June 9, 2025

A Decade of Cyberattacks Targeting NATO Summits

Key Insights:

- NATO summits are now cyber battlefields by default. Cyber disruptions are no longer anomalies but expected elements of summit planning.
- DDoS attacks are strategic tools in hybrid warfare.
- Even unsuccessful cyberattacks generate extra work and anxiety for defenders.
- DDoS attacks are not merely nuisances; they have the potential to interfere with real operations.
- Recent summits, like the 2024 Washington event, needed an even more integrated counter-hybrid game plan.

NATO summits are high-profile events that attract intense cyberthreat activity due to their geopolitical significance. Over the past decade, as NATO member states' leaders convened to make strategic decisions, state-sponsored hackers and hacktivist groups have repeatedly targeted summit infrastructure, communications and information. These cyberattacks range from website defacements and distributed denial-of-service (DDoS) attacks to sophisticated espionage operations and disinformation campaigns, often mirroring the geopolitical confrontations of the day.

Russian state-linked actors have featured prominently, leveraging cyber operations to protest NATO expansion, spy on or embarrass Alliance officials, and undermine NATO's unity in conflicts like the Ukraine war. At the same time, an ecosystem of patriotic or ideologically motivated hacktivists has emerged to harass NATO with denial-of-service attacks, defacements and leaks. The technical details of these incidents reveal an evolving toolkit, ranging from crude DDoS botnets that knock websites offline using volumetric attacks to targeted phishing using zero-day malware exploits and sophisticated, highly focused Web DDoS attacks. The geopolitical context often explains the timing and tone, whether it was Russia's retaliation for NATO's support to post-Maidan Ukraine in 2014, or proxy cyberattacks during NATO's summits at the height of the Kremlin's 2022 invasion of Ukraine.

In the following sections, we will provide a timeline summary with year-by-year incidents, followed by a more detailed examination of incident reports for each major cyberattack related to the summit. A special focus section on DDoS attacks highlights patterns in the use of denial-of-service as a tactic against NATO summits. This analysis draws on credible public sources and NATO statements to illuminate both the technical aspects (malware used, attack vectors, etc.) and the geopolitical motivations (attribution to nation-states or groups and international reactions) of each incident.

The Cyber Battlefield of Diplomacy

Over the last decade, cyberattacks on NATO summits have become a persistent reality, with spikes corresponding to periods of heightened East–West tension. In 2014, as Russia seized Crimea, NATO's summit was met with a disruptive DDoS attack by pro-Russian hacktivists – a signal that cyber protests would accompany kinetic confrontations. The mid-2010s saw NATO formally recognize cyber warfare as on par with traditional warfare, even as suspected attacks in 2016, briefly knocking out summit websites, hinted at hostile actors testing NATO's resolve. By 2017, Russian cyber units were actively targeting countries in NATO's orbit and the accession of Montenegro, for example, triggered an espionage campaign by Fancy Bear (APT28) targeting Montenegrin officials to steal documents in an attempt to discourage Montenegro from joining NATO.

Following a period of reduced activity, a major turning point came with Russia's full-scale invasion of Ukraine in 2022. NATO's 2022 Madrid Summit, focused on bolstering defense against Russia, took place amid an unprecedented wave of hacktivist aggression. Hacktivist threat group KillNet mobilized volunteers online to target NATO networks with DDoS attacks, loudly claiming victories on social media. This marked the resurgence of ideologically driven cyberattacks, no longer confined to stealthy espionage but now openly disruptive and politically charged.

In 2023, the trend escalated further as NATO's summit in Vilnius faced multi-pronged attacks combining exploits with information warfare. Suspected Russian operatives deployed phishing malware against summit attendees and spread forged NATO announcements and "leaked" documents – tactics aimed at fracturing allied consensus. Concurrently, pro-Russia hacktivists targeted the host nation, Lithuania, with DDoS attacks, seeking to cast doubt on NATO's security guarantees. NATO officials noted the sheer volume of cyberattacks during that summit, though thankfully none achieved significant disruption of the proceedings.

By 2024, cyberthreats to NATO summits had effectively normalized. Ahead of the Washington summit, NATO publicly warned of intensifying campaigns by coordinated hacktivist groups intent on undermining its meetings. Indeed, during the 2024 summit, these actors launched concurrent DDoS attacks on NATO web assets and dumped allegedly stolen internal data online.

The incidents of the last decade reveal a clear pattern: whenever NATO gathers to make major decisions, especially those involving Russia or the addition of new members to the Alliance, a flurry of cyberattacks of various types tends to follow. The Alliance has had to treat summit cybersecurity as a frontline, investing in stronger defenses and real-time monitoring to stay ahead of the threats.

