



# T3.2: Developing and Piloting a DDoS Clearing House for Europe

## CONCORDIA Final Review

### May 23, 2023

**Thijs van den Hout (SIDN Labs)**

**Partners:** SIDN, SURF, University of Twente, Telecom Italia, FORTH, University of Zürich





# DDoS Attacks Remain Relevant

Sweden, May 2023

REUTERS | Reuters

### Swedish parliament website hit by DDoS attack

Reuters  
3 May 2023 · 1-min read

STOCKHOLM (Reuters) -Sweden's parliament has been hit by a so called distributed denial-of-service (DDoS) attack that has disrupted access to its web page, it said on Wednesday.

The web page was partially down on Tuesday and appeared slow on Wednesday.

"The analysis shows that it is a denial-of-service attack," a parliament spokesperson said.

February 2023

### Cloudflare blocks record-breaking 71 million RPS DDoS attack

By Sergiu Gatlan

February 13, 2023 02:50 PM 2

The Netherlands, September 2020

nieuw vinden grootschalige ddoS-aanvallen op Nederlandse providers plaats

Door Tjia Hofmans  
Redacteur privacy & security  
Feedback

01-09-2020 - 16:50

178

House of Representatives of The Netherlands, Oct 2020



## Akamai Mitigates Record DDoS Attack in Asia-Pacific (900 Gbps)

Craig Sparling  
March 08, 2023



Following last summer's record-setting attacks on Europe, the distributed denial-of-service (DDoS) threat landscape continues to morph and intensify.

March 2023



DigiD was urenlang beperkt beschikbaar vanwege ddoS-aanvallen

Door Lennart 't Hart

12 sep 2022 om 20:29  
Update: 6 maanden geleden

213 reacties

DigiD was maandagavond urenlang beperkt beschikbaar vanwege een storing. De website werd geteisterd door ddoS-aanvallen. Veel gebruikers

The Netherlands, September 2022

massive DDoS attack took large sections of country's internet offline

in 200 organisations across Belgium including the government and internet were affected by a DDoS attack that overwhelmed them with bad

By Danny Palmer | May 5, 2021 - 11:14 GMT  
(2:14 BST) | Topic: Security

DDoS attacks: simple but effective: Why DDoS attacks are still a major threat to your network

Security Ransomware: There's been a big rise in double extortion attacks as gangs try out new tricks

Security This malware has been rewritten in the Rust programming language to make it harder to spot

