



DDoS Clearing House for Europe (Task 3.2)

7th CONCORDIA General Assembly

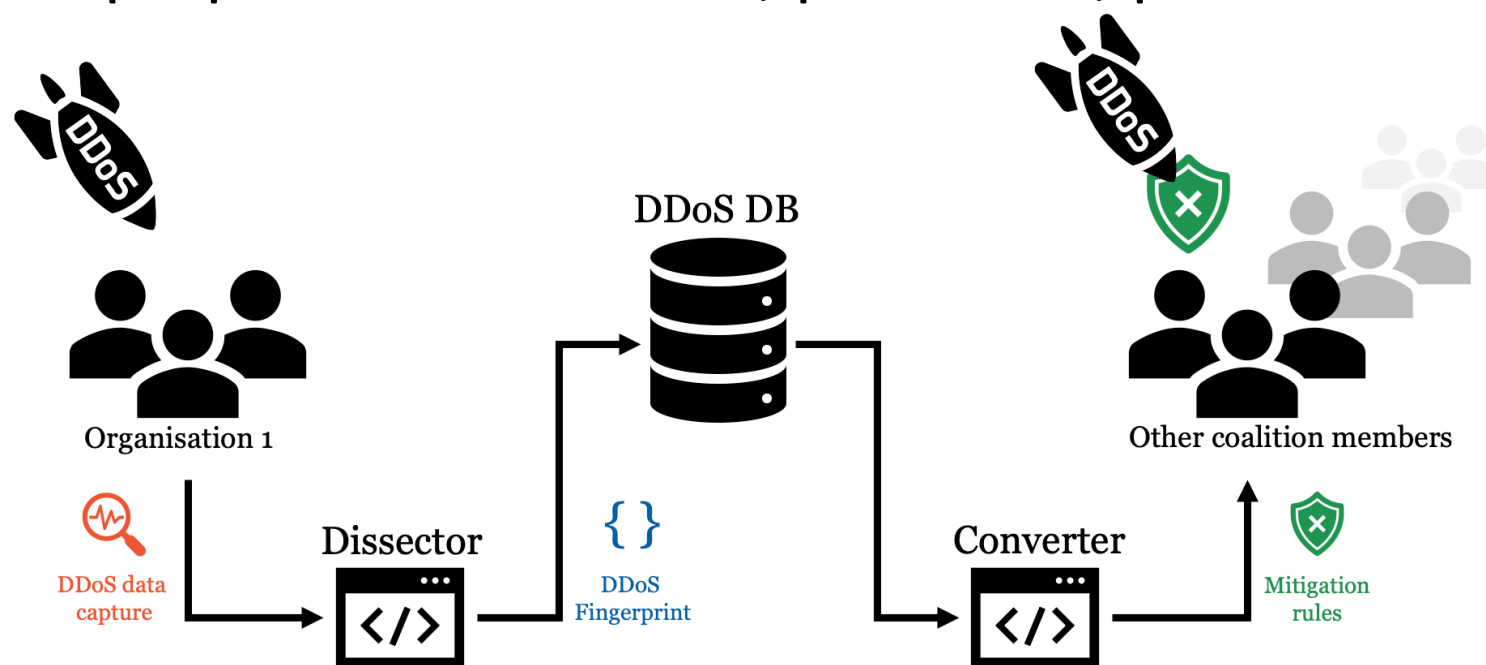
**Cristian Hesselman &
Thijs van den Hout**
(SIDN Labs)

Partners: SIDN, UT, TI, FORTH, UZH, SURF, ULANC, CODE



DDoS Clearing House Concept

- Continuous and automatic sharing of “DDoS fingerprints”, buys providers time (proactive)
- Extends DDoS protection services that critical service providers use and does not replace them
- Generic concept: per Member State, per sector, per business unit, etc.



