No More DDoS
Anti-DDoS-Coalitie

A multi-stakeholder approach to DDoS protection

Thijs van den Hout

nomoreddos.org

GFCE Triple I, CIGF | August 22, 2024

Introduction

Thijs van den Hout
thijs.vandenhout@sidn.nl

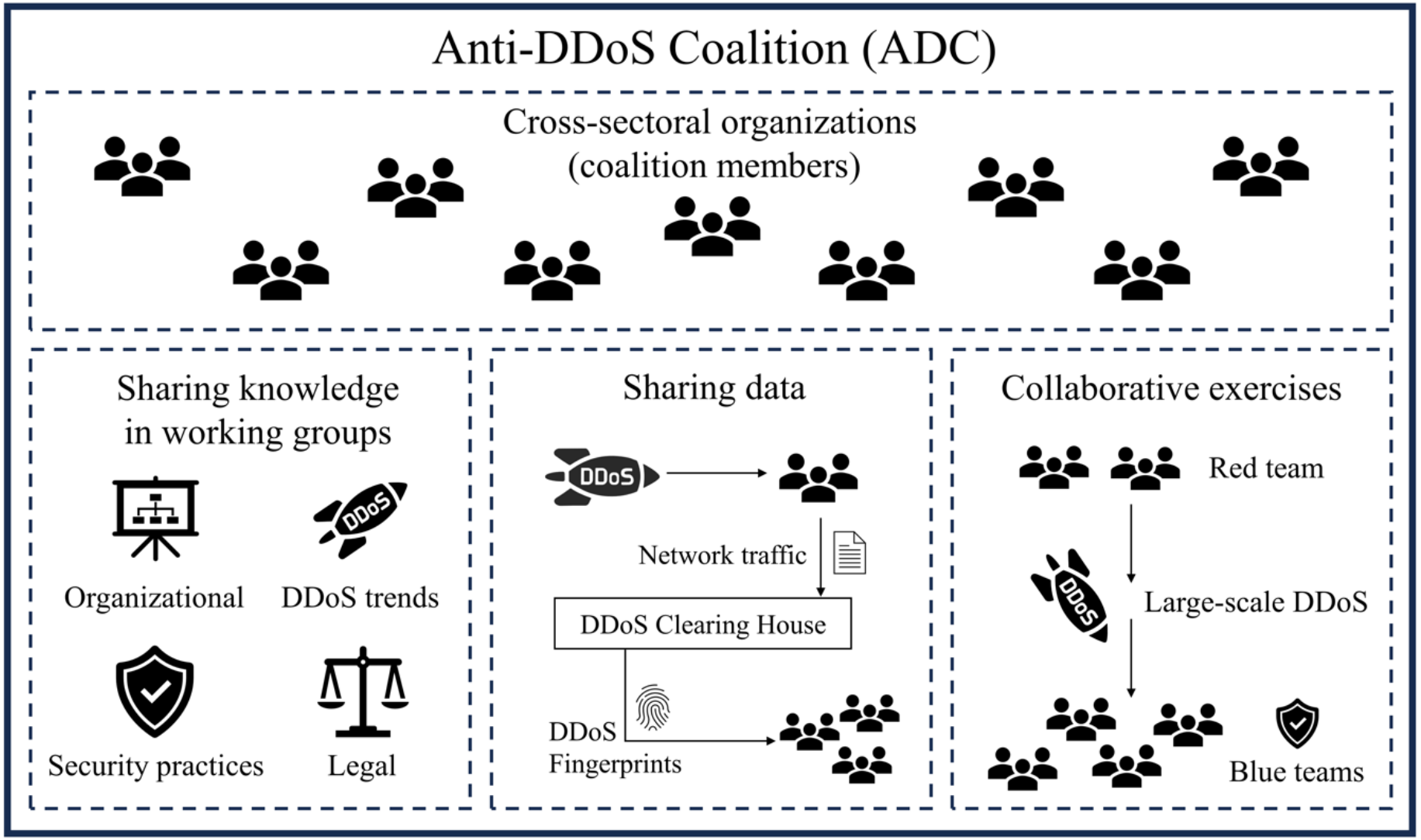
Researcher @ SIDN Labs (.nl)