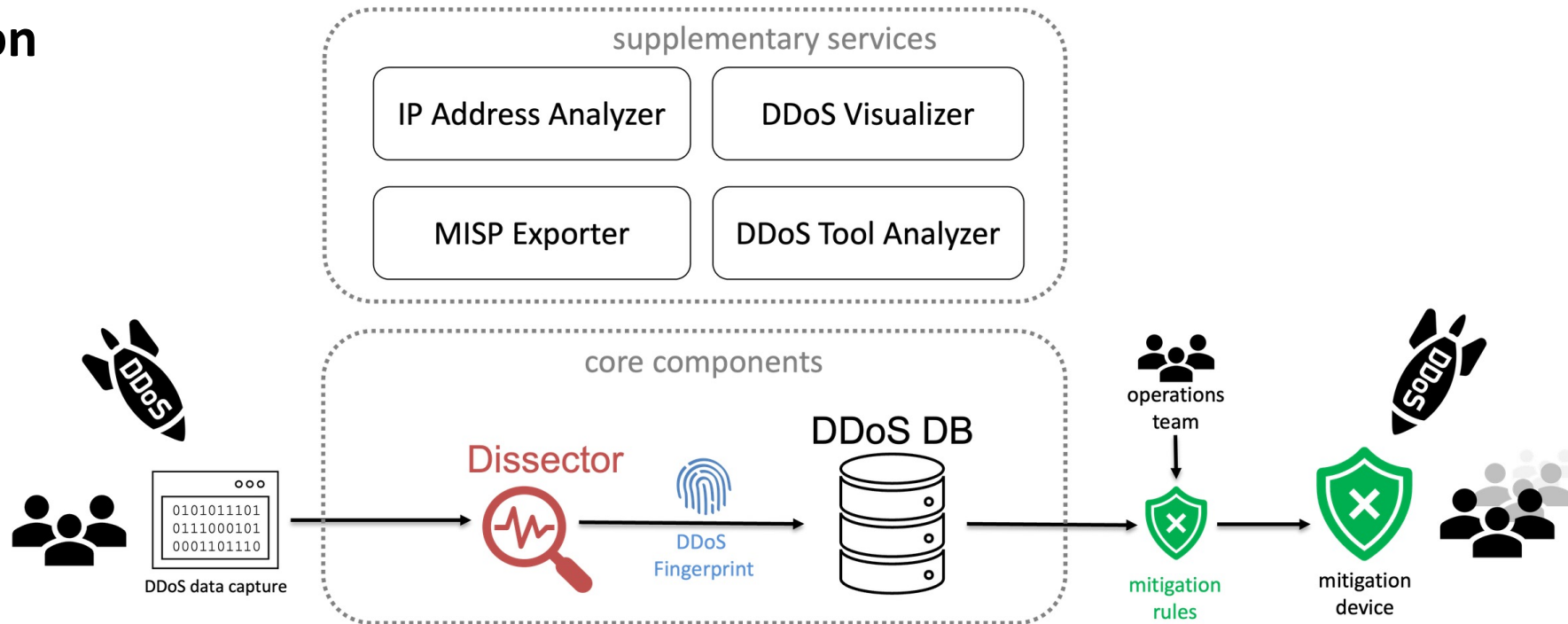
Belgium, May 2021

# Problem Statement

- Mature DDoS mitigation services (e.g., scrubbing), routinely handling large numbers of DDoS attacks
- **BUT no sharing of DDoS data and expertise across organizations**
  - Limited victim-specific view worsens response time and learning
  - Reduces innovation of mitigation processes and systems at ecosystem level
  - DDoS data “stuck” in systems of (US-based) DDoS mitigation providers
- Increases probability of societal disruptions, especially through critical (cyberphysical) systems (cf. WP2)

# DDoS Clearing House Concept

- Continuous and automatic sharing of **DDoS fingerprints**, buys providers time (proactive)
- **Extends DDoS protection services** that service providers use and does not replace them
- Anti-DDoS Coalition: across sectors, Member States, business units, etc.





# DDoS Fingerprint



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: [
        "192.168.1.1"
        "192.168.1.2"
        "192.168.1.3"
        "192.168.1.4"
      ]
    }
  ]
  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 the **multidisciplinary** gap to **deployment**
  - DDoS Clearing House
  - Anti-DDoS coalitions
  - Validation of both in practice
- DDoS **cyber range**
- **Open-source** design: proven in pilots, documented in a *cookbook*
- Operates across **heterogeneous networks**, offers extensible services
- ★ EC Innovation radar 2021
- ★ Key CONCORDIA results

