect intelligence, disrupt critical logistics, or pre-position for escalation.

China

Chinese state-sponsored groups tasked with the collection of foreign intelligence, and particularly those under the MSS — China's primary civilian intelligence service — are likely to engage in some level of opportunistic cyber-espionage operations against select attendees with the goal of understanding policy discussions and outcomes of the 2025 NATO Summit. Additionally, groups may use the summit as a theme for either malicious domains or lures to gain initial access or harvest credentials. In keeping with global trends, Chinese state-sponsored groups targeting the 2025 NATO Summit are likely to gain initial access via phishing and targeting of vulnerabilities in edge devices. While we have no indications of such campaigns at this time, based on recent targeting of European governments and organizations, threat groups that may target the 2025 NATO Summit could include, but are not limited to, RedBravo (APT31), RedDelta (Mustang Panda, Earth Preta), and RedGolf (APT41).

RedBravo

RedBravo (APT31) is a Chinese state-sponsored threat activity group that the US Department of Justice (DOJ) has linked to a front company, Wuhan Xiaoruizhi Science & Technology Company, operating on behalf of China's MSS. The group has historically targeted government, finance, media, aerospace and defense, law firms, non-governmental organizations, and managed service providers (MSPs), predominantly within the US and Europe. In May 2025, the Czech government stated that RedBravo targeted an unclassified network of the Czech Ministry of Foreign Affairs starting in 2022. In December 2024, the group used a new backdoor dubbed NanoSlate on the network of an undisclosed Central European government entity.

RedBravo has used web beacons (web bugs/tracking pixels) in spearphishing emails to conduct initial reconnaissance of targets. Initial access vectors have included spearphishing and, historically, password spraying, brute-forcing, and exploitation of vulnerabilities in external-facing appliances (ProxyLogon (CVE-2021-26855) and CVE-2018-13379). In recent years, the group has used custom capabilities often configured to communicate with legitimate services such as Dropbox, OneDrive, and Yandex Disk for C2 (for example, PERIODICCLOUD). The group uses shared tools such as Trochilus, EvilOSX, and Cobalt Strike and custom malware, including FourteenHi, MeatBall, YaRAT, Stealer0x3401, and Rekoobe.

RedDelta

RedDelta (Mustang Panda, Earth Preta, TA416) has been active since at least 2012 and has focused on Southeast Asia, Mongolia, Europe, and more. The group has routinely adapted its targeting in response to global geopolitical events. For instance, RedDelta targeted the Vatican and other Catholic organizations with PlugX in the lead-up to 2021 talks between China and the Vatican. In 2022, the group shifted toward increased targeting of European government and diplomatic entities following Russia's invasion of Ukraine. Since at least 2022, the group has used various versions of an infection chain delivering files via spearphishing that ultimately lead to DLL search order hijacking that loads the group's customized PlugX backdoor.

In the last year, RedDelta has persistently targeted European governmental institutions and maritime transportation companies in Norway, the Netherlands, the UK, Bulgaria, Greece, Denmark, Poland, and Hungary with PlugX and malicious USB drives. The group has used Delphi-, Go-, and Nim-based PlugX loaders, as well as Microsoft Management Console Snap-In Control (MSC) files.

RedGolf

RedGolf (APT41, Brass Typhoon, Earth Baku) is a China-based threat activity group that carries out state-sponsored espionage activity in parallel with financially motivated operations for personal gain, which has been active from at least 2014 onward. In September 2020, the US DOJ announced charges against five RedGolf operators, one of whom allegedly boasted of connections to the Chinese MSS; US officials also stated that three of the individuals were employees of the Chengdu-based company Chengdu 404 Network Technology.

The group has historically exploited public and zero-day vulnerabilities in internet-facing devices for initial access, including Citrix, Cisco, and Zoho. Following this initial access, the group deploys lightweight web shells like AntSword and BLUEBEAM for persistent access. Additionally, RedGolf continues to develop custom malware, such as StealVector and SneakCross, using stealthy techniques like in-memory-only payloads and legitimate services (Google Workspace, OneDrive) for C2 to avoid detection. The group also uses advanced anti-detection tactics, including API unhooking, DLL sideloading, and AES encryption.

