



CONCORDIA

Cyber security cOmpeteNCe fOr Research and InnovAtion

Developing and Evaluating a DDoS Clearing House for Europe

Euritas Summit, Brussels, Sep 30, 2021

Cristian Hesselman (SIDN Labs)

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





High-impact DDoS Examples

Mirai botnet, 2016

Mirai botnet attackers are trying to knock an entire country offline

The nation state has a single point of failure fiber, recently installed in 2011, and it could stop other countries.

By Zach Whitaker for Zero Day | November 3, 2016 - 10:08 GMT | Topic: Security

Since the cyberattack on Dyn two weeks ago, the internet has been on edge, fearing another massive attack that would throw millions off the face of the web. The attack was said to be operated by L3370 - made that double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 400,000 in size, said to be one of the largest at the time. The attack was made possible by the Mirai botnet, an open-source botnet that anyone can use, which harnesses the power of insecure Internet of Things (IoT) devices.

This week, another Mirai botnet, known as Botnet 2.0, began targeting a small, little-known African country, Liberia, sending

HERE SECURITY NEWS
Powers Broad data leak reportedly exposed millions of customer records
LLN: How to use Cloudflare's DNS service to speed up and secure your internet
How: We now won't ever patch Spectre variant 2
Windows 10 security...

Liberia, 2016

Estonia, 2007



Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

19 MA 19 JANUARI, 10:55 AANGESMET MA 19 JANUARI, 17:37 BINNENLAND ECONOMIE

DigiD je eigen inlogcode voor de hele overheid

Handige links
• Wachtwoord vergeten?
• Missie-middel nummer opgevoerd?
• Helpcode ontvangen?

Laatste nieuws
• Wachtwoord vergeten? mals DigiD
• Wachtwoorden in nieuw versie DigiD
• Is uw computersysteem geschikt om

De golf van DDoS-aanvallen op Nederlandse instellingen houdt aan. Vandaag is de Belastingdienst tweemaal getroffen, en sinds 15.45 uur heeft ook DigiD last van een DDoS-aanval waardoor de site slecht bereikbaar is.

Volgens een woordvoerder van DigiD "gebeurt een aanval wel vaker, maar dit is wel zwaar". Er wordt hard gewerkt aan een oplossing. Hoelang dat nog gaat duren, kan de woordvoerder niet zeggen.

The Netherlands, January 2018

The Netherlands, September 2020

Opnieuw vinden grootschalige ddoS-aanvallen op Nederlandse providers plaats

Dinsdag worden opnieuw meerdere Nederlandse providers getroffen door ddoS-aanvallen. Dit is het grootste in omvang te worden en ook ruimtelijk geconcentreerd te zijn. Onder andere Sigmet, Calway en Delta zijn dinsdag slachtoffer.

De ddoS-aanvallen vinden onder andere plaats bij Calway, Delta, Sigmet, en Delta. Eerder op donsdagochtend had provider Delta (010.000.0000) de meest overrompeld door een ddoS-aanval. Verder wordt er dinsdagmiddag een grote aanval gedaan op Sigmet. Dit is een tip die de infrastructuur voor veel kleine providers versorgt. Dit betreft Sigmet infrastructuur voor TransIP. Daar hadden klanten vermelding van updates door de aanval, al op diezelfde dag.

Het lijkt erop dat het om dezelfde aanvallen gaat als die vorig week Nederlandse providers troffen, al is het niet met zekerheid te zeggen. Volgens een woordvoerder van het NISII gaat het voornamelijk om dns amplification- en tcp-aanvallen. Het Nederlands Belastingagentschap (Belastingdienst) heeft de aanval op de website van de Belastingdienst. Het is niet bekend of de Belastingdienst de aanval heeft overleefd. Het is niet bekend of de Belastingdienst de aanval heeft overleefd.

House of Representatives of The Netherlands, Oct 2020



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

More than 200 organisations across Belgium including the government and parliament were affected by a DDoS attack that overwhelmed them with bad traffic.

