Securing the Backbone:

Defending Peering Networks Against DDoS, Blackholing Risks, and VPN Threats

Yolandi Cloete
Interconnection Community & Academy Manager

DE CIX

Security in Peering Environments

Importance

What is it? Security in peering refers to the measures and controls implemented to protect the interconnected networks that exchange traffic directly. It involves safeguarding routing protocols, access controls, and data integrity between peers.

Peering enables efficient, low-latency data exchange and greater control over traffic routing, improving network performance and reducing costs.

Security is vital to maintain service availability, data confidentiality, and trust between peering partners.

What if the attacker is already inside your peering relationship?

2024 Cyber Security Events

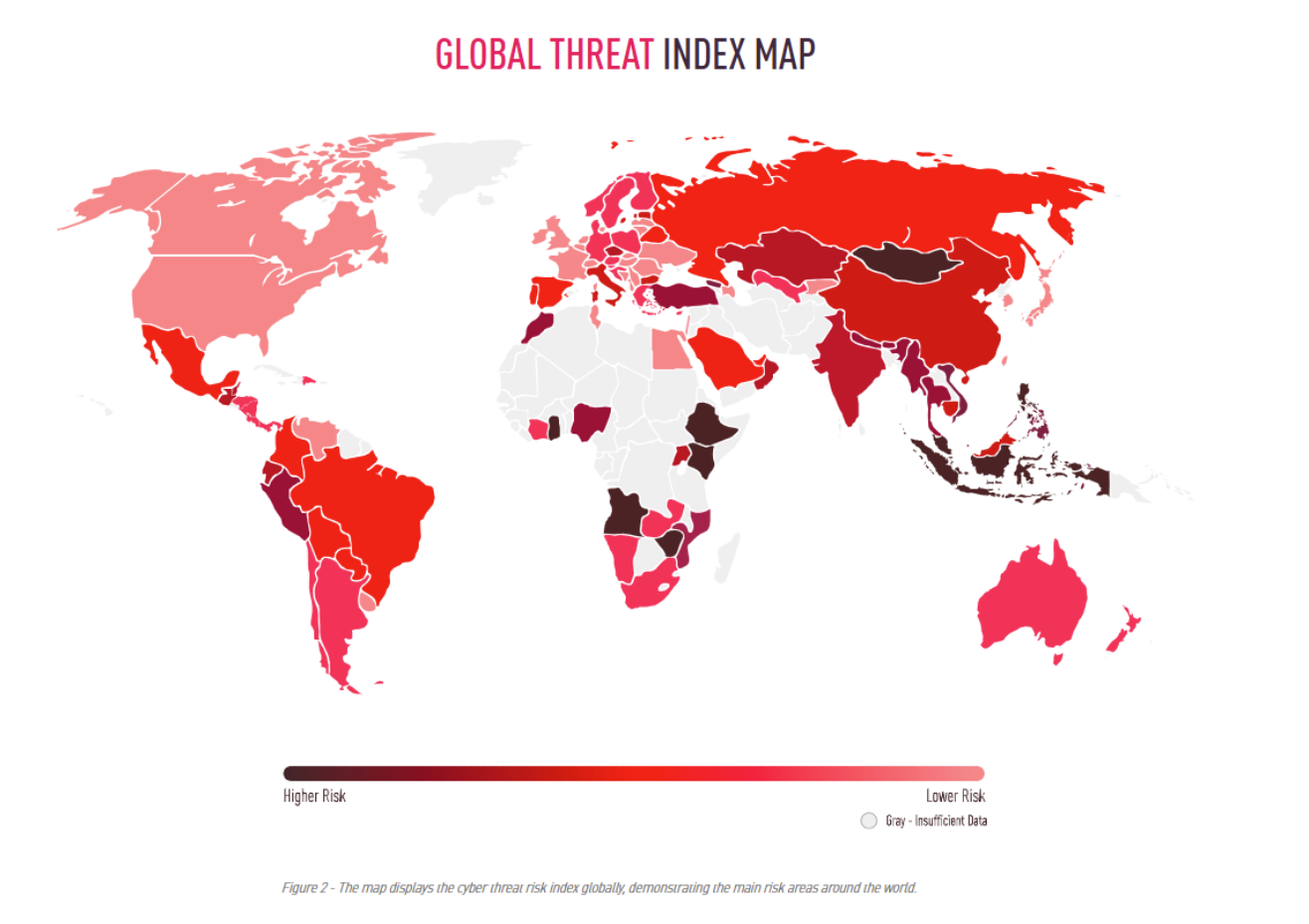


Figure 2 - The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.