In recent years, RedGolf has persistently targeted Europe. A report from August 2024 described a campaign from 2022 onward in which RedGolf targeted entities in the government, media, communications, telecommunications, technology, healthcare, and education sectors across Europe, the Middle East, and Africa. The group targeted public-facing applications such as Microsoft IIS for initial access and deployed the Godzilla web shell to maintain access to compromised systems. The StealthVector and StealthReacher loaders were introduced to deploy backdoor components, including

Cobalt Strike and the modular backdoor SneakCross (MoonWalk). SneakCross uses Google services for C2. The group executes various post-exploitation routines, including persistence through reverse tunnels and data exfiltration via MEGAcmd.

A July 2024 report found that RedGolf had actively targeted multiple organizations across sectors such as shipping, logistics, media, technology, and automotive since at least 2023, affecting countries including Italy, Spain, Türkiye, and the UK. The group used a combination of AntSword and BLUEBEAM web shells on compromised servers to establish persistence, executing the DUSTPAN malware to deploy BEACON for C2. As the intrusion evolved, RedGolf used DUSTTRAP, a multi-stage dropper that decrypts payloads directly in memory, minimizing forensic evidence. The campaign further leveraged SQLULDR2 to extract data from Oracle databases and PINEGROVE to exfiltrate this data to Microsoft OneDrive, capitalizing on legitimate cloud services for stealth. The group's advanced techniques, including memory-only payloads and using Google Workspace accounts for C2, demonstrate sophisticated evasion tactics and underscore RedGolf's ability to blend malicious traffic with legitimate network activity.

A May 2024 report found that RedGolf has also targeted various Italian industries with the KEYPLUG implant. KEYPLUG is a modular, cross-platform backdoor that has been active since at least 2021, supporting Windows and Linux. This malware evades detection using encrypted configurations and secure WebSocket protocols (WSS) for C2. It also includes unique features, like manipulating Windows privileges and employing anti-analysis techniques, to maintain persistence.

Cybercrime and Hacktivism

As the 2025 NATO Summit approaches, cyber threat activity linked to non-state actors is intensifying in scope and scale. Insikt Group's continuous monitoring of cybercriminal sources reveals an observable increase in threat actors referencing NATO-related data, access points, and targeted intrusion services. This pattern fits an increasingly common trend in which malicious actors leverage geopolitical flashpoints and multinational gatherings as staging grounds for either advancing influence operations, described more in-depth above, or conducting financially motivated attacks. The convergence of hacktivism, information warfare, and cybercrime at this moment carries strategic implications that warrant attention from NATO and allied cyber defense teams.