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

DDoS attacks: Simple but effective: Why DDoS attacks are still a major cyber threat to your networks

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



Reduced Digital Autonomy

- Society increasingly depends on online services => disruptions
- DDoS mitigation services (e.g., scrubbing) getting more important
 - Fortunately, providers usually able to routinely handle DDoS attacks
 - For example, NBIP/NaWas handled 715 attacks in Q2 2021, 164Gbps peak rate [1]
 - DDoS attacks increasingly involve ransom demands [2]
- But no sharing of DDoS intelligence and expertise across organizations
 - Lowers response time and learning because of limited victim-specific view
 - Reduces innovation of mitigation processes and systems at ecosystem level
 - DDoS data “stuck” in systems of (US-based) DDoS mitigation providers

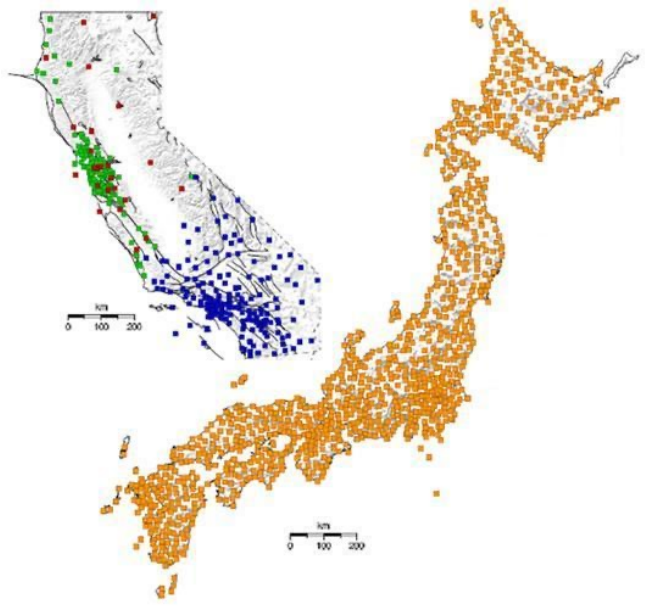
[1] <https://www.nbip.nl/wp-content/uploads/2021/07/NBIP-Infographic-DDoS-data-Q2-2021-EN.pdf>

[2] <https://www.zdnet.com/article/voip-company-battles-massive-ransom-ddos-attack/>



Need: “DDoS early warning system”

Earthquake early warning systems



<https://www.usgs.gov/media/images/earthquake-sensor-density-california-versus-japan>

Examples of protective earthquake actions:

- Safely stop vehicles (cars, trains)
- Open elevator doors
- Shut down production lines
- Stop delicate medical procedures
- Protect electricity grid



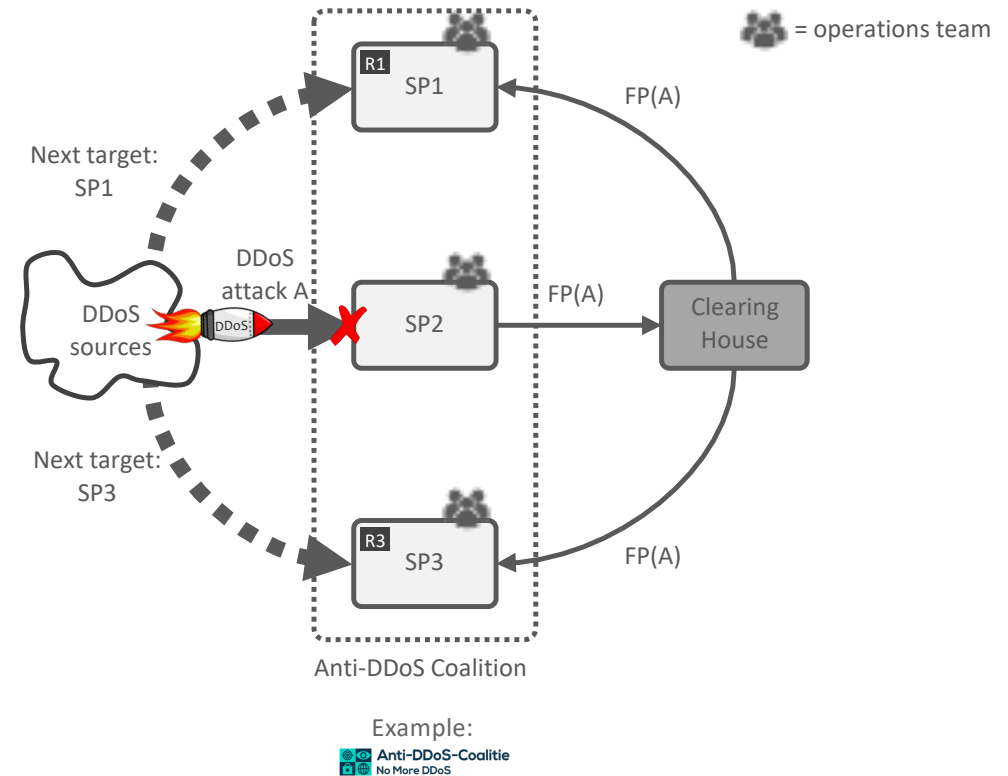
DDoS attacks:

- **Potential** victims prepare their networks
- DDoS sensors across organizations
- Capture incoming attacks



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
- Generic concept: across sectors, Member States, business units, etc.





