NERIUM

NATO summit 2025

A cyber security threat assessment for municipalities

Executive summary

- As the NATO Summit approaches, public institutions in the host country and municipalities in close proximity to the summit locations are experiencing an increased cyber threat environment, fuelled by state-sponsored actors, hacktivists, and cybercriminal groups.
- Historical data from previous summits reveal a pattern of cyber espionage, denial-of-service attacks, phishing campaigns, and disinformation efforts targeting government networks and public services.
- To mitigate these threats, a proactive, multi-layered security approach is essential. Key measures include enhancing cybersecurity hygiene among municipal employees, deploying advanced network monitoring and endpoint detection tools, and collaborating closely with national cybersecurity authorities and law enforcement agencies.
- Early warning signs - such as increased phishing attempts, unusual network activity, and social media disinformation - must be monitored to detect and thwart potential threats.
- The NATO Summit's high-profile nature increases the risk of public disruptions, targeted disruption, and extremist activity, necessitating enhanced protection of municipal infrastructure, coordinated crowd management, and close collaboration with law enforcement.
- In the recent days, the MIVD reported the first Russian cyber sabotage attempt in the Netherlands occurring in 2024, targeting a public service's digital control system. Although the attack was thwarted without causing damage, it underscores the escalating threat to municipal digital infrastructure.

Introduction

The upcoming NATO Summit in The Hague, scheduled for 24–26 June, 2025, will attract global attention, including world leaders, delegates, and media representatives. While the summit is a significant diplomatic event, it also presents heightened cybersecurity risks for municipalities in the surrounding area. This briefing outlines potential cyber threats, mitigation strategies, the importance of early warning mechanisms, and historical precedents to help the municipality prepare effectively.

Cyberthreats for municipalities

As the Netherlands prepares to host the upcoming NATO Summit, municipalities must be aware of an increasingly complex cyber threat landscape. Large-scale international summits have historically attracted the attention of state-sponsored actors, hacktivists, and cybercriminal organisations, all seeking to exploit vulnerabilities for espionage, disruption, or financial gain. The municipality, as a key logistical and administrative body, plays a crucial role in ensuring the security and continuity of essential public services while maintaining the resilience of its own digital infrastructure.

The municipality faces various cyber threats from state-sponsored threat actors, hacktivist groups, and opportunistic criminals. State-sponsored threat actors have a track record of conducting

cyber espionage, targeting government communication channels, municipal networks, and critical infrastructure. These operations typically aim to intercept sensitive diplomatic communications or disrupt local government functions, creating embarrassment or operational challenges for the host nation. Hacktivist groups, often motivated by geopolitical grievances or ideological agendas, may attempt to undermine trust in public institutions by defacing municipal websites, launching denial-of-service attacks, or leaking internal government data. In the lead-up to such actions, these actors frequently engage in covert reconnaissance – such as scanning for vulnerabilities, mapping infrastructure, or monitoring employee behaviour online – often using stealthy techniques that make early detection difficult. At the same time, cybercriminals are likely to exploit the heightened operational tempo surrounding the summit, targeting municipal employees and contractors with phishing campaigns, ransomware, and financial fraud.