From Crimea to Washington: A Timeline of Evolving NATO Summit Cyberthreats

2014: Wales Summit – DDoS Disruption by Pro-Russian Hacktivists

In September 2014, during NATO's Wales Summit, several NATO public websites were taken offline by a sustained DDoS attack. The attack began on the summit's opening weekend, at a moment when NATO was condemning Russia's intervention in Ukraine, and lasted several hours before services were restored. NATO's main website (nato.int) went down intermittently, and the website of NATO's Cooperative Cyber Defence Centre of Excellence in Estonia was also hit. There were reports of NATO's unclassified email system experiencing slowdowns under the onslaught.

The assault was a classic DDoS attack. The perpetrators bombarded NATO servers with massive volumes of illegitimate requests, overloading the sites and rendering them inaccessible. NATO's spokesperson, Oana Lungescu, acknowledged the attack on Twitter and assured that core NATO operations remained unaffected. NATO officials emphasized that no classified networks were at risk, as the Alliance's sensitive command-and-control systems are segregated and remained untouched. The attack was confined to public-facing sites and communications, illustrating the attackers' intent to cause public embarrassment and communication delays rather than to steal data. The Alliance's cyber defenders restored the websites within a day. Strategically, the Wales Summit itself proceeded with its agenda, which, fittingly, included elevating cyber defense in NATO's doctrine.

A hacktivist group calling itself "CyberBerkut" claimed responsibility for the attacks. On their website, CyberBerkut stated the attack was the work of "patriotic Ukrainians" protesting what they perceived as NATO meddling in Ukraine's affairs. "Berkut" referred to the notorious riot police of the former pro-Russian Ukrainian regime, signaling the group's alignment with Moscow's narrative. While the claim couldn't be independently verified, cybersecurity experts noted that CyberBerkut had consistently acted as a pro-Russian proxy, believed to act with indirect support or oversight from Russian security services.

Western analysts assessed the motivation as twofold: geopolitical messaging (retaliation for NATO's stance against Russia's annexation of Crimea) and a show of capability to unsettle NATO. As one expert noted, these cyber strikes were akin to "kicking sand in NATO's face" at a moment of confrontation. NATO refrained from officially pinning blame on Russia, but the incident marked the beginning of a new era. It was one of the first times a NATO summit event had been directly disrupted in cyberspace, highlighting the blurred lines between state conflict and hacker activism.

In the aftermath, NATO officials cited the incident as validation of their decision to treat cyberattacks as potentially on par with armed attacks under its Article 5 collective defense clause. Although the 2014 DDoS attacks were nowhere near that threshold, they served as a wake-up call, demonstrating that even NATO's own events could be targeted by politically motivated cyber disruptions. This prompted NATO to invest in greater resilience for its public communications and to closely monitor hacktivist threats in future high-profile meetings.

2016: Warsaw Summit – The Unconfirmed Cyber Disruption

During the NATO Summit in Warsaw in July 2016, some of NATO's official websites experienced unexplained outages and slowdowns, prompting concerns of a cyberattack in progress. The disruptions were noted around the time Alliance leaders were discussing major policy announcements, including the recognition of cyberspace as a warfare domain. While the downtime was brief and no public announcements of an attack were made, NATO tech staff suspected a malicious external cause, given the timing and context. Essentially, the summit's public web presence abruptly went offline in a manner consistent with a denial-of-service attack.

Because NATO did not formally confirm the cause, details are sparse. However, officials privately indicated that the symptoms appeared to be a DDoS attack on web servers. It's likely that hostile actors directed a flood of traffic or crafted requests to NATO's public websites to overwhelm them, like the 2014 incident. Unlike in 2014, this may have been a lower-intensity attack, or NATO's improved defenses may have absorbed most of it, resulting in only intermittent outages. No breaches or data losses were reported, and the impact was limited to public-facing web services. The incident occurred in an environment of already high cyber alertness, where NATO's cybersecurity teams were monitoring network telemetry throughout the summit, which enabled them to quickly detect these anomalies.

2017: Fancy Bear Hacking Montenegro Ahead of NATO Membership

In the spring of 2017, as NATO held a special meeting in Brussels and prepared to add Montenegro as its 29th member, a covert cyber-espionage campaign targeted Montenegrin officials. The perpetrators were identified as APT28, also known as "Fancy Bear," a notorious Russian state-linked hacking unit. In January and February 2017, just months before Montenegro's accession was formalized, APT28 hackers sent carefully crafted phishing emails to Montenegrin government and defense personnel. These emails carried malicious Microsoft Word attachments with file names suggesting NATO-related content. When opened, the documents silently executed malware, effectively breaching the targets' computers.