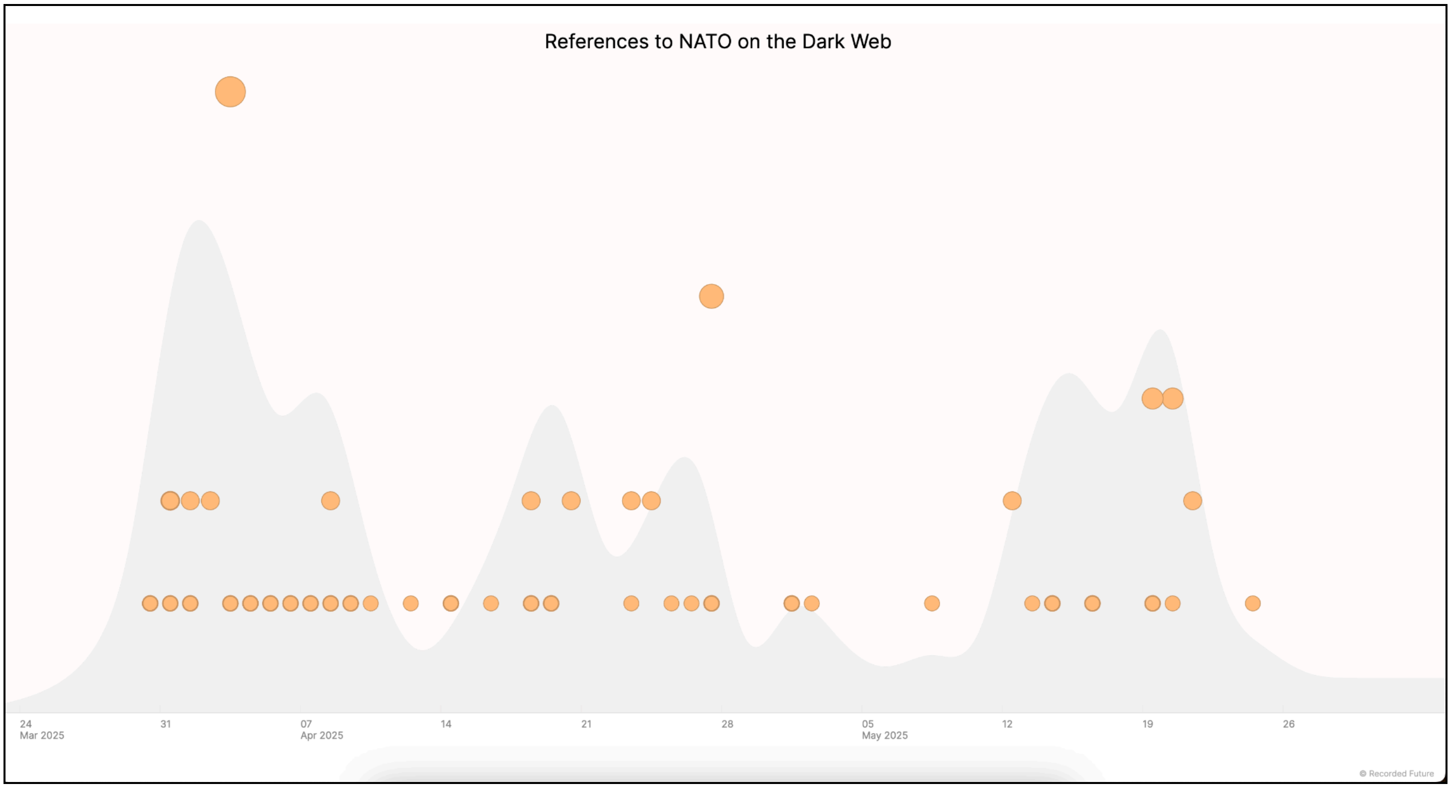


***Figure 12**: References to NATO on dark web and special-access sources. (Source: Recorded Future)*

Non-state cyber threat actors have historically been observed capitalizing on high-visibility international events for financial or political gain. In the context of the 2025 NATO Summit, Insikt Group identified several references to threat actors on dark web and special-access sources claiming to advertise access and databases related to NATO over the past three months. These advertisements include reposted databases previously attributed to groups like SiegedSec, text files allegedly containing personally identifiable information (PII) related to NATO personnel, vague databases of unspecified Cosmic Top Secret (CTS) information related to NATO, and more. Other threat actors have solicited the sale of access, databases, and documents related to NATO, but did not offer any assets of their own. The overwhelming majority of this activity took place on English- and Russian-language dark web forums like LeakBase, BreachForums, and XSS. In several cases, Insikt Group identified threat actors selling databases affecting military or defense industrial base (DIB) organizations based in NATO member states. It is presently unclear whether these advertisements are related to the 2025 NATO Summit, as NATO is always a popular and high-value target of cybercriminal activity, but the timing and volume of these listings may suggest high potential for targeting ahead of the summit.

NATO is also a common target of hacktivist groups and has been a focal point for pro-Russian groups, such as NoName057(16), since the beginning of the war in Ukraine. This targeting often manifests as distributed denial-of-service (DDoS), website defacement, or hack-and-leak attacks targeting NATO or its member states; however, the transient nature of these campaigns and their indirect relationship with influence operations make them difficult to assess and corroborate. Following the onset of the war in Gaza and recent tensions flaring between India and Pakistan, hacktivist groups located in South Asia, Southeast Asia, and the Middle East and North Africa (MENA) have also begun targeting NATO due to its perceived support for Israel and India.

This renewed surge in dark web activity focused on NATO-aligned infrastructure and databases ahead of the 2025 Summit should not be interpreted as merely background noise within the cybercriminal underground. Instead, this sustained chatter — especially across multilingual forums and in conjunction with known hacktivist groups — signals a rising probability of coordinated, multi-vector campaigns timed to disrupt, embarrass, or coerce NATO stakeholders. For NATO member states, particularly those in the defense industrial base and intelligence-sharing communities, these developments require immediate preemptive measures. The advertisement of Cosmic Top Secret content, for example, even if unverified, indicates potential insider breaches or compromised staging environments that adversaries may exploit during the summit. Additionally, the alignment of anti-Western hacktivist ecosystems across regions suggests ideological convergence that could escalate during key diplomatic events.

