CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Collaborative DDoS Mitigation & The DDoS Clearing House

Thijs van den Hout (SIDN Labs)

Partners: SIDN, University of Twente, Telecom Italia, FORTH, University of Zurich, SURF, University of Lancaster, CODE, Siemens

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

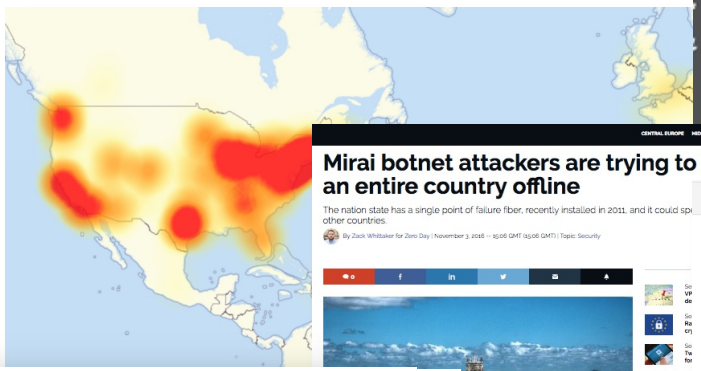
DDoS remains relevant

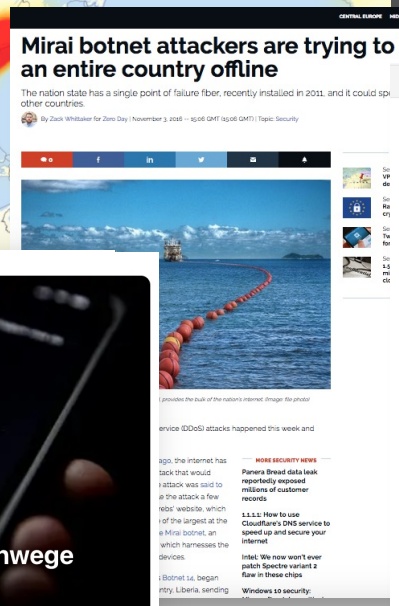
Estonia, 2007

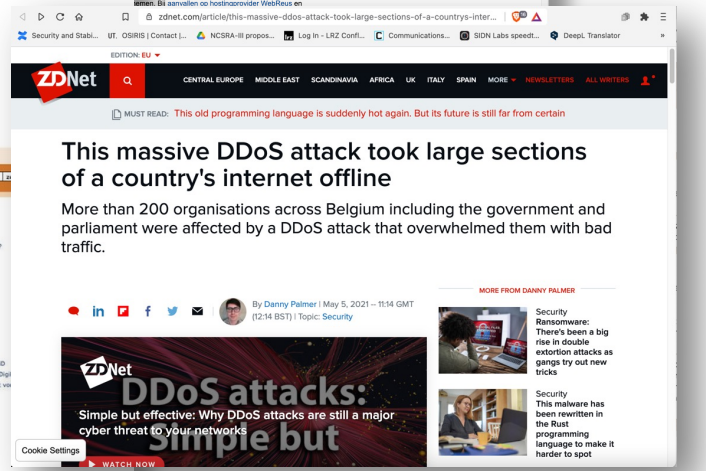
The Netherlands, September 2020

House of Representatives of The Netherlands, Oct 2020

Mirai botnet, 2016







Belgium, May 2021

The Netherlands, 3 days ago!

Liberia, 2016

The Netherlands, January 2018

Problem

- Mature DDoS mitigation services (e.g., scrubbing), routinely handling large numbers of DDoS attacks

- BUT no sharing of DDoS data and expertise between organizations
  - Increases response time and prevents learning because of limited view
  - Reduces innovation of mitigation processes and systems at ecosystem level
  - DDoS data “stuck” in systems of DDoS mitigation providers