The spear-phishing attachments were found to use a sophisticated Flash exploit framework called "DealersChoice.B," which had been previously seen in APT28 operations. This exploit would trigger a hidden Flash object in the document to download additional payloads from the attackers' servers. In this case, the malware delivered was a known APT28 tool dubbed "GameFish" (a

remote access trojan or backdoor), which allowed the attackers to remotely control the infected systems. The use of DealersChoice indicated access to a then-novel exploit, highlighting APT28's technical skill. Notably, at least two different lures were used: one related to a "European military exercise schedule" and another to a "NATO meeting schedule," suggesting that the attackers were attempting to use multiple NATO-themed baits to entice clicks. Once inside a system, GameFish malware could steal documents, log keystrokes, and exfiltrate emails.

This operation was clearly attributed to APT28 by the U.S. cybersecurity firm FireEye, based on the malware code and tactics used. APT28 is linked to Russia's GRU military intelligence. The timing and target leave little doubt about motivation: Russia fiercely opposed Montenegro's NATO membership, even allegedly backing a failed coup in Montenegro in 2016 to stop it. Failing to prevent Montenegro's accession by physical means, Russian actors turned to cyberspace. The goal was likely to gather sensitive information on Montenegro's NATO negotiations, plans, and communications of pro-NATO officials – intelligence that could be used to undermine or retaliate against the Balkan nation. It also sent a warning to other aspirants, such as Macedonia or Bosnia at the time, that aligning with NATO might invite Russian hacking. There's an element of sabotage as well: had the hackers found compromising or scandalous information, they might have leaked it to erode Montenegrin public support for joining NATO. In essence, this was an extension of Russian foreign policy by cyber means, directly tied to a NATO milestone.

Montenegro joined NATO in June 2017 despite these efforts. The phishing campaign was eventually uncovered and publicized by cybersecurity experts by mid-2017, likely after some damage had been done, as FireEye noted the campaign in retrospect. Montenegrin officials did not report any major breach of classified info, but it is possible the hackers obtained some internal documents or correspondence before detection. The incident rattled NATO members and it underscored that Russian cyber units would actively target nations on the path to NATO membership. It pushed NATO to improve information security for Partnership for Peace countries and new invitees. Internally, NATO's intelligence and security bodies increased briefings to allied states about spear-phishing threats using NATO-themed content. This was one of the first confirmed cases of a NATO partner's government being hacked as a direct consequence of a NATO summit decision. It reinforced the need for collective cyber defense assistance under NATO's umbrella even before a country formally joins the Alliance.

2018–2019: Heightened Vigilance and Disinformation

By 2018, NATO was actively bolstering its cyber capabilities – the Brussels Summit 2018 established a new Cyberspace Operations Centre and emphasized cyber deterrence measures. Although there were no headline-making summit attacks that year, NATO officials remained vigilant. Russia's hacking groups were busy elsewhere in 2018–2019, targeting Western think-tanks, election campaigns, and international organizations. For instance, the Russian disinformation outfit later dubbed "Secondary Infektion" was actively spreading fake news across

Europe, while other GRU hackers were engaging in espionage against NATO allies, such as the 2018 attempted hack of the OPCW in the Netherlands. The absence of a known direct attack on the 2018 Brussels Summit may partly reflect NATO's improved security; it may also be that any attempts (like phishing of delegates) were handled quietly.

In 2019, NATO's Leaders Meeting in London marked the Alliance's 70th anniversary. No cyber disruptions were reported during the event. However, it's worth noting that Russian information operations remained active around that time, aiming to undermine Allied cohesion. A notable case from late 2019 involved the leak of forged or stolen documents to stir discord between allies. A Russian campaign leaked UK-US trade papers during the UK elections. While not directly tied to the NATO summit, such operations fed into the same strategic goal of sowing distrust among NATO members. Allied security agencies were busy countering these subtler threats. In short, 2018–2019 can be seen as a period of relative respite in overt summit attacks, but with a pivot toward disinformation and behind-the-scenes espionage.

