Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

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.

Contractual date of delivery	*M48 (31/12/2022)*
Actual date of delivery	*22/12/2022*
Deliverable dissemination level	*Public*
Editors	*Thijs van den Hout (SIDN)*
Contributors	*Thijs van den Hout (SIDN)* *Cristian Hesselman (SIDN, UT)* *Remco Poortinga (SURF)* *Ramin Yazdani (UT)* *Mattijs Jonker (UT)* *Christos Papachristos (FORTH)* *Paolo De Lutiis (TIM)* *Madalina Baltatu (TIM)* *Bruno Rodrigues (UZH)*
Quality assurance	*Walter Thomann (RUAG)* *Luis Barriga (Ericsson)* *Antonio Ken Iannillo (SnT)* *Claudio Ardagna (UMIL)*

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

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
ADS	Airbus Defence and Space GmbH (as a replacement for Airbus Protect GmbH)	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURF	SURF BV	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as a replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as a replacement for EFACEC Energia)	Portugal
ARTHUR’S LEGAL	Arthur’s Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~Germany~~

NCSA	Ministry of Digital Governance - National Cyber Security Authority	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany
FER	University of Zagreb, Faculty of Electrical Engineering and Computing	Croatia
ICENT	Innovation Centre Nikola Tesla	Croatia
Utilis	Utilis d.o.o	Croatia
Polito	Politecnico di Torino	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. Walter Thomann (RUAG)
2. Luis Barriga (Ericsson)
3. Antonio Ken Iannillo (SnT)
4. Claudio Ardagna (UMIL)

Revisions

Ver.	**Date**	**By**	**Overview**
0.1	*11/11/2022*	*All authors*	*First complete draft of document*
0.2	*23/11/2022*	*Internal reviewers*	*First internal review round*
0.3	*30/11/2022*	*All authors*	*Review 1 comments addressed*
0.4	*07/12/2022*	*Internal reviewers*	*Second internal review round*
1.0	*14/12/2022*	*All authors*	*Review 2 comments addressed*
1.1	*19/12/2022*	*Editor*	*Format document*
1.2	*22/12/2022*	*All authors*	*Final pass of entire document*

Disclaimer:
The sole responsibility of this document lies with the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

DDoS Clearing House Cookbook

Table of Contents

Abstract

Collaborative DDoS mitigation is the term used for the collection of activities organizations can engage in to fight DDoS attacks collaboratively. This includes sharing (meta) data on incoming DDoS attacks and participating in joint DDoS drills. Collaborative DDoS mitigation enables the members of so-called "anti-DDoS coalitions" (ADCs) to widen their view of the DDoS landscape beyond their own local perspective, which is crucial to proactively defend digital societies against large-scale disruptive DDoS attacks, for instance on critical infrastructures such as telecommunication networks, energy grids, water systems, and financial services. However, to the best of our knowledge, there has been no actual deployment of services for sharing DDoS intelligence in an ADC in a production context. This is because similar systems focus on developing the required technology and do not develop non-technical constructs, such as a governance model and data sharing agreements. The contribution of our work is that we solve this problem by addressing both perspectives: (1) we develop a technical system called the "DDoS Clearing House" for ADCs to share DDoS metadata and evaluate the system through pilots in the Netherlands and Italy, and (2) we co-develop the governance and legal constructs of the Dutch national ADC, which deploys the DDoS Clearing House as a production service. With this document, we intend to motivate and facilitate other groups of organizations to form an anti-DDoS coalition, with the DDoS Clearing House as a technical anchor.

Keywords: collaborative DDoS mitigation, DDoS data sharing, deployment, anti-DDoS coalitions, DDoS Clearing House

1 Introduction

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic[1]. Societies around the globe (e.g., Europe) are increasingly dependent on online services, even more so after the Covid-19 pandemic [1]. These dependencies increase the impact of Distributed Denial-of-Service (DDoS) attacks, with societies increasingly connecting their critical infrastructure to the Internet, such as telecommunication networks [2], energy grids [3], water supply systems [4], cooperative vehicle ecosystems [5], ambulances [6], and healthcare robots [7].

DDoS attacks on these critical infrastructures reduce societies' digital autonomy because they result in losing control over critical processes. For example, the DDoS attacks on Estonia in 2007 took down all government websites, sites of political parties, as well as those of two major banks [4]. Similarly, the series of DDoS attacks in the Netherlands in 2018 caused service disruptions at three banks, the Dutch Tax Services, and at "DigiD" [8], the identity system for Dutch citizens to interact with government services. DDoS strikes may also affect the underlying Internet infrastructure, as illustrated by the attack on the DNS root in 2015 [9], the IoT-powered DDoS attack on DNS operator Dyn in 2016 [10], and the DDoS attacks on several Dutch ISPs in September 2020 [11]. This last event led to parliamentary questions in the Netherlands [12], which shows an increased societal awareness of the problem. The

[1] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

impact of DDoS attacks may even extend to physical space [13], for instance when they disrupt future services such as unmanned aerial vehicles and connected ambulances.

Organizations protect themselves against DDoS attacks through mitigation services, which use techniques such as sinkholing of traffic or “scrubbing” network traffic to remove malicious traffic. Many outsource this service to a third-party because DDoS mitigation requires highly specialized expertise (e.g., in terms of types of DDoS attacks, Internet routing, and distributed computing) and a high-capacity infrastructure (e.g., fiber optic links and scrubbing capacity). A typical setup is that the potential victim has a basic DDoS mitigation service on-site to handle smaller attacks (e.g., through a DDoS appliance) and redirects attack traffic to the third party if they cannot handle the load. Third parties are typically US-based commercial companies, such as Arbor, Akamai, and Cloudflare. A notable exception is NBIP’s NaWas, the National Scrubbing Center of the Netherlands[2], a not-for-profit organization that offers scrubbing as a shared service to its member organizations.

The problem with this way of handling DDoS attacks is that it focuses on mitigating them for individual organizations rather than across organizations, such as for a specific sector of society or a specific country. Therefore, organizations cannot learn from the DDoS attacks targeted at another organization and are forced to go through the same learning curve as the first organization. Broadly speaking, mitigating DDoS attacks across organizations is important because the same attack may hit different organizations over time.

The root cause of this soloistic stance is that victims do not have the technical, legal, and organizational means to easily build up a joint pool of data (e.g., traffic measurements and successful mitigation rules), best practices (e.g., for incident response procedures or for selecting a DDoS mitigation service), and experiences (e.g., with a particular mitigation service) irrespective of the DDoS mitigation provider they use. At the same time, DDoS mitigation providers do not have the business incentive to share this information because that is how they make their money.

One of the consequences is that it prevents a more proactive way of DDoS mitigation. For example, when victim V1 (cf. Figure 1) gets hit by a particular DDoS attack, it will not be able to easily share metadata about that attack (e.g., its traffic characteristics or mitigation rules) with victim V3 because they use different mitigation providers. As a result, V3 will have to go through the same learning curve as V1 when that same attack hits them. This unnecessarily increases the time it takes V3 to mitigate the attack and might extend the service unavailability for their customers. It also increases pressure on V3’s operations teams because they must handle attacks unprepared while their services are starting to degrade, which increases the probability of human error and further extended outages. This process might repeat itself for the next few victims until operations teams manage to reactively share details about the attack through communications channels such as secure chat or email. At that point, however, the attacks could already have created significant disruptions to V3 and others. An example is the series of DDoS attacks that took place in the Netherlands in January of 2018 [8].

[2] https://www.nbip.nl/en/nawas/

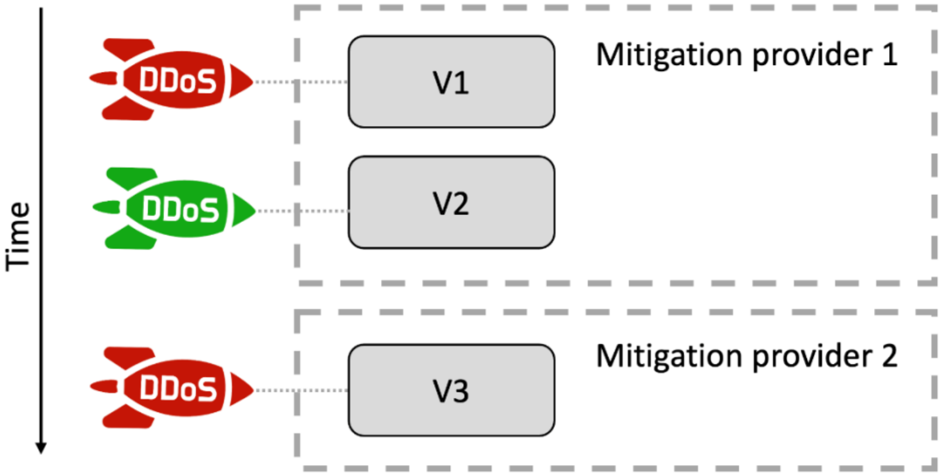


Figure 1: Lack of inter-organizational DDoS coordination

Another consequence of optimizing DDoS mitigation for individual victims is that it creates an obstacle for victims to innovate their anti-DDoS procedures and systems. For example, without DDoS data it is more difficult for organizations to learn from the evolution of attacks and from each other. The reason is that an in-depth post-mortem analysis of large DDoS attacks may require several datasets from several operators to fully understand what happened. For example, the analysis of the IoT-powered DDoS attack on DNS operator Dyn in 2016 involved 11 datasets (e.g., telnet honeypots, passive and active DNS datasets, and DDoS traces) across 9 different organizations [10]. With organizations' current soloistic mitigation strategy, it is difficult to get an overview of which organization has which datasets about the attack and then collaboratively analyze and learn from the data. This reduces the DDoS response and innovation capabilities of sectors and even entire societies, making them more susceptible to large service disruptions. It also makes it more difficult for organizations to formulate requirements for DDoS mitigation services, which increases their capital and operational expenses.

The solution to this problem is that groups of victims build up a shared pool of data, expertise, and knowledge by adopting a collaborative way of DDoS mitigation. While this concept has been around for a long time [14], previous work focused on the technical dimension of collaborative DDoS mitigation [15]. Also, it had yet to see any significant uptake because it is not only a technical problem but also (and predominantly) an organizational and legal one. Additionally, only sharing DDoS metadata is not enough to increase a society's incident response capabilities: it requires collaboration on all fronts, such as sharing expertise and carrying out joint DDoS drills.

The contribution of this document is (1) a multi-disciplinary cookbook on how to enable organizations to fight DDoS collaboratively and (2) our experience and lessons learned in setting up such a collaboration. The novelty comes from the combination of perspectives and not just from the technical work alone.

2 Collaborative DDoS mitigation through anti-DDoS coalitions

2.1 Concept

Our work aims to address the above problems by **changing the model of handling DDoS attacks** from a soloistic activity to a collaborative one [15]. This enables critical service providers to (1) increase their insight into DDoS attacks from their own narrow view to an ecosystem-wide view, and (2) increase their control over DDoS attacks because the new insights give them more grip on the requirements that they need to put on their DDoS mitigation facilities (their own or those of a contracted third party). As a result, a collaborative DDoS mitigation strategy contributes to increased digital autonomy, not only at the level of sectors and society but at the level of individual organizations as well.

To change to a collaborative DDoS mitigation strategy, we introduce the notion of an **Anti-DDoS Coalition** (ADC): a community of organizations that pledge to a **common goal**: to improve the resilience of the services that group members offer to their users by fighting DDoS attacks on a cooperative basis. The members of an ADC attain their joint objective through **three types of activities** (see Figure 2): the sharing of metadata on DDoS attacks through a DDoS Clearing House (see below for details) [16], large-scale DDoS drills to test members' DDoS resilience, and sharing DDoS expertise. Sharing metadata and expertise is done like in an ISAC (Information Sharing and Analysis Center), a sector-specific central resource for gathering information on cyber threats.

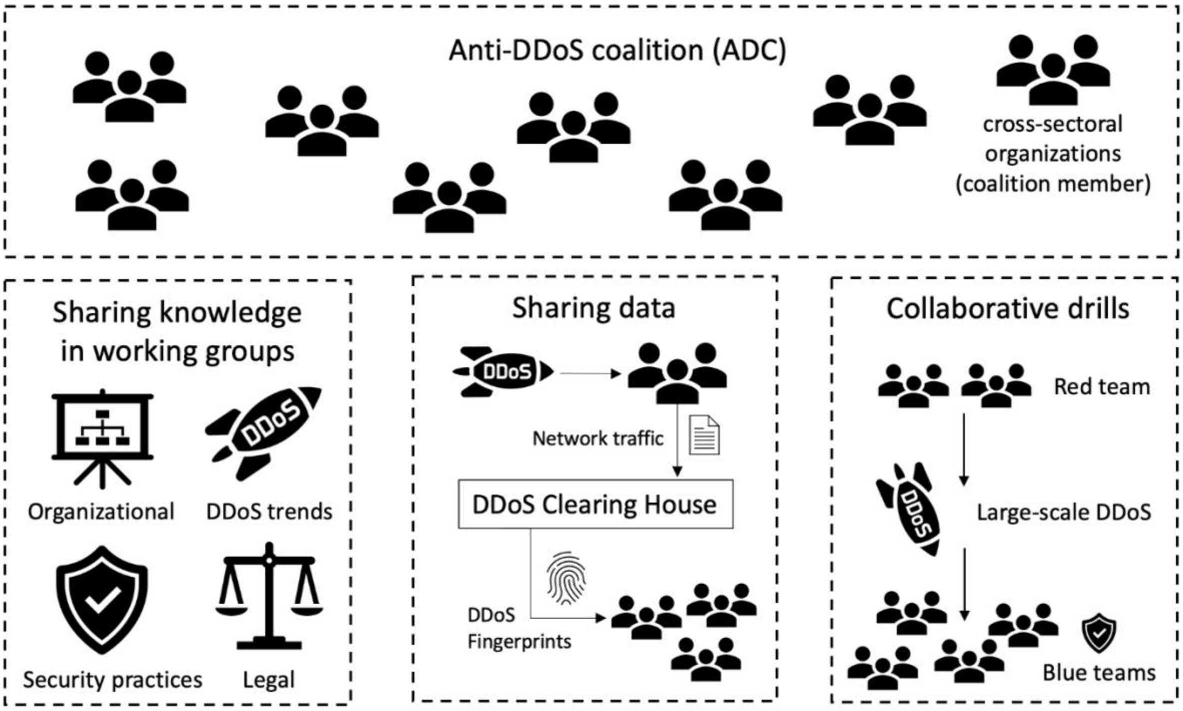


Figure 2: An anti-DDoS coalition and its activities

The **members of an ADC** can consist of public and/or private organizations that are potential DDoS victims (e.g., grid operators, financial institutions, and government agencies). For example, the Dutch ADC[3] has a cross-sector membership (e.g., telecommunications, finance, and governments) and a national focus (the Netherlands). An alternative way to organize ADCs is based on a specific sector (e.g., financial services, e-health providers, or the energy sector), potentially across EU Member States. Another example of ADCs are ISACs, but they typically focus on sharing expertise and do not share DDoS metadata. ADCs can also have different governance models, ranging from membership organizations with a board and bylaws to more informal collaborations like MANRS[4]

In addition to potential victims, an ADC can also include DDoS mitigation providers willing to share the metadata of the DDoS attacks they handle or that provide shared DDoS mitigation services for the members of the ADC [16]. An example is NBIP, a not-for-profit scrubbing provider and member of the Dutch national ADC. ADCs can also work without such shared mitigation facilities; in which case each member is responsible for providing their own.

Another type of ADC member is law enforcement agencies, who can potentially use the DDoS metadata for criminal investigation and subsequent court trials. For such members, the ADC needs to offer safeguards that prevent incorrect data from entering the legal system, such as an accurate timestamp that indicates when DDoS metadata was generated, cryptographic proof that it was not tampered with, as well as legal constructs to draw a clear line between gathered information (through the Clearing House) and using it for criminal investigation (by law enforcement agencies). The latter is important considering the ongoing discourse on the role of the private sector actions in fighting cybercrime [17].

Organizations may be part of multiple ADCs at the same time. For example, a pan-European bank could share its DDoS metadata with national cross-sector ADCs in the different Member States where they have offices, as well as with the pan-European banking ADC. These coalitions will typically have different objectives, such as protecting the Netherlands' critical infrastructure against DDoS attacks versus protecting European banks against DDoS attacks.