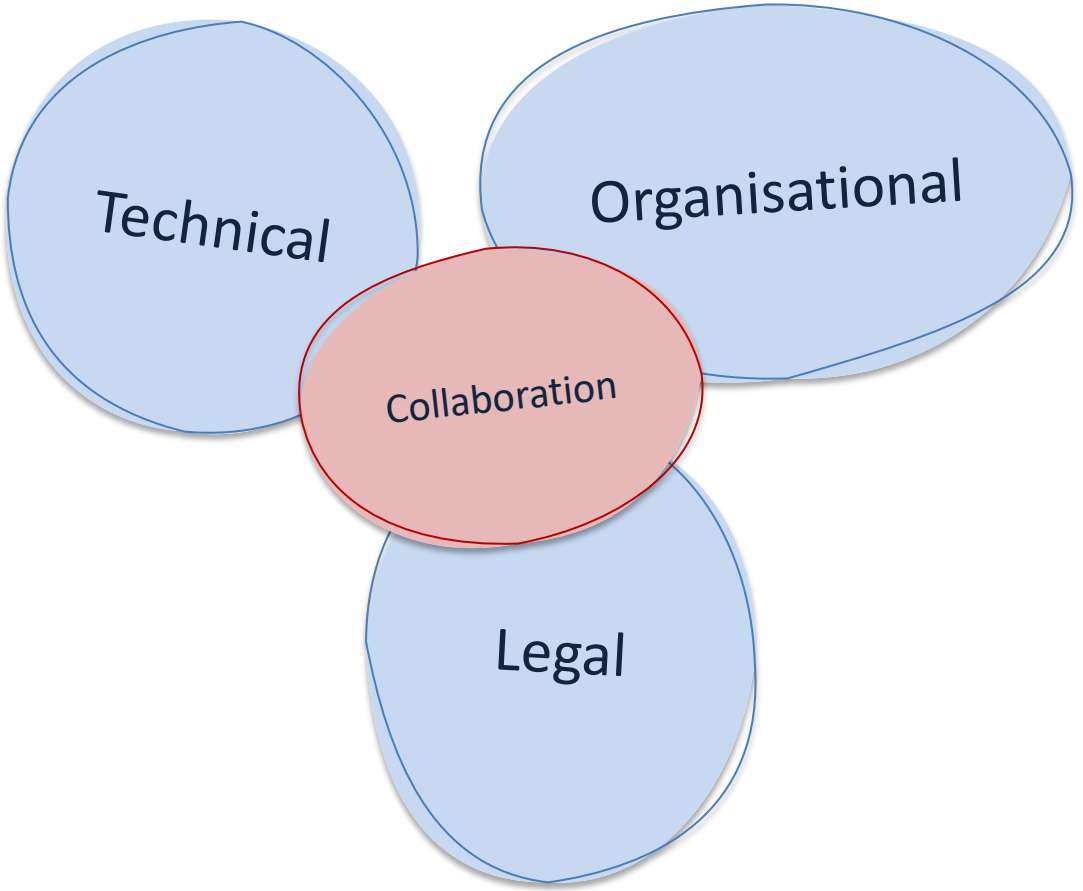
- Increases probability of societal disruptions through online services