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

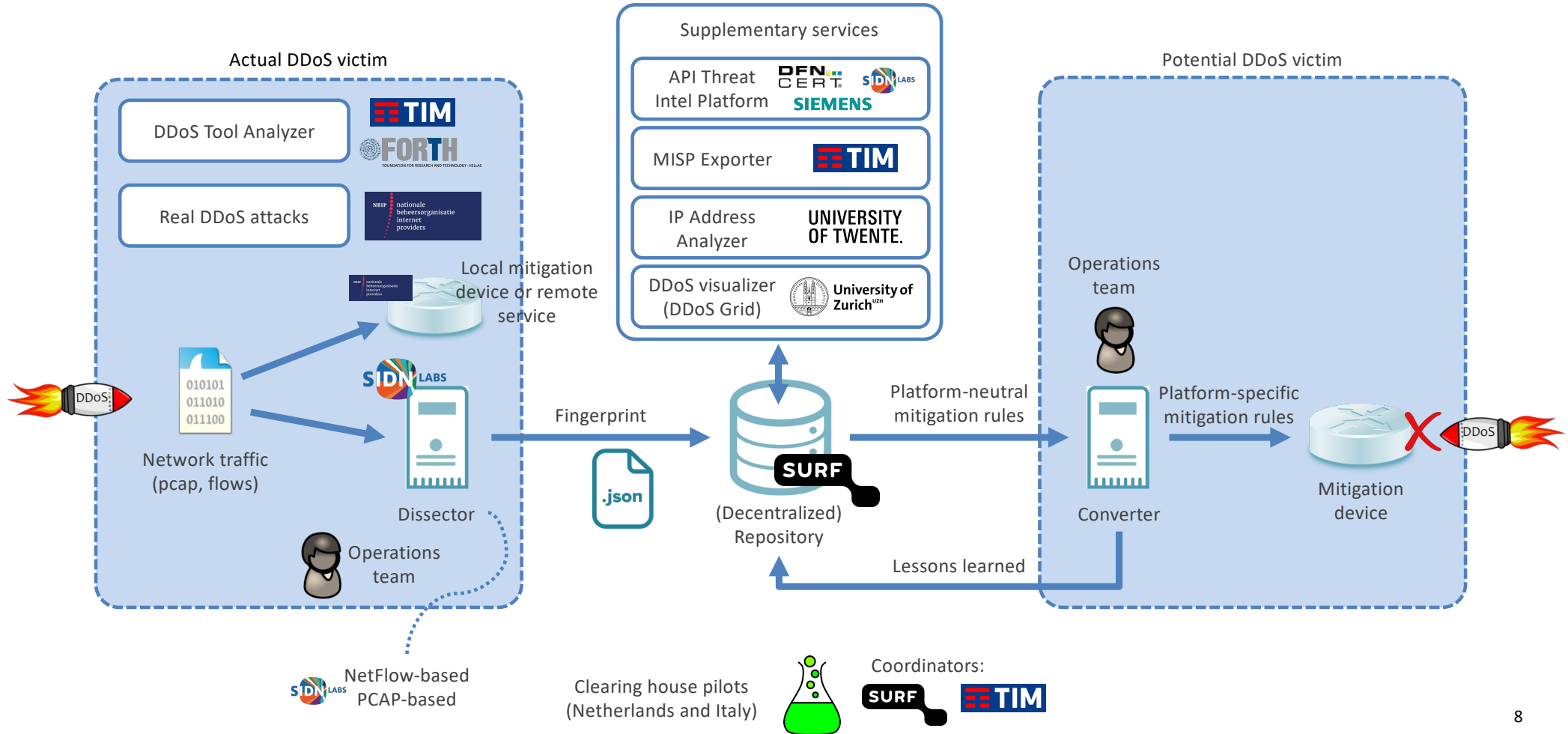


Clearing House increases Digital Autonomy

- 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



Main Components and Data Flows





DDoS Fingerprint Example

```
{
  "attack_vector": [
    "src_ips": [
      omitted;
    ],
    "attack_vector_key": "66f2e83fde0e6351d3f5ad967c6230aa3b60dbc498ad13b074296cb5f84c7734",
    "one_line_fingerprint": "{ 'dns_qry_type': 1, 'ip_proto': 'UDP',
    'highest_protocol': 'DNS', 'dns_qry_name': 'a.packetdevil.com',
    'frame_len': 1514, 'udp_length': 4103, 'srcport': 53,
    'fragmentation': True, 'src_ips': 'omitted' }"
  ],
  "start_time": "2013-08-14 23:04:00",
  "duration_sec": 0.16,
  "total_dst_ports": 4649,
  "avg_bps": 143426993,
  "total_packets": 16471,
  "ddos_attack_key": "44518107642b9ac7098174a16cbf220395c862bf26389c734e0b109b318e9291",
  "key": "44518107642b9ac",
  "total_ips": 2065,
  "tags": [
    "AMPLIFICATION",
    "DNS",
    "FRAGMENTATION",
    "UDP_SUSPECT_LENGTH",
    "DNS_QUERY",
    "SINGLE_VECTOR_ATTACK"
  ]
}
```