Our **main ADC use case** is the Dutch Anti-DDoS Coalition. We have been working on the topic of joint DDoS mitigation with them since 2018. The Dutch ADC consists of 16 organizations from various sectors (e.g., governments, internet exchanges, internet service providers, and academic institutes). They formulated four requirements for joint DDoS mitigation: (1) organizations must be able to share DDoS data, (2) organizations must be able to exchange experiences and expertise, (3) organizations must be facilitated to regularly carry our joint large-scale DDoS drills, and (4) the initiative should have a flexible membership model.

To facilitate the realization of these requirements, the Dutch ADC set up working groups, each of which concerns itself with a cog on the wheel of the coalition. The five working groups are Legal matters, Communication, Clearing House, Practice, and Architecture & Society. Each working group holds monthly meetings during which they discuss their progress, and each quarter the entire coalition comes together in a plenary meeting.

The following subsections briefly elaborate on the four requirements for a functional and effective anti-DDoS coalition that the Dutch ADC formulated.

[3] https://www.nomoreddos.org/en

[4] https://www.manrs.org/

2.2 Requirement #1: DDoS data sharing

The first requirement is that members of an anti-DDoS coalition should share their data on the DDoS attacks they receive with the rest of the coalition, independent of the particular (commercial) DDoS mitigation services they are using (e.g., Cloudflare, Arbor, or Akamai). DDoS data from a large group of organizations gives each organization a broader insight into the DDoS landscape of the anti-DDoS coalitions they are a part of, which leads to a wider set of mitigation actions than they would have with their own narrow view of the problem. For example, shared DDoS measurements help potential targets identify new types of attacks and assess better if their current mitigation strategy is still fit for their purpose. As a result, targets become more independent of DDoS mitigation providers and their (proprietary) techniques. This increases the digital autonomy of organizations and of the societies they serve.

Anti-DDoS coalitions require standardized methods for sharing measurements and other data on the DDoS attacks they receive among their members. To this end, we developed the DDoS Clearing House. The DDoS Clearing House enables organizations to create a standardized summary (or "fingerprint") of the network traffic during a DDoS attack. Such fingerprints can easily be shared with other coalition members through the DDoS-DB. We elaborate further on the technical specifications of the DDoS Clearing House in Section 4.

Because the source IP addresses of DDoS traffic are considered Personally Identifiable Information (PII), organizations must sign a data sharing agreement in compliance with the GDPR in Europe. We provide the data sharing agreement used in the Dutch anti-DDoS coalition in appendix 2 (14.2).

2.3 Requirement #2: Knowledge sharing

Besides sharing measurements of DDoS attacks and other relevant *data*, anti-DDoS coalitions need to provide a platform for organizations to exchange knowledge and expertise on DDoS mitigation. For example, the five working groups in the Dutch anti-DDoS coalition enable members to meet and exchange knowledge about DDoS in their respective fields, be it legislative, technical, or otherwise.

The sharing of knowledge and expertise can take on the form of the more familiar concept of ISACs (Information Sharing and Analysis Center).

2.4 Requirement #3: Joint DDoS drills

The third requirement is that members of an anti-DDoS coalition should be able to carry out joint DDoS drills. For example, the Dutch Anti-DDoS Coalition created the opportunity to collaboratively generate network and application-level DDoS attacks and practice responding to them. Such activities fit naturally in the context of an anti-DDoS coalition because of its inter-organizational nature and because it helps to increase DDoS resilience.

The partners in the Dutch anti-DDoS coalition carried out a practice drill in October of 2019, which involved launching previously approved DDoS attacks on each other's infrastructures to learn how their systems and teams would respond. Since then, joint DDoS drills have become a bi-yearly occurrence and are part of the coalition's foundation. In Section 5 we elaborate further on the design and execution of joint DDoS drills in anti-DDoS coalitions.

2.5 Requirement #4: Flexible and open governance model

A well-defined governance model is crucial to providing continuity to an anti-DDoS coalition. We identified this early on because we had to develop and maintain various "products" such as a website, iterations of the Clearing House's data sharing agreement, procedures and waiver agreements for DDoS exercises, and the rules of engagement for coalition members (e.g., membership rules). These products require supervision from some form of governance body. That is why we organized the coalition into several working groups, such as a technical working group to develop the Clearing House software. A legal working group is particularly important, for instance for developing new versions of the data sharing agreement and new versions of the pilot, which are crucial for speeding up the development and the deployment of the Clearing House.

There is no technical approach or formal method for establishing trust between different organizations. In this regard, when setting up an ADC, we found it is best to start with a small group of organizations we know and trust and grow from there (trust scaling). We started the development of the Clearing House with ten partners. Keeping the group small facilitated the development of mutual trust, for instance through frequent face-to-face meetings. As a result, the group was confident that it could reach consensus on the technical direction, and therefore opted for unanimous decision-making in our current "governance model" (formalized as part of the data sharing agreement). This enabled us to make decisions quickly in the initial stages, although a model based on unanimous decision-making will not scale up to an organization with dozens of partners. A challenge is to scale up trust, requiring the transition from a model where the ten service providers trust each other on a person-to-person basis (personal trust) to a model with a larger group of organizations that trust the Clearing House and its procedures and governance mechanisms (impersonal trust [18]).

We chose to make the initial data sharing agreement for the Clearing House simple and scalable. The data sharing agreement needs to clearly articulate the purpose of the first iteration of the pilot, which is to assess the usefulness and effectiveness of the Clearing House by experimenting with exchanging DDoS fingerprints across different organizations and sectors. It also needs to cover other legal aspects (e.g., liability, security, privacy, and governance), but only in outline. That is important to keep the data sharing agreement simple and scalable and allow for technical experimentation. A future challenge will be to evolve the data sharing agreement so that its simplicity and scalability continue to be appropriate for the coalition's state.

The complete translated governance regulation document of the Dutch Anti-DDoS Coalition is attached in Appendix 3 (14.3). The membership agreement is attached in Appendix 4 (14.4).

3 Existing solutions

Existing collaborative DDoS mitigation initiatives [14][19][20] focus on facilitating data sharing from a technical perspective only (e.g., TAXI, STIX), which may also be why they are seeing less uptake.

The concept of collaborative DDoS defense has been around for a long time. Such systems face many challenges imposed by the need to provide a distributed defense in a similar proportion of the distribution of attacks, such as the high complexity of operation and coordination, the need for trusted and secure communications, and the determination of how operations of these systems are affected by different legislation, regions, and countries. To the best of our knowledge, we are the first solution encompassing technical and organizational requirements of an anti-DDoS coalition into a fully operational solution. The first step towards the materialization of the solution is to understand that the fight against DDoS attacks goes beyond the materialization of a technical solution for information sharing - there must be a collective effort to establish organizational norms and standards.

Recent papers, such as “United We Stand” [21] propose a central hub that allows the information exchange of amplification DDoS attacks. The idea is that attack mitigation platforms, i.e., the Internet Exchange Points (IXP), collaborate by detecting attacks locally and sharing this information so that each IXP can drop the traffic, effectively weakening the later attack significantly. One issue with their proposal is that the underlying infrastructure of the Internet is highly heterogeneous. Thus, cooperative defense solutions imposing hardware requirements also limit their deployment and operation. This approach was not taken by the DDoS Clearing House, which works on standard data (e.g., PCAP- Packet Capture, NetFlow) retrieved from networking equipment to generate DDoS fingerprints alleviating such burden of requiring specialized infrastructure. In a similar direction [20], it makes use of consortium-based blockchain and smart contracts to share DDoS attack information collaboratively. Although such an approach can be run on general-purpose servers, it still imposes a communication overhead due to the use of a blockchain to propagate attack information. Nonetheless, the authors reinforce the view taken by the DDoS Clearing House by stating that a collaborative DDoS defense goes beyond the adoption of a purely technical solution - it also requires efforts toward the establishment of a legal basis, potential financial aspects, and the interplay of trust within a cooperative setting. An ideal solution should avoid extra hardware or software requirements on the underlying network infrastructure, which can be achieved either by using a novel technology (e.g., SDN – Software-Defined Network, and NFV – Network Function Virtualization) or a novel architecture, such as IETF DOTS and DefCOM.

The Internet Engineering Task Force (IETF) Distributed-Denial-of-Service Open Threat Signaling (DOTS) architecture [22] was devised as a standardization attempt for collaborative DDoS defense. Thus, it tackles the heterogeneity issues of the Internet's infrastructure by proposing a standard architecture and protocol for signaling DDoS information. Through the DOTS protocol, data models are provided to enable intra and inter-organizational DDoS defense with multiple parties. The DOTS protocol provides data models to enable intra- and inter-organizational DDoS defense with multiple parties. The DOTS client requests mitigation from the DOTS server after detecting an ongoing attack. Communication between the DOTS server and client takes place over a data as well as a signal channel. The client uses the signal channel to request mitigation from the server, and the server uses the signal channel to inform the client about the status of the mitigation. As part of the client's information to signal the server for help, attack targets, as well as telemetry data about the attack, can be provided through the signal channel to simplify the mitigation for the server.

Although presented in 2003, DefCOM is one of the significant proposals for cooperative network defenses [19]. It proposes an overlay network based on a Peer-to-Peer (P2P) gossip-based protocol to facilitate coordination among peers with inherent scalability. DefCOM is specifically geared toward protection against flooding DDoS attacks and focuses on three critical defense functionalities. The strength of the DefCOM system lies in the highly distributed and scalable overlay network used for communication. However, the overlay network is only used for control messages; data packets still travel on the data links defined by the underlying routing protocols.

The emerging paradigm of NFV is often used in conjunction with SDN. Through SDN, the data plane is decoupled from the networking infrastructure's control plane, allowing tailored solutions for specific networking needs. Bohatei [23] is a clear indicator of the scalability advantages in using SDN- and NFV-based networking to tackle the DDoS defense problem. The Bohatei proof-of-concept implementation is realized with the OpenDaylight SDN controller together with an assortment of open-source tools to facilitate routing and mitigation, such as Open vSwitch, Snort, Bro, and Iptables. In a similar direction, CoFence [24] is an approach that leverages NFV for a collaborative defense system. This can help incentivize potential new members to join a DDoS alliance. since device upgrading and creation are relatively fast and low-cost due to the virtualized nature of all networking components. Instead of relying on fixed hardware-based networking solutions, commodity hardware can launch virtualized networking appliances on-demand. Although Bohatei is an easily adoptable solution, the fact that it operates in SDN-based domains, which are not yet widely adopted, is considered a negative factor for wide adoption. In this regard, the DDoS Clearing House combines in its intrinsic design characteristics of NFV, being a network application ready to be executed out-of-the-box in a container environment that provides well-defined interfaces allowing, for example, its management from a central viewpoint offered by SDN controllers.

As of today, many service providers mitigate DDoS attacks single-handedly, focusing on protecting their own infrastructures (soloistic approach). Some do participate in group protection services such as NBIP’s Nawas to share equipment and expertise, and to spread the cost. The lack of deployment also means a limited insight into other parameters besides technology. Examples include software that can easily be deployed in operational environments, software auditing, anti-DDoS drills, operational costs, and organizational and legal constructs. The DDoS Clearing House that we piloted in CONCORDIA (cf. Section 7 on DDoS Clearing House pilots) advances the state of the art by developing and evaluating the mechanisms needed for these different perspectives combined, and not only from a technical perspective.

4 DDoS Clearing House

4.1 System design

An important building block of an anti-DDoS coalition is the DDoS Clearing House, a shared system that enables participating organizations to exchange metadata about DDoS attacks in the form of so-called "DDoS fingerprints". A fingerprint contains the key characteristics of a DDoS attack, such as the source IP addresses, source and target ports, protocols and services used, and information regarding the size, time, and duration of the attack. A Clearing House thus provides an extra layer of security information on top of the DDoS mitigation services that the members of an ADC need to have in place (e.g., scrubbing and blackholing services) and does not replace them.

Sharing DDoS fingerprints with other members warns them that new attacks may be underway. Figure 3 illustrates this for three service providers (SP1, SP2, and SP3). SP2 gets hit by DDoS attack A, generates a fingerprint that describes A (denoted as FP(A)), and shares it with the other members of the ADC (SP1 and SP3), with SP2's operations team potentially adding pointers as to the best way to mitigate A. The operations teams of SP1 and SP3 use the fingerprint to derive traffic filtering rules (R1 and R3) and install them in their network equipment in case A comes their way next. Alternatively, SP1 and SP3 can request their upstream transit providers to block A's address blocks (e.g., using DOTS [25]). The three service providers also use the Clearing House to get fingerprints of past attacks and compare them to in-progress attacks on their infrastructure.

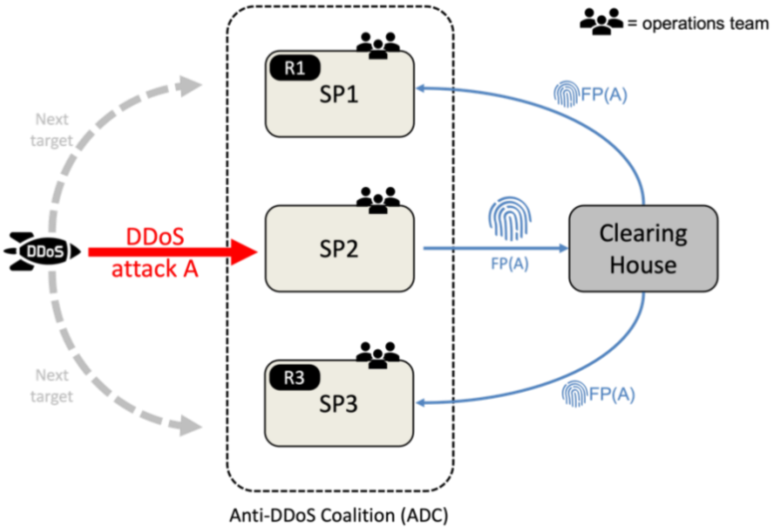


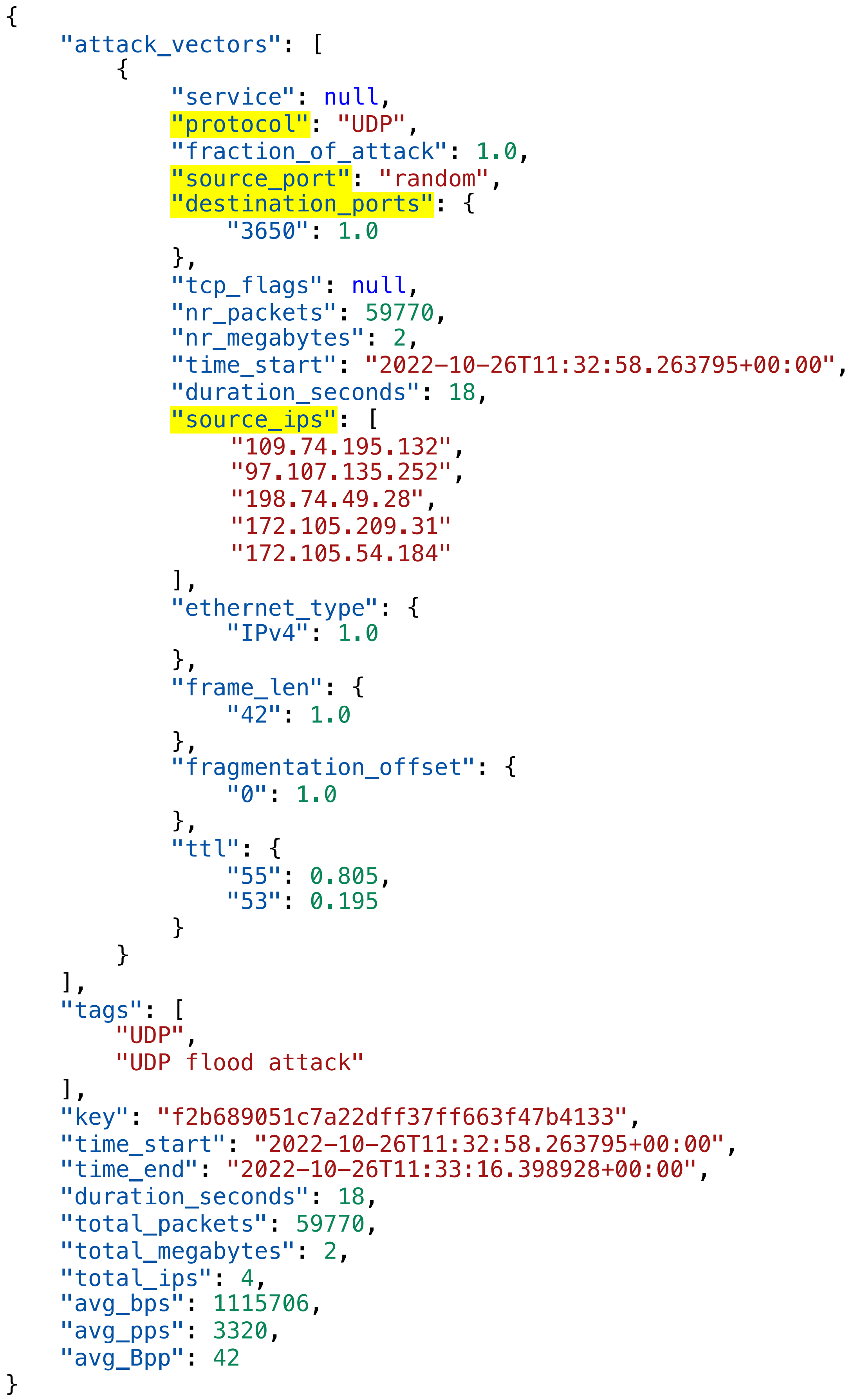
Figure 3: Anti-DDoS Coalition information flow

The advantage of the Clearing House is that the fingerprints help its members derive packet filter rules in advance of DDoS attacks, which usually takes place under intense pressure during an attack. For example, if SP1 were to be the next target of DDoS attack A without having A's fingerprint, then SP1's operations team would have to inspect the incoming DDoS traffic, write a packet filtering rule (R1) for the different types of equipment in their network, and push it into their network while, at the same time, the availability of SP1's services might start degrading. Having A's fingerprint beforehand gives them more time to implement R1, which increases the probability that they will be able to mitigate the attack effectively. Further analysis of the collected fingerprints can also provide more information that may be useful in DDoS mitigation, such as the appearance of new attack techniques or trends in DDoS attacks behavior over time.