MSc Artificial Intelligence

Radboud University

Dutch anti-DDoS coalition working group chair

Collaborative DDoS mitigation



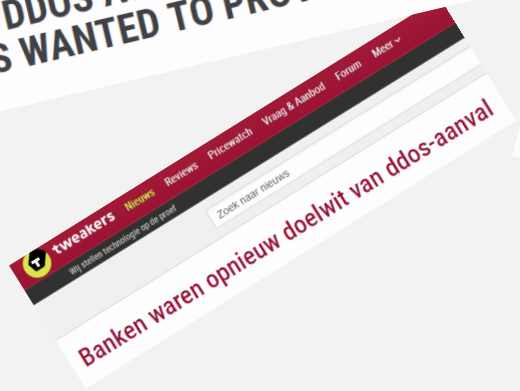
Motivation: DDoS attacks in the Netherlands

2018

Directeuren NBIP en DINL uiten kritiek op ABN Amro, ING, Rabobank en Volksbank

Banken moeten meer samenwerken om te voorkomen dat cybercriminelen hun diensten platleggen met DDoS-aanvallen. Ze zouden zich vaker moeten aansluiten bij collectieve initiatieven tegen cybercrime. Nu kiezen ze nog te vaak voor een individuele aanpak van netwerkbeveiliging bij één security-leverancier, daardoor missen ze de kennis en kunde van een grote achterban. Criminelen zijn namelijk ook in groepsverband georganiseerd.

Lees verder op: https://www.computable.nl/artikel/nieuws/security/6290656/250449/banken-moeten-meer-samenwerken-tegen-ddos.html



Dutch anti-DDoS Coalition

Governance model & working groups

- Coalition Core Team
  - Daily governance
  - Bookkeeping
  - New members
- Working groups
  - Legal Affairs
  - Communication
  - Exercises
  - Intel & Attribution
  - DDoS Clearing House
- Plenary meetings

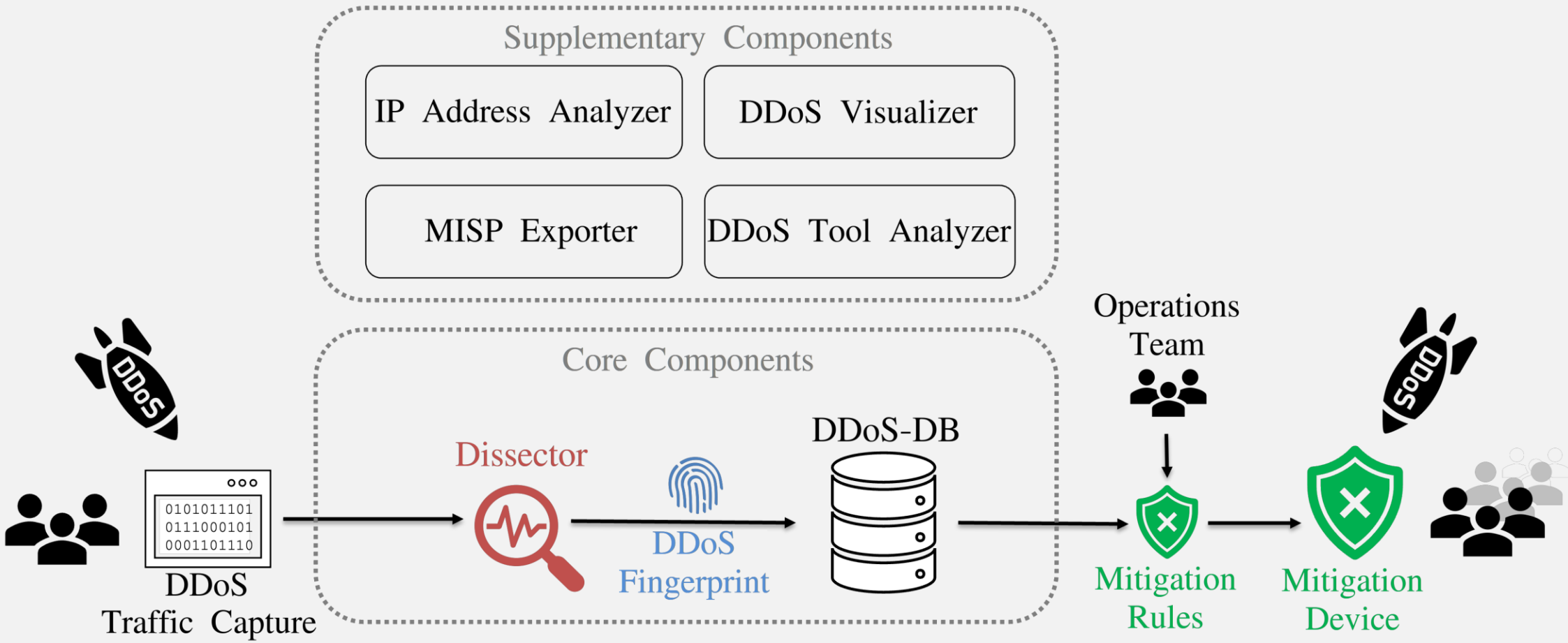
CONCORDIA (2019 – 2023)