2021: Brussels Summit – Emerging Threats

NATO's Brussels Summit in June 2021 was notable for its strong language on cybersecurity and for addressing, for the first time, threats posed by China's cyber activities. While the summit itself did not suffer a known cyberattack, it took place against a backdrop of escalating global cyber incidents (e.g., the SolarWinds breach by hackers believed to be directed by the Russian intelligence service and the Microsoft Exchange hacks by the Chinese APT Silk Typhoon). NATO leaders jointly affirmed that cyberattacks could potentially trigger Article 5 and condemned malign cyber behavior by both state and non-state actors. In the communiqué, NATO explicitly warned that China's "malicious cyber and hybrid activities" were a growing concern.

Anticipating possible cyber trouble, NATO and Belgian authorities had hardened the summit's networks. They deployed cyber rapid reaction teams to monitor for intrusions or DDoS attempts in real time. The lack of a disruptive incident in 2021 might be attributed to this robust preparation, and perhaps adversaries held off, preferring not to tip their hand before the major conflict that was brewing (Ukraine). Intelligence later suggested that Russian cyber units were preoccupied in 2021 with laying groundwork in Ukraine (malware pre-positioning) rather than attacking NATO directly.

2021's summit passed without incident, but it set the stage for a more confrontational cyber stance. NATO issued a cyber defense strategy that year, and by the summit, it had a new Comprehensive Cyber Defense Policy. This proved timely, as within months the world would be plunged into a security crisis in which cyberattacks on NATO and its partners would dramatically increase.

2022: Madrid Summit – Hacktivist Onslaught Amid the Russia/Ukraine War

The NATO Summit in Madrid (June 29–30, 2022) convened as Russia's invasion of Ukraine raged, and the gathering became a magnet for pro-Russian cyber aggression. In the weeks surrounding the summit, a collective of pro-Russian hacktivist groups, spearheaded by the group KillNet, executed numerous cyberattacks on NATO members' digital infrastructure. Notably, on June 28 – the eve of the summit – Lithuania, a NATO member vocal against Russia, was hit by a massive DDoS attack that downed government websites and transportation systems. Although not directly on the summit host, this was part of the broader campaign tied to NATO's support for Ukraine.

During the summit itself in Spain, NATO's IT monitoring picked up attempts to disrupt NATO public websites and those of the summit organizers. Days earlier, KillNet had explicitly threatened NATO, even declaring an "all-out cyber war" on countries providing financial or military aid to Ukraine. True to their word, the group and its affiliates targeted various NATO-related servers. Thanks to enhanced defenses, the impact was minimal and NATO officials reported only minor, brief outages on some external pages. However, one incident stood out: media reports indicated that the DDoS attacks spilled over to affect a logistical network used by NATO's Strategic Airlift Capability. Communications with a military C-17 aircraft transporting search and rescue equipment to Incirlik Air Base in Turkey were temporarily disrupted due to network overload. The mission was part of relief efforts following the Turkish-Syrian earthquake, which claimed at least 28,000 lives. Although contingency systems prevented any accidents, this highlighted that DDoS attacks were not merely nuisances to websites. They had the potential to interfere with real operations.

The attacks were botnet-driven DDoS floods. KillNet and its supporters likely leveraged networks of compromised devices to generate huge volumes of traffic. They also used volunteer-based DDoS attacks, urging sympathizers on Telegram to run attack scripts against target URLs. KillNet's tactics included targeting login portals and APIs to maximize disruption. The group even boasted of crippling 40% of NATO's online infrastructure – an unverified claim. Separate from DDoS, Western agencies were wary of Russian APTs possibly attempting quieter hacks (e.g. espionage or sabotage) during the summit. Spain's defense ministry confirmed that it thwarted several phishing attempts targeting the email accounts of summit delegates, although details were not made public.

KillNet, an umbrella group of pro-Russia hackers, openly took credit on social media for many of these attacks. Its rhetoric framed the campaign as retaliation for NATO's military aid to Ukraine. Other hacktivist brands, such as NoName057(16) and Anonymous Russia, also joined in, forming a broader "hacktivist front" aligned with Russian interests. NATO and EU officials strongly implied the Kremlin's hand behind these groups. While perhaps not directly orchestrated by Russian intelligence, the actors operated in line with Russia's strategic narratives, and Moscow showed no intention of stopping them. The motivation was a mixture of ideology and opportunism: these

hackers sought to punish NATO countries, rally pro-Russia audiences with visible successes, and demonstrate Russia's displeasure at the summit's decisions, which included inviting Finland and Sweden to join NATO and bolstering force posture against Russia.

NATO's cybersecurity center had anticipated such attacks; they had drilled for DDoS scenarios and coordinated closely with private sector providers for traffic scrubbing. As a result, the attempted disruptions in Madrid were handled with little fanfare. Secretary-General Jens Stoltenberg acknowledged at a press conference that NATO had "seen cyberattacks" and was actively "deploying additional protective measures" during the summit.