Clearing House increases Digital Sovereignty


- Increased **insight** of potential victims into DDoS attacks from their own narrow view to an ecosystem-wide view
- Increased **control** because the new insights give organizations more grip on how to handle DDoS attacks and the requirements for their DDoS mitigation facilities (their own or those of a contracted third party)
- ADCs also build up a joint **pool of expertise** independent of particular DDoS mitigation providers through drills and best common practices



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 DDoS clearing house
 - Main use case is the Dutch Anti-DDoS Coalition (NL-ADC)
- Operates across **heterogeneous networks** and offers **rich** set of services

Key takeaways

- Key achievements Y3: DDoS clearing house distributed testbed and improved clearing house components
- Dutch ADC: Consortium agreement finalized, new member  **No More DDoS**
Anti-DDoS-Coalition
- Y4 focus: (1) running pilots in the Dutch ADC + Italy, (2) production system development with Dutch ADC, (3) publish cookbook

DDoS clearing house in the Netherlands



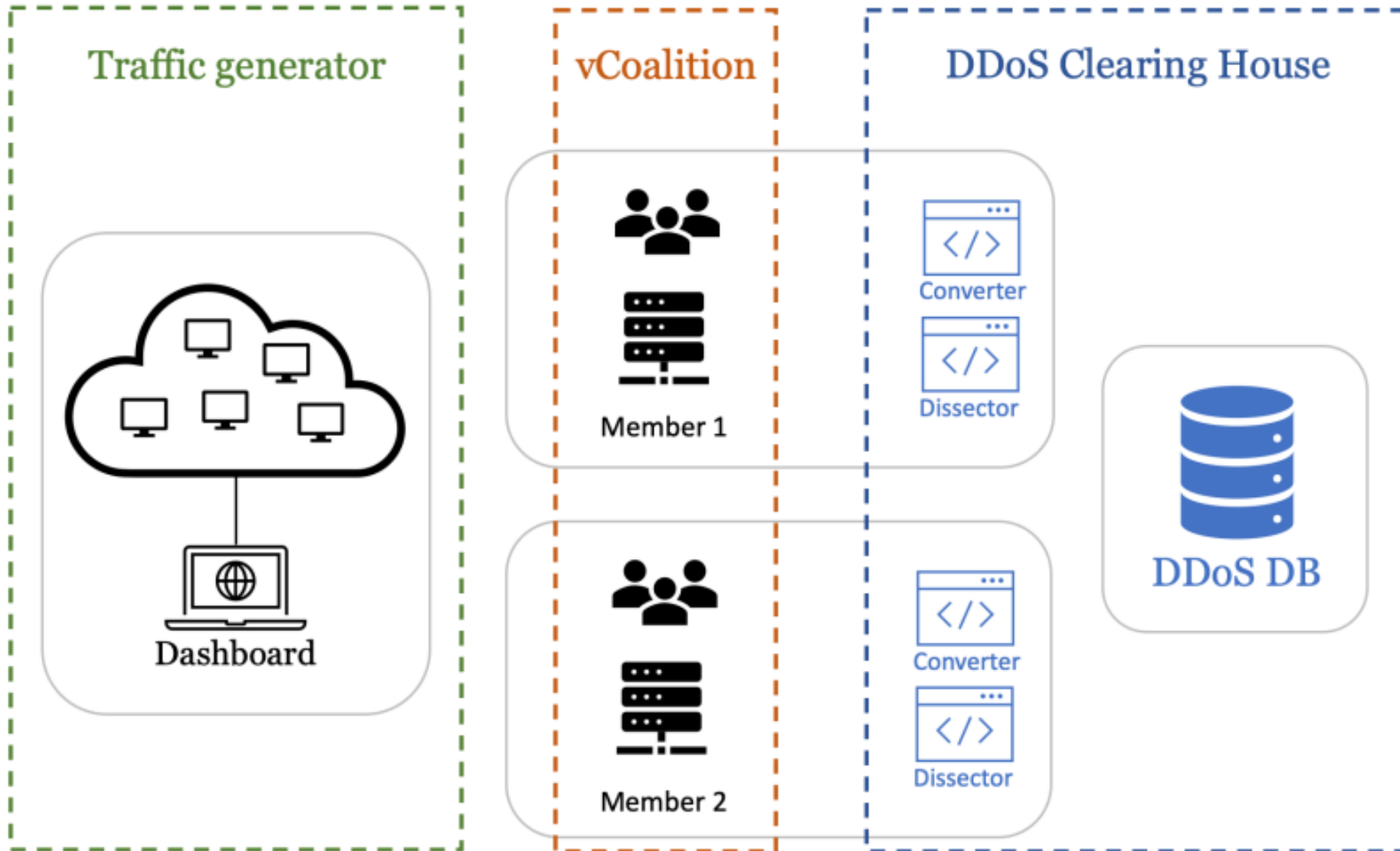
- DDoS clearing house R&D
- Clearing house distributed testbed
- Technical evaluation through pilots in the Netherlands and Italy
- DDoS clearing house cookbook
- Sharing of operational experience
- Large-scale multi-party DDoS drills
- **DDoS clearing house operations**
- Operational ADC organization