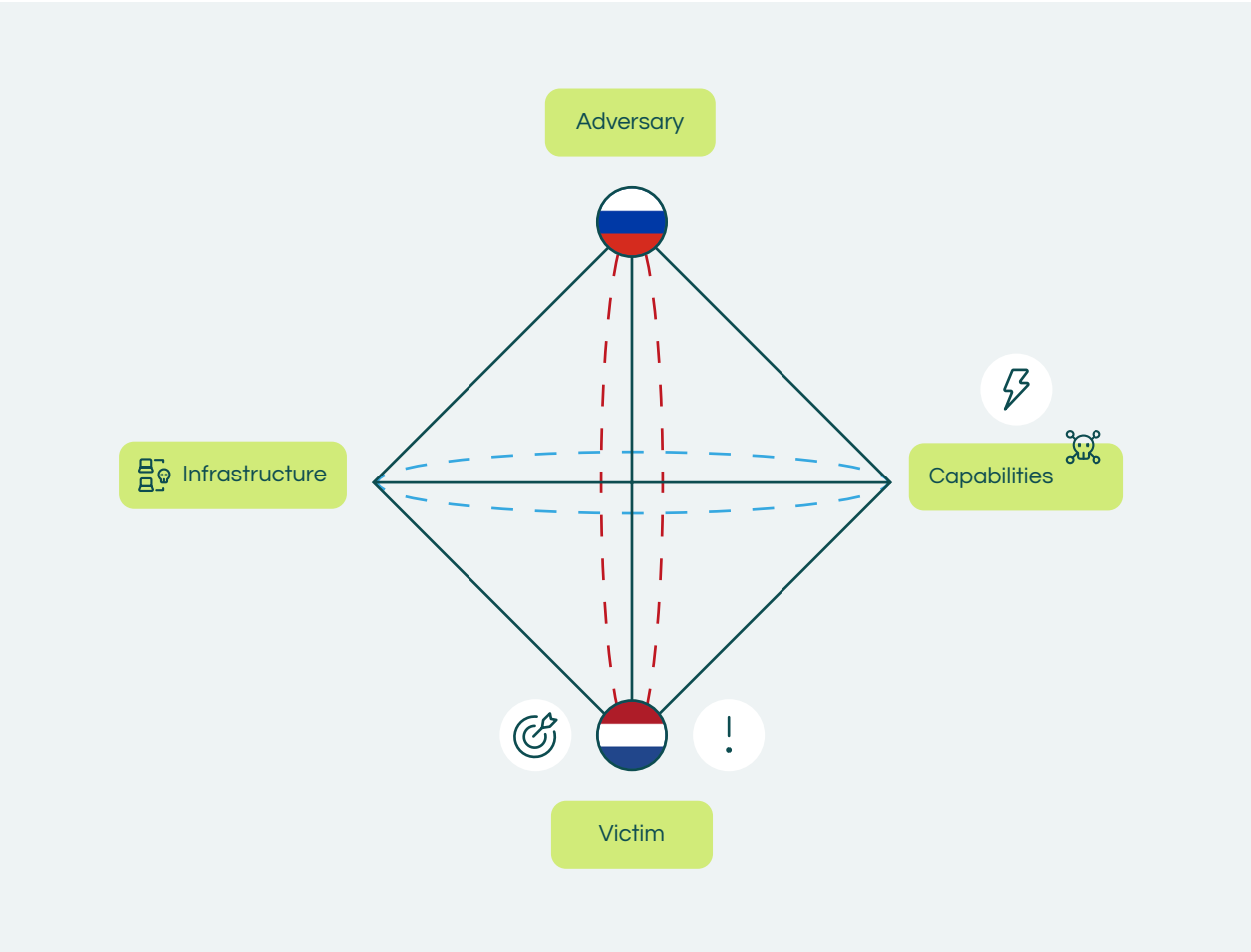
In the recent days, the MIVD reported the first Russian cyber sabotage attempt in the Netherlands, targeting a public service's digital control system. Which took place in 2024. Although the attack was thwarted without causing damage, it underscores the escalating threat to vital digital infrastructure.

Strengthening the municipality's cybersecurity posture begins with a layered defence strategy. Establishing sound cyber hygiene practices across departments provides the foundation for resilience. Tailored training for public servants and third-party vendors – focusing on phishing, manipulation tactics, and recognising abnormal online behaviour – helps prevent attackers from gaining an initial foothold. Deploying advanced tools such as endpoint detection and response (EDR) systems, alongside real-time network monitoring, enhances the municipality's ability to detect and contain threats swiftly. Partnerships with national and international authorities such as the NCSC-NL, ENISA and relevant law enforcement bodies can offer timely intelligence and strategic support.

On the operational side, identifying early signs of malicious activity is essential for preventing larger incidents. A noticeable increase in phishing messages masquerading as communications from NATO, EU, or Dutch government institutions could indicate adversary reconnaissance. Other red flags – such as heightened scanning of municipal infrastructure, repeated login attempts from foreign IP addresses, or unexpected data transfers – should prompt immediate investigation. To respond effectively, municipal IT teams must have clear, rehearsed response procedures in place, enabling decisive action before threats escalate.