NATO's role as a symbolic and operational bulwark of Western defense architecture makes it a perennial cyber target. However, the timing, thematic focus, and diversity of actors involved in this current wave — ranging from financially motivated actors to politically charged collectives — demands a heightened posture of cyber readiness. Member states should increase active monitoring of dark web forums, prepare for cyber-enabled influence operations, and consider joint contingency planning in anticipation of DDoS or leak-based coercion campaigns during the summit window.

Physical Security Threats

A range of violent non-state actors — including terrorists, violent extremists, criminals, and disruptive protesters and demonstrators — have very likely demonstrated their capability to conduct physical threat activities in The Hague and the Netherlands during the past six to twelve months. However, Insikt Group has not identified evidence that these threat actors intend to target, or are interested in targeting, the 2025 NATO Summit. Moreover, the Netherlands' law enforcement, intelligence, and security agencies assess the 2025 NATO Summit will represent "the largest logistical and security operation in the Netherlands, ever," and are almost certainly preparing extensive physical security measures to protect the event from physical threats. These measures will very likely mitigate the probability and effect of physical risks to the summit, although even foiled or unrelated attacks during the event are likely to generate psychological effects among attendees and drive malign influence operations.

Terrorism and Violent Extremism

Insikt Group has not observed instances of terrorist and violent extremist groups planning threats to the 2025 NATO Summit, but the Netherlands and The Hague currently face a heightened threat environment from terrorists and violent extremists.[24] The ongoing conflict between Israel and Hamas, foreign terrorist organization (FTO) media content promoting attacks in Western Europe against high-profile events, and networked links between FTO attack and logistics coordinators and homegrown violent extremists (HVEs) within Western Europe all almost certainly continue to shape the threat environment. Due to the conference's extensive physical security measures, a mass-casualty terrorist attack at the 2025 NATO Summit is very unlikely, although HVEs in the Netherlands — especially supporters of the Islamic State (IS) — are very likely capable of carrying out low-sophistication attacks using bladed weapons, vehicles, and rudimentary improvised explosive devices (IEDs).

Homegrown Violent Extremists

Since December 2023, the Netherlands National Coordinator for Counterterrorism and Security (NCTV) has assessed that the country faces an overall terrorism threat level of four on its five-point scale, indicating it believes "there is a real chance of a terrorist attack in the Netherlands." The NCTV last updated this assessment in December 2024, maintaining the threat level at level four and underscoring the major factors behind the threat landscape. Specifically, Dutch intelligence and counterterrorism agencies assess that the threat from jihadist Salafis remains the predominant threat to the country, and that the Israel-Hamas conflict continues to represent a "significant driving force" in motivating individuals or small groups of jihadist Salafis to conduct violence in the Netherlands. NCTV also pointed to the activation of networks of jihadist Salafis from the Caucasus and Central Asia in Europe, and their connections to attack planners affiliated with IS Khorasan Province (ISKP), as magnifying the risk of terrorist attacks in the Netherlands and Western Europe.

[24] Insikt Group uses definitions of terrorism and violent extremism adapted from US Intelligence Community (IC) definitions, academic research, and open-source reporting.

During the past several years, jihadist Salafis in the Netherlands have carried out, or attempted to carry out, several terrorist attacks within the country. Successful attacks typically involve lone attackers using bladed weapons; sophisticated plots involving firearms, IEDs, or other more lethal means are more likely to be disrupted by law enforcement. The most recent jihadist attack in the Netherlands took place in September 2024 when an individual stabbed several people near Rotterdam's Erasmus Bridge. The last attack in The Hague took place in May 2018, where an attacker stabbed three people near The Hague's central train station; however, the perpetrator was found to have significant mental health issues and was sentenced to mandatory institutionalized psychiatric treatment. Although they have been disrupted, IS supporters in the Netherlands likely continue to explore more extensive plots involving transnational networks, the use of more lethal attack methods, and the development of connections to IS attack planners in the Middle East or Central Asia. For instance, Dutch police arrested one Tajik and one Kyrgyz citizen in July 2023 for their involvement in a cell in the Netherlands and Germany that was planning to conduct a substantial attack on behalf of ISKP.