In summary, the 2022 NATO Summit weathered an onslaught of hacktivist cyberattacks with negligible disruption, but it underscored the new normal: geopolitically charged summits now come with coordinated cyber harassment. The incident also blurred lines between state and non-state aggression online, raising policy questions for NATO. For instance, if a volunteer hacker collective causes real damage, could that trigger Article 5? NATO didn't have to answer that in Madrid, but the question would loom larger after 2022.

2023: Vilnius Summit – Coordinated Cyber and Disinformation Blitz

The Vilnius Summit in July 2023 faced one of the most concerted and multifaceted cyber offensives against a NATO event to date. In the days leading up to and during the summit, Lithuania (the host nation) and NATO networks were targeted by a combination of cyberattack vectors: phishing campaigns delivering malware, hack-and-leak disinformation operations, and aggressive DDoS attacks – all seemingly coordinated to disrupt the summit and shake allied unity. Lithuanian authorities described the situation as "everything was red when the summit was taking place," with dozens of incidents detected and mitigated in real time.

A threat actor dubbed RomCom, believed to be a criminal group moonlighting as political hacktivists, carried out a targeted phishing campaign. They spoofed the Ukrainian World Congress, an NGO supportive of Ukraine, by creating a fake website using a .info domain instead of the real .org. From there, they distributed malicious documents to summit invitees and support organizations. The documents were rigged RTF (rich text format) files that exploited a then-unknown Microsoft Office vulnerability (CVE-2023-36884) to execute code. Once opened, the files would download the RomCom RAT (remote access trojan), giving attackers a foothold in the victim's system. This malware could then steal data or deploy further payloads. Targets included government officials, NATO staff and contractors involved in organizing or securing the summit. The use of a zero-day exploit made this attack particularly sophisticated.

In parallel, two Russia-linked influence operations attempted to derail the summit's messaging. According to research by social media analysis firm Graphika, one group created forged NATO press releases and fake social media accounts to spread false announcements, such as claims that NATO was doubling its budget or deploying Ukrainian troops to France, exploiting current

events to sow confusion. They went so far as to register lookalike domains that mimicked NATO's site. Another group leaked documents purportedly stolen from the Lithuanian government, including what they claimed were internal plans for summit security. These were posted to fringe forums and Telegram channels associated with Russian disinformation. Graphika noted that the style matched known Russian information warfare units ("Secondary Infektion" and the newer "Doppelganger" campaign). While the authenticity of the leaked documents was dubious, their aim was likely to suggest that NATO and Lithuania had been compromised and to undermine public trust in the summit's security. NATO's media team had to work double time to debunk these fake stories.

Throughout the summit (July 11–12, 2023), pro-Russian hacktivists, including NoName057(16), targeted Lithuanian government and private sector websites with DDoS attacks. Targets included the foreign ministry, transportation agencies, and conference-related services. The goal was to disrupt logistical support and grab headlines. Although most DDoS attempts were successfully deflected by Lithuania's National Cyber Security Center, a few services experienced slowdowns. NoName057(16), a group known for crowd-sourcing DDoS attacks via a Telegram botnet dubbed "DDoSia," bragged on their channel about any site that became unresponsive, claiming it as a win for Russia's cause. These attacks were L7 application Web DDoS floods, leveraging large amounts of web requests engineered to look like legitimate requests while randomizing content to overwhelm online applications and service backends.

Attribution points overwhelmingly to Russian state and proxy actors. The phishing/malware operation, while perhaps executed by a criminal group (RomCom has ties to former ransomware actors), aligns with Russian interests, targeting NATO and Ukraine supporters. The disinformation campaigns were traced to known Russian information warfare units that have been active for years in meddling with Western politics. And the DDoS attacks were openly claimed by Russian patriotic hacktivists. In sum, the motivation was to sabotage and embarrass the Vilnius Summit, which was significant for its focus on supporting Ukraine and expanding NATO with the invite to Sweden.

Despite the breadth of the assault, NATO and Lithuania largely thwarted the attackers' objectives. Lithuanian cyber officials, as noted, detected hundreds of incidents but reported that essentially all were mitigated before causing significant damage. NATO's own networks were not breached, per official statements, and summit activities (meetings, communications among leaders) went on undisrupted. On the disinformation front, NATO's spokesperson, Oana Lungescu, promptly alerted the media to the existence of fake websites and releases, enabling quick debunking. Many mainstream outlets carried warnings about possible fake news, blunting the impact of the Russian propaganda. Social media companies also removed some of the fake accounts once they were identified.