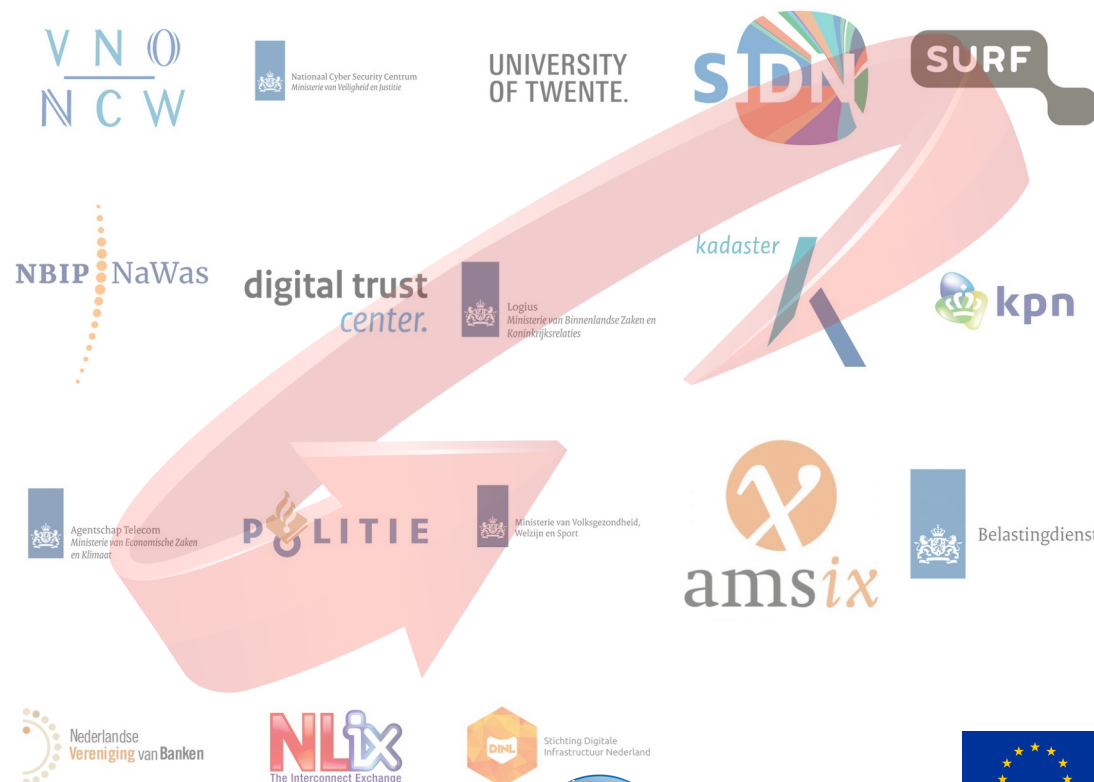


[github.com/ddos-clearing-house](https://github.com/ddos-clearing-house)

# Dutch Anti-DDoS Coalition

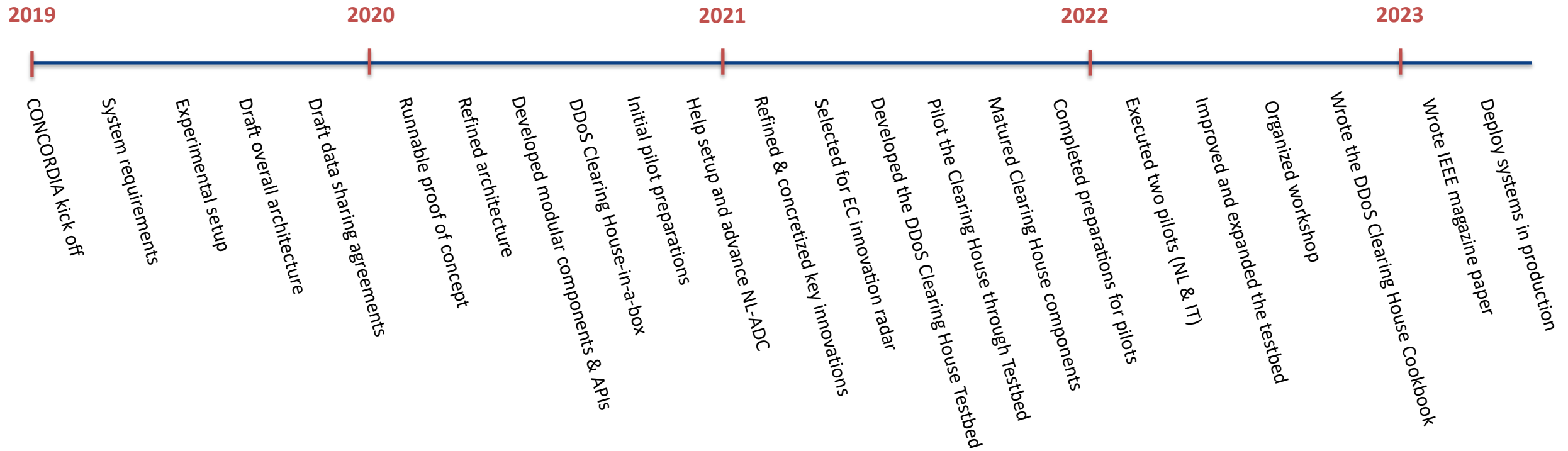


- 18 cross-sectoral critical infrastructure operators in NL
- Sharing DDoS data through Clearing House
- Large-scale DDoS drills (Red/blue team)
- Sharing DDoS expertise and knowledge
- Small-scale DDoS exercises (Cyber range)



[nomoreddos.org](http://nomoreddos.org)

# CONCORDIA T3.2 Timeline





# Two Coalitions – Two and a Half Pilots

1. Dutch Anti-DDoS Coalition (TRL 8)
  - Shared 270 DDoS fingerprints through DDoS-DB
  - External collaboration
  - Iteratively improve the platform
2. Italian Anti-DDoS Coalition (TRL 7)
  - Telecom Italia + university of Torino
  - Internal and external collaboration
  - Share fingerprints via MISP
- 2½. Testbed (TRL 6)
  - pilot with simulated data



