# DDoS Landscape

# 2026

## GEANT Project Task Member View

*Detection · Mitigation · MARnet Deployment · Collaboration*

Detect | Mitigate | Deploy | Collaborate

GEANT Security Days 2026 | Presented by Vladislav Bidikov — vladislav.bidikov@finki.ukim.mk

# Agenda

## 01 Detection Landscape

NeMo · fastnetmon · akvorado · ntopng · Kentik · Nokia Deepfield

## 02 Mitigation Landscape

FOD · NeMo · nScrub · Flowspec · A10 · Nokia Deepfield Enforcer

## 03 New Players

prefixd and emerging tools

## 04 MARnet 2026 Deployment Plan

Full detect + mitigate stack · Klasus · Flow replication

## 05 Challenges & Things to Learn

Traffic diversion at speed: VRF · BGP Community · Other

## 06 Network ↔ Security Collaboration

Rebuilding the bridge we seem to have lost

DETECTION

# Detection Tools Landscape

## NeMo

Open Source

Network Monitoring developed within GEANT. Anomaly detection, flow analysis and alerting across NREN infrastructure.

## fastnetmon

Open Source

Ultra-fast DDoS detection via NetFlow, sFlow, IPFIX and mirror ports. Fires mitigation triggers within seconds.

## akvorado

Open Source

Rich flow collector with ClickHouse storage and Grafana dashboards. Excellent for long-term trending and capacity planning.

## ntopng

Open / Comm.

Network traffic monitoring with DPI, flow collection and historical analysis. Feature-rich web interface for operators.

## Kentik

Commercial

Enterprise network observability SaaS. Full-stack visibility, DDoS detection, BGP analytics and threat intelligence feeds.

## Nokia Deepfield

Commercial

Real-time flow telemetry analysis at full network scale. DDoS fingerprinting, traffic intelligence, and ISP/NREN-grade visibility.

Nokia

**Also seen in the NREN community:**

Arbor / NETSCOUT | Corero SmartWall | Cisco Stealthwatch | SCION-base

MITIGATION

# Mitigation Tools Landscape

## GEANT FOD

Flowspec

GEANT portal for pushing BGP Flowspec rules upstream. NRENs can black-hole or rate-limit attacks at the GEANT backbone.

## NeMo Mitigation

Scrubbing

NeMo's mitigation modules complement its detection engine. Scrubbing integration and automated response for NREN infrastructure.

## nScrub

Scrubbing

Open-source scrubbing solution for NRENs. Traffic diversion and cleaning at scale, integrating with fastnetmon and BGP communities.

## Flowspec

Flowspec

BGP extension distributing traffic filter rules. IPv4, IPv6, VPN flavours. Provider-side filtering via standard BGP sessions.

## A10 & Hardware

Hardware

A10 TPS and similar appliances deliver highest-throughput cleaning. Used by large NRENs. See Security Days 2025 talk for details.

## Nokia Deepfield Enforcer

Commercial

Works alongside Nokia Deepfield analytics to push surgical BGP/Flowspec mitigation rules. Integrates with scrubbing centres for precision filtering.

**Also seen in the NREN community:**

Radware DefensePro | Cloudflare Magic Transit | Arbor APS / Sightline | F5 DDoS P

NEW PLAYERS

# Emerging Tools & New Entrants

## prefixd

OPEN SOURCE | EARLY STAGE

*github.com/lance0/prefixd*

A daemon focused on prefix-based traffic handling and policy enforcement at the data plane. Designed for high-speed environments where per-prefix routing decisions must be made in real time — filling a gap between coarse RTBH and full scrubbing.

*Early development — evaluate carefully before production use*

## Watch This Space

- eBPF-based mitigators at high speed
- Cloud-native scrubbing (hyperscalers)
- AI/ML-driven anomaly detection
- BGP community automation frameworks
- NREN toolsharing via GEANT task forces

MARNET 2026

# MARnet Planned Deployment (2026)

## DETECTION

### NeMo
Primary anomaly detection + alerting

### fastnetmon
High-speed flow-based DDoS trigger

### ntopng
Visibility, DPI, historical analysis

**Flow Replication Required**

NetFlow must reach all detection tools. Evaluating: NetFlow → ClickHouse pipeline

## MITIGATION

### nScrub
Traffic scrubbing / cleaning

### NeMo Mitigation
Automated response workflows

### FoD (Flowspec)
GEANT upstream flowspec filtering

### Klasus
Flowspec – FCSE/UKIM local project

LOCAL PROJECT

CHALLENGES

# Things We Need to Learn

## Key Challenge: Traffic Diversion at High Speed

### VRF-based Diversion

PROVEN

- Dedicated VRF for the scrubbing path
- Clean traffic re-injected via GRE or MPLS
- Works with existing routing infra
- Complexity grows at high throughput

### BGP Community Signaling

COMMON

- Tag attack traffic via BGP communities
- Upstream provider diverts to scrubbing PoP
- Multiple standards: RTBH, RFC 7999…
- Requires pre-agreed provider setup

### Other Approaches?

EXPLORE

- MPLS-TE traffic engineering
- Policy Based Routing (PBR)
- OpenConfig / Segment Routing
- Need to test at full NREN scale

COLLABORATION

# Network & Security: We Need Each Other

*"We seem to have lost some of the collaboration between Network and Security teams."*

## Network Team Brings

- Routing architecture & AS topology knowledge
- BGP policy enforcement capabilities
- Traffic engineering & capacity planning
- Router/switch access for diversion setup
- ISP / upstream peering relationships

## Security Team Brings

- Threat detection & attack pattern recognition
- Flow analysis and anomaly baselines
- Mitigation tooling knowledge & operations
- Incident response procedures
- Vulnerability & risk context for prioritization

# Summary & Call to Action

### Detection ecosystem is maturing

NeMo, fastnetmon, akvorado, ntopng cover the open-source spectrum. Kentik and Nokia Deepfield for commercial-grade observability and analytics.

### Mitigation options are diverse

FOD/Flowspec for upstream, nScrub + NeMo for scrubbing, Nokia Deepfield Enforcer for automated BGP enforcement. A10 and hardware for scale.

### MARnet deployment in progress

Full detect + mitigate stack planned for 2026. Klasus (local Flowspec, FCSE/UKIM) adds homegrown capability alongside GEANT FOD.

### Traffic diversion is our homework

VRF, BGP communities, and other methods need hands-on evaluation and testing at NREN speed and scale.

### Rebuild Network ↔ Security collaboration

Effective DDoS mitigation requires both teams at the table. Let's make this happen formally at GEANT level.