While Insikt Group is unaware of instances of IS supporters, or official IS media outlets, discussing the 2025 NATO Summit or The Hague as a potential target of violent attacks during the last six months, during that timeframe IS media has almost certainly incited attacks against large and high-profile events in the Netherlands. For instance, on January 10, 2025, an infographic published by the ISKP media arm al-Azaim Foundation for Media Production provided a list of public events in Western Europe and the US during 2025 that its supporters could target — including the October 2025 Amsterdam Dance Event in Amsterdam.[25] A January 9, 2025, issue of IS's weekly newsletter al-Naba encouraged the group's supporters in the West to "search on the web for a date of a concert, a fair, or a market ... find the most serious targets and strike without mercy."[26] Notably, during the past 12 to 24 months, ISKP media and supporter publications have increasingly focused on planning attacks targeting public events with unmanned aerial vehicle (UAV)-borne IEDs; an ISKP supporter or cell interested in conducting attacks against the 2025 NATO Summit would likely consider this option.

Domestic Violent Extremists

Aside from disruptive protests and demonstrations, which are covered below, domestic violent extremist (DVE) networks in the Netherlands are very unlikely to plan physical threat activities targeting the 2025 NATO Summit. The NCTV assesses that neo-Nazi and white supremacist violent extremist milieus in the country, particularly white supremacist active clubs, are growing in number and are "more willing to take action" by meeting in-person and engaging in hand-to-hand combat training. However, these groups are very unlikely to conduct mass-casualty attacks or violence; the NCTV frames white supremacist active clubs as a threat for "undermining the democratic legal order" through their ideologies rather than posing a major risk of conducting violent attacks.

Since 2020, several Netherlands citizens have been arrested for their alleged role in The Base, a transnational neo-Nazi accelerationist group that focuses on conducting paramilitary training to prepare for a hypothesized future race war. In September 2024, Dutch authorities arrested three individuals for

[25] Source documents held by Insikt Group, available on request.
[26] Source documents held by Insikt Group, available on request.

participating in the organization, following The Base's July 2024 EU designation as a terrorist group. Per communications reviewed by Insikt Group, The Base very likely does not intend to conduct attacks in Europe and has not publicly discussed the NATO Summit. However, The Base's interests in the destabilization of the Ukrainian government and its leader's purported ties to Russia's intelligence services would likely give the organization a theoretical motive to conduct anti-NATO operations, particularly if allegations made by The Base's former members that the organization operates as an asset of the Russian government have basis in fact.

The NCTV has also identified a growing trend of sovereign citizen violent extremism (SCVE) within the Netherlands, noting eight 2024 arrests of Dutch SCVEs on terrorism offenses. Their ideology rejects the legitimacy of the Netherlands government, and a "small group of sovereign citizens who are willing to use violence" have incited violence against the government or stockpiled firearms in anticipation of a future confrontation. However, Dutch government and independent assessments of the Netherlands-based SCVE movement do not indicate their intent to target NATO interests or the interests of other member countries.

Violent Crime

Elements of transnational criminal organizations (TCOs) present in The Hague or in the Netherlands are very unlikely to directly target the 2025 NATO Summit, although they almost certainly possess the capability to conduct destructive attacks with firearms and IEDs. According to Recorded Future data, there have been several incidents during the past year of likely gang-related targeted attacks in The Hague, in which individuals allegedly affiliated with TCOs used guns or explosives to assassinate high-profile figures. These incidents are very unlikely to directly affect the 2025 NATO Summit or its venues, although if they occur in coincidence with the event, law enforcement will very likely deploy additional security measures that can affect transit routes inside and outside the city and affect normal business operations.

According to the Central Statistics Bureau of the Netherlands, The Hague recorded approximately 68 violent and non-violent crimes per 1,000 residents in 2024, an approximately 2% increase from 2023. This figure is higher than the Netherlands-wide rate of 45 crimes per 1,000 residents. Europol assesses that Netherlands-based TCOs have very likely become increasingly violent due to the decreasing relative age of their individual members, the lifting of taboos on attacking individuals associated with a particular target (such as the target's family members and associates), and increased competition between TCOs. Netherlands-based TCOs often have ties to networks in nearby countries — particularly Germany and Belgium — allowing them to facilitate cross-border transfer of materials needed to conduct violent attacks, such as firearms and explosive material.