Distributed testbed

- Allows testing of the DDoS Clearing House without changes to production systems in Anti-DDoS coalition members
- No sharing of PII (generated traces of DDoS traffic)
- Precursor to pilots in the Netherlands and Italy
- Useful for iteratively developing and testing the clearing house in a representative environment

Distributed testbed



Advancements of components in Y3

- Dissector: improved stability, usability, containerized deployment
- DDoSDB: automated syncing between DBs, improved UI, stable release
- Converter: new features in MISIP are in testing phase

- Tool analyzer: incorporated into testbed
- DDoS grid: included financial implications of an attack (demo on confluence)
- IP address analyzer: map with geolocation information of source Ips, network speed measurements

Component Maturity Indication

Name	Function	Maturity
Dissector	Generate DDoS fingerprints using PCAP files or flow data	High
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High
Converter	Generate mitigation rules based on DDoS fingerprints	Medium
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Medium
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Medium
MISP Exporter	Generate MISP events based on DDoS fingerprints	Medium

Overall: **stable framework**, most thrusts in the Dissector (adding and updating DDoS fingerprinting algorithms) and in the Converter (adding and updating rule-specific converters).



Dissemination in Y3

- 2 technical **blogs** (DDoS classifiers and testbed)
- **Demo video** on the clearing house distributed testbed:
<https://www.youtube.com/watch?v=UwRB74kabn8>
- **11 presentations**: at Dutch ADC, EURITAS, Inter-ISAC meeting NL, ABNAMRO bank, ICANN71 TechDay, NBIP, CyberHOT Summer School
- **Conferences**: La Fabrique Défense (Dec., France), FUSION event (Nov., NL)
- CONCORDIA Open Door event next week

Dutch National Anti-DDoS Coalition



CONCORDIA partner

CONCORDIA partner

CONCORDIA partner





Updates Dutch Anti-DDoS Coalition

- New coalition member
- Consortium agreement finalized
- Preparing request for additional funding for starting up production



DDoS Clearing House Planning @NL-ADC

Phase		Q1-2021	Q2-2021	Q3-2021	Q4-2021	Q1-2022	Q2-2022
-1	Distributed testbed 						
0	Pilot						
1	Basic production						
2	Full production						

Dev: CONCORDIA team
Ops: SIDN Labs + CONCORDIA team

Dev: CONCORDIA team
Ops: database operator (NBIP) + NL-ADC members

Dev: CONCORDIA team
Ops: SIDN Labs + NL-ADC members

Dev: software developer (TBD)
Ops: database operator (NBIP) + NL-ADC members







Lessons learned in Y3

- Piloting a new system in production is difficult: build a testbed used to demonstrate the software helps this process along
- A simulated production environment is useful for iteratively developing a system such as the clearing house

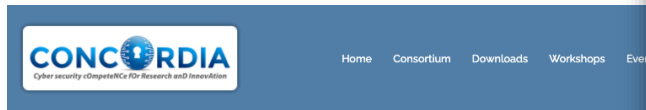


Outlook Y4 (project end)

- Pilot in the Netherlands: 3+ member organizations of the Dutch ADC sharing fingerprints  
- Pilot in Italy: 3+ partners sharing fingerprints: Telecom Italia Security LAB & internal SOC, University of Turin  
- Further development focusses on Dissector and pilot infrastructure
- Cookbook and tech report combined in a peer-reviewed paper



Further reading



POSTED APRIL 9, 2020 ADMIN CONCORDIA

Increasing the Netherlands' DDoS resilience together

First lessons learned from setting up a national anti-DDoS initiative, part I of III

The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together. In this series of three blogs, we'll first discuss the rationale behind our initiative, then describe a technical facility called the DDoS clearing house that enables coalition members to automatically measure and share the properties of DDoS attacks (e.g. attack duration and source IP addresses), before finally reviewing our key challenges, the lessons learned and the way forward. Our lessons learned are an important input for a "cookbook" to set up anti-DDoS coalitions elsewhere in Europe.