# Improved Testbed as Cyber Range

- DDoS sample traffic
- Test the Clearing House cycle
- Target yourself and low traffic volumes = fewer agreements
- Use as cyber range

The screenshot shows a web browser window with the URL <https://www.ddosclearinghouse.eu/sidnlabs>. The page title is "DDoS Testbed Dashboard" and the user is logged in as "SIDNLABS". The main section is titled "Generate DDoS traffic for SIDNLABS" and contains several configuration fields:

- Attack Type: Custom packets
- Highest protocol: TCP
- Packets per second: 10,000
- Destination port: 80
- Packet data bytes: 100
- Duration: 45 seconds (with a slider)

On the right side, there are checkboxes for various flags:

- Fragment packets
- More fragments flag
- No more fragments flag
- SYN flag
- ACK flag
- FIN flag

Below the configuration fields is a green "Next" button. To the right of the configuration area is a "Stop traffic" button with a red "Stop!" button inside it.

A yellow warning box at the bottom of the dashboard contains the following text:

**WARNING**  
Disclaimer: this web page is part of a pilot of the DDoS Clearing House. It is meant to initiate simulated DDoS traffic to one of the partners of this pilot: SIDNLABS. The goal of sending test traffic is solely to test the DDoS Clearing House; not to send a *real* DDoS attack to load test the target. Traffic will originate from five identical sources in parallel. In no event is SIDN (Labs) liable for any claim, damages, or other liability as a result from the actions performed on this web page.

At the bottom of the page, there is a footer: "This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927".



# Workshop on Collaborative DDoS Mitigation

- 35 guests (10 CONCORDIAns)
- CONCORDIA introduction
- Four Tech Talks
- Panel discussion

## Takeaways:

- *Exchange DDoS metadata at multiple levels*
- *Operational measures are just as important as technology*
- *On-premises, hybrid, or cloud-based mitigation?*



# D3.6: DDoS Clearing House Cookbook

- Documentation of the DDoS Clearing House
- Template agreements / contracts
- Description of pilots
- Notes on implementation
- Lessons learned
- IEEE Communications Magazine submission

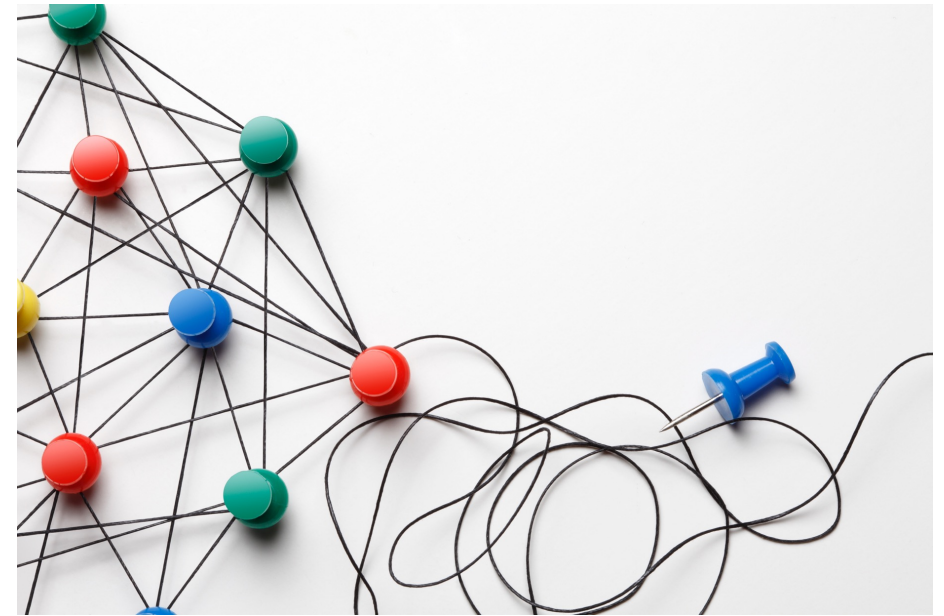


[ddosclearinghouse.eu/cookbook](https://ddosclearinghouse.eu/cookbook)