Figure 4 shows an example of the DDoS fingerprint of a UDP flood attack. We see the attack originates from five IP addresses, from random source ports, targeting port 3650 of the victim's server (see highlighted sections). As this example is generated with our testbed (see Section 6), the amount of traffic is very low.

All components of the DDoS Clearing House, as well as any supplementary software written in CONCORDIA is open source and available on the DDoS Clearing House GitHub organization[5].

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



```
{
    "attack_vectors": [
        {
            "service": null,
            "protocol": "UDP",
            "fraction_of_attack": 1.0,
            "source_port": "random",
            "destination_ports": {
                "3650": 1.0
            },
            "tcp_flags": null,
            "nr_packets": 59770,
            "nr_megabytes": 2,
            "time_start": "2022-10-26T11:32:58.263795+00:00",
            "duration_seconds": 18,
            "source_ips": [
                "109.74.195.132",
                "97.107.135.252",
                "198.74.49.28",
                "172.105.209.31"
                "172.105.54.184"
            ],
            "ethernet_type": {
                "IPv4": 1.0
            },
            "frame_len": {
                "42": 1.0
            },
            "fragmentation_offset": {
                "0": 1.0
            },
            "ttl": {
                "55": 0.805,
                "53": 0.195
            }
        }
    ],
    "tags": [
        "UDP",
        "UDP flood attack"
    ],
    "key": "f2b689051c7a22dff37ff663f47b4133",
    "time_start": "2022-10-26T11:32:58.263795+00:00",
    "time_end": "2022-10-26T11:33:16.398928+00:00",
    "duration_seconds": 18,
    "total_packets": 59770,
    "total_megabytes": 2,
    "total_ips": 4,
    "avg_bps": 1115706,
    "avg_pps": 3320,
    "avg_Bpp": 42
}
```

Figure 4: Example fingerprint of a UDP flood attack

4.2 Functional architecture

The functional architecture of the DDoS Clearing House consists of two types of components:

- Core components: enable operations teams to generate, store, distribute, and use fingerprints.
- Supplementary services: can enrich and visualize fingerprints or provide analyses across multiple fingerprints.

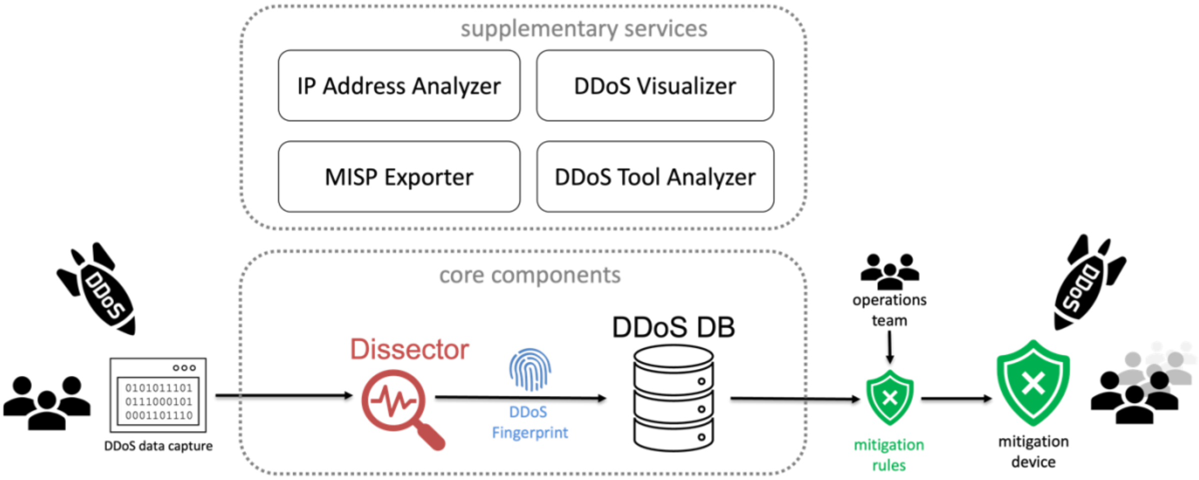


Figure 5: DDoS Clearing House schematic overview

Figure 5 shows the functional architecture. The arrows in the figure illustrate how a fingerprint typically flows through the system, from its creation based on network traces at the member that gets hit by the DDoS attack (left) to its use by a potential victim to create some form of mitigation based on the information provided by the fingerprints (right). How DDoS data is captured and how the information from fingerprints can be converted into mitigation measures, depends on the technology in use by the different members. Each member of an ADC can run one, more, or all the Clearing House's components.

Table 1 provides a short description of the function of each component or service. The Sections on core components (4.2.1) and supplementary services (4.2.2) will provide a more detailed description for each.

Table 1: DDoS Clearing House components

Name	Function
Dissector	Generates fingerprints based on DDoS network traffic samples.
DDoS-DB	Stores fingerprints generated by the Dissector, for use by other components. Access is via a token-authenticated REST API.
IP Address Analyzer	Enhances fingerprints with additional information on IP addresses/ranges involved.
MISP Exporter	Generates MISP events based on a fingerprint.
DDoS Visualizer	Provides a dashboard for the visualization of fingerprints.
DDoS Tool Analyzer	Creates fingerprints of traffic generated by tools frequently used by attackers.

4.2.1 Core components

The core components are self-contained and so they can be executed either on different systems or on one machine.

Dissector

The Dissector generates fingerprints based on DDoS network traffic traces. It aggregates the network traffic characteristics of the attack traffic to construct summaries of the attack vectors that make up the attack. Therefore, it is not specifically designed to summarize specific attack types, meaning it can cope with the evolving characteristics of DDoS attacks. The Dissector looks for significant outliers of attack characteristics such as source port, network protocol, and TCP flags to construct attack vector summaries. For each attack vector, the characteristics are further described. Finally, a complete summary of the entire attack, containing information such as the duration, number of packets, and average bytes per second is added to the fingerprint.

The complete format of all available fields in a DDoS fingerprint is included in Appendix 1 (14.1).

The Dissector can take as input PCAPs and network flows (e.g., from NetFlow, IPFlow). The need for Flow support came from real-life experience in the Dutch ADC, where one of the partners typically uses NetFlow to get an insight into the network traffic. Therefore, the ability to process NetFlow files makes it much easier to integrate with the existing operations and procedures.

The Dissector outputs fingerprints that describe an attack using several fields, such as attack vectors (e.g., amplification attack) and several labels that describe the attack's characteristics, such as “amplification” and “suspicious packet length”. Fingerprints can be stored locally or uploaded to a DDoS-DB. Multiple DDoS-DBs can be configured, giving the user a choice of which fingerprint to upload to which DDoS-DB. This enables them to directly share fingerprints with other members of an ADC rather than through the central DDoS-DB, allowing for several options when setting up an ADC, which contributes to increasing the resilience of the DDoS Clearing House.

The latest version of the Dissector also has the MISP Exporter functionality built-in, allowing for even more versatile options for setting up an ADC.

DDoS-DB

Stores fingerprints, enables Dissectors and supplementary services to insert, retrieve or update DDoS fingerprints in DDoS-DB via a protected API. DDoS-DB also provides a web interface to allow operations teams to search and view fingerprints, add/edit comments of fingerprints, and manage the DDoS-DB itself.

DDoS-DB can synchronize its fingerprints with other instances of a DDoS-DB, either in push or in pull mode or both. Push mode is useful, for example, if a local DDoS-DB is behind a firewall that only allows outgoing connections (connections initiated from the inside, going out), making it unreachable from the internet. If these local fingerprints need to be synchronized with a central DDoS-DB then they need to be pushed from the local DDoS-DB to the central

DDoS-DB since the central DDoS-DB cannot initiate a connection to the local DDoS-DB. Only fingerprints marked as 'shareable' are synchronized with other DDoS-DB instances and only those unknown by the other DDoS-DB are transferred to avoid unnecessary network traffic. Synchronization is done at regular (configurable) intervals (e.g., every hour or once a day). Section 4.3 provides examples for the push and pull synchronization. The ability to synchronize between DDoS-DBs allows for multiple setups of an ADC, e.g., a simple centralized setup, with only one central DDoS-DB and each member uploading directly, or a more elaborate centralized version with each member having a local DDoS-DB instance, or even a fully distributed setup, with no central DDoS-DB. See Section 4.4 for a description of possible setups.

Like the Dissector, the DDoS-DB also has MISP Exporter functionality built in, enabling the DDoS-DB to create MISP events based on the fingerprints it has stored. The exports to a MISP happen at regular (configurable) intervals and only fingerprints marked 'shareable' that are unknown to the MISP are exported.

The web interface makes searching for fingerprints more intuitive for operations teams. For example, it is possible to browse all fingerprints and filter or order them based on properties such as size, duration, or submitter. This is easier than entering search terms to find (types of) fingerprints, which can be difficult at first if one is unfamiliar with the associated search terms. Uploaded fingerprints can also be annotated, allowing comments to be added to them. This can be useful for providing mitigation notes that may help other operators to handle the attacks. Editing is limited to either admins of the DDoS-DB or the original provider of the fingerprint, to prevent tampering with ill-intent.

4.2.2 Supplementary services

The supplementary services of the Clearing House aim at enriching fingerprints and making the system intuitive for operations teams. Together, they further enhance the added value of the core components.

MISP Exporter

Generates MISP events based on DDoS fingerprints. MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform, widely used in cybersecurity contexts. The MISP Exporter takes as input a fingerprint file describing a DDoS attack and maps fingerprint attributes to the attributes of a MISP event. For example, it stores the fingerprint’s source IP addresses in the MISP attribute Network activity/ip-src and the original fingerprint itself in the MISP attribute External analysis/attachment. Next, the Exporter publishes the event to the MISP instance, as shown in Figure 6.

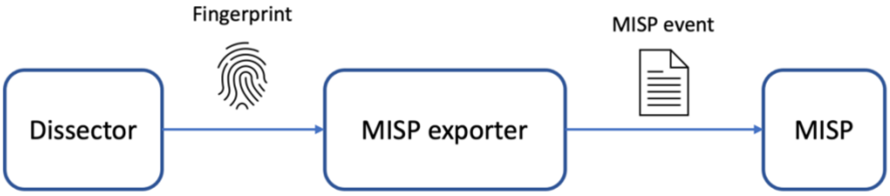


Figure 6: MISP Exporter component

Although MISP can generate mitigation rules based on this information, the challenge is that currently it only supports very simple Snort mitigation rules, which additionally only use the ip-src attributes in MISP events. This makes it less suited for mitigating real-life DDoS attacks, that may involve hundreds of thousands of source IP addresses. Creating MISP events based on fingerprints is still useful for recording DDoS incidents.

Despite MISP Exporter being part of the supplementary services, the latest versions of the Dissector and the DDoS-DB incorporate its functionality to facilitate using MISP in an ADC setting.

DDoS Visualizer (DDoS Grid)
Provides a dashboard for the visualization of DDoS fingerprints based on PCAP files or DDoS fingerprints. The DDoS Grid allows operations teams to extract the main features of large PCAPs (traces of packet capture) observing trace characteristics such as protocols and ports, IP addresses. For example, the DDoS Grid allows rendering charts of all source IP addresses on the X-axis and their aggregated traffic bandwidth on the Y-axis of a scatter plot chart. In this regard, DDoS Grid implements several specific miners that allow for the orchestration of feature extraction modules allowing a detailed analysis of PCAPs. In addition, the DDoS Grid uses the Dissector API to generate fingerprints, and analyze fingerprints stored in DDoS-DB by relying on the DDoS-DB's API). Besides network operators, we expect these functions will also be useful for researchers to create showcases for educational purposes.

IP Address Analyzer
Analyzes source IP addresses in a fingerprint using various IP intelligence datasets provided by third parties and public datasets and adds these details to the fingerprint. Examples are the geolocation details, the networks where the attacker hosts reside and the type of those networks. The provided metadata of the IP Address Analyzer gives operations teams and security researchers a better understanding of the similarities and differences between various attacks and attacking hosts. The analyzer can process a large set of IP addresses, which is common for DDoS traffic. The component also provides a world map plot to show the geolocation of public IP addresses in a DDoS fingerprint, to get a visual insight into where the DDoS traffic is coming from.

4.3 Interfaces (API)

A critical element in our modular architecture is the interaction between the Clearing House's components, with (instances of the) DDoS-DB as the central element(s).
All interaction and synchronization between the different components is done via the API that a DDoS-DB provides. Authentication is done via tokens using a header in the form of 'Authorization: Token <TOKEN>'. See also 'API access' in Section 4.5.2 for more details on handling tokens.

The following API endpoints are provided:

- **/api/permissions**
    - *GET* Returns all the permissions (authorizations) associated with the provided Token.
- **/api/fingerprint**

    - *GET* Returns the keys of all the fingerprints set to 'shareable' present in this DDoS-DB in an array called 'shareable'. If the Token also has permission to view fingerprints not set to 'shareable' this endpoint will also return those keys in an array called 'non-shareable' (otherwise the 'non-shareable' array will be empty).
    - *POST* Stores the fingerprint(s) provided by the caller in the DDoS-DB. The caller needs to have permission to upload new fingerprints. If a fingerprint already exists in the DDoS-DB, the existing fingerprint will be overwritten.
- **/api/fingerprint/<key>**
    - *GET* Returns the full fingerprint identified by the key.
- **/api/unknown-fingerprints**
    - *POST* Returns the set of keys unknown by this DDoS-DB from the array of keys provided by the caller. The caller needs to have permission to upload new fingerprints (since otherwise there is no need to do this check). DDoS-DB instances that synchronize with each other use this call to make sure only fingerprints that are unknown by the remote instance are transferred.

4.3.1 API usage

The /api/permissions endpoint allows other components to check which permissions their token has. Components with a GUI can use the returned permissions to (visually) enable or disable specific functions.

The other API endpoints are for getting or creating fingerprints and for checking which fingerprints are already known to that DDoS-DB instance. The Dissector uses the /api/fingerprint endpoint for uploading fingerprints. The endpoints are also used for synchronization between DDoS-DB instances, as described below.