2024 Cyber Security Events

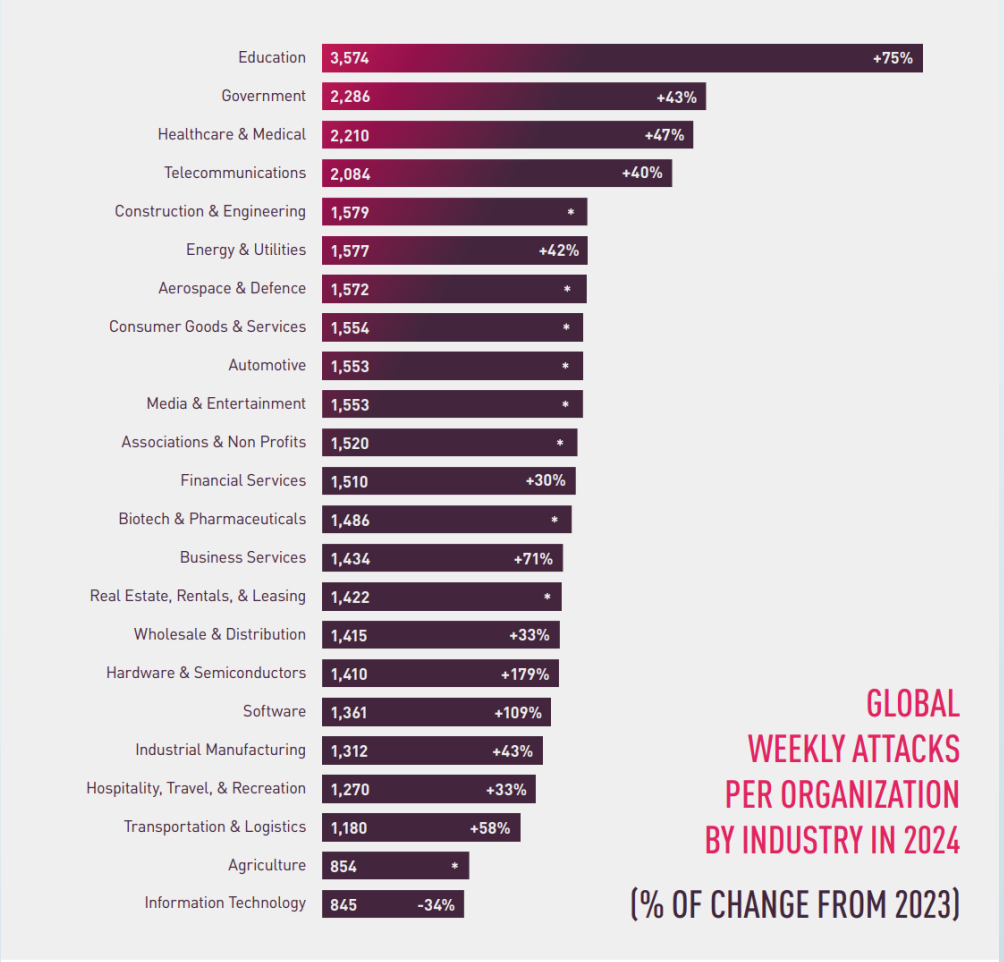


Figure 3 - Global average of weekly attacks per organization by industry in 2024 [% of change from 2023].
[*] Newly introduced sectors which were not part of the previous report.