- European Commission-funded research project for a cybersecurity competence network
- Development of DDoS Clearing House with 6 European partners
- Symbiotic relationship with Dutch anti-DDoS coalition

CONCORDIA

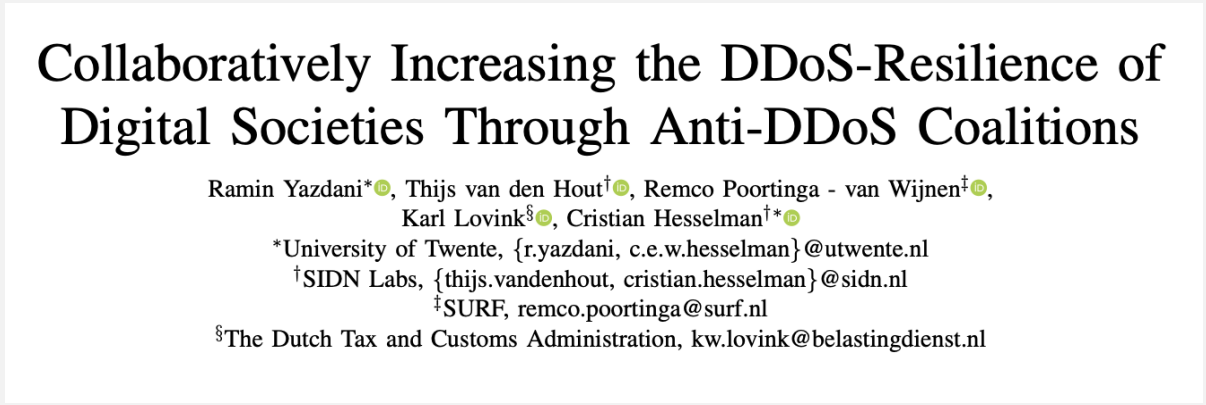
Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House