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	Low
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low
MISP Exporter	Generate MISP events based on DDoS fingerprints	Medium

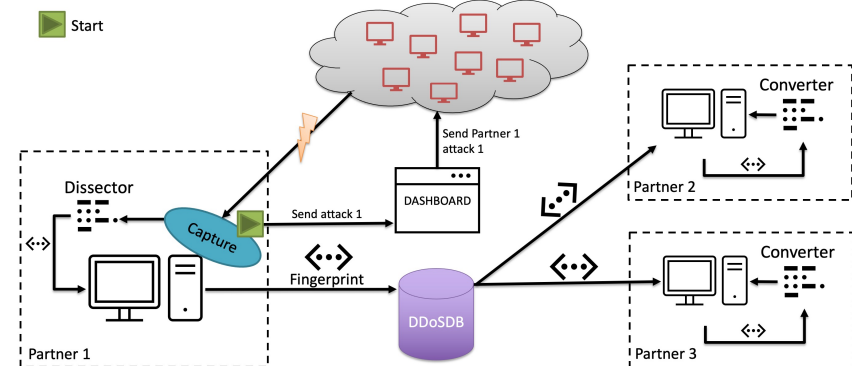
Overall: **stable framework**, most thrusts in the Dissector (adding and updating DDoS fingerprinting algorithms) and in the Converter (adding and updating rule-specific converters).



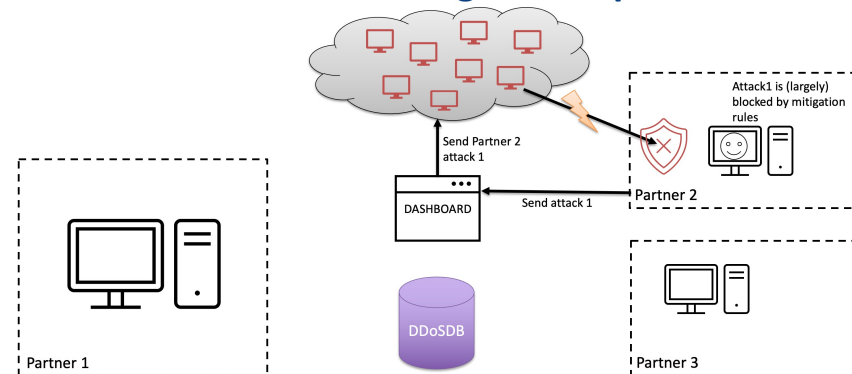
Distributed Clearing House Testbed

- The “DDoS target” manually initiates a stream of **test traffic** to itself through distributed cloud VMs
- Target’s Dissector creates fingerprint and sends it to the other partners through DDoS-DB, **without PII**
- Receivers locally construct filtering rules and manually initiate the same stream to **test the rules**

Simulation Diagram: step 1



Simulation Diagram: step 2





DDoS clearing house in the Netherlands



Anti-DDoS-Coalitie
No More DDoS

- DDoS clearing house R&D
- Clearing house distributed simulator
- 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



Dutch Anti-DDoS Coalition (NL-ADC)



UNIVERSITY
OF TWENTE.