However, the incident wasn't entirely toothless. The phishing campaign by RomCom resulted in some infections (exact numbers are classified), necessitating a post-summit cleanup. Affected organizations had to purge malware and assess whether any sensitive information had been stolen. The leaked "summit security" documents, although possibly fake, prompted the Lithuanian police to investigate and confirm whether any breach had occurred. In other words, even unsuccessful cyberattacks created extra work and anxiety for defenders. Internationally, the Vilnius cyber onslaught drew condemnation. The EU had just prior sanctioned certain Russian entities for disinformation, and events like this validated that approach. NATO's Cyber Defence Committee convened special sessions to analyze the summit attacks and glean lessons. One outcome was a decision to hold a dedicated Cyber Defense Conference later in 2023 to improve collective readiness.

The 2023 Vilnius Summit episode demonstrated NATO's growing skill at cyber resilience – absorbing punches without faltering – but also the evolution of adversary tactics. Russia showed it would orchestrate everything from stealthy hacks to loud DDoS strikes and fake news as one package. This set a precedent, and NATO planners took note that future summits (like the 2024 Washington event) would need an even more integrated counter-hybrid game plan.

2024: Washington Summit – Hacktivist Coalitions and Data Leaks

In July 2024, NATO's 75th Anniversary Summit in Washington, D.C., became the target of a broad hacktivist-led cyber campaign with clear pro-Russian overtones. As top officials met to discuss the future of NATO and the ongoing Ukraine war, multiple hacktivist groups allied together to disrupt the summit. This loosely knit coalition included well-known pro-Russian actors, such as NoName057(16), Cyber Army of Russia Reborn, UserSec and several earlier KillNet affiliates. They launched coordinated DDoS attacks, website defacements, and leaked allegedly stolen files to coincide with high-profile moments of the summit.

In the days leading up to NATO's July 2024 Summit, multiple threat actors and pro-Russian hacktivist groups launched coordinated data leak operations targeting NATO-affiliated systems and personnel. On June 29, a threat actor posted stolen documents on an active data leak forum, allegedly sourced from a NATO unclassified information-sharing platform. The files span from 2016 to June 2024 and include details on NATO frameworks, budget execution processes, and portal configurations. The leak also exposed a list of 362 members along with their professional email addresses. On July 7, just two days before the summit, a threat actor leaked personally identifiable information (PII) of participants in NATO's biannual event. The dataset contains names, profile images, nationality, organization, designation, email addresses, and phone numbers. The same day, the pro-Russian hacktivist group SiegedSec released almost 250MB of allegedly stolen data from a NATO cyber defense operations portal via Telegram. The data includes member access records, invitations, agendas, and announcements labeled NATO UNCLASSIFIED, dating from 2004 to June 2024. Another pro-Russian group, Anonymous

Central, published three internal NATO documents, none of which were classified. On June 26, prior to the above events, SiegedSec had also shared a link containing previously leaked data from two separate NATO breaches that occurred in 2023. This link and its contents circulated actively across hacking forums.

In the weeks leading up to the summit, Russian hacktivist groups, in coordination with hacktivist groups from other regions such as CyberVolk (India), the Hacker Council (international) and 7 October Union (alliance of pro-Palestine and Anti-Israeli groups), claimed to have launched DDoS attacks targeting NATO's Crisis Management and Disaster Response Centre of Excellence, the Allied Special Operations Forces Command, the Munitions Safety Information Analysis Center (MSIAC), and several other sites. Two days before the summit, NoName057(16) claimed DDoS attacks against the NATO Munitions Safety Information Analysis Center (MSIAC) portal, the NATO NEC CCIS Support Center portal, and GLOBSEC, a global think tank based in Bratislava and a partner of NATO. Throughout the summit week, NATO's public websites and those of member-state governments, particularly those of the U.S. and its Eastern European allies, experienced surges in traffic. The attackers employed botnets and crowd-sourced DDoS attack tools, advertising specific target URLs and timings in advance on Telegram channels. While many DDoS attacks were thwarted, a few succeeded in temporarily knocking sites offline. The methods employed in 2024 echoed those of 2022 and 2023, utilizing readily available IoT and volunteer DDoS networks, as well as well-targeted Web DDoS attacks. This involved repeatedly querying web applications' search functions on NATO sites to overload servers, while leveraging anonymizing proxy providers and anonymous VPN solutions to evade simple IP-based blocking.