Push synchronization

Figure 7 shows push synchronization of fingerprints, from DDoS-DB1 (left) to DDoS-DB2 (right). Before synchronization DDoS-DB1 has shareable fingerprints with keys A, B and C. DDoS-DB2 has fingerprints with keys X, Y and C.

Synchronization starts with DDoS-DB1 posting the keys of all its shareable fingerprints to the /api/unknown-fingerprints endpoint of DDoS-DB2. DDoS-DB2 checks which of these fingerprints it does not have (A and B in this example) and returns those keys to DDoS-DB1 in response. DDoS-DB1 now knows that fingerprints A and B are unknown to DDoS-DB2 and pushes these fingerprints to DDoS-DB2 by posting them to the /api/fingerprint endpoint. Pushing only fingerprints that are unknown to DDoS-DB2 saves bandwidth and prevents two DDoS-DBs endlessly pushing their fingerprints to the other if they each have set up the other for push synchronization.

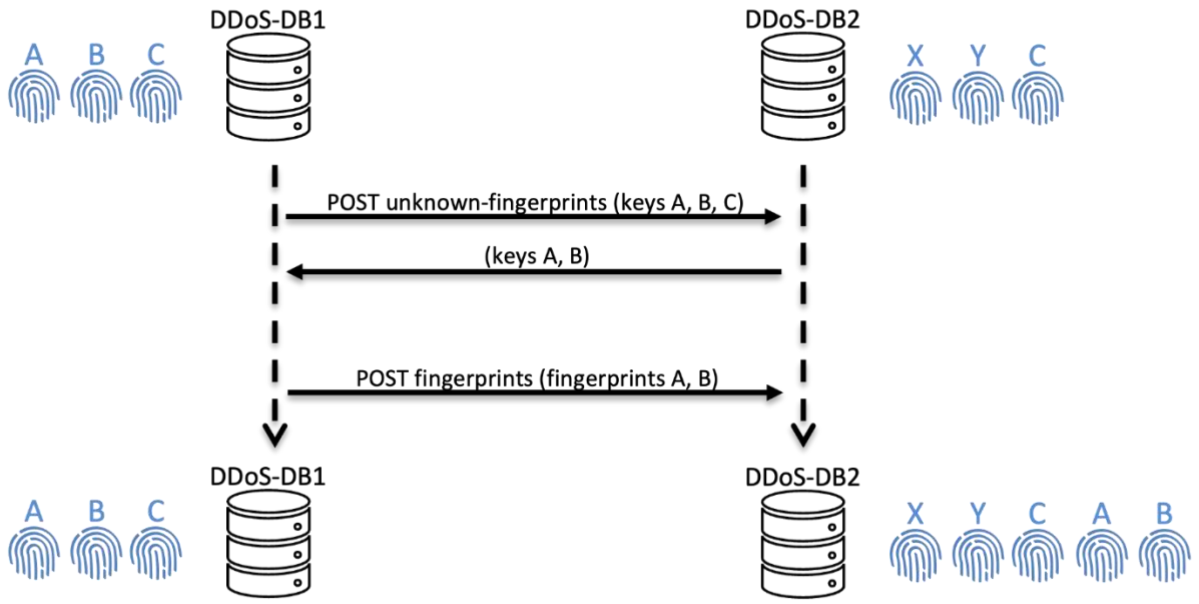

DDoS-DB1
DDoS-DB2
A B C
X Y C
POST unknown-fingerprints (keys A, B, C)
(keys A, B)
POST fingerprints (fingerprints A, B)
DDoS-DB1
DDoS-DB2
A B C
X Y C A B

Figure 7: Push synchronization between DDoS-DBs

After the synchronization DDoS-DB2 has fingerprints X, Y, C, A and B.

Pull synchronization

Figure 8 shows pull synchronization, where DDoS-DB1 pulls fingerprints from DDoS-DB2,

Synchronization starts by DDoS-DB1 getting the keys of all shareable fingerprints of DDoS-DB2 by doing a GET on the /api/fingerprint endpoint of DDoS-DB2.
DDoS-DB1 compares this list of keys (X, Y, C, A and B) with its own list of fingerprints (A, B and C) and determines the fingerprints it does not have yet (X and Y).
DDoS-DB1 then retrieves those fingerprints one after the other by calling the /api/fingerprint/<key> endpoint multiple times.

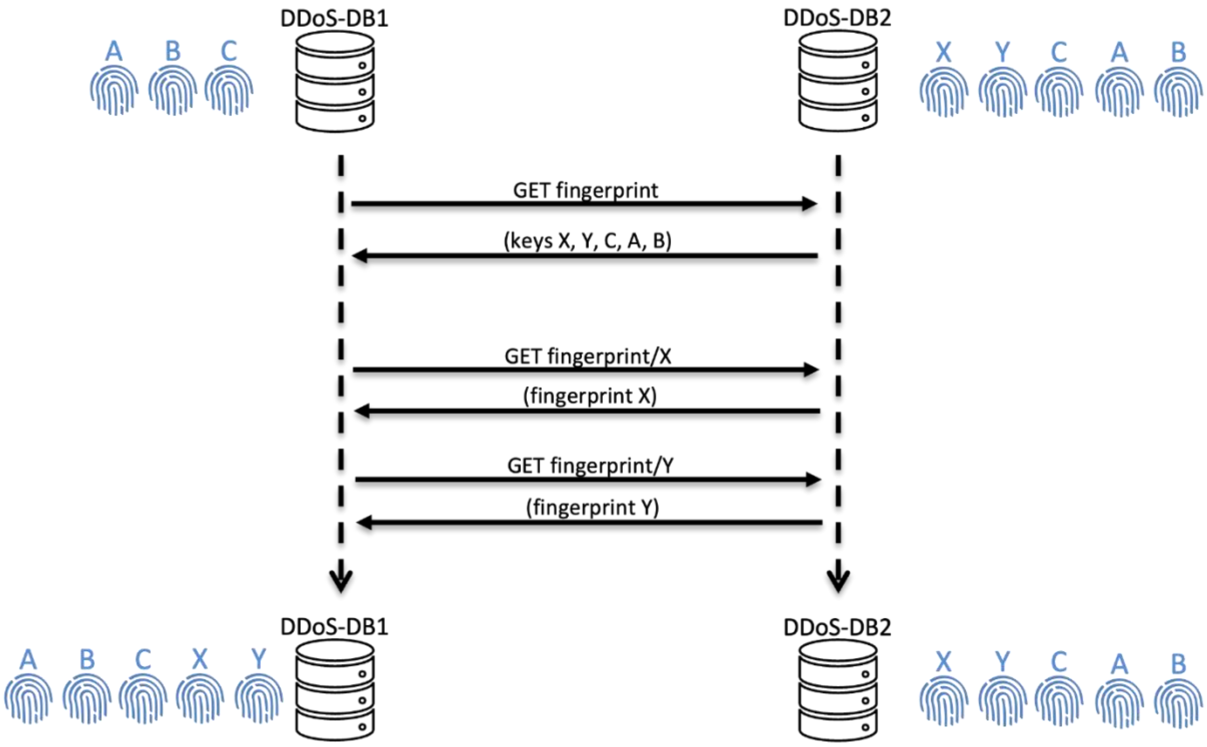


Figure 8: Pull synchronization between DDoS-DBs

The examples above show that the combination of one push and one pull synchronization provides a full synchronization of shareable fingerprints between two DDoS-DB instances.

4.4 Distribution of components

Each member of an ADC can upload fingerprints to a DDoS-DB and/or retrieve them for (being used in) mitigation or for other means.
As described earlier, a DDoS-DB can synchronize its fingerprints with one or more other DDoS-DB instance(s). Tools that interact with a DDoS-DB do not know whether a DDoS-DB is a 'central' or 'local' DDoS-DB, the synchronization settings of sets of DDoS-DBs fully determine this. Functionally it makes no difference whether an instance is 'central' or 'local'. Only fingerprints marked as 'shareable' are synchronized with other instances, which means that it is possible to determine which fingerprints will be shared and which fingerprints will remain at this DDoS-DB only.

The way each DDoS-DB in an ADC is configured determines how functions are distributed across the different components, two examples of which are given below.

4.4.1 Centralized model

The simplest and most straightforward form of an ADC uses a single centralized DDoS-DB for this purpose, as shown below. The top-right member only retrieves fingerprints from the DDoS-DB but does not upload them.

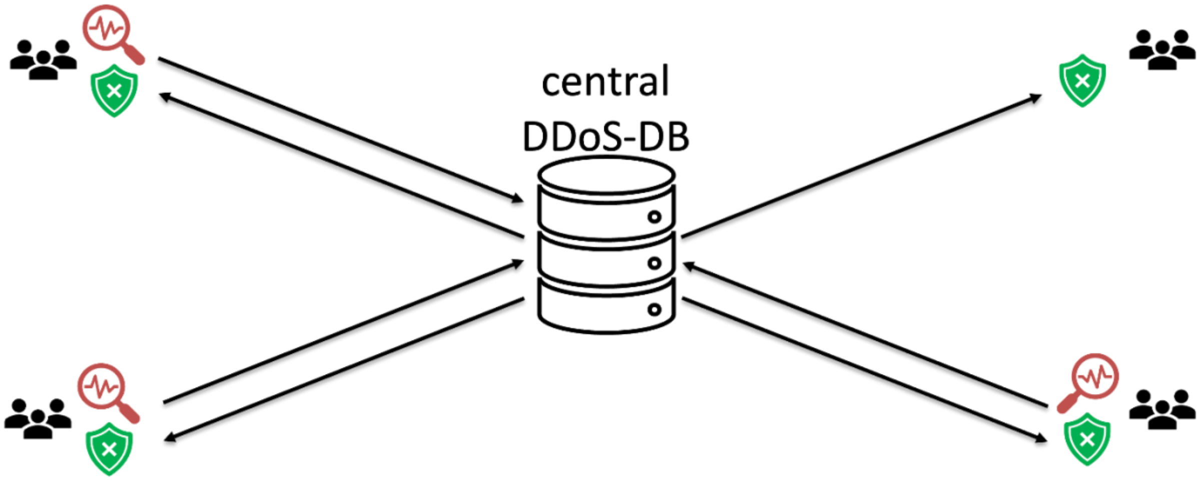


Figure 9: Centralized setup of a DDoS Clearing House

In this setup, each tool used by an ADC member talks directly to a central DDoS-DB. This makes configuration straightforward, since only one DDoS-DB needs to be managed. However, for some members placing all fingerprints directly in a shared central DDoS-DB may not be acceptable. In such cases, it makes sense to combine the central DDoS-DB with one or more local instances.

4.4.2 Distributed model

A more distributed setup is created by combining a central DDoS-DB with one or more local instances. This allows ADC members to store all their fingerprints locally first and then selectively choose which fingerprints they find suitable for sharing with the other ADC members by setting those fingerprints to 'shareable'.

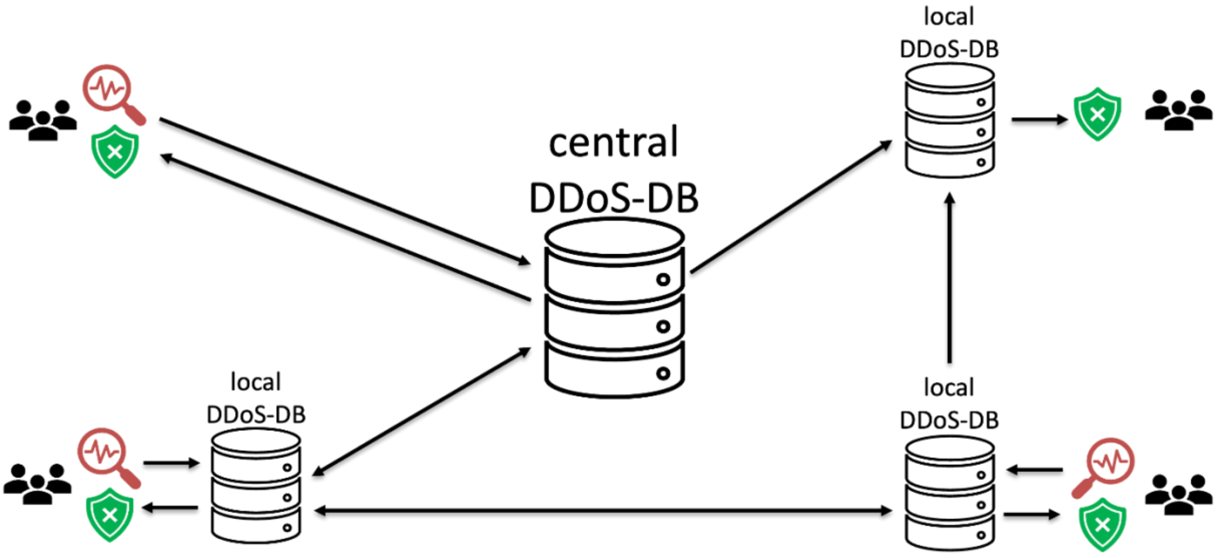


Figure 10: Decentralized setup of a DDoS Clearing House

A more distributed setup also makes an ADC less vulnerable to disruption (by attacks or otherwise) since tooling can use its local instance rather than the central DDoS-DB. Local instances can also be placed behind a firewall for further protection if so needed.

Local instances in this setup have the central DDoS-DB configured as the remote DDoS-DB to synchronize with. By enabling both push and pull modes, locally generated (shareable) fingerprints will be pushed to the central instance, and new fingerprints at the central instance that are unknown locally will be pulled from it. Configured this way, the central DDoS-DB acts as a synchronization 'hub' for all local instances. This also allows tooling used by an ADC member to interact with the local instance, rather than the central one, creating a more robust setup against interference.

Note that a fully distributed setup, with only local instances and no central DDoS-DB is possible as well. This means that care must be taken to ensure that all instances that need to synchronize can connect with each other, which may be difficult to achieve and maintain if all are behind firewalls or in shielded network segments. Therefore, in most cases, a distributed setup combining a central DDoS-DB with local instances is preferred if a more robust setup than the single centralized DDoS-DB is required.

4.5 Deployment

The default installation of a DDoS-DB and the Dissector (whether for testing or for deployment) uses Docker, which allows for easy deployment using a standardized container environment and circumvents issues such as the 'versioning hell' associated with a more traditional direct installation on a host platform.
DDoS-DB can be deployed on Linux or Mac OS platforms.

4.5.1 Installation

Installing a DDoS-DB consists of:

1. Installing Docker and docker-compose
2. Cloning the repository
3. Running the build script
4. (optionally) configuring DNS entries to the machine and deploying certificates

The build script asks for superuser credentials (username and password) needed to provide further configuration and creates, configures, and runs all docker containers used in this deployment.
Since the detailed instructions for deployment may change over time, please see the documentation provided at the repository for full instructions: https://github.com/ddos-clearing-house/DDoS-DB

For a full production system that has a domain name with a DNS record point to it, we provide a script which requests a Let's Encrypt certificate for that domain and configures the system accordingly. This means people can visit the DDoS-DB with a web browser using the domain name without getting a warning from the browser (or a flat-out refusal by the browser to show the website). The expiry date of the certificates is automatically checked daily by the system and, if the certificate expires within 30 days, automatically renews them; greatly reducing the time needed for system management.

NOTE: The use of Let's Encrypt certificates does mean that the system must be reachable from the Internet on ports 80 (http) and 443 (https), since that is how Let's Encrypt can check that the web server behind a domain is the same as the one requesting the (renewed) certificate. This may be difficult for local DDoS-DB instances behind a firewall (depending on organizational policies), but if the system is not intended to be reachable from the Internet, then the need for certificates really is debatable anyway. Besides: This would only be the case in a distributed deployment scenario (a centralized DDoS-DB for an ADC with local instances), in which case the local instances would push/pull synchronize with the central DDoS-DB (which then does need to be reachable).

4.5.2 Configuration

After installation, the system needs to be configured for the deployment scenario, since this determines who will need access to this system (either the web frontend and/or API access) and possibly other systems (either other DDoS-DB instances or MISP systems) this installation needs to synchronize with.