CONCORDIA partner

CONCORDIA partner

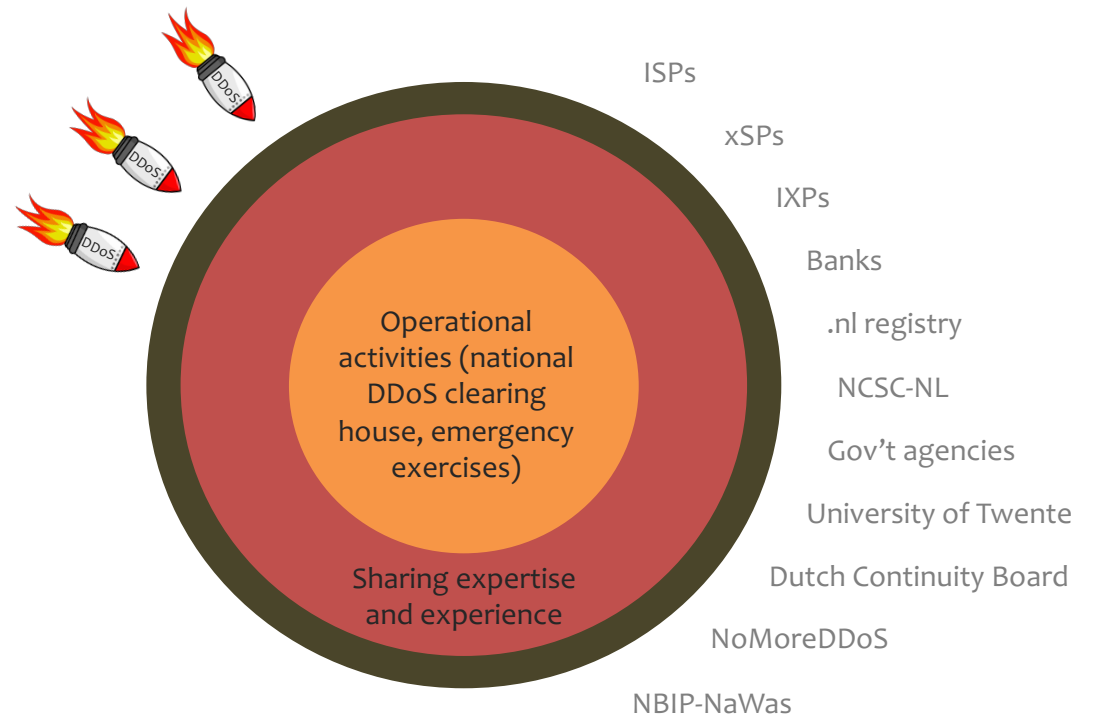
CONCORDIA partner





Approach

- Objective: further improve the resilience of Dutch critical services
- Strategies: sharing of DDoS measurements (clearing house), large scale collaborative drills, sharing expertise





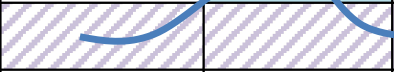



NL-ADC Status

- Approved consortium agreement
- Fee-based budget (EUR 114K total)
- Structure of WGs, clearing house operator and software developer
- Core team governing the initiative



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: SIDN Labs + NL-ADC members

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

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



DDoS Challenges for Public Administrations

- Fight DDoS attacks collaboratively 😊
- Keep the problem of DDoS attacks on the public and gov't radar
- Get your DDoS measurements from your third-party providers
- Governments in unique position to lead by example



Further reading

<https://www.sidnlabs.nl/en/news-and-blogs/new-ddos-classifiers-for-the-ddos-clearing-house>

<https://www.sidnlabs.nl/en/news-and-blogs/work-in-progress-the-concordia-platform-for-threat-intelligence>

<https://www.sidnlabs.nl/en/news-and-blogs/new-version-of-the-ddos-clearing-house-core-components>

<https://www.sidnlabs.nl/en/news-and-blogs/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward>

<https://www.sidnlabs.nl/en/news-and-blogs/setting-up-a-national-ddos-clearing-house>

<https://www.sidnlabs.nl/en/news-and-blogs/increasing-the-netherlands-ddos-resilience-together>



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

Thijs van den Hout
thijs.vandenhout@sidn.nl
[@thijsvandenhout](https://twitter.com/thijsvandenhout)