The government of the Netherlands has repeatedly expressed concern that the availability of explosive devices and material within the country creates a significant threat to public safety, as IEDs and illegal fireworks are used "not only [in] criminal conflicts, but also [in] domestic or relationship conflicts." Although the motive is not publicly known, an explosive device was detonated at a cafe on The Hague's Rijswijkseweg on May 21, 2025. On December 7, 2024, a detonation of an incendiary device made from

175 liters of gasoline and fireworks at an apartment block in the Mariahoeve neighborhood of The Hague caused a massive fire that killed six individuals and destroyed a significant portion of the targeted building. Law enforcement later arrested four individuals allegedly involved in plotting the blast, one of whom confessed that the attack was the result of a dispute with his ex-girlfriend.

On May 1, 2025, Cemil Önal, a former associate of the deceased Turkish Cypriot organized crime figure Halil Falyalı, was shot and killed at the Hoevevoorde Hotel in The Hague's Rijswijk district. Önal had previously been imprisoned in the Netherlands for his role in financially managing Falyalı's alleged extensive illegal online gambling and money laundering operations, which he detailed in a February 13, 2025, interview with the Organized Crime and Corruption Reporting Project (OCCRP). Önal's allegations also implicated several current and former senior government officials in Türkiye, including claims that Türkiye's former interior minister and vice president accepted bribes from Falyalı. Dutch law enforcement has identified, but not publicly named, a suspect in Önal's assassination.

In addition, police broke up a fight reportedly involving hundreds of teenagers in the Scheveningen district of The Hague on the night of May 1, 2025. Subsequently, the situation devolved into a riot, as the participants in the fight assaulted and threw projectiles at law enforcement, causing the deployment of riot police to the area. Four teenagers, ranging in age from fourteen to eighteen years old, have been arrested for their roles in the riot.

Protests and Disruptive Demonstrations

Large-scale protests and demonstrations will almost certainly occur in The Hague during the 2025 NATO Summit, although authorities will very likely cordon off protests to specially designated zones, reducing the risk of escalations disrupting the summit. To mitigate the potential for "large-scale social unrest," Dutch law enforcement will restrict demonstrators from conducting large-scale protests around the World Forum, the venue for the 2025 NATO Summit, although small-scale demonstrations are still permitted to take place "within sight and hearing distance" of the venue. The police are encouraging larger demonstrations at "other well-known sites" in The Hague, particularly in the Malieveld event venue.

Several Netherlands-based and international organizations, particularly those describing themselves as "anti-war activists," have already announced their intent to hold anti-NATO protests in The Hague. The New Peace Movement (De Nieuwe Vredesbeweging), in conjunction with several Dutch socialist, environmentalist, and pro-Palestinian political organizations, has announced that it will hold a "counter-NATO summit" (NAVO Tegentop) and a subsequent demonstration on June 21 and 22, 2025, respectively, at the Koekamp park.

Many of the large-scale demonstrations and protests in The Hague in recent years have taken place in an area in the city's central district near the Malieveld event venue, the Koekamp park, and other buildings and areas in the vicinity (**Figure 13**). This area is approximately two miles (3.5 kilometers) from the World Forum.