Physical threats are also a significant concern. Large gatherings attract both organised and spontaneous protests, increasing the risk of public disorder, vandalism, and confrontations with law enforcement. There is also a latent threat from extremist actors who may view the summit as a symbolic high-value target. Key municipal assets – including administrative buildings, public transport nodes, emergency services, and critical infrastructure – must be assessed and protected accordingly. Effective crowd control, coordination with police, and visible deterrence measures will be essential in mitigating these risks.

Threat' s Diamond Model



Adversary

- **State-sponsored actors APT29 & other Russian afficiliated groups such as the Pro-Russian group NoName**
  - Motivations: Espionage, disruption, diplomatic embarrassment
- **Hacktivists - UAC-0118**
  - Motivations: Ideological or geopolitical grievances
- **Cybercriminals - Killnet**
  - Motivations: Financial gain (phishing, ransomware, fraud)

Capabilities

- **Cyber Espionage:** Interception of sensitive communications and data exfiltration
- **Website Defacement & DDoS:** Used by hacktivists to disrupt services and spread messages
- **Phishing:** Spoofed emails pretending to be from NATO or Dutch institutions
- **Reconnaissance:** Network scanning, vulnerability mapping and behavioral monitoring
- **Ransomware:** Encrypting files and demanding payment
- **Credential stuffing & brute force attempts:** Used to gain unauthorised access
- **Use of stealthy, low-noise tactics:** To evade early detection

Victim

- **Municipality:** Including internal networks and systems
- **Municipal employees and contractors:** Targeted via phishing or social engineering
- **Public-facing services and websites:** Subject to defacement or disruption
- **Critical infrastructure tied to the municipality:** Utilities, emergency services, and transportation
- **Digital trust in public institutions:** Undermined through public-facing attacks or leaks

---

Infrastructure

- **Spoofed or hijacked domains:** used to mimic NATO or government communications
- **Botnets and DDoS infrastructure:** employed to launch denial-of-service attacks
- **Malicious email infrastructure:** for the delivery of phishing campaigns
- **Command-and-control servers:** enabling remote access and data exfiltration
- **Dark web platforms and Telegram groups:** used for coordination, reconnaissance, or the sale of stolen data

---

Threat History

Past NATO, EU, and UN summits provide valuable lessons regarding the nature of cyber threats ahigh-profile events:

2023 NATO Summit (Vilnius, Lithuania)

a. Killnet and pro-Russian actors launched DDoS attacks on government portals. Source 1, source 2

b. GPS spoofing and jamming in the Baltic region reported around summit dates. Source 1

2025 Provinces and municipalities (Netherlands)

a. DDoS-attacks against Dutch Provinces and municipalities by pro-russian actor 'NoName'. Source

2022 & 2025 EU Summit (Brussels, Belgium)

a. APT 29 conducting targeted phishing campaigns against EU Commission staff. Source 1

b. Credential harvesting linked to APT groups. Source 2

2021 UN General Assembly (New York) Source

a. Disinformation campaigns targeting social media, especially around international UN-led initiatives (e.g. Covid 19 policy)

b. Disinformation operations surged, with fake social media profiles spreading mis-leading content to undermine public trust and discredit policymakers.

2018 OPCW Incident
(The Hague, Netherlands) Source

a. Russian GRU operatives attempted to hack into the OPCW's Wi-Fi network to access sensitive data on chemical attack investigations.
b. Dutch MIVD disrupted the operation, apprehended the operatives, and expelled them, highlighting the ongoing threat of cyber espionage against international organisations.

Recommendation

A. Technical Controls

- Patch vulnerabilities promptly; prioritise external-facing services.
- Implement geo-fencing or rate-limit access from high-risk regions.
- Deploy DDoS protection and Web Application Firewall (WAF) rules tailored to current threats.
- Endpoint Detection and Response (EDR) with Indicators of Compromise (IOC) updates from threat intelligence feeds.
- Implement custom detection content (e.g. SIEM correlation rules, YARA signatures, EDR threat hunting queries) tuned to summit-related threat activity – such as anomalous access patterns, DDoS staging behaviour, or summit-themed phishing lures – to enhance early warning capabilities.
- Retain Wi-Fi authentication and session logs for a minimum of 180 days

B. Operational Readiness

- Freeze non-essential system changes during summit week.
- Review and test incident response plans and communications protocols.
- Ensure critical personnel are on-call and aware of escalation procedures.
- Isolate or actively monitor high-value assets (e.g. identity providers, DNS).