Collaborative DDoS Mitigation

Goal: Improve collective DDoS resilience with additional activities

+ Sharing
  - DDoS metadata
  - Mitigation strategies
  - Tools and services

+ Practice together
  - DDoS drills
  - Cyber ranges



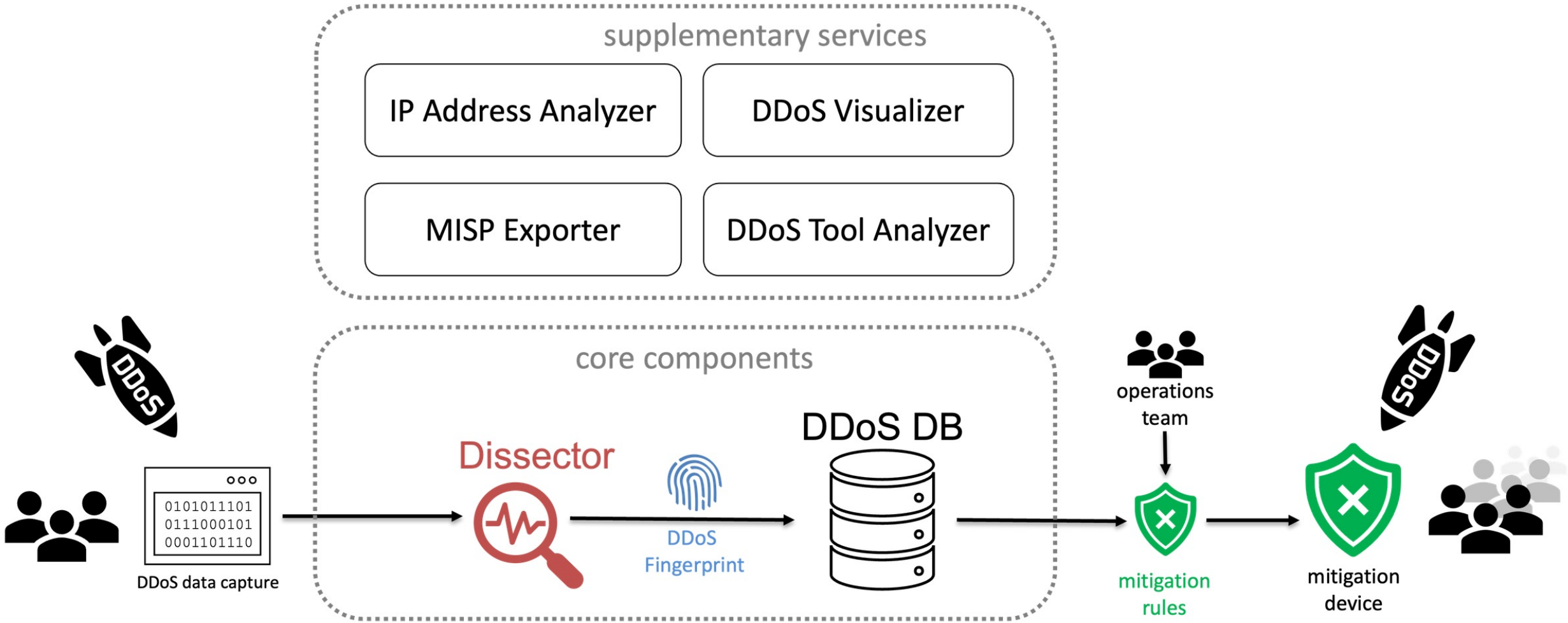
Examples

- Network playbook sharing for DNS Anycast (Tech talk II)
- IXP scrubber (Tech talk III)
- MANRS (Mutually Agreed Norms for Routing Security)
- DDoS Clearing House

DDoS Clearing House

- Sharing of **DDoS fingerprints** between organizations
- Generic concept: **Anti-DDoS Coalitions** across sectors, Member States, business units, etc.
- **Extends DDoS protection services** that service providers use and does not replace them

DDoS Clearing House



DDoS Fingerprint Example

fingerprint a38e5062b69fd7b8c5194fa7698398a7


```
{
  attack_vectors: [
    {
      service: "HTTP"
      protocol: "TCP"
      source_port: 80
      fraction_of_attack: 1.0
      destination_ports: "random"
      TCP_flags: {
        ...A....: 0.989
      }
      nr_flows: 5077
      nr_packets: 20308000
      nr_megabytes: 30599
      time_start: "2022-01-23 01:28:00"
      time_end: "2022-01-23 01:29:56"
      duration_seconds: 116
      source_ips: [
        "[redacted]"
        "[redacted]"
        "[redacted]"
        "[redacted]"
      ]
    }
  ]
  target: "Anonymous"
  tags: [
    "TCP"
    "TCP ACK flag attack"
  ]
  key: "a38e5062b69fd7b8c5194fa7698398a7"
  time_start: "2022-01-23 01:28:00"
  duration_seconds: 116
  total_flows: 5077
  total_megabytes: 30599
  total_packets: 20308000
  total_ips: 4
  avg_bps: 2110318068
  avg_pps: 175068
  avg_Bpp: 1506
  submitter: "thijs"
  submit_timestamp: "2022-01-25T13:50:13.818348"
  shareable: False
}
```

Key innovations

- Bridge **multidisciplinary gap** to deployment, more than tech!
- **Opensource design** that we make available through a “cookbook”
  - Technology, legal, organizational, lessons learned based on pilots
  - Enable federations of organizations to set up their own anti-DDoS coalition
  - Main use case is the Dutch Anti-DDoS Coalition (NL-ADC)
- Operates across **heterogeneous networks** and offers rich set of services