Cyberattacks in the Baltics

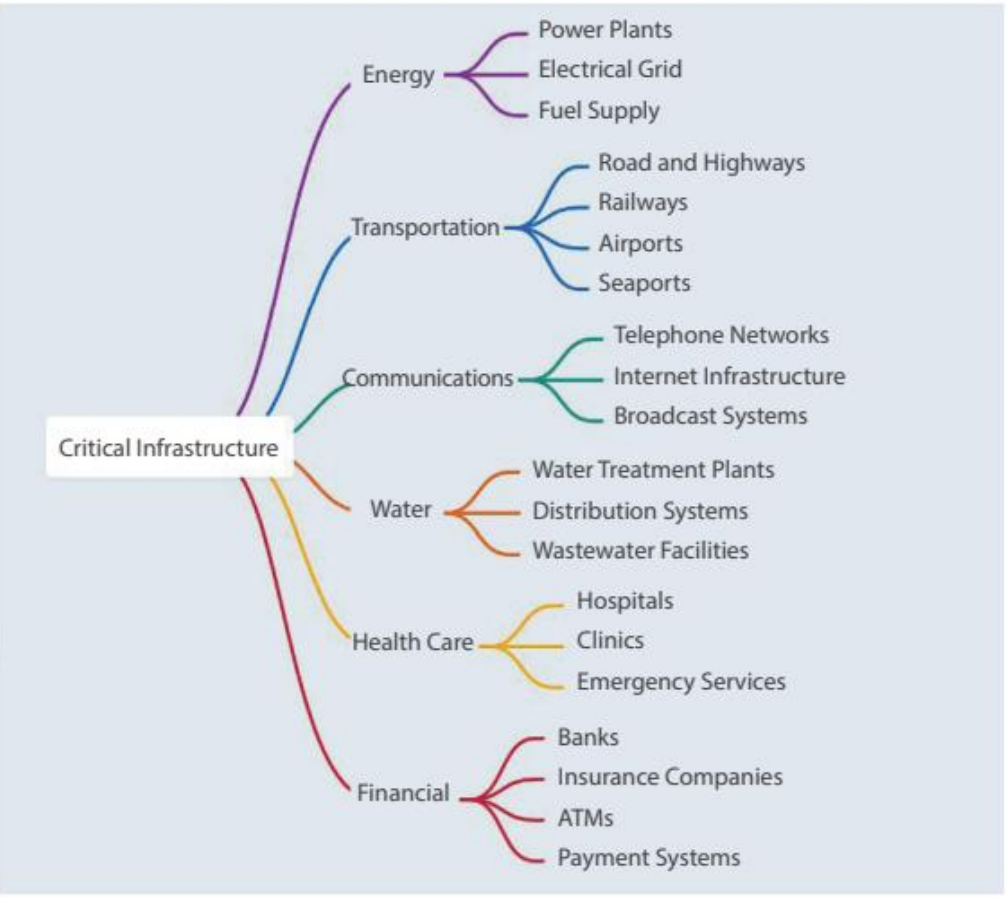


Figure 1. Critical infrastructure sectors and their components

According to the National Cyber Security Centre:

‘There had been an increase in targeting of the region ranging from ransomware to sophisticated state sponsored attacks.’

‘The most targeted sectors are energy, especially oil and gas, transportation sector, including maritime and aviation, and communication networks.’

DDoS Attacks in Peering

What is it? A Distributed Denial of Service (DDoS) attack is a malicious attempt to overwhelm a network or service by flooding it with excessive traffic from multiple sources, causing disruption or downtime.

Risks

- Overwhelmed peering links lead to network downtime and service degradation.
- Collateral damage to other networks sharing peering infrastructure.
- Increased operational costs due to mitigation efforts and potential SLA penalties.

DDoS Attacks in Peering

Real-World Example: Crypto Sector Under Siege

- In Q2 2025, Cloudflare mitigated over 6,500 hyper-volumetric DDoS attacks, averaging 71 per day.
- One notable incident involved a crypto exchange targeted during a major token launch, causing multi-hour outages and $12M in trading losses.
- Attackers exploited Layer 7 (HTTP) vectors to mimic legitimate traffic, bypassing basic defenses.

MAKE SLIDE INTERESTING

DDoS Attacks in Peering

Real-Life Examples & Impact

1. **Dyn DNS Attack (2016):** Disrupted major websites globally.
2. **GitHub DDoS Attack (2018):** Massive attack mitigated quickly but demonstrated threat scale.

Business Impact: Loss of revenue (network downtime costs businesses $5,600+ per minute on average), customer churn, and reputational damage.

Network Impact: Congestion, increased latency, and potential overload of mitigation resources.

Layered defenses and collaboration are your best shields.

DDoS Attacks in Peering

What is the motivation?

