

Networks that speak your LANGUAGE

# IP Trends in Internet, Digitalization, Big Data Analytics Security, and AI

Ivo Lansky

Snr. Director, Central/East Europe, Türkiye and Central Asia

Nokia IP Business, Networks Infrastructure

**NOKIA**

9<sup>th</sup> November 2023

Ashgabat, Turkmenistan

# Internet & IP Peering Trends in Europe and Central Asia

## Traffic Growth

- Europe – East Asia (25 Tbps)
- Network Designs (10 / 100 / 400 / 800 GE), Leaf / Spine / Chassis, ...

## Geopolitical Factors

- Public Peering common in both West and East Europe ...  
... but Central Asia countries still mostly regulated and w/ private peerings only
- ~50% Europe - Asia Internet traffic routed via Central Asia / Kazakhstan & Russia

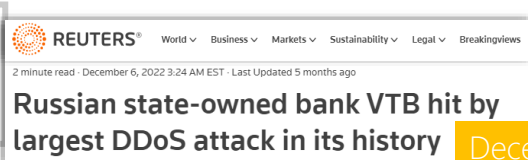
## Security

- Big Data DDoS Analytics and Auto-mitigation
- Secure Boot, IPSec/Security, Quantum Safe MACsec / ANYsec Encryption

# DDoS spares no one – targeting all Network/services/customer segments



**UK government assess Russian involvement in DDoS attacks on Ukraine**



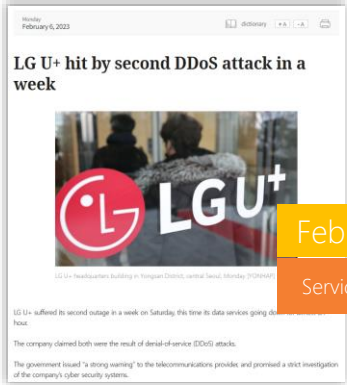
**Russian state-owned bank VTB hit by largest DDoS attack in its history**

December 6  
Customers



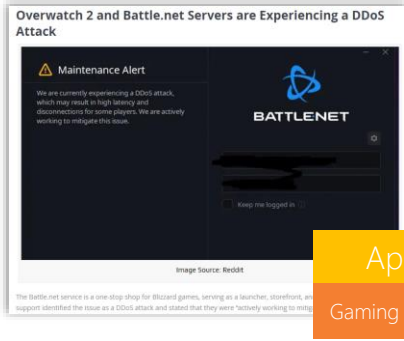
**Hackers infect TP-Link router firmware to attack EU entities**

May 16  
Customers



**LG U+ hit by second DDoS attack in a week**

February 6  
Service provider



**Overwatch 2 and Battle.net Servers are Experiencing a DDoS Attack**

April 8  
Gaming company



<https://www.bleepingcomputer.com/news/security/hackers-infect-tp-link-router-firmware-to-attack-eu-entities/>



<https://koreajoongangdaily.joins.com/2023/02/06/business/industry/Korea-LG-U-DDoS/20230206175514381.html>

<https://thenerdstash.com/overwatch-2-ddos-attack-blizzard-servers-down/>



**Worst cyberattack in Greece disrupts high school exams, causes political spat**

May 30  
Education



**IOTW: Russian hackers target NATO sites with DDoS attack**

February 17  
Government sites



**DDoS attacks strike Indian airports. Here's how the threat was mitigated**

April 16  
Critical infra



<https://ciso.economictimes.indiatimes.com/news/cyber-crime-fraud/ddos-attacks-strike-indian-airports-heres-how-the-threat-was-mitigated/99461876>

<https://abcnews.go.com/International/wireStory/worst-cyber-attack-greece-disrupts-high-school-exams-causes-990924300>



# The nature of DDoS changed dramatically over last year

## 2002–2022:

- Majority DDoS is crafted or spoofed using amplification/reflection
  - 'Easy' to mitigate based on packet pattern match or protocol challenges