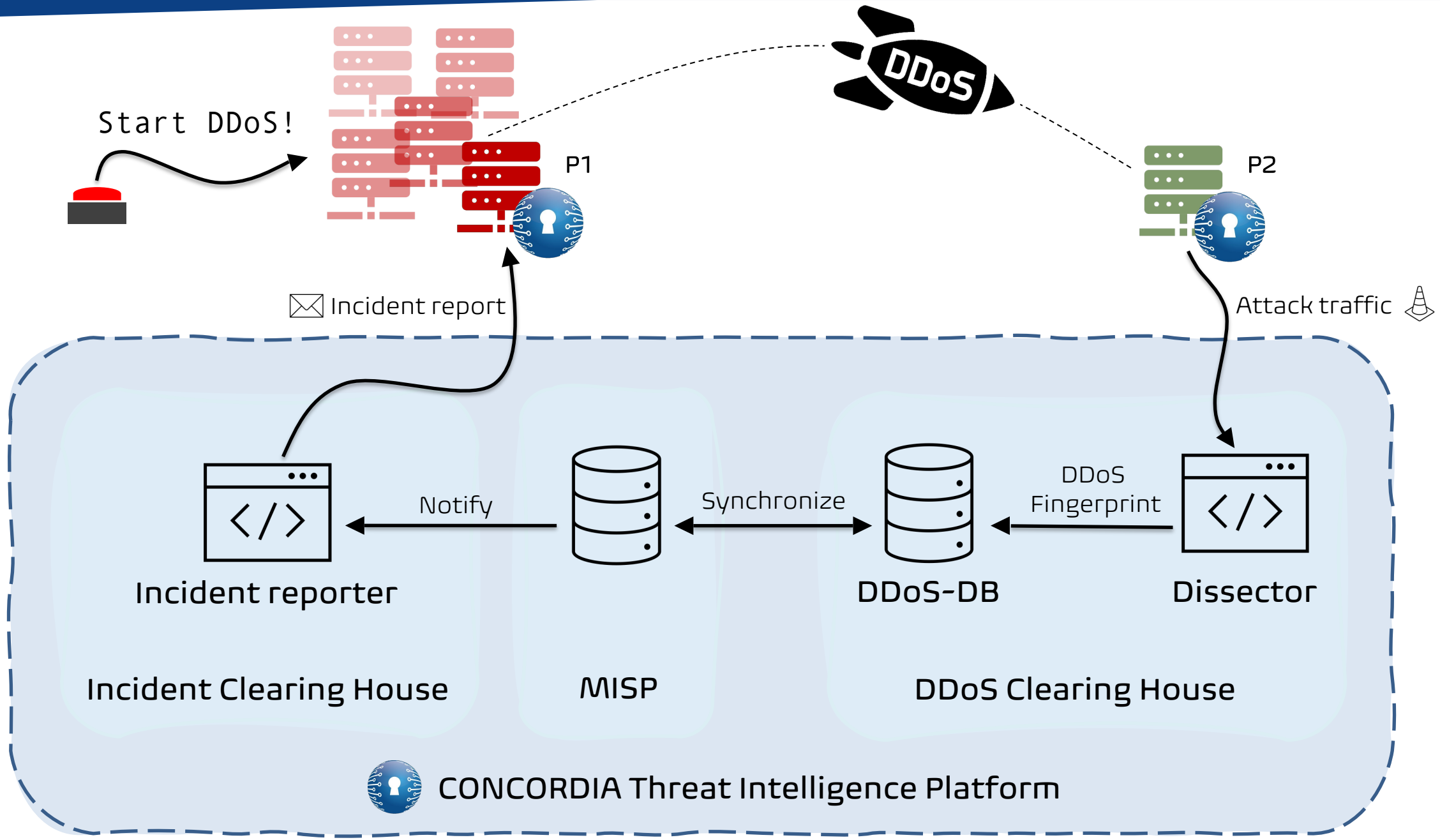
DDoS Clearing House pilots

- The Netherlands
  - In the existing Dutch Anti-DDoS Coalition (17 partners)
  - Cross-sectoral
  - One producer of fingerprints
- Italy
  - Smaller scale: Telecom Italia SOC & Security Lab + University of Turin
  - Intra-organizational
  - MISP

DDoS Testbed

- Representative environment used to
  - Test the technical developments of the Clearing House
  - Demonstrate our work
  - Cyber range for practicing DDoS

- DDoS traffic simulator
  - Small scale
  - Dashboard for attack customization


Start DDoS!
DDoS
P1
P2
Incident report
Attack traffic
Notify
Synchronize
DDoS
Fingerprint
Incident reporter
DDoS-DB
Dissector
Incident Clearing House
MISP
DDoS Clearing House
CONCORDIA Threat Intelligence Platform

What's next?

- DDoS Clearing House Cookbook
- Production phase at the NL-ADC
- Wrap up CONCORDIA with demonstration & reports

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020

Dutch Anti-DDoS Coalition:
https://www.nomoreddos.org/en/

Clearing house on GitHub:
https://github.com/ddos-clearing-house/

Thijs van den Hout
thijs.vandenhout@sidn.nl
@thijsvandenhout

This work was funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/