1. Employees
2. Customers
3. Litigations
4. Disgruntled Hackers

1. Reputational Damage
2. Operations are halted
3. Decrease in sales

1. Political Organizations
2. Terrorists

1. Cloaking other hacking efforts (Distraction)
2. Used to prevent companies from warning customers of fraud, etc.

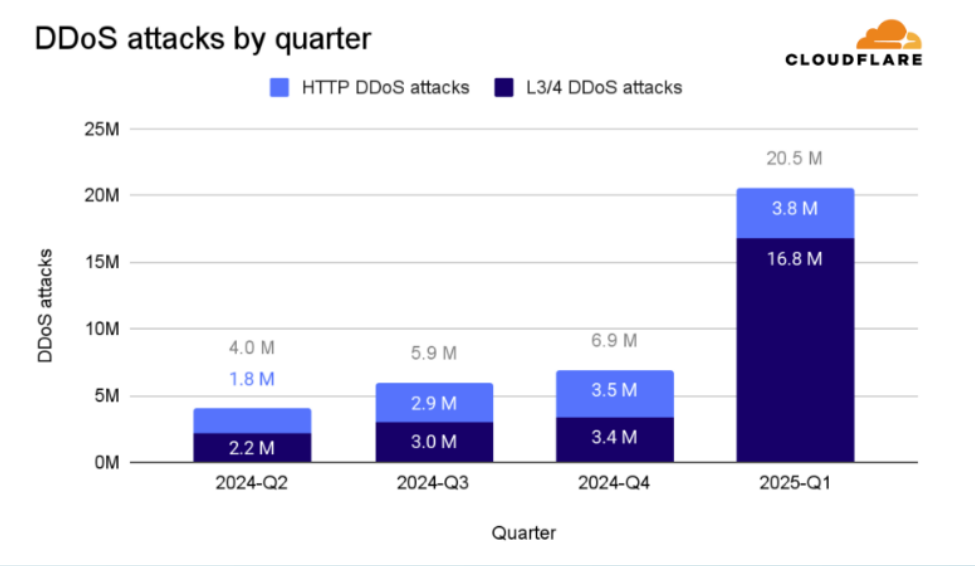
There are three common types of DDoS attacks:

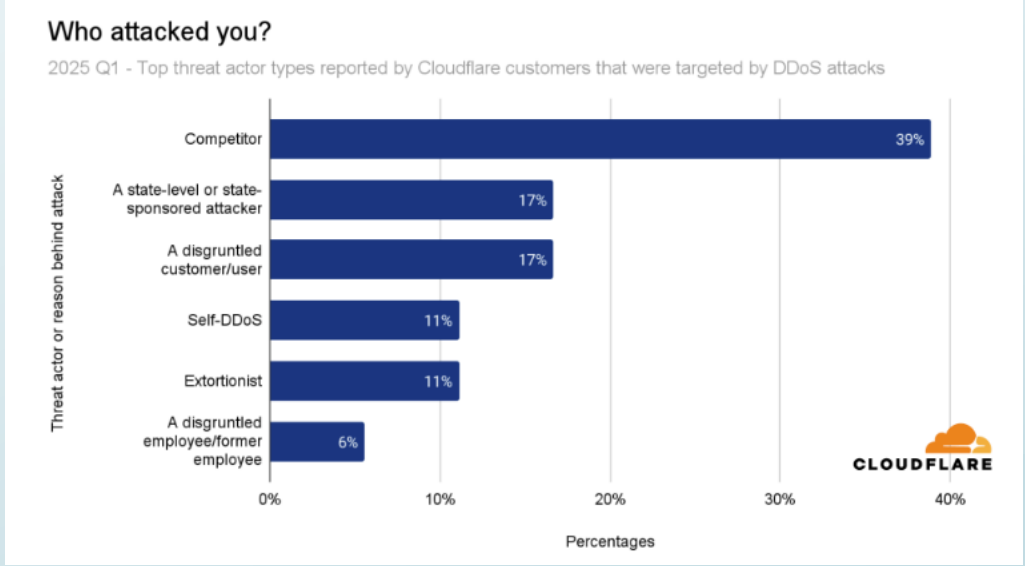
- Volumetric (Gbps)
- Protocol (pps)
- Application layer (rps) attacks.