DDoS Clearing House Cookbook

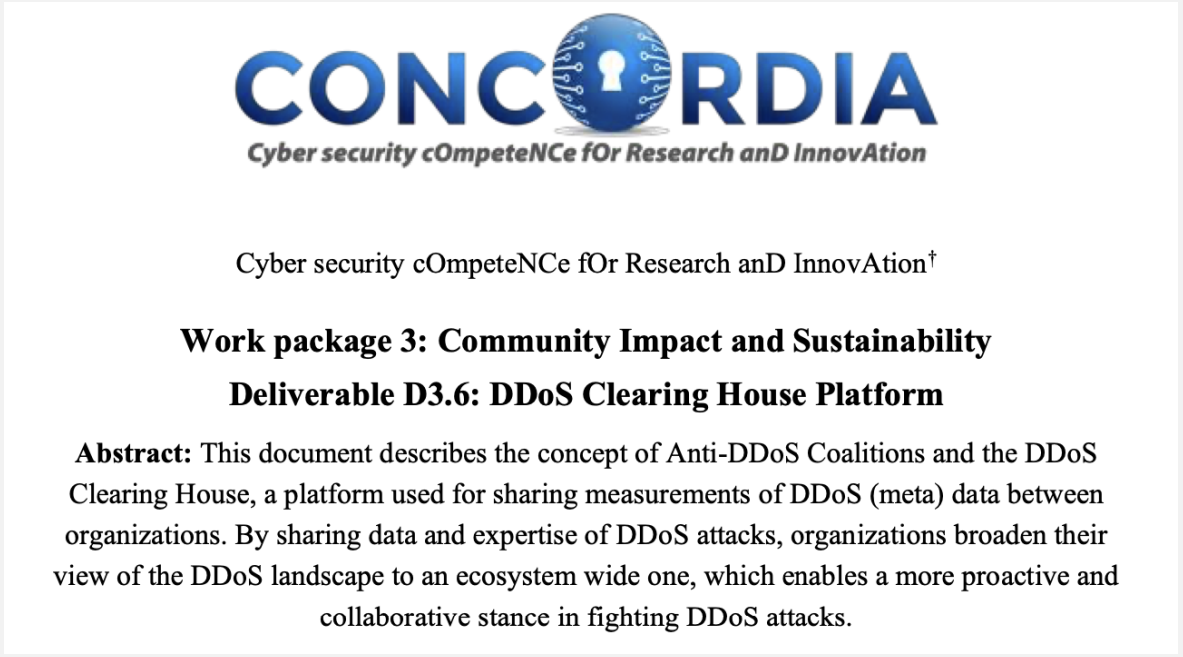
- DDoS Clearing House Cookbook & paper



Collaboratively Increasing the DDoS-Resilience of Digital Societies Through Anti-DDoS Coalitions

Ramin Yazdani*, Thijs van den Hout†, Remco Poortinga - van Wijnen‡, Karl Lovink§, Cristian Hesselman†*
*University of Twente, {r.yazdani, c.e.w.hesselman}@utwente.nl
†SIDN Labs, {thijs.vandenhout, cristian.hesselman}@sidn.nl
‡SURF, remco.poortinga@surf.nl
§The Dutch Tax and Customs Administration, kw.lovink@belastingdienst.nl

https://sidnlabs.nl/en/publications
(March 2024)



CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Cyber security cOmpeteNCe fOr Research anD InnovAtion†

Work package 3: Community Impact and Sustainability

Deliverable D3.6: DDoS Clearing House Platform

Abstract: This document describes the concept of Anti-DDoS Coalitions and the DDoS Clearing House, a platform used for sharing measurements of DDoS (meta) data between organizations. By sharing data and expertise of DDoS attacks, organizations broaden their view of the DDoS landscape to an ecosystem wide one, which enables a more proactive and collaborative stance in fighting DDoS attacks.

https://ddosclearinghouse.eu

Large-scale DDoS exercises

- (Bi-)yearly DDoS practice hosted by the coalition
- Red-team / blue-team
- Volume-based & application based
- 1Tb+/s traffic bandwidth
- Indemnity agreements between organizations
- Organization and communication is key

Working group intel & attribution

- Collaboration with law enforcement
- Gathering DDoS booter information & fingerprints
- Attribution of DDoS attacks in the wild
- Discover new attack types to prepare for in exercises

Summary & resources

- DDoS is everywhere, so collaboration is crucial
- Sharing information, data, and best practices *really* helps
- Our contributions are open source & open access

DDoS Clearing House Cookbook: https://ddosclearinghouse.eu
Cookbook paper & this presentation: https://sidnlabs.nl/en/publications
DDoS Clearing House software (+ more): https://github.com/nladc
General information: https://nomoreddos.org/en
Email: info@nomoreddos.org