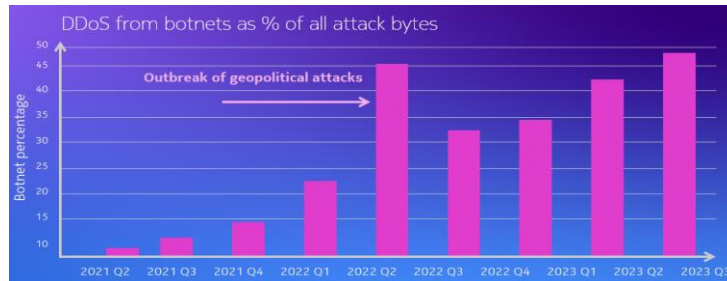
## Today:

- Botnets generate most complex attacks and most DDoS volume
  - Top Botnet device types: webcams, DVRs, routers, NAS, business IOT,...
- Exponential Botnet DDoS Growth driven by:
  - Exponential growth in IOT devices
  - Growth in CVE's
  - Dramatic drop in DDoS Black Market prices
  - Botnet traffic comes from anywhere

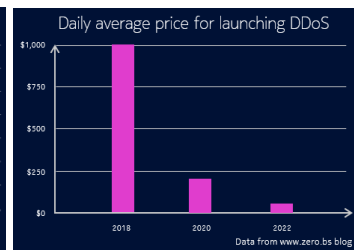
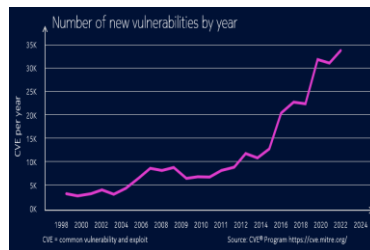
## Trend:

- Roll-out of symmetric GE/10GE access will make things worse...

Botnet DDoS protection requires 360° edge monitoring and protection



Source: Nokia Deepfield



## The Botnet DDoS detection challenge...

- is no longer about looking what's inside the packet
  - instead, it's about **who/what** is sending the packet
- ... has become a Big Data challenge

# Nokia's Deepfield Defender DDoS protection solution

Scalable cost-performant DDoS Protection

## 1 Plug-and-Play DDoS Detection

- Zero Touch DDoS classification based on big data principles
- No manual thresholds nor baselines setup

## 2 Use IP silicon to filter DDoS attacks

- Scalable and cost-efficient DDoS protection compared to DPI based scrubbers
- Surgical DDoS mitigation
- DDoS protection lifecycle orchestration