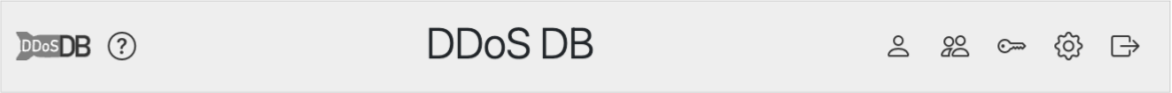


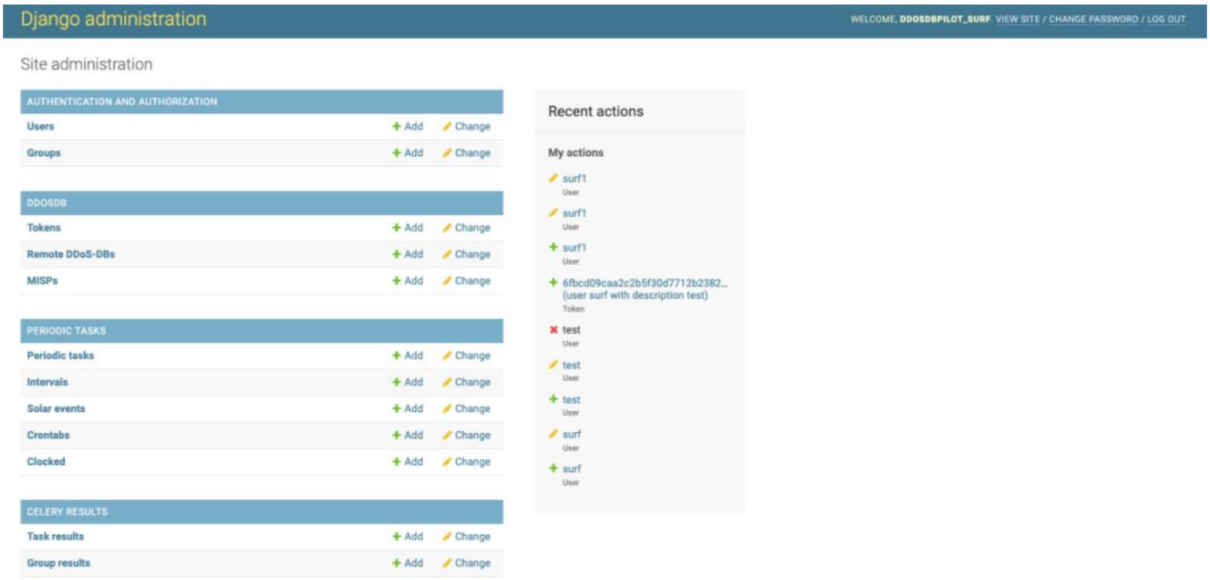
Figure 11: DDoS-DB web interface menu bar

DDoS-DB is built using the Django[6] web framework. Django provides a lot of the requirements common to (database driven) web applications like DDoS-DB, such as user management, authentication and authorization and an admin panel for configuration and management of the application.

All configuration of DDoS-DB is done from this admin panel. It can be reached by visiting the address or domain of the DDoS-DB instance with a browser, clicking on the login button (most top-right icon in the menu bar), and logging in as superuser (or admin), then clicking on the cog wheel icon (second to right icon). From the admin panel users and groups can be configured, as can tokens, remote DDoS-DB instances (for synchronization) and MISP instances (for exporting fingerprints to).

The periodic tasks are used for scheduling the (intervals of) remote synchronizations, which can be set to occur daily, hourly, every 15 minutes or every minute. The default setting is to synchronize daily, which can be changed to an appropriate interval.

[6] https://www.djangoproject.com/



✎ surf1
User

✎ surf1
User

+ surf1
User

+ 6fbcd09caa2c2b5f30d7712b2382...
(user surf with description test)
Token

✖ test
User

✎ test
User

+ test
User

✎ surf
User

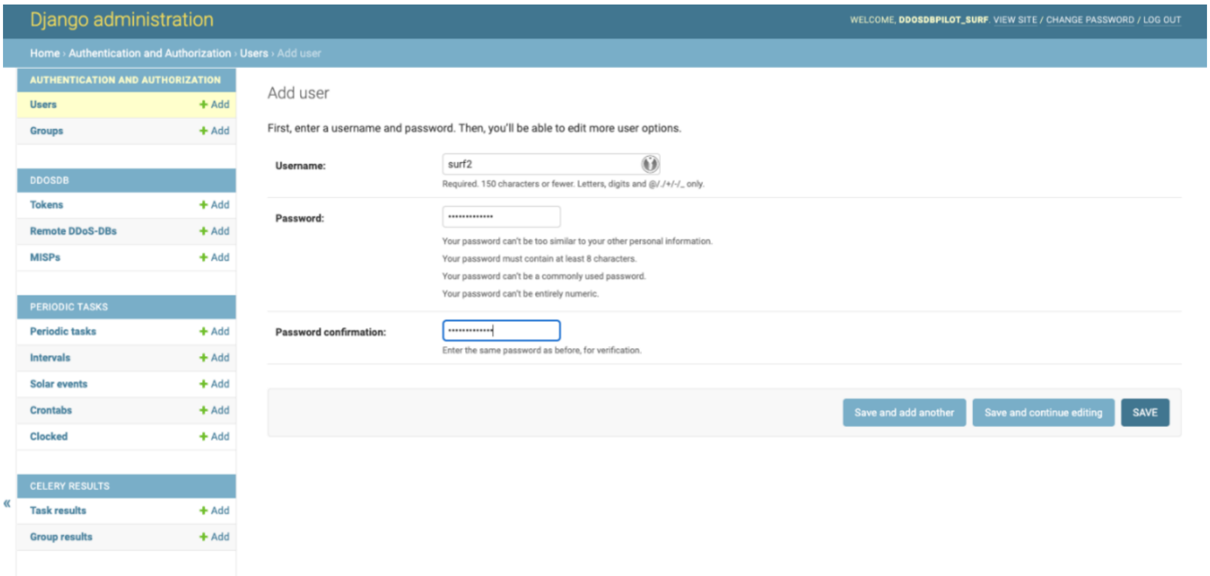
+ surf
User

Figure 12: DDoS-DB admin panel

Accounts and authorizations

At first the system only knows the superuser. It is the task of the superuser to add other users and assign them the proper authorizations/permissions (which may include the permission to create further users).

New users can be added via the admin site by clicking the '+ Add' link next to the 'Users' entry in the left-hand panel. In the first step, the username and passwords can be specified.



Add user

First, enter a username and password. Then, you'll be able to edit more user options.

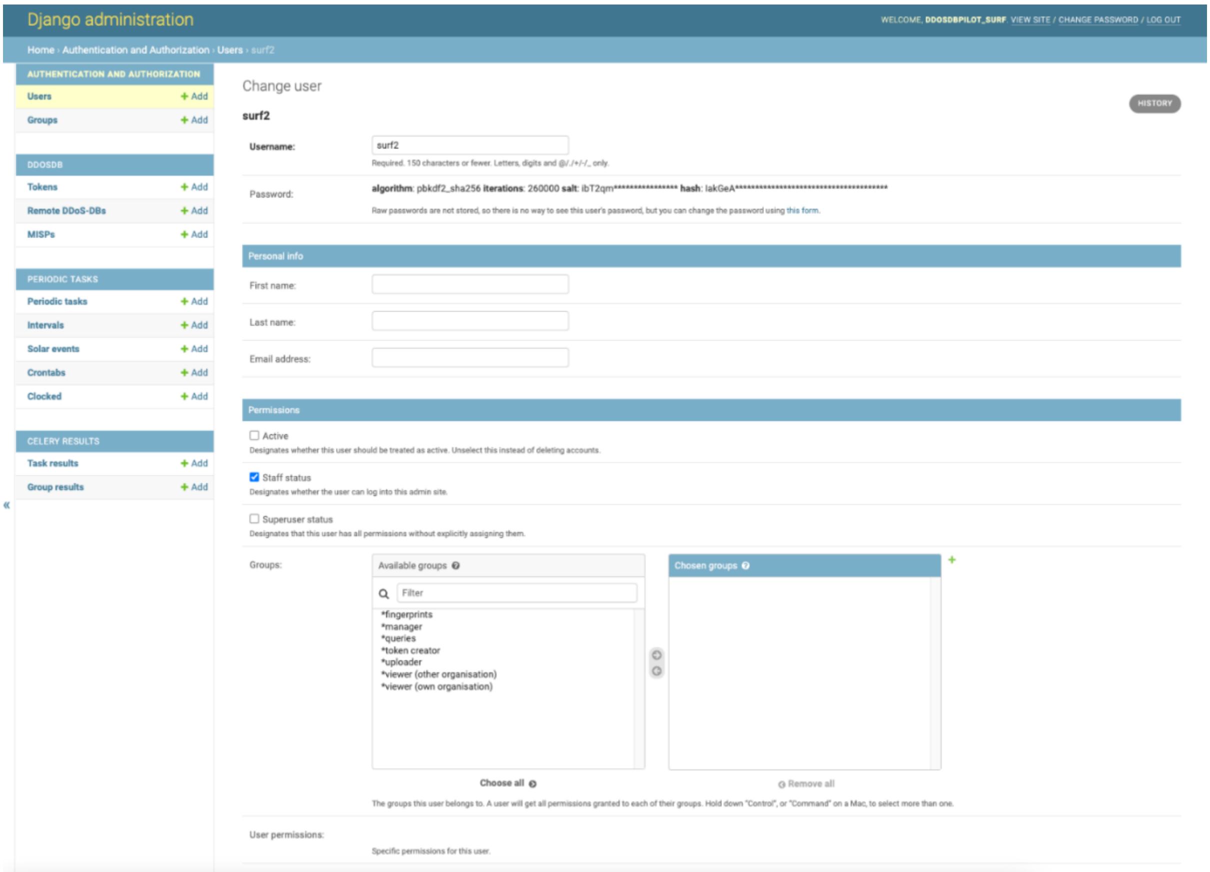
Username: surf2
Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Password: ••••••••••••••
Your password can't be too similar to your other personal information.
Your password must contain at least 8 characters.
Your password can't be a commonly used password.
Your password can't be entirely numeric.

Password confirmation: ••••••••••••••
Enter the same password as before, for verification.

Figure 13: Adding a user on DDoS-DB, step 1

In the second step, user details (first and last name, e-mail address; all optional) can be added, whether the user belongs to 'staff' (meaning: can access the admin site, only needed for superusers and managers), whether the user is a superuser, as well as the groups the user belongs to.



Change user

surf2

Username: surf2
Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Password: **algorithm**: pbkdf2_sha256 **iterations**: 260000 **salt**: ibT2qm**************** **hash**: lakGeA**************************************
Raw passwords are not stored, so there is no way to see this user's password, but you can change the password using this form.

Personal info

First name:

Last name:

Email address:

Permissions

☐ Active
Designates whether this user should be treated as active. Unselect this instead of deleting accounts.

☑ Staff status
Designates whether the user can log into this admin site.

☐ Superuser status
Designates that this user has all permissions without explicitly assigning them.

Groups:
Available groups
Filter
*fingerprints
*manager
*queries
*token creator
*uploader
*viewer (other organisation)
*viewer (own organisation)

Chosen groups

The groups this user belongs to. A user will get all permissions granted to each of their groups. Hold down "Control", or "Command" on a Mac, to select more than one.

User permissions:
Specific permissions for this user.

Figure 14: Adding a user to DDoS-DB, step 2

NOTE: Django uses groups to implement Role Based Access Control (RBAC). **E**very group has a set of associated permissions and any user that is a member of a group inherits those same permissions. So, to assign permissions to a user, make them a member of the relevant group(s).

(Default) groups and permissions

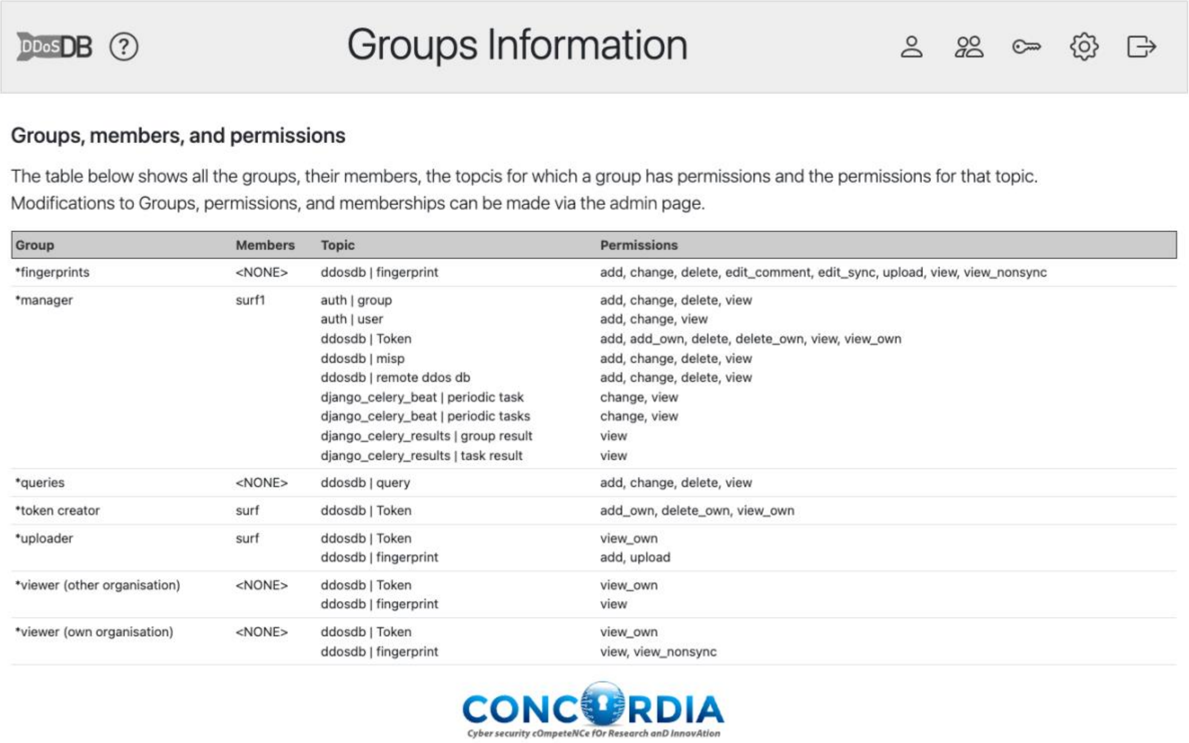
To facilitate setting the right permissions for each user, several predefined/default groups are available. Default groups can be recognized by their name, as they all start with an asterisk. Different permissions can be added by creating new groups with the required permissions. The default groups and their associated permissions are (re)created at the startup of the system, so any changes made to those will be lost at the next system startup.

Table 2: Default user groups and their permissions

Group	Permissions	Remarks
*fingerprints	Add/Upload/Change/Delete fingerprints, add/edit comments, change 'shareable' status of fingerprints.	Fingerprint refers to any fingerprint present in this DDoS-DB. Members of this group are essentially 'fingerprint superusers' as they can do anything with any fingerprint.

*manager	Manage Users, Groups, Tokens, Remote DDoS-DBs, MISPs and view Periodic Tasks/Results	Users that belong to this group must have the 'Staff status' checkbox set, otherwise they will not be able to access the admin panel! Managers cannot delete users, but can de-activate their accounts which amounts to the same thing (and is better for multiple reasons, such as traceability)
*queries	Perform queries on the database	Make a user a member of this group if they must be able to use the Search page from the web front-end.
*token creator	Create and delete (their own) tokens, view own tokens	Members of this group can manage their own tokens from the web front-end (on the token page).
*uploader	Upload/add, change, and delete their own fingerprints, view own tokens	An uploader can upload new fingerprints and change or delete them but cannot view them. If users need to be able to view fingerprints as well (e.g. it is not a user account made for tooling to upload fingerprints) you should add the user to one of the viewer groups as well.
*viewer (other organization)	View own fingerprints, view (other) fingerprints set to shareable, view own tokens	
*viewer (own organization	View all fingerprints (also those not set to shareable), view own tokens	

NOTE: Superusers/managers can see an overview of groups and their members by clicking on the 'Groups and permissions' icon in the menu bar (second icon on the right-hand side). This will list every group, its members, and associated permissions. Such an overview is not available via the default Django admin site.