DDoS Attacks in Peering

Stats & Trends

- 27.8 million DDoS attacks blocked in the first half of 2025 — **already 130% of all attacks in 2024**.
- 358% year-over-year increase in attack volume in Q1 2025.
- DNS-layer attacks surged by 876%, and HTTPS floods now account for 21% of all DDoS traffic.

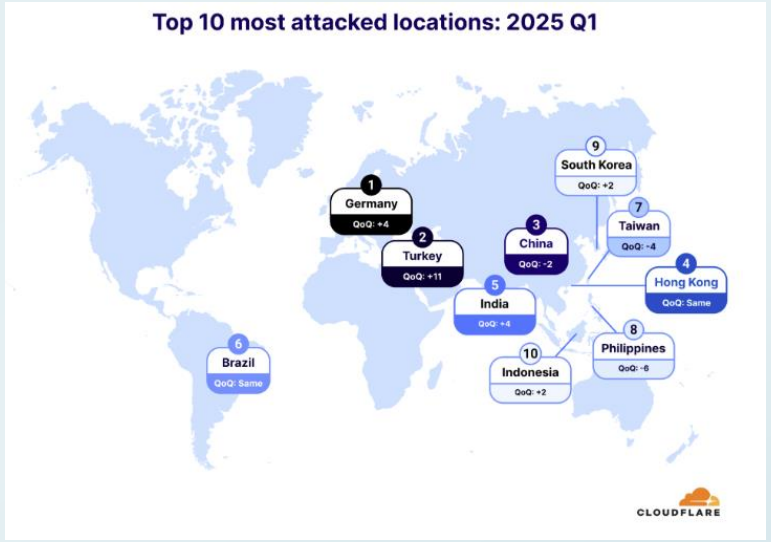


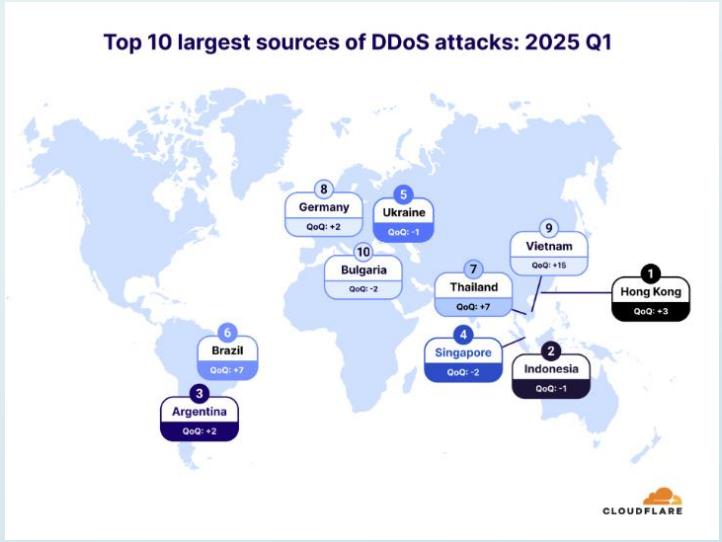


DDoS Attacks in Peering

Emerging Trends to Watch

- AI-generated DDoS traffic (mimicking human behaviour)
- Attacks on BGP sessions themselves
- DDoS-for-hire services becoming more sophisticated
- IPv6-based DDoS vectors