C. Staff Awareness

- Conduct a rapid awareness refresh on phishing and social engineering.
- Simulated phishing tests prior to the event.
- Clearly communicate reporting channels for suspicious activity.

D. Threat Intelligence & Coordination

- Subscribe to updates from NCSC-NL, Europol EC3, and NATO CERT.
- Coordinate with regional cybersecurity coalitions or CERTs for real-time intelligence sharing.
- Consider tabletop exercises or red team simulations before the summit to test resilience.

MITRE ATT&CK Mapping for Threats to Municipality During NATO Summit

Tactic	Technique	Technique ID	Description
Reconnaissance	Search Open Websites / Domains	T1596.001	Scanning municipal infrastructure, open ports, or public resources.
	Search Victim-Owned Websites	T1596.002	Scanning municipal websites for vulnerabilities or outdated plugins.
	Gather Victim Identity Information	T1589	Profiling municipal employees for phishing and impersonation.
	Gather Victim Network Information	T1590	Identifying IP ranges and external services to target.
Initial Access	Phishing: Spearphishing Attachment	T1566.001	Delivering malware via malicious attachments.
	Phishing: Spearphishing Link	T1566.002	Linking to credential capture or malware-hosting pages.
	Drive-by Compromise	T1189	Compromising users via malicious web content.
Execution	Malicious File Execution	T1204.002	Executing payloads when attachments or links are opened.
	Command and Scripting Interpreter	T1059	Using PowerShell, Bash, or similar tools to run attacker commands.
Persistence	Create Account	T1136	Adding local or domain accounts for ongoing access.
	Valid Accounts	T1078	Using stolen credentials to maintain access.
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Exploiting vulnerabilities to gain higher privileges.
Defense Evasion	Obfuscated Files or Information	T1027	Encoding or encrypting payloads to avoid detection.
	Masquerading	T1036	Impersonating legitimate software or processes.
Credential Access	Phishing for Credentials	T1566.002	Harvesting login details via deceptive emails.
	Brute Force	T1110	Trying common or leaked credentials to gain access.
Discovery	Network Service Scanning	T1046	Identifying active services, ports, and protocols.
	System Information Discovery	T1082	Enumerating OS, hardware, and software information.
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001	Using RDP for lateral movement within the network.
	Remote Services: SMB	T1021.002	Moving through the network via file sharing services.

Collection	Data from Local System	T1005	Extracting files and data from infected hosts.
	Screen Capture	T1113	Capturing visuals of sensitive information on screens.
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Using HTTP/S for communication with C2 servers.
	Encrypted Channel	T1573	Hiding traffic via SSL/TLS to avoid detection.
Exfiltration	Exfiltration Over C2 Channel	T1041	Sending data out through existing C2 links.
	Exfiltration Over Web Service	T1567.002	Uploading stolen data to cloud services (e.g., Dropbox, OneDrive).
Impact	Data Encrypted for Impact (Ransomware)	T1486	Encrypting municipal systems to demand ransom.
	Defacement	T1491	Altering websites to spread political or ideological messages.
	Service Stop	T1489	Disrupting services by shutting down processes.
	Network Denial of Service	T1499	Disrupting availability via DDoS-style attacks.

Nerium is a cybersecurity company specialising in monitoring, detecting, and responding to digital attacks. Our specialists have years of experience in digitally protecting organisations and recovering from large-scale cyber incidents. Nerium is a 100% independent Dutch company based at the High Tech Campus in Eindhoven.

Nerium B.V.
High Tech Campus 9
5656 AE Eindhoven
Netherlands

E-mail: Info@nerium.nl
Website: nerium.nl
Phone +31 (0) 8 548 958 57
24/7 Hotline: +31(0) 800 0699
KVK: 89366891
POB number: 8467