Groups Information

Groups, members, and permissions

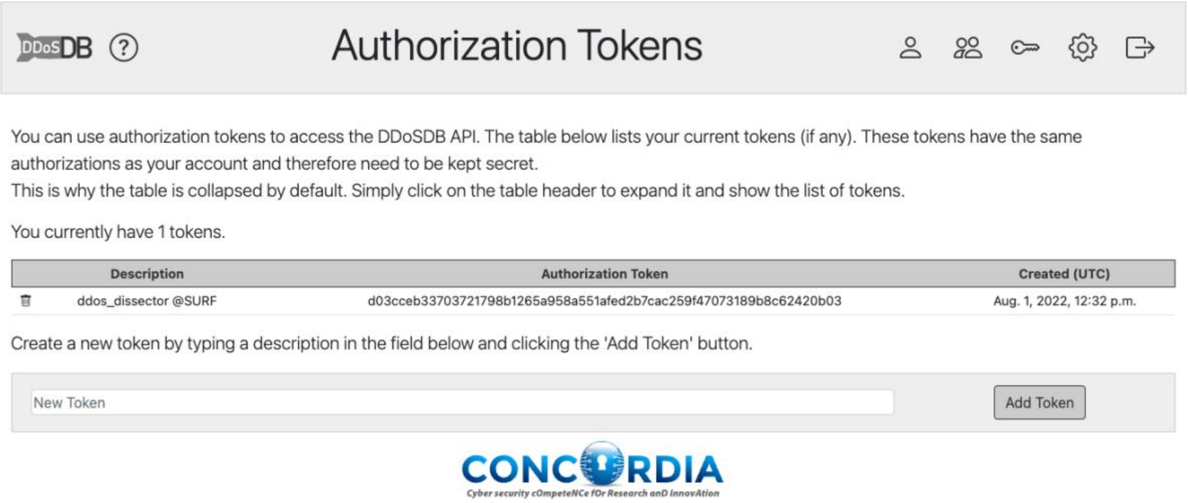
The table below shows all the groups, their members, the topcis for which a group has permissions and the permissions for that topic. Modifications to Groups, permissions, and memberships can be made via the admin page.

Group	Members	Topic	Permissions
*fingerprints	<NONE>	ddosdb | fingerprint	add, change, delete, edit_comment, edit_sync, upload, view, view_nonsync
*manager	surf1	auth | group auth | user ddosdb | Token ddosdb | misp ddosdb | remote ddos db django_celery_beat | periodic task django_celery_beat | periodic tasks django_celery_results | group result django_celery_results | task result	add, change, delete, view add, change, view add, add_own, delete, delete_own, view, view_own add, change, delete, view add, change, delete, view change, view change, view view view
*queries	<NONE>	ddosdb | query	add, change, delete, view
*token creator	surf	ddosdb | Token	add_own, delete_own, view_own
*uploader	surf	ddosdb | Token ddosdb | fingerprint	view_own add, upload
*viewer (other organisation)	<NONE>	ddosdb | Token ddosdb | fingerprint	view_own view
*viewer (own organisation)	<NONE>	ddosdb | Token ddosdb | fingerprint	view_own view, view_nonsync

Figure 15: DDoS-DB User groups overview

API access

DDoS-DB provides a simple API for uploading and retrieving fingerprints, as described in Section 4.3. Tokens are used for authentication. They are always linked to a specific user account and inherit the permissions of that account. Users who are members of the '*token creator' group can manage their own tokens (generate new ones and delete existing ones) by accessing the 'Authorization Tokens' page (via the Key icon on the top right). Superusers or managers can create tokens for users that cannot create tokens themselves. Most users (member of *uploader or one of the *viewer groups) can view their own tokens on the 'Authorization Tokens' page.



Authorization Tokens

You can use authorization tokens to access the DDoSDB API. The table below lists your current tokens (if any). These tokens have the same authorizations as your account and therefore need to be kept secret.
This is why the table is collapsed by default. Simply click on the table header to expand it and show the list of tokens.

You currently have 1 tokens.

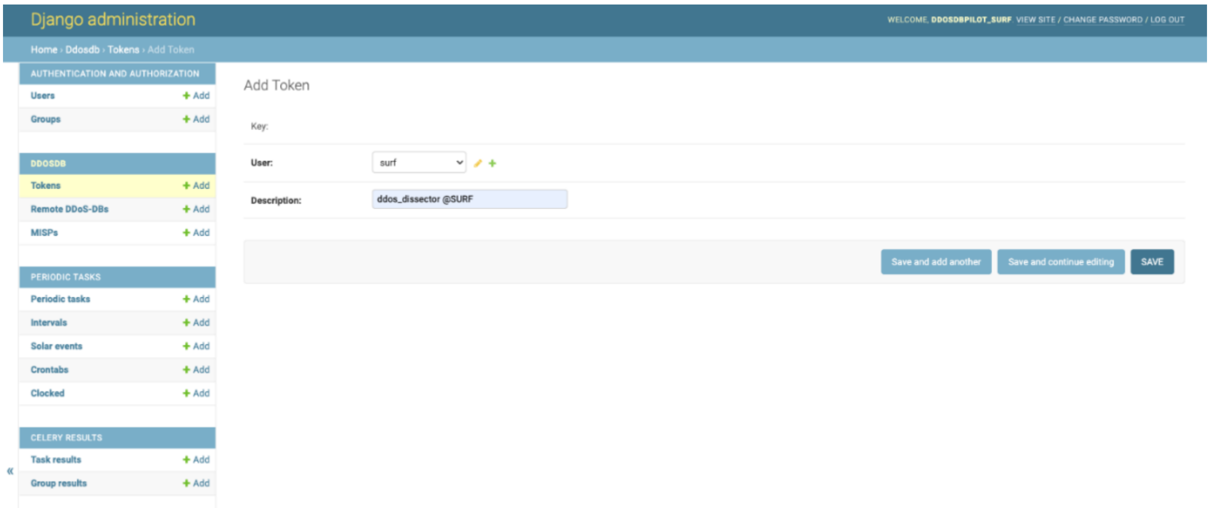
	Description	Authorization Token	Created (UTC)
🗑	ddos_dissector @SURF	d03cceb33703721798b1265a958a551afed2b7cac259f47073189b8c62420b03	Aug. 1, 2022, 12:32 p.m.

Create a new token by typing a description in the field below and clicking the 'Add Token' button.

New Token

Figure 16: API Authorization token page

Superusers and managers can generate tokens for specific users via the admin panel by simply clicking the 'Add' link next to the 'Tokens' entry in the left panel, selecting the user/account for which the token is intended and adding a description (useful to remind for which purpose or tooling the token was generated). This ability to generate tokens is especially useful for cases where you want to hand out tokens for access to the API for tooling purposes only (e.g., for a Dissector for uploading fingerprints, or for another DDoS-DB instance for synchronizing fingerprints with), but not for providing access to the web interface: simply create a user with the right permissions, but do not hand out the username and password. Instead, simply create a token for that account and hand that out instead.



Add Token

Key:

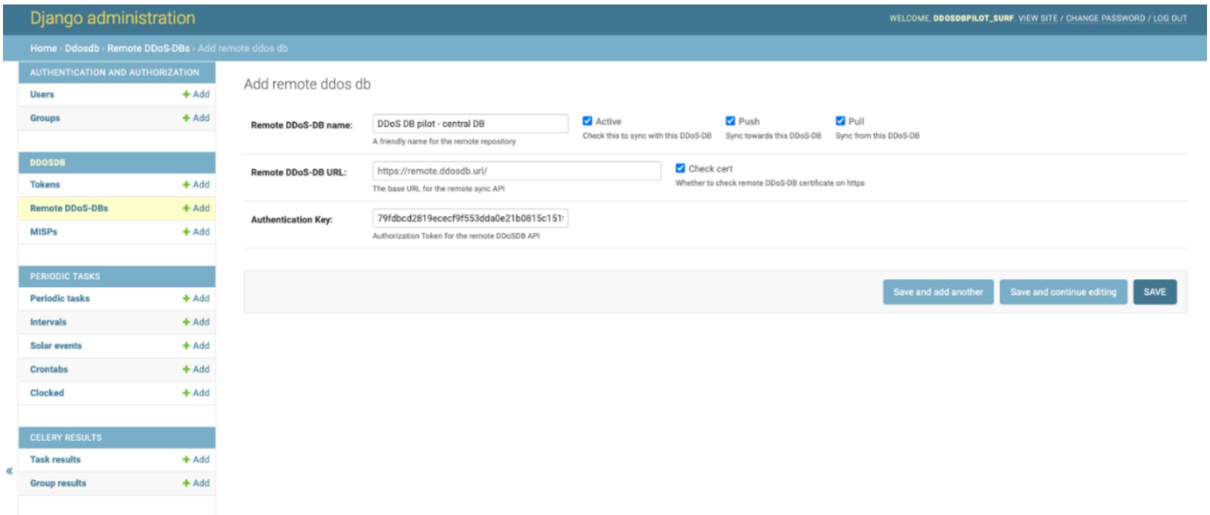
User: surf

Description: ddos_dissector @SURF

Figure 17: DDoS-DB token administration page

Remote synchronization

Any DDoS-DB instance can synchronize their fingerprints with other instances. Management of these remote DDoS-DB instances is done via the Remote DDoS-DBs entry in the admin panel.



Add remote ddos db

Remote DDoS-DB name: DDoS DB pilot - central DB
A friendly name for the remote repository

☑ Active
Check this to sync with this DDoS-DB

☑ Push
Sync towards this DDoS-DB

☑ Pull
Sync from this DDoS-DB

Remote DDoS-DB URL: https://remote.ddosdb.url/
The base URL for the remote sync API

☑ Check cert
Whether to check remote DDoS-DB certificate on https

Authentication Key: 79fdbcd2819ececf9f553dda0e21b0815c151
Authorization Token for the remote DDoSDB API

Figure 18: Remote DDoS-DB configuration page

The Authentication Key is an Authorization Token valid at the remote instance, so a superuser or manager of the remote DDoS-DB must provide you with this (or with account details for an account that can manage its own tokens, in which case you can generate your own token via the Authorization Tokens page of the remote DDoS-DB).

Synchronization can be done via push (push local fingerprints that the remote instance does not know yet), pull (retrieve fingerprints from the remote instance that are unknown locally), or both. For a setup that contains local DDoS-DBs and one centralized DDoS-DB, it makes sense for the local DDoS-DBs to set up the centralized DDoS-DB as a remote instance and do both a push and a pull synchronization.

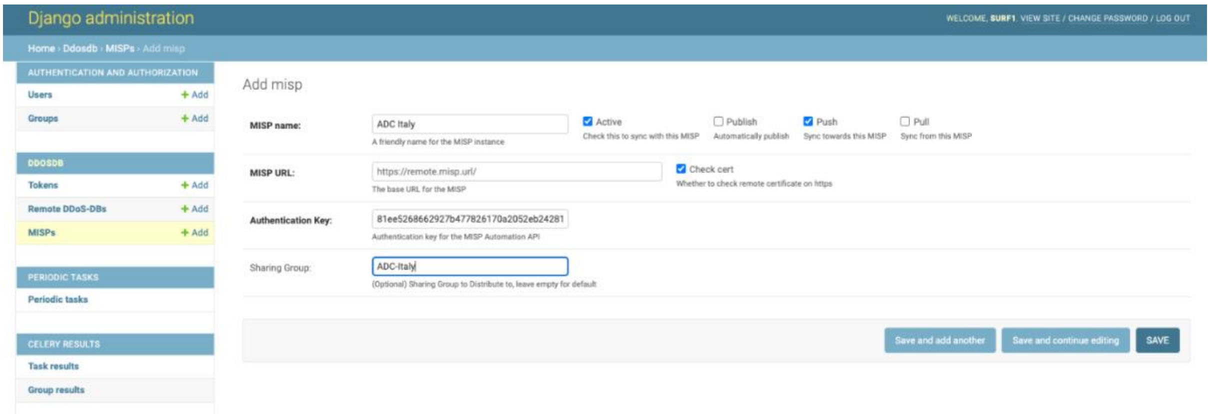
By default, the synchronization will happen once a day, but this can be changed by editing the 'Periodic Tasks' in the admin panel (The 'Remote push sync' and 'Remote pull sync') and setting the Interval to hourly, for example. Note that this means that push and pull can happen at different intervals, e.g., Push new fingerprints to the central DDoS-DB every hour, but only retrieve/Pull new fingerprints from the central DDoS-DB once a day. New intervals can also be created if the predefined intervals do not suffice.

MISP export

Fingerprints can be exported to a MISP instance, an open-source Threat Intelligence platform used by many CERTs/CSIRTs. Fingerprints are exported as events with associated DDoS objects. Exporting fingerprints to MISP happens at regular intervals (like synchronization with remote DDoS-DB instances), by default, once a day. As with remote synchronization, the default interval can be changed by editing the 'Periodic Tasks' in the admin panel (the 'MISP push sync' task).

The MISP instance(s) to export to can be defined via the 'MISPs' entry in the admin panel. An admin of the MISP needs to provide the token needed to access the MISP API, with the appropriate authorizations needed to create events and objects.

By checking the 'Publish' checkbox, newly created events are automatically published on creation as well. If left unchecked, new events must be published manually via the MISP web interface.
Optionally a 'sharing group' can be specified. Please note this means that the token needs to have the right permissions for this to work (the user/organization the token is associated with needs to be a member of that - already defined - sharing group).



Add misp

MISP name: ADC Italy
A friendly name for the MISP instance
☑ Active
Check this to sync with this MISP
□ Publish
Automatically publish
☑ Push
Sync towards this MISP
□ Pull
Sync from this MISP

MISP URL: https://remote.misp.url/
The base URL for the MISP
☑ Check cert
Whether to check remote certificate on https

Authentication Key: 81ee5268662927b477826170a2052eb24281
Authentication key for the MISP Automation API

Sharing Group: ADC-Italy
(Optional) Sharing Group to Distribute to, leave empty for default

Figure 19: Adding a MISP instance to synchronize with DDoS-DB

NOTE: To be able to check if a fingerprint already exists at a MISP, DDoS-DB adds the tag 'DDoSCH' to each event it creates. This means that the token should have the permission to create this tag, or the tag must already exist in the MISP.
NOTE: Because MISP events and associated DDoS objects cannot express all information and relations present in a fingerprint, the reverse action (pulling fingerprints from a MISP) is not implemented.

5 Joint DDoS Drills

The Dutch anti-DDoS coalition hosts biannual DDoS drills during which its members can practice their readiness and resilience to DDoS attacks in realistic scenarios. Organizations can learn a lot from each other in terms of both technical and organizational skills. During the drill, participants learn why one organization can successfully mitigate an attack, while another is struggling, what is the best way to set up a response team, and how to organize the work most efficiently. This section will describe the design of DDoS drills, how they are executed, and their results.

5.1 Drill design

We distinguish between four roles during the drills. The Red team is responsible for coming up with an attack plan and carrying out the attack at the time of the drill. The Blue teams are the defending teams of each organization. They must mitigate the incoming DDoS attack. Besides these two main roles, there is a team of observers that walk around and evaluate the drills. Lastly, every participating organization appoints one coordinator, who oversees the drill from their organization's point of view.

Each DDoS drill is executed according to an elaborate attack plan set up by the red team in the months leading up to the drill. The attack plan is a schedule that indicates for each time slot and each organization what type of attack will be executed and by whom. Each DDoS attack lasts 15 minutes. This allows a large variety of DDoS attacks to be executed during the drill. The attack plan shows for each participating organization at what time they will be targeted with which attack, by whom, and with what bandwidth. Of course, this information is only available to the red team. The Blue team does not know in advance which attacks will be targeted at their organization.

In the months leading up to a DDoS drill, the red team meets regularly to form the attack plan. During these meetings, they discuss possible attack vectors to exploit in the upcoming drill, as well as who oversees executing the various parallel DDoS attacks. In these meetings, the available bandwidth and maximum allowed bandwidth is also discussed. A DDoS drill requires a few organizations that have access to sufficiently large networks and bandwidth to send large-scale DDoS attacks.

The coordinators meet regularly before a DDoS drill to discuss the event in detail and evaluate the drill afterward.