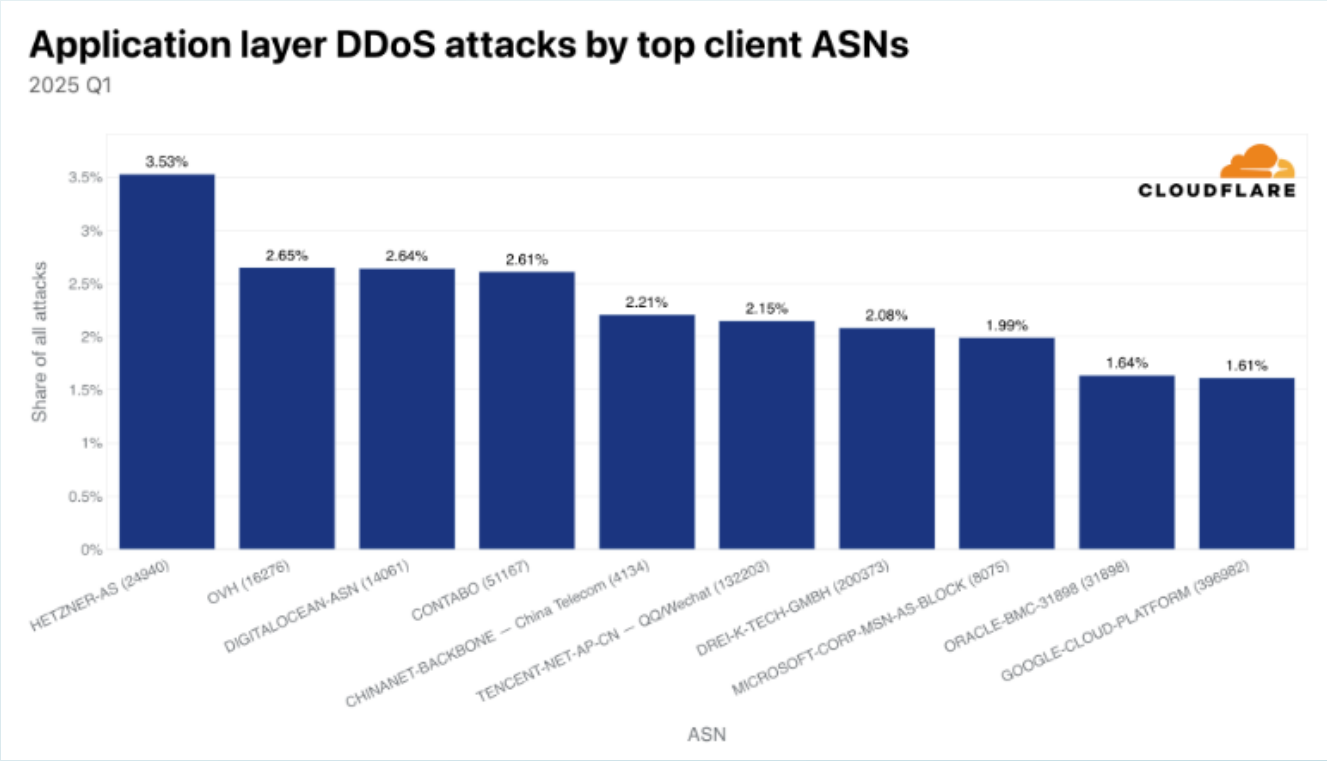




Tomorrow's attacks won't look like yesterday's.

DDoS Attacks in Peering

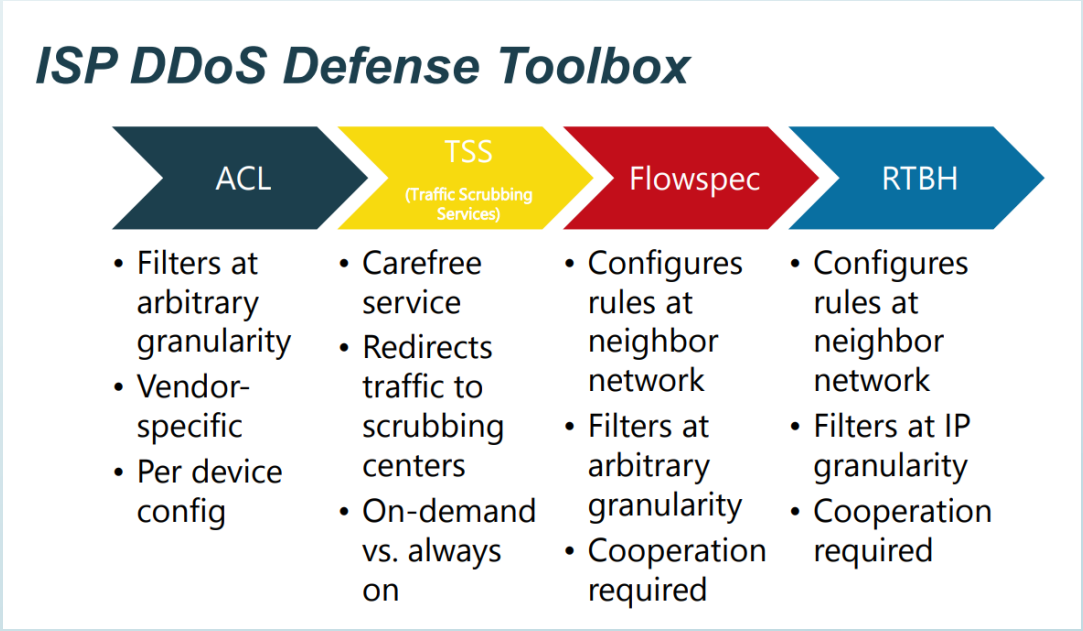
When looking at where the DDoS attacks originate from, specifically HTTP DDoS attacks, there are a few autonomous systems that stand out.