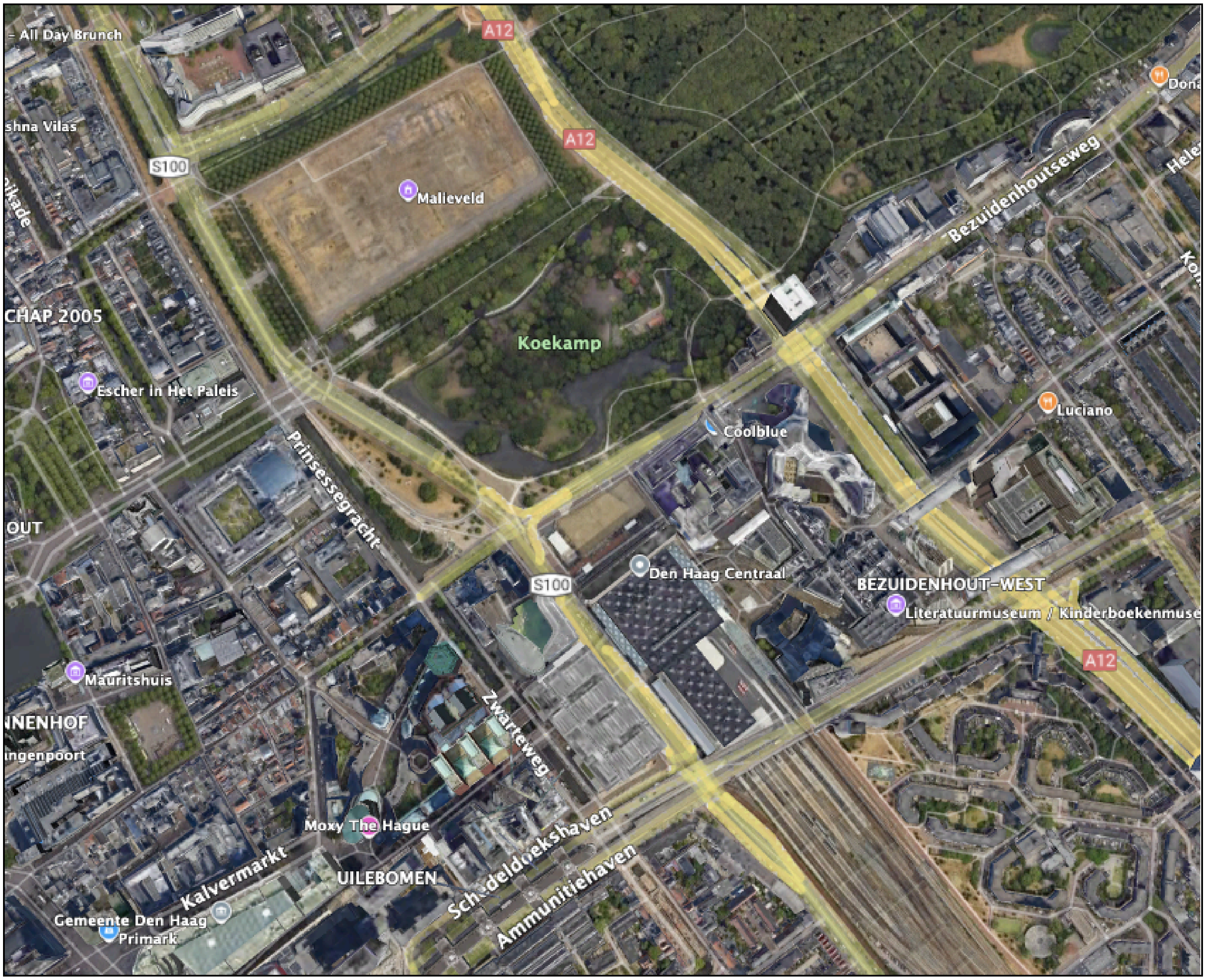


***Figure 13**: Area in The Hague with a significant history of large-scale protest activity, including the Malieveld facility (Source: Google Earth)*

Political Activists

Almost certainly due to its concentration of sites of international political importance, The Hague is frequently the site of significant protest activities. During the past several months, there have been a number of major demonstrations regarding the Israel-Hamas conflict, which will almost certainly be a motivating factor for protesters to demonstrate against the 2025 NATO Summit and have the potential to turn out a significant number of attendees. On May 18, 2025, approximately 100,000 people joined a march in The Hague calling for the Dutch government to restrict its political ties to Israel; organizers claimed it was the largest political demonstration in the Netherlands in twenty years.

Demonstrations over the Israel-Hamas conflict have the potential to disrupt normal business activities of locations in The Hague or escalate to violence between protesters and law enforcement, although the security measures in place will very likely prevent protests from disrupting the 2025 NATO Summit. On May 6, 2025, more than 100 activists occupied a building on Leiden University's campus in The Hague to protest Israeli military activity in Gaza. After police ordered the demonstrators to leave the building, approximately 75 refused to comply, resulting in law enforcement removing the activists from the facility and arresting them.

In recent months, protests have also taken place in The Hague regarding international political matters that demonstrators believe should be taken up by The Hague-based International Court of Justice (ICJ), or over the detention of individuals by the International Criminal Court (ICC). For instance, on May 5, 2025, there were limited demonstrations outside the ICJ following the court's rejection of Sudan's complaint against the United Arab Emirates (UAE); there were also protests in The Hague following the arrest and transfer into ICC custody of former Philippines President Rodrigo Duterte on March 11, 2025, on charges of crimes against humanity.