Nokia Deepfield

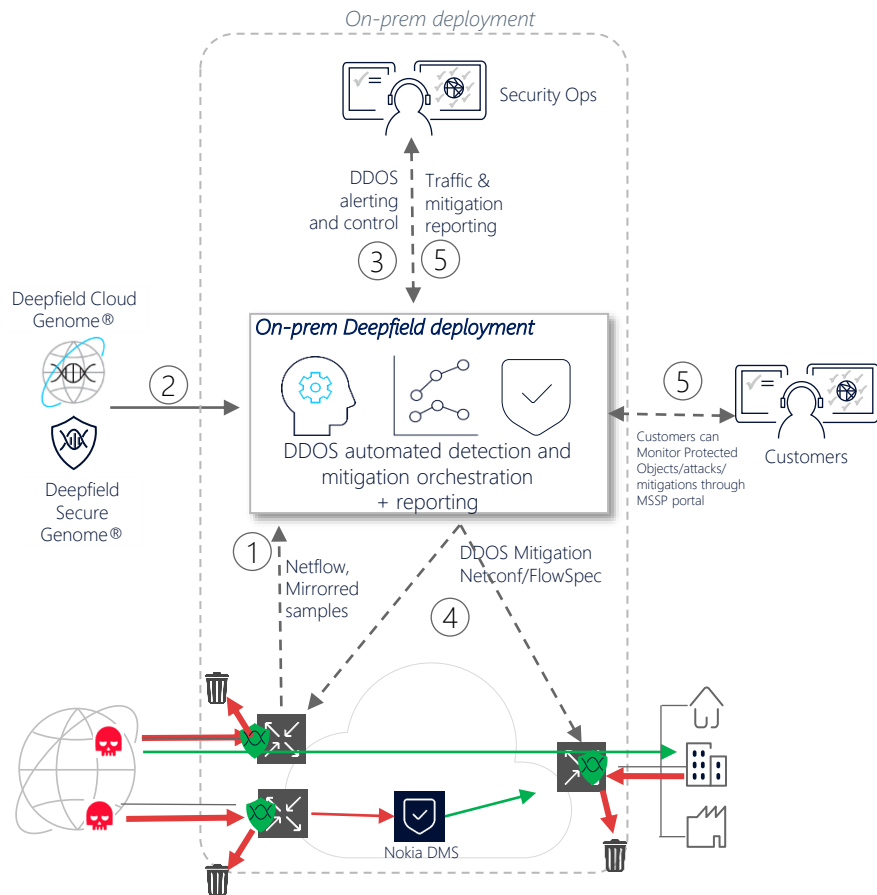


Nokia Routers or  
Defender Mitigation  
System (DMS)

# Nokia Deepfield Defender

A high-scalable **software platform** combining

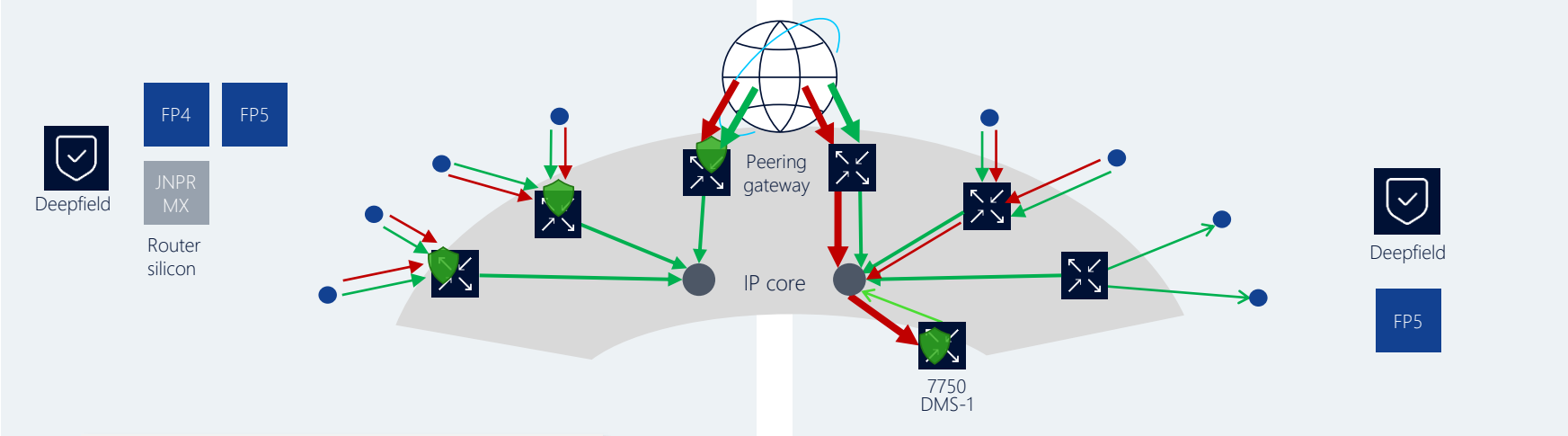
- ① **Telemetry** (Netflow or mirrored traffic samples) from your routers
- ② **big data** based security map of the Internet to provide
- ③ **Automated DDOS detection** for high-volume/high-packet rate DDoS attacks
- ④ **Fast DDoS filtering at line-rate**
  - leveraging Nokia IP silicon
  - on all Nokia edge routers or Nokia DMS
- ⑤ **Flexible Reporting**
  - Including MSSP Portal for participants to see attacks & mitigations to their Protected Objects