Pro-Russian hacktivists have closely monitored media reactions to their attacks and data leaks. One of their primary goals has been to highlight the capabilities of Russian hacktivists to a domestic, Russian-speaking audience, reinforcing state-aligned propaganda narratives. At the same time, they sought to captivate foreign audiences, using these operations as part of a broader influence campaign aimed at weakening international support for Ukraine.

This campaign was one of the first to involve a conglomerate of hacktivist entities from different regions and with diverse motivations, working seemingly in concert. Besides the usual pro-Russia suspects, there were mentions of groups aligned with other anti-West causes joining in – a trend of "the enemy of my enemy is my friend" in cyberspace.

NATO's response was swift and firm. Within hours of the data leaks, NATO's IT officials acknowledged a breach of an unclassified platform and announced an investigation. They noted that while any unauthorized access is serious, there was "no impact on NATO missions, operations and military deployments." This underscored that classified networks were untouched. Most of the leaked files, upon inspection, turned out to be low-level documents or even open-source info compiled to look sensitive. Nonetheless, NATO asked member states to double-check their account security, and some NATO web portals were temporarily taken offline as a

precaution. The defacements were quickly reversed, and forensic teams traced those attacks to known IP addresses associated with prior hacktivist activity. The DDoS attacks did not result in a crippling blow. Thanks to improved cloud-based defenses, key NATO web services remained largely accessible, barring a few brief hiccups.

At the 2024 NATO Summit in Washington, D.C., allies agreed to establish the NATO Integrated Cyber Defence Centre to enhance network protection, situational awareness and the implementation of cyberspace as an operational domain. Also, NATO's public messaging highlighted Chinese and other actors in cyberattacks. For the first time, China was directly blamed in a summit communiqué for malicious cyber activities. NATO's Secretary-General used the incidents to reinforce in his closing speech that, despite attempts by NATO adversaries to divide the alliance through cyberattacks and propaganda, they will fail, and NATO is more united and prepared than ever.

The 2024 summit cyber incidents accelerated NATO's plans for collective cyber defense, information sharing, and possibly an offensive cyber posture to deter such attacks. While NATO emerged relatively unscathed operationally, the incident underlined that hacktivist-driven threats, often egged on by nation-states, would remain a persistent challenge for the alliance's high-profile events.

Flooding the Frontline: How DDoS Became a Core Tactic Against NATO

One recurring form of cyber aggression against NATO summits has been DDoS attacks. Over the past decade, DDoS attacks have proven to be a favored tactic for adversaries ranging from state-backed hackers to patriotic hacktivist mobs. This section explores the patterns in these DDoS incidents, including the methods used, the typical sources (actors), and their overall impact on NATO summit security.

A Decade of DDoS: From CyberBerkut to KillNet

The use of DDoS against NATO came into view with the 2014 CyberBerkut attack during the Wales Summit. That incident established a template: politically motivated hackers, aligned with Russian interests, unleashing network traffic floods to knock NATO websites offline as a form of protest. The “CyberBerkut” attack in 2014 was relatively straightforward: a brute-force flood that downed public sites but caused no lasting damage. Its significance lay in its symbolism and timing (happening alongside NATO’s statements on Ukraine), essentially a digital street protest spilling onto NATO’s virtual doorstep.

Following 2014, a period of calm is observed, followed by a sharp resurgence of DDoS attacks in 2022–2023, coinciding with the war in Ukraine. By this time, DDoS techniques and players had evolved. The mantle passed from CyberBerkut to new hacktivist brands like KillNet, NoName057(16), Anonymous Sudan, and other loosely organized groups, often coordinating via Telegram channels. These groups formed a hacktivist ecosystem aligned with Russian objectives. They share tools, lists of targets, and even compete in claiming credit for attacks. A notable pattern is the emergence of crowd-sourced DDoS platforms such as NoName057(16)’s DDoSia Project that provides volunteer hacktivists with a tool and tutorials on how to contribute their own resources to the cause, rewarding them with cryptocurrency. This “people’s DDoS” approach reflects an attempt to involve sympathizers in launching large-scale DDoS attacks against perceived enemies. KillNet distinguished itself by the scale and brazenness of its campaigns. In 2022, it declared an all-out assault on NATO countries, publishing long target lists (government websites, airports, financial institutions, etc.) and encouraging hackers to take them down. NATO, being the overarching symbol of the anti-Russia coalition, was a prized target. KillNet’s Telegram propaganda boasted of infiltrating NATO networks and “bringing down 40% of NATO’s infrastructure” via DDoS. No evidence supports this hyperbolic claim, but it still illustrates the strategy to use DDoS for psychological impact.