Environmental Activists

During the past several months, environmentalist activists have conducted large-scale disruptive demonstrations in the vicinity of The Hague that affected transportation corridors and normal business activities. Most of the notable incidents were almost certainly organized by elements of the group Extinction Rebellion (XR), which almost certainly has a presence in the Netherlands through a dedicated branch and its activist wing, XR Justice Now! The organization is part of the coalition that announced it planned to protest the 2025 NATO Summit, likely indicating that XR may plan similar activities during the summit.

On April 5, 2025, over 500 XR members stormed a tunnel in front of the Ministry of Economic Affairs and Climate Policy in the central district of The Hague, formed a blockade, and briefly obstructed traffic on the A12 motorway. Using the exact same method and location, XR protesters had previously blocked traffic on the A12 in a January 11, 2025, demonstration that led to over 700 arrests and required police to deploy water cannons and other anti-riot measures to disperse.

Mitigations

- International media, governments, and researchers should collaborate on proactive messaging to inoculate domestic and international audiences against potential malign influence narratives. Likewise, these groups should also issue early public warnings of likely influence themes to preempt narrative uptake.
- NATO member states should increase active monitoring of dark web forums, prepare for hybrid influence operations, and consider joint contingency planning in anticipation of DDoS or leak-based coercion campaigns during the summit window.
- Recorded Future customers can use the 2025 NATO Summit Intelligence Kit to monitor for cyber, malign influence, and physical threats. Recorded Future Intelligence Kits feature centralized information, including custom advanced queries and Intelligence Cards, based on specific industries or areas of interest.
- Customers can use Recorded Future's Facility Risk Event Playbook to identify real-time physical security and protest event activities occurring in The Hague and near the World Forum.
- The Recorded Future Brand Intelligence module can be used to identify potential impersonation attempts of public figures, government bodies, or international institutions such as NATO, including typosquats, logotype detection, and other potential forms of brand abuse.
- Customers with access to the Recorded Future Geopolitical Intelligence module can analyze emerging 2025 NATO Summit narratives from Russian and Chinese state-sponsored media and review the Netherlands' Country Risk scores. These scores are useful for pre-travel assessments and are based on the following categories: governance and institutions, physical security and travel, cybersecurity, data privacy and surveillance, and supply chain.

Outlook

The June 2025 NATO Summit in The Hague is almost certainly a prime target for a range of adversaries seeking to exploit internal tensions and geopolitical divisions among alliance members. Russia and China, in particular, are almost certain to ramp up influence operations ahead of and during the summit to amplify perceptions of NATO disunity and undermine the alliance's credibility. Potential influence operations could very well include increased use of AI-enabled tooling, from voice cloning to synthetic “leaks” or carefully crafted deepfakes to heighten doubts about allied unity on Ukraine aid, Arctic posture, and burden-sharing.

NATO leaders and summit participants should anticipate attempted cyber-espionage activity from both Russia and China intended to facilitate the collection of the summit agenda, topics, points of disagreement, and outcomes. Both Russia and China will likely use summit-themed lures and domain spoofing to harvest credentials or facilitate initial access for use at this time or for future campaigns. Russia, in particular, may use data successfully exfiltrated from the summit to disrupt NATO processes and Western coordination; alternatively, absent the collection of any damaging information, Moscow may fabricate “leaked” data to discredit and embarrass NATO and member states to the public.

Concurrently, hacktivist collectives and profit-driven cybercriminal group crews are likely to converge around NATO-branded targets, coordinating DDoS, data-leak extortion, and defacement campaigns aimed at embarrassing host-nation authorities during peak media coverage. Even if Dutch security measures prevent a kinetic incident, a single well-timed cyber disruption, or even a fabricated claim of one, could dominate headlines and hand malign influence actors a successful “perception hack.”

To counter the heightened digital threat environment as NATO convenes in The Hague, the alliance, each member state, and all partners involved in the summit should ensure last-mile cyber hygiene around summit infrastructure, push pre-emptive takedowns of spoofed domains and synthetic news clips, and deliver rapid, transparent debunks to emerging, non-credible reporting. Continuous liaison between NATO StratCom, member-state computer emergency response teams (CERTs), trusted information streams and intelligence partners, as well as the public, will be critical as a cohesive public-messaging cadence may prove as important as technical defenses in preserving summit integrity and, by extension, NATO’s cohesion, its strategic narrative, and its mission.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com