DDoS Attacks in Peering

Key Considerations

- Multi-layered DDoS defenses and early detection.
- Collaboration with upstream providers and peers.
- Investment in scalable mitigation infrastructure.



Advanced Blackholing

What is it? Blackholing is a network defense technique where traffic destined for a targeted IP address or prefix is dropped (sent to a “black hole”) to mitigate DDoS attacks.

Advanced blackholing allows for more granular and selective filtering - this advanced method allows selective filtering of malicious traffic based on protocols, ports, and packet headers — preserving legitimate traffic and improving mitigation accuracy.

How It Works

1. **Detection:** Anomaly detection systems identify malicious traffic patterns.
2. **Trigger:** A blackholing request is sent via API or portal.
3. **Filtering:** DE-CIX hardware filters traffic based on Layer 2–4 attributes (e.g., MAC, IP, TCP/UDP ports).
4. **Telemetry:** Real-time visibility into dropped traffic and attack behavior.
5. **Recovery:** Once the attack subsides, filtering is lifted automatically or manually.

Advanced Blackholing

Why it’s different

Traditional Blackholing	DE-CIX Advanced Blackholing
Drops all traffic to prefix	Filters by protocol, port, and prefix
Manual Activation	Automated triggers via telemetry
High collateral damage	Minimal impact on legitimate traffic
No visibility	Real-time monitoring and analytics
Peer-dependent	Hardware-based, peer-independent

Precision and automation in blackholing can save your network and your customers.

VPN Encryption in Peering

What is it? VPN (Virtual Private Network) encryption secures data traffic between peered networks by creating an encrypted tunnel, ensuring confidentiality and integrity of exchanged data.

Importance

- VPNs protect data confidentiality and integrity between peered networks.
- Critical for compliance and securing sensitive inter-network traffic.

Risks

- Weak or outdated encryption exposes data to interception.
- VPN endpoints can be targeted for attacks, including DDoS.
- Misconfigurations may allow unauthorized access.

VPN Encryption in Peering

Real-Life Examples & Impact

- Colonial Pipeline Attack (2021): Compromised VPN credentials led to ransomware, causing fuel shortages and economic disruption.

- Brute-Forced VPN Access: Resulted in lateral movement and data breaches.

Business Impact: Direct financial losses, regulatory penalties, reputational damage.

Network Impact: Service outages, compromised network integrity, increased remediation **costs.**

VPN Encryption in Peering

Key Considerations

- Use strong encryption standards (AES-256, IKEv2).
- Enforce multi-factor authentication and strict access controls.
- Regular patching and monitoring of VPN endpoints.
- Network segmentation to limit exposure.

Strong encryption, MFA, and vigilant monitoring are non-negotiable.

Securing the Backbone in the Baltic Region

Why It Matters

- The Baltic states are strategic digital gateways between Western Europe and Eastern networks.
- Peering infrastructure here is critical for resilience, especially amid rising hybrid threats and geopolitical tensions.

Regional Trends

- Estonia leads in **digital governance**, but all Baltic states face **Russian-linked cyber threats**.
- Increasing use of **hybrid warfare tactics**, blending cyber attacks with disinformation and kinetic threats.
- Fragmented **incident response coordination** across borders.

Securing the Backbone: Strategic Actions

1. **Layered DDoS defences** at peering points and IXPs.
2. **Advanced blackholing** with automation and telemetry.
3. **BGP monitoring tools** like BGPStream and Cloudflare Radar.
4. **Regional CTI sharing platforms** and joint cyber exercises.
5. **Zero-trust architectures** and endpoint hardening for VPNs.