# Deepfield - IP silicon based DDOS mitigation options

## Edge router-based mitigation

## Alternative: Off-ramp to Deepfield Mitigation System (DMS)

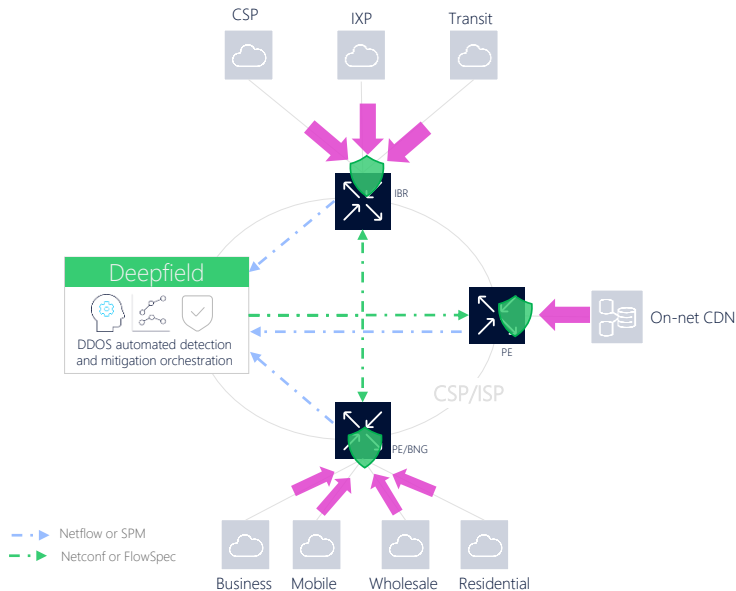


**Mitigation at the edge:**  
Use existing routers (Nokia SR or Juniper MX) to drop DDoS traffic at the edge.

**Scrubbing Center approach:**  
Deploy dedicated FP5 based Defender Mitigation System (DMS) to provide terabit-class scrubbing

# On-Net DDoS Protection solution for CSP/ISP networks

Making the Network part of your DDoS Protection Architecture with Nokia Deepfield



- 360° Monitoring – covering all network edges
- Big Data based DDoS detection
  - Fast, reliable, working out-of-the-box
  - Covering Botnet DDoS next to traditional DDoS
- IP Silicon based DDoS mitigation
  - Surgical Edge mitigation @Line-rate using Nokia FP4/FP5 (or Juniper) routers
  - or divert through Nokia DMS mitigation appliance

But for huge attacks (that would congest your peering links) or when you don't have the resources for on-prem DDoS mitigation: → complement with DDoS service from upstream provider



# Future Networks that speak your language

## SR Linux AI chat application

1. Ask question in SR Linux Command Line
2. Send question to Embedded Knowledge Graph
3. Return closest match lookup
4. SRL-GPT agent selects the sections of documentation or state output to send (OpenAI) as context along with the original
5. OpenAI summarizes an answer
6. Answer sent back to SRL-GPT agent
7. Answer provided to user in Command Line

### Example:

```
A:srlinux1# askai to show the health of your BGP peerings and explain this in Russian language
```

```
Состояние BGP peering можно определить из состояния сессии каждого соседа. Вот состояние BGP peering:
```

```
1. Сосед с адресом 192.0.2.2:
```

```
- Состояние сессии: Установлено (established)
```

```
- Последнее состояние: Активно (active)
```

```
- Последнее событие: recvOpen
```

```
- Последний раз установлено: 14 дней назад
```

```
- Установленные переходы: 1
```

```
2. Сосед с адресом 192.0.2.3:
```

```
- Состояние сессии: Активно (active)
```

```
- Последнее состояние: Активно (active)
```

```
- Последнее событие: Нет (none)
```

```
3. Сосед с адресом 192.0.2.4:
```

```
- Состояние сессии: Активно (active)
```

```
- Последнее состояние: Активно (active)
```

```
- Последнее событие: Нет (none)
```



**THANK YOU!**

Nov-09, 2013

**NOKIA**