Note: we're using two types of reference in this blog series: hyperlinks for more information, while numbers between straight brackets ([1]) link to internal references.

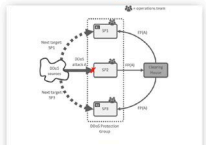
DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with traffic that prevents the network from serving legitimate requests from their clients. This is done by simultaneously transmitting traffic from a large number of machines distributed across the globe. For example, by infecting those machines with malware that carries out the attack. The attacking machines exhausts a server's resources (rather than swamp it) and the server could repeatedly start a login session with the server, thus forcing it to repeatedly start a login session with the server, thus forcing it to repeatedly start a login session with the server.



Dutch Anti-DDoS Coalition: lessons learned and the way forward
24 March 2020
Increasing the Netherlands' DDoS resilience together, part III of III Cristian Hesselman (SIDN and University of Twente), Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBIIP) and
[Read More](#)

Blog



Setting up a national DDoS clearing house
12 March 2020
Increasing the Netherlands' DDoS resilience together, part II of III Cristian Hesselman (SIDN and University of Twente), Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBIIP) and
[Read More](#)



Increasing the Netherlands' DDoS resilience together
10 March 2020
The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together.
[Read More](#)



Developing and running a testbed for the DDoS Clearing House

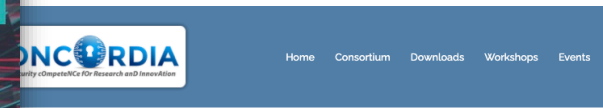
Demonstrating the DDoS Clearing House in a representative simulated environment



Wednesday 19 October 2020

Article by: Thijs van den Heuvel, Remco Poortinga van Wijnen, Cristian Hesselman, Christos Papachristos, en Karin Vink CPPE

We have created a distributed testbed that enables us to realistically test the [DDoS Clearing House](#): a system that enables organisations to handle DDoS attacks more proactively by automatically sharing measurements of the DDoS attacks they handle. Our testbed allows us to temporarily skip typically time-consuming organisational processes such as setting up data sharing agreements and deploying software in production systems, which helps to advance the system towards a pilot and a production version. We discuss the motivation for developing our testbed, its requirements, implementation and our lessons learnt. We're developing the Clearing House and the testbed as part of the CONCORDIA project, and we'll be using both in the Dutch Anti-DDoS Coalition.



SEPTEMBER 24, 2020 ADMIN CONCORDIA

Work in Progress: the CONCORDIA Platform for Threat Intelligence

steps to improve Europe's information position in cybersecurity
present CONCORDIA's vision for a cross-sector, pan-European platform for collecting, analyzing, and sharing threat intelligence, which combines datasets built up in different parts of the project.

What is threat intelligence?

Threat intelligence can be defined as the process of acquiring knowledge from multiple sources about threats to an environment. Threat intelligence supports informed decision-making on cybersecurity by providing information about attack techniques, indicators of compromises, and vulnerabilities. The process is essentially collaborative and based on real-world datasets.

CONCORDIA's approach

The two cross-sector pilots in CONCORDIA ("Building a Threat Intelligence for Europe" and "Piloting a DDoS Clearing House for Europe") are developing the basic building blocks for a pan-European and cross-sector threat intelligence platform, which conceptually forms a central point of contact for all services within the CONCORDIA ecosystem that are related to threat intelligence.

We are developing the CONCORDIA threat intelligence platform based on three primary principles:

- **Multi-source:** the platform uses multiple datasets available through heterogeneous technologies and providing different data management services (e.g., two clearing houses and their specific services).
- **Combine datasets:** the platform uses algorithms to integrate datasets into new derived datasets (e.g., coupling reported botnet infections and DDoS attacks, see the scenario below).



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/>

Cristian Hesselman (T3.2 lead)
cristian.hesselman@sidn.nl
[@hesselma](https://twitter.com/hesselma)
+31 6 25 07 87 33