In the Baltic region, securing the backbone isn't just about uptime — it's about sovereignty, stability, and trust in the digital age.

Engineer’s Toolkit for Peering Security

Category	Tools & Platforms
DDoS Mitigation	**Cloudflare Magic Transit** – Combines DDoS protection with BGP hijack detection . **Arbor Networks APS** – Widely used in IXPs for high-volume attack mitigation. **Radware DefensePro** – Behavioral-based DDoS detection and mitigation. **NetIX Smart Blackholing** – Automated blackholing based on traffic thresholds **DE-CIX Advanced Blackholing** – Fine-grained filtering by protocol, port, and prefix

Engineer’s Toolkit for Peering Security

Category	Tools & Platforms
BGP Monitoring	**BGPStream** – Open-source tool for real-time BGP anomaly detection. **Cisco Crosswork Cloud Network Insights** – Formerly BGPmon; monitors route anomalies and hijacks. **Kentik** – Offers traffic analytics and BGP anomaly detection with compliance insights. **Site24x7** – Cloud-based hybrid monitoring with BGP, NetFlow, and SNMP support. **ManageEngine OpManager** – Tracks BGP sessions and alerts on route instability

Engineer’s Toolkit for Peering Security

Category	Tools & Platforms
VPN Hardening & Endpoint Security	**Cisco AnyConnect** – Enterprise-grade VPN with endpoint posture checks. **OpenVPN + MFA** – Lightweight and secure with multi-factor authentication. **Microsoft Defender for Endpoint** – Integrates VPN security with threat detection. **CISA/NIST Guidelines** – Use as a checklist for VPN configuration best practices.

Engineer’s Toolkit for Peering Security

Category	Tools & Platforms
Threat Intelligence Sharing & Collaboration	**MISP (Malware Information Sharing Platform)** – Open-source CTI sharing platform. **Cybercation** – Baltic-Nordic initiative for cross-border cybersecurity collaboration. **CyberBazaar** – Baltic-focused platform showcasing cybersecurity innovations and partnerships . **NKSC Lithuania CTI Framework** – National-level CTI sharing and incident coordination

Engineer’s Toolkit for Peering Security

Category	Tools & Platforms
Threat Detection	**FastNetMon** – Real-time DDoS and anomaly detection using NetFlow/sFlow. **ARTEMIS** – BGP hijack detection and mitigation automation. **MANRS (Mutually Agreed Norms for Routing Security**) – Best practices and monitoring for routing security. **UnderDefense MAXI** – AI-native XDR platform with rapid containment and integration. **Cynet 360 AutoXDR** – Unified detection across endpoints, networks, and users. **LogRhythm NextGen SIEM** – Advanced analytics and automated threat response. **Rapid7 InsightIDR** – Detects lateral movement and insider threats.

Engineer’s Toolkit for Peering Security

Category	Tools & Platforms
DDoS Mitigation	Cloudflare Magic Transit, Kentik RTBH, DE-CIX Advanced Blackholing, Arbor Networks APS, Radware DefensePro
BGP Monitoring	BGPStream, Cisco Crosswork, Cloudflare Radar, Kentik, Site24/7, ManageEngine OpManager
VPN Hardening	Cisco AnyConnect, CISA/NIST Guidelines, OpenVPN & MFA, Microsoft Defender for Endpoint
Threat Detection	FastNetMon, ARTEMIS, MANRS, UnderDefense MAXI, Cynet 360 AutoXDR, LogRhythm NextGen SIEM, Rapid7 InsightIDR
Community & Learning	RIPE, NANOG, DE-CIX Academy, MISP, Cyberaction CyberBazaar, NKSC Lituania CTI Framework

Summary & Recommendations

- Peering enhances performance and reduces costs but introduces security and operational risks that can severely impact business and network health.
- Proactive security measures and collaborative mitigation strategies are essential to protect peering infrastructure.
- Real-world incidents illustrate the high stakes: downtime costs, reputational damage, and regulatory consequences.
- Investing in strong authentication, precise blackholing, layered DDoS defenses, and robust VPN encryption safeguards both network integrity and business continuity.

Thank You!

Email: yolandi.cloete@de-cix.net

Yolandi Cloete
Interconnection Community & Academy Manager

DE CIX