Tactics and Techniques

One reason attackers like DDoS is that it does not require breaching the target’s systems. Instead, it exploits the openness of services by crowding them out with fake traffic, which is easier and carries less risk of detection or direct retaliation.

Across all incidents, the tactics have remained relatively consistent, even as scale increased. Techniques, on the other hand, have undergone significant changes. While the 2014 hacktivists used crowdsourcing to perform manual browser attacks, the new generation of hacktivists relies on IoT botnets, bulletproof hosting services, crowd-sourced botnets and new attack vectors such as HTTP/2 rapid reset, CAPTCHA bypass and CAPTCHA-solving farms. Reflection and amplification attacks can now generate volumes of traffic ranging up to over five Terabits per second. DDoS attacks also often involve multiple vectors ranging from volumetric floods to overwhelm bandwidth, HTTP request floods to exhaust web servers and APIs, and more specialized targeting of DNS services to impact entire domains. Techniques such as source spoofing, carpet bombing and per-request proxy switching render detection and mitigation more difficult.

A key method in sustaining these attacks has been the recruitment of volunteers through Telegram and private forums. Attack organizers share URLs of NATO-related targets and user-friendly tools that less-skilled supporters can run to join the DDoS attack. This crowdsourced approach can drastically multiply the attacking power and muddle the source of the attack. Other hacktivists have been advertising DDoS-for-hire or booter/stresser services in exchange for free access to their services, targeting highly visible organizations and institutions, such as NATO.

In terms of timing, DDoS attacks are often synchronized with sensitive moments, such as the release of a summit communique or the commencement of a high-profile speech, with the aim of disrupting live streams or press Q&As. They are also repeated in waves: If a first wave is mitigated by defenses, attackers sometimes shift strategy and try again a day later, aiming to exploit any lapse in vigilance.

DDoS attacks often accompany or signal broader campaigns. It’s often a component of a larger strategy, either as a distraction while more covert hacks are attempted or as a public show of force to complement quieter espionage. NATO’s cyber defenders are well aware of this: a flurry of DDoS attacks can be a smokescreen for other activities. Thus, during summit DDoS incidents, NATO likely doubles its vigilance for any sign of concurrent stealthy breaches.

Conclusion

The pattern of DDoS attacks on NATO summits reveals a tug-of-war between attackers' intent to cause chaos and defenders' success in maintaining continuity. Adversaries have found DDoS attractive because it's immediate, attention-grabbing, and relatively low-risk – no need to pierce through firewalls or encryption when you can simply overload the front door. The actors, primarily pro-Russian hacktivists, see it as a digital battering ram to batter NATO's public image. They have refined their coordination, even as NATO has strengthened its shields.

For NATO, these incidents, although mostly not crippling, serve as a constant reminder of the hostile environment in which modern diplomacy operates. Summits now come with an expectation of background cyber noise. NATO's strategy has been to mitigate and communicate: mitigate the technical effects and message unity and resolve despite the attacks. In public, NATO often downplays the impact as "business as usual despite some cyber incidents", which denies attackers the full impact of fear or disruption they seek. Privately, NATO takes these events seriously as tests of its cyber defense integration among allies.

Going forward, the focus on DDoS in summit security planning is likely to remain high. There is an understanding that as long as NATO is involved in contentious issues, such as adding members or providing military support to contested regions, adversaries will attempt to disrupt its high-level gatherings via cyberspace. Future DDoS attacks may attempt to exploit new vulnerabilities. For instance, targeting mobile networks, summit venues or public transportation to disrupt delegates, or attacking third-party service providers (as seen when pro-Russian hackers disrupted satellite internet providers in other contexts). NATO's challenge will be to anticipate these shifts.

In conclusion, DDoS attacks on NATO summits over the past decade have been frequent but ultimately unsuccessful in achieving their strategic objectives, not because the attacks are unsophisticated or easy to stop, but because NATO has continually evolved its cyber resilience. The attacks serve as noisy propaganda tools for Russia and its sympathizers, and as drills for NATO's cyber defenders. As evidenced by summits proceeding smoothly despite "red" level cyber alerts, the Alliance's improved cyber resilience has thus far prevented DDoS from being anything more than an irritant. However, the trend highlights the evolving nature of hybrid warfare, where even a diplomatic summit is not immune to the ripples of conflict. NATO summits will likely continue to be accompanied by barrages of bits and bytes, as adversaries attempt to make digital thunder when they cannot directly stop NATO's decisions. The Alliance's goal will be to keep treating that thunder as background noise – heard but not allowed to disturb the course charted by its member nations in those critical meetings.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.