5.2 Execution

The Dutch anti-DDoS coalition developed a custom infrastructure to efficiently run the DDoS drills in a controlled environment. This includes a game board that provides an overview of what attacks are being executed at each moment, and how much bandwidth is being used. The appointed coordinators can stop the DDoS drill at any moment if the attack proves too large or difficult for their infrastructure or mitigation devices.

The DDoS drills can have a real impact on the production services of participating organizations as the simulated attacks are large in volume and exploit real attack vectors. Therefore, the drills take place in the middle of the night when the fewest users are interacting with the organization’s services. In the case that services do experience downtime, the effect on its users is minimal. Some organizations preemptively announce a window for technical maintenance so as not to surprise their users with any downtime. Still, the participating organizations find a lot of support within their organization for participating in DDoS drills. It is understood that practicing their response to DDoS attacks is crucial in today’s cyberthreat landscape.

To effectively prepare organizations for real DDoS attacks, the aim is to reproduce DDoS attacks as accurately as possible. However, the members of the Dutch ADC only use their own systems, whereas real DDoS attacks often make use of botnets. This is because using a botnet would be a computer intrusion, which is illegal, and because a botnet is much more difficult to control than an organization’s own resources. This means the attack traffic during drills originates from a single or a few Internet networks, which practically would render mitigation trivial by blocking those IP addresses. In a real DDoS scenario, this would however not be feasible, as IP addresses are often spoofed. Because of that, the blue teams are not allowed to simply block the IP addresses from which the attacks originate.

To legally allow one organization to DDoS another within a specified timeframe, the organizations participating in the DDoS drill sign a waiver. An example (anonymized) waiver agreement is attached in Appendix 5 (14.5)

5.3 Results

After a drill, the participating organizations thoroughly evaluate it, both in a plenary session, as well as within their organization. During the evaluation, organizations examine what they have learned and how they can improve their networks to better ward off DDoS attacks in the future.

The goal is to practice the response to many kinds of DDoS attacks. By doing so, we learn which attacks are relatively easy to ward off and which attacks require a more hands-on mitigation strategy. By learning this in a controlled setting, the response to a real DDoS attack is made faster and more effective. During the drill, blue teams from different organizations are allowed to ask each other if they have seen a specific DDoS attack and what their mitigation strategy is. Hence, collaboration between organizations during the drill make them even more educational.

The drills also improve the internal knowledge of an organization's network. It reveals the strong and weak points in a network and what is defined as normal or abnormal behavior. When a DDoS attack is successful, the opportunity for learning is the greatest.

6 DDoS Clearing House Testbed

We developed a testbed to learn how the DDoS Clearing House operates in a realistic setting, without the members of an Anti-DDoS Coalition having to use the Dissector to generate fingerprints from real-life data. This is important because we have experienced that such processes often take a significant amount of time, typically in the order of months. For example, organizations need to modify their production networks to add the Dissector, and they need to sign a data sharing agreement because the IP addresses in DDoS fingerprints are personally identifiable information (PII). While such processes are indispensable for a production version of the Clearing House (TRL8-9), they can significantly slow down the development and evaluation of the system. We aimed to achieve TRL6 with our testbed ("Technology demonstrated in relevant environment"). Experiments on the testbed preceded an actual pilot with the Dutch Anti-DDoS Coalition, which is at TRL7 ("System prototype demonstration in operational environment"). In the pilot, the members of the coalition use the Dissector in their networks and sign data sharing agreements covering the exchange of fingerprints via the DDoS-DB. We used the Testbed as a preliminary pilot before the infrastructure in the Dutch and Italian anti-DDoS coalitions was ready to pilot the system in a production environment. Furthermore, we used the testbed to demonstrate the DDoS Clearing House at various events.

The testbed consists of three essential elements: The remote cloud-hosted traffic generator, a so-called "Virtual anti-DDoS coalition", and the DDoS Clearing House components, deployed at the members of the Virtual anti-DDoS coalition. In our design, we distributed these components over the Internet, as opposed to virtualized in a single network, because this is more representative of the situation in which the DDoS Clearing House will operate.

Figure 20 gives an overview of the testbed components.

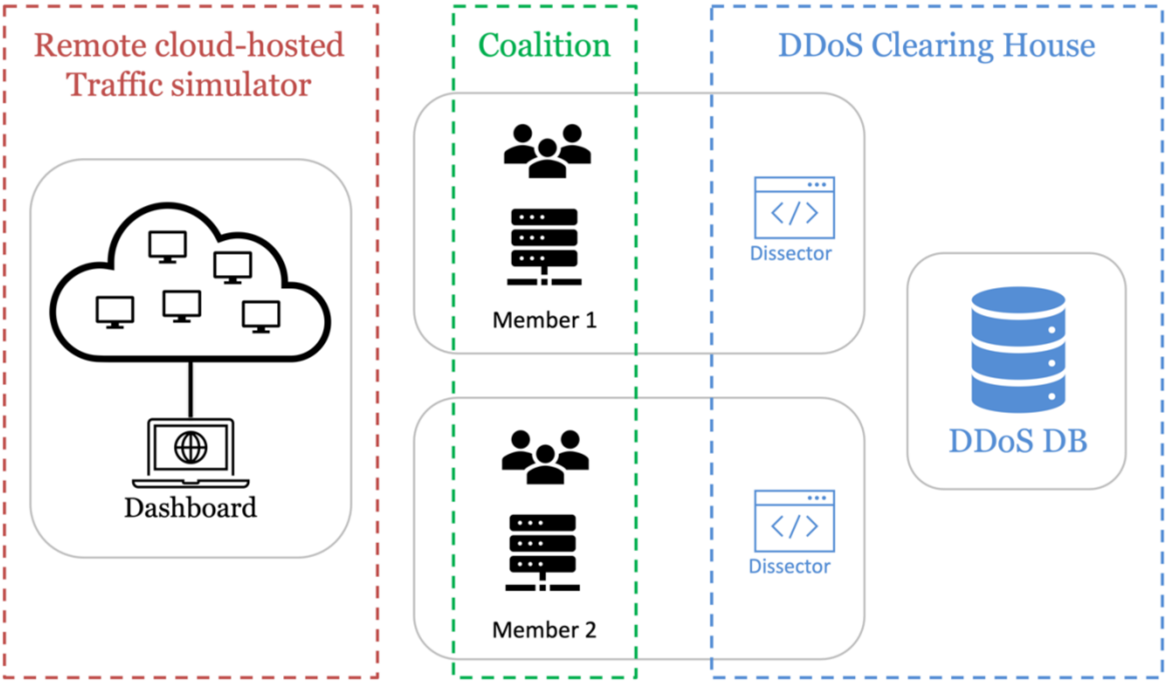


Figure 20: DDoS Clearing House testbed components

We designed the Clearing House testbed based on four requirements:

1. The testbed must enable the testing of the DDoS Clearing House without the typically time-consuming deployment and legal processes needed for a production-level system.
2. It must closely resemble the technical operational setting in which the Clearing House will be deployed after development, by which we mean that it operates in an environment distributed over the Internet, and not in an isolated virtualized network.
3. It must allow us to test and demonstrate each component of the Clearing House, and importantly, the system as a whole: from DDoS traffic captures at an anti-DDoS coalition member to the use of mitigation rules by other members, the potential victims.
4. The testbed must be able to emulate DDoS attacks in which distributed remote sources send traces of DDoS traffic to a target participant on the testbed. This does not mean that it should send a real DDoS attack; a smaller volume of representative attack traffic is sufficient to adequately test the Clearing House. The testbed should therefore prevent members from sending more traffic than required by the Dissector.

6.1 Virtual anti-DDoS coalition

To test the Clearing House in a realistic environment, we need to deploy its components in a virtual anti-DDoS coalition (vCoalition, for short). In the pilot of the DDoS Clearing House using the testbed, our vCoalition consists of SIDN Labs, SURF, and FORTH three CONCORDIA partners tasked with the development of the DDoS Clearing House. The reason we can execute pilots on this platform without a data sharing agreement is that no real DDoS data is used. To avoid sharing PII, we generate traces of DDoS attack traffic using our traffic

generator. We are free to share these traffic captures with whomever since they do not contain any personal IP addresses.
To be safe, we drafted working arrangements between SIDN as the testbed operator and the connected CONCORDIA partners. It is attached in Appendix 6 (14.6).

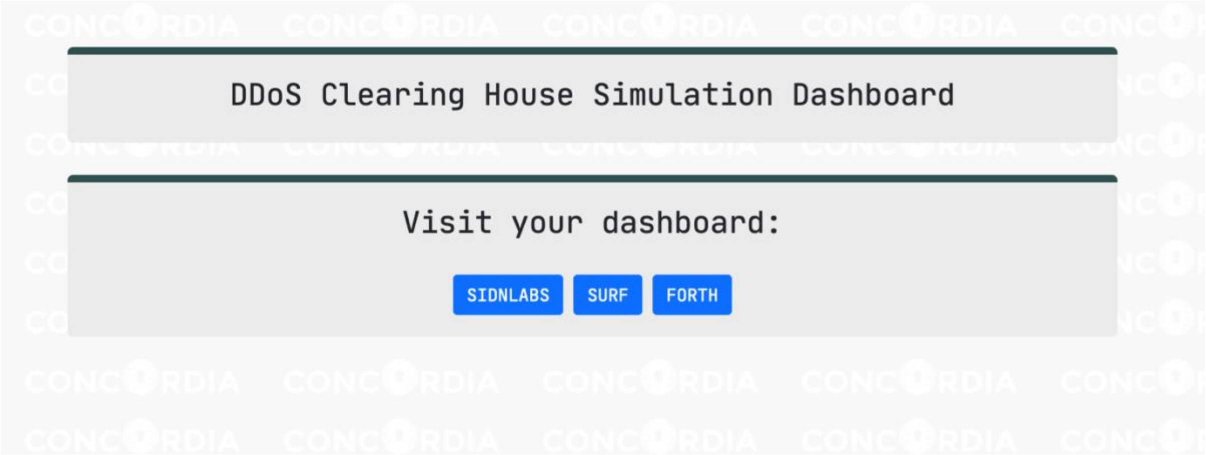
6.2 Remote cloud-hosted traffic generator

The traffic generator allows a member of a vCoalition to generate traffic samples of various kinds of DDoS attacks and send them to themselves, and only to themselves. It does not launch real DDoS attacks but only allows for negligible traffic volumes (a couple of Mbit/s at most). As such, the traffic generator is not meant to test the DDoS resilience of a partner connected to the testbed. Instead, it is meant to generate small samples of DDoS network traffic with which the DDoS Clearing House can be tested in its entirety. Since the connected members can only send simulated attack traffic to a server defined in their own network, the testbed does not require legal agreements regarding liability, or waivers of any kind, which would be required when organizations would target each other.

The remote cloud-hosted traffic generator consists of a web-based dashboard and five virtual machines, distributed over the world, which together emulate a botnet capable of sending DDoS attacks.

6.2.1 Dashboard

The web dashboard is only accessible to the partners connected to the testbed, enforced by an IP whitelist and login credentials. From the dashboard, users can select and customize a DDoS attack that will be simulated. Each connected partner has their own dashboard page, which is presented after selecting their organization in a portal. The dashboard is designed such that each partner can only connect to their own dashboard page. The portal page is shown in
Figure 21.

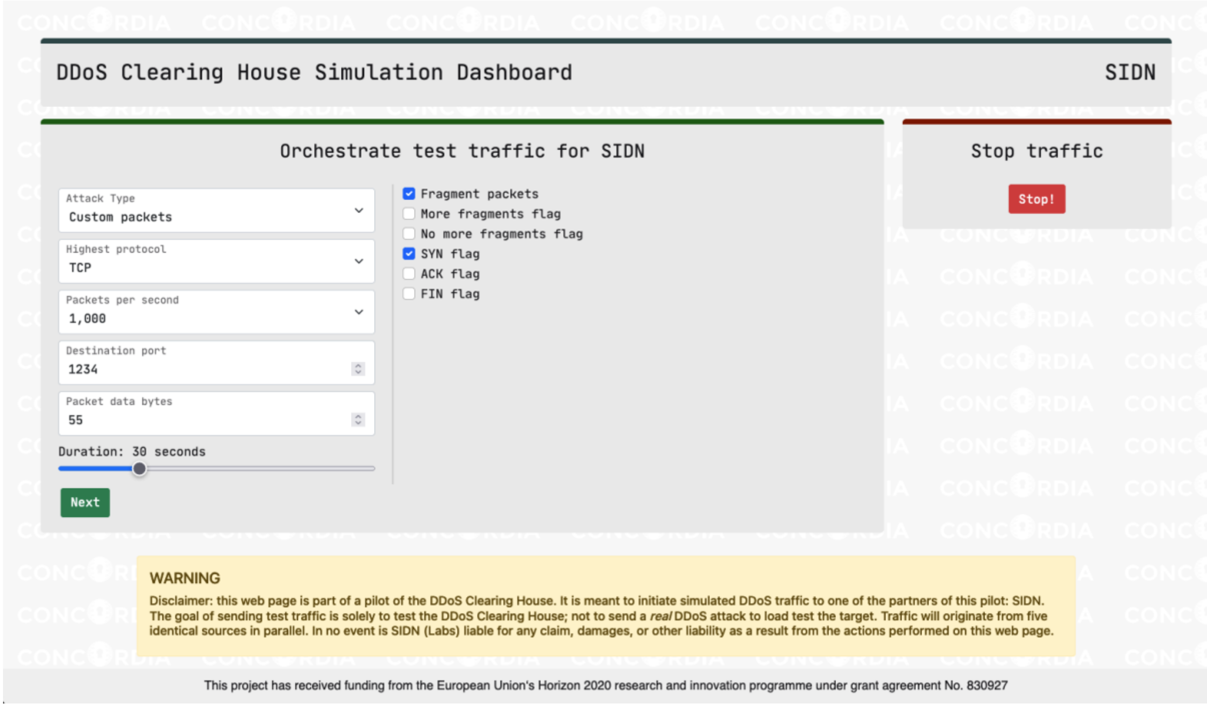


DDoS Clearing House Simulation Dashboard

Visit your dashboard:

Figure 21: DDoS Clearing House testbed dashboard portal

After going through the login portal, the partners are given access to their dashboard. On the dashboard, the user can select an attack preset, or opt for custom packets. Aspects such as destination port, packet size, traffic speed, and TCP flags can be customized on this page (see Figure 22).



DDoS Clearing House Simulation Dashboard

SIDN

Orchestrate test traffic for SIDN

Attack Type: Custom packets

Highest protocol: TCP

Packets per second: 1,000

Destination port: 1234

Packet data bytes: 55

Duration: 30 seconds

☑ Fragment packets
☐ More fragments flag
☐ No more fragments flag
☑ SYN flag
☐ ACK flag
☐ FIN flag

Stop traffic

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: SIDN. 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.

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

Figure 22: Testbed dashboard

6.2.2 Technical architecture

In this section, we outline the technical architecture of the DDoS Clearing House testbed. We distinguish between the testbed's dashboard and the attack infrastructure.

The dashboard is a simple web application developed with python Flask. It is served with Nginx, which limits access to the dashboard through IP allowlisting and HTTP Basic Authentication. Interaction with the dashboard triggers API endpoints, for example, to start a particular attack, or to stop all traffic. The API is tightly integrated in the dashboard with Flask-RESTful. Upon calling the API endpoints, the attack infrastructure is instructed to start or stop attacks using Ansible. Ansible is an infrastructure-as-code software tool, which enables running commands on multiple machines at the same time. Using Ansible, the dashboard can instruct the attack nodes to start or stop sending traffic in unison. Each DDoS attack is defined in an Ansible "playbook" and is executed on all attack nodes simultaneously. The code for the dashboard, as well as all the Ansible configurations are open source on the DDoS Clearing House GitHub organization[7].

[7] https://github.com/ddos-clearing-house/testbed

6.2.3 Attack tools

The actual DDoS traffic that is sent to the target is generated by several open-source DDoS tools, which are installed on each of the attacking machines. The following describes these attack tools and the traffic that they generate.