# Connecting the Threat Intelligence Platform

- CONCORDIA Threat Intelligence Platform
  - T3.1 Incident Clearing House
  - T3.2 DDoS Clearing House
  - MISP
- MISP DDoS Fingerprint object
- DDoS-DB – MISP connection
- Demo video:  
<https://www.youtube.com/watch?v=TJfOMzXh1ik>





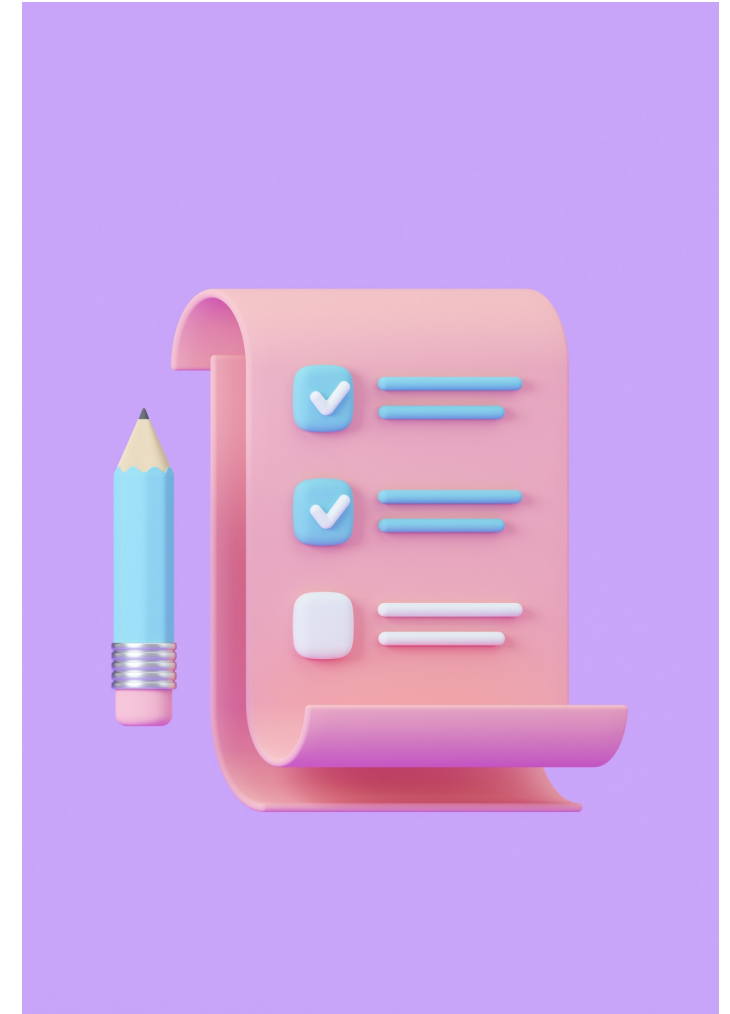
# Looking Ahead: Beyond CONCORDIA

- Production-level services for Dutch ADC
  - DDoS Clearing House (at NBIP)
  - Testbed for purple team exercises (at Tax & Customs Admin)
  - Contracts currently being finalized
  - Further development at TU Delft
- Dissemination of our work
  - Paper in IEEE Communications Magazine
  - Workshop on Collaborative DDoS Mitigation
  - Interest from IXP community
  - Potentially in MANRS+



## T3.2 Summary

- Developed DDoS Clearing House
- Helped shape the concept and implementation of anti-DDoS coalitions (ADC)
- Piloted the system in two ADCs and a simulated platform
- Tackled organizational and legal requirements for deployment
- Developed Testbed & Cyber Range
- Contributions moved to industry, deployment in production
- Active dissemination (cookbook, paper, workshop)



### Contact

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

[contact@concordia-h2020.eu](mailto:contact@concordia-h2020.eu)

### Follow us



[www.concordia-h2020.eu](http://www.concordia-h2020.eu)



[www.twitter.com/concordiah2020](https://www.twitter.com/concordiah2020)



[www.facebook.com/concordia.eu](https://www.facebook.com/concordia.eu)



[www.linkedin.com/in/concordia-h2020](https://www.linkedin.com/in/concordia-h2020)



[www.youtube.com/concordiah2020](https://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](mailto:thijs.vandenhout@sidn.nl)  
[@thijsvandenhout](https://twitter.com/thijsvandenhout)

Cristian Hesselman  
[cristian.hesselman@sidn.nl](mailto:cristian.hesselman@sidn.nl)  
[@hesselma](https://twitter.com/hesselma)