Hping3[8] - This general-purpose networking tool is commonly used to check whether a remote computer is responsive or not, using ICMP, TCP and UDP packets. It is similar to the ping tool and is usually used to test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, perform traceroute-like actions, fingerprint remote operating systems, etc. Based on the previously mentioned functionalities hping3 tool can also be used to flood the network with packets, thus creating a potential DDoS attack. We have included the hping3 tool in the DDoS Clearing House testbed and created network traffic to the victim servers. Hping3 allows the user on the testbed to construct custom packets with which to flood the target at a packet speed of their choosing.

Hping3 is used to send a customized DDoS attack to the target. The following tools are simpler options with predefined attack vectors. They are generally well-known DDoS attack tools, and they function as attack templates that are ready to be sent.

GoldenEye[9] - GoldenEye is an HTTP DoS Test Tool that sends a lot of HTTP traffic to a web server (HTTP flood attack). It creates many concurrent HTTP GET or POST requests, using random User Agent headers.

Slowloris[10] - Slowloris creates many HTTP requests and sends headers periodically to keep the connections open. By never closing the connections it exhausts the target’s connection pool, rendering it unable to respond to legitimate users. It uses very little bandwidth.

HTTP Unbearable Load King (HULK)[11] - Similarly to Goldeneye, it attempts to overload the target with many concurrent HTTP GET or POST requests, using random User Agent headers.

Low Orbit Ion Cannon (LOIC)[12] - This attack tool attempts to bring down the target network by overloading it with HTTP, UDP, and TCP packets.

6.3 Use as cyber range

Besides the testbed's intended use as a platform on which to run pilots and demonstrations, it can be used as a cyber range for smaller-scale DDoS drills. By connecting more powerful attack nodes, not limited to small traffic samples, organizations can use the platform to send DDoS attacks to themselves in a controlled environment. The DDoS Testbed as a DDoS drill platform would be complementary to the bi-yearly large DDoS drills organized by the Dutch anti-DDoS coalition.

[8] https://tools.kali.org/information-gathering/hping3
[9] https://github.com/jseidl/GoldenEye
[10] https://en.wikipedia.org/wiki/Slowloris_(computer_security)
[11] https://github.com/grafov/hulk
[12] https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

Since December 2022, the Dutch tax and customs administration – member of the Dutch ADC – are hosting the testbed in their Security Operation Center (SOC) network, for use by other coalition members. The testbed instance for the Dutch ADC has a maximum bandwidth of 10Gb/s. Members of the Dutch ADC can request an account and use the cyber range to test their DDoS resilience in a safe and controlled manner at their leisure. Before the testbed becomes a fully operational service in the Dutch ADC, a more thorough evaluation of the security and legality is required; it is not yet in operational use. The Dutch ADC's method of practicing DDoS resilience in large-scale, collaborative exercises, as well as through the testbed, was presented at the Black Hat conference in London, December 2022[13].

7 DDoS Clearing House pilots

7.1 Pilot in the Netherlands

SURF, SIDN, and the UT actively contribute to the Dutch ADC, which currently consists of 16 critical service providers across the sectors in the Netherlands (e.g., banks, telcos, and governments).

SIDN has written a document for members of the Dutch ADC on the technical requirements for production networks to fingerprint DDoS attacks using the Dissector and to upload these fingerprints to DDoS-DB.

Also, SIDN, SURF, and the UT actively participated in the Clearing House Working Group (WG) of the Dutch ADC. One of SIDN's legal experts joined the Dutch ADC's Legal WG and contributed to their legal framework (e.g., the consortium agreement) and the Code of Engagement being developed in T4.2. SIDN also contributed to the Dutch ADC's Communications working group and the new working group "Architecture and Society".

To share data about the DDoS attacks that organizations handle in the context of the pilot, the ADC set up a data sharing agreement, which was required for the participating organizations to share the source IP addresses of the attack. IP addresses are personally identifiable information and cannot freely be shared under the GDPR. Hence, agreements were signed between the participating organization and SIDN, being the operator of the DDoS-DB instance used for the pilot.

The DDoS Clearing House pilot in the Netherlands involved six coalition members: NBIP, SIDN, KPN, UT, National Payments Association, and the Tax and Customs administration. NBIP, with their DDoS scrubbing service, has provided the coalition with 269 fingerprints of real DDoS attacks they handled. These fingerprints could be used by the other participating coalition members, and, at the same time, were used to further improve the Dissector component.

After sharing many unique DDoS fingerprints, the pilot was deemed successful and halted. The pilot in the Netherlands provided added value in two aspects: (1) it enabled the developers to further improve the technical system, and (2), it showed the members of the

[13] https://www.blackhat.com/eu-22/briefings/schedule/index.html#how-we-organize-large-scale-ddos-exercises-in-the-netherlands-28542

Dutch anti-DDoS coalition the maturity of the platform and the viability of sharing DDoS data using it.

The sharing agreement between SIDN and the participating Dutch ADC members is attached in Appendix 2 (14.2).

7.2 Pilot in Italy

The DDoS Clearing House Italian pilot started at the end of 2021 and is based on an initial coalition of three members: the Telecom Italia Security Lab, part of the Cybersecurity department (and directly involved in the CONCORDIA Project), the Security Operation Center (SOC) in charge of the monitoring and protection of the Telecom Italia (TIM) network infrastructures and the University of Turin. Figure 23 shows the logical view of the pilot in Italy.

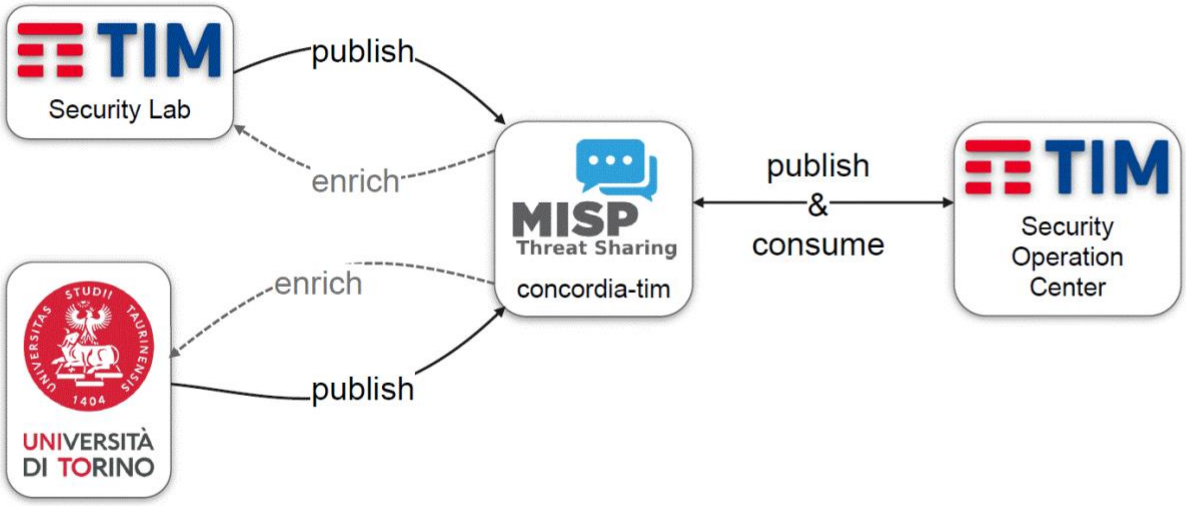


Figure 23: Overview of the partners in the pilot in Italy

Each partner is publishing the relevant events they detect within the scope of their network, whereas only the Telecom Italia SOC is currently interested in "consuming" the provided information for the protection of the network services. That is because only the SOC is operating in a production environment. In detail:

- University of Turin - producer:
  - collects PCAP samples from real-life attacks to a honeynet
  - publishes MISP events through the DDoS-DB pipeline
- TIM Security Lab - producer:
  - collects real attack data from threat intelligence feeds (both OSINT and CLOSINT)
  - publishes MISP events through the DDoS-DB pipeline
  - generates MISP events with threat intelligence data
- TIM Security Operation Center - producer / consumer:
  - generates MISP events with data collected from real-life attacks
  - uses MISP events to drive response and mitigation

The main goal of the pilot in Italy is to share DDoS attacks' fingerprints and related DDoS attack Threat Intelligence information through a common MISP instance hosted by Security Lab. The three interconnected partners (TIM SOC, Security Lab, Turin University) regularly share information related to detected and/or analyzed DDoS attacks. All partners run at least two core components of the DDoS Clearing House developed by Task 3.2 of the CONCORDIA EU Project: the Dissector and the MISP Exporter.

The architecture of the pilot is presented in Figure 24. Each partner involved in the pilot uses the same tools interconnected to the central dedicated MISP instance.

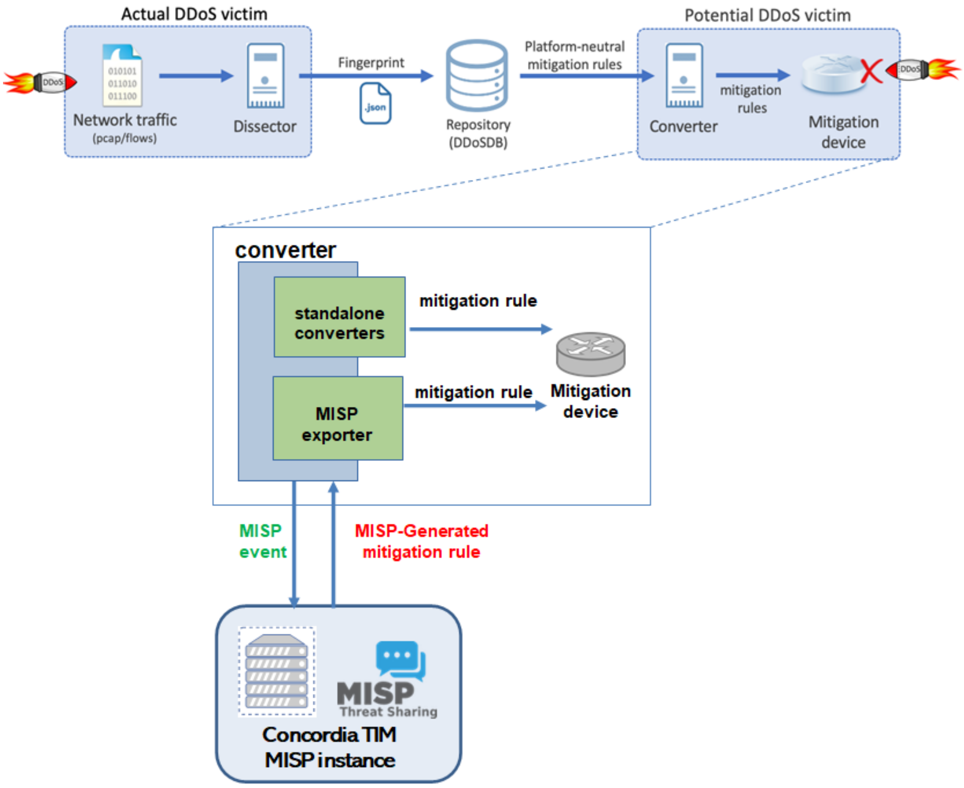


Figure 24: Architecture of the pilot in Italy

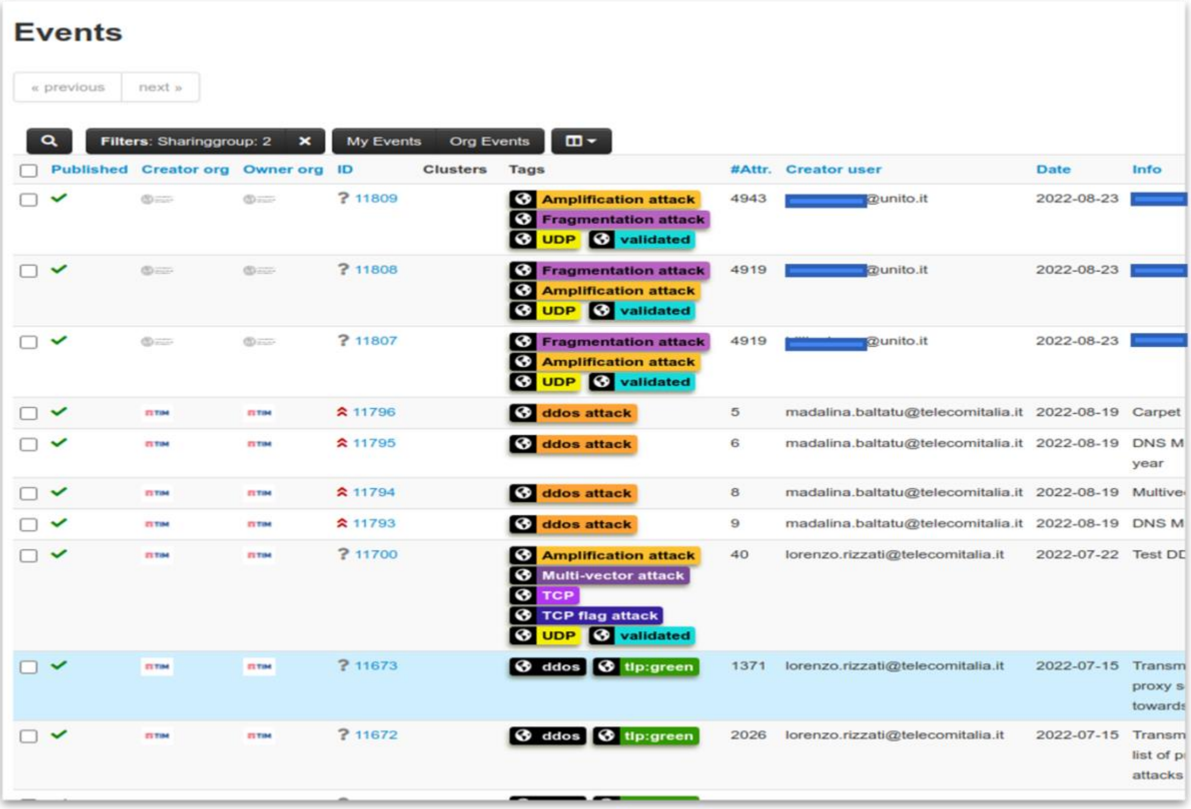
A MISP instance is configured and running for Threat Information sharing on DDoS attacks inside the Italian pilot. A dedicated sharing group (DDoS pilot IT SG) was created on this instance and all events created by a partner are shared among all other Italian partners. All partners have both GUI and API access, and events can also be created manually. The MISP Exporter creates events automatically from fingerprints produced by the Dissector component. The MISP events can be enriched with DDoS fingerprints as well as other kinds of attachments, depending on the rules and tools available to each partner.

The University of Turin shares fingerprints, generated with the Dissector, based on PCAP traces of real traffic captured by their publicly exposed honeypot battery.

TIM Security Lab shares fingerprints from synthetic DDoS traffic generated by security tools in the Telecom Italia testing laboratory and can use the full list of tools developed by the CONCORDIA Project.

TIM's SOC shares Threat Intel information, in the form of snort rules/regular expressions generated from real DDoS attacks, that can be used to detect and block such attacks. Security Lab can also share DDoS Threat Intel information from OSINT sources, collected by their internal TIP (Threat Intel Platform). The main reason behind such a decision is because TIM already uses advanced commercial products and techniques to detect and block/limit DDoS attacks. The current anti-DDoS architecture has been built in several years and in partnership with its main providers. In some special cases (e.g., new emerging sophisticated DDoS attacks) the SOC experts can proceed with a manual configuration of specific mitigation/detection rules, but in general, the detection is based on proprietary rules configured and updated by the vendors. Hence, TIM's Security Operations Center (SOC) plans to use the DDoS fingerprints as Cyber Threat Intelligence information to support their Threat Hunting and Incident Response activities, as well as enrichment information to their current investigations and incidents. Moreover, fingerprints are considered useful if they are not focused on the list of attackers' IPs, but if they can give additional specific information on the DDoS attacks, e.g., the type of attack (reflection, amplification, etc.), specific patterns present in the packets, statistics on packet flows (packet dimensions, TTL, etc.). Such elements, if present, could permit to create, for example, snort rules or regular expressions useful to set up mitigation rules, usually rate-limiting mechanisms implemented at the edge routers. Blackhole (completely discarding the incoming traffic) is almost avoided, to protect legitimate traffic.

The entire set of shared fingerprints is present inside the MISP instance because the Italian pilot does not use (at least not initially) the DDoS-DB (see
Figure 25).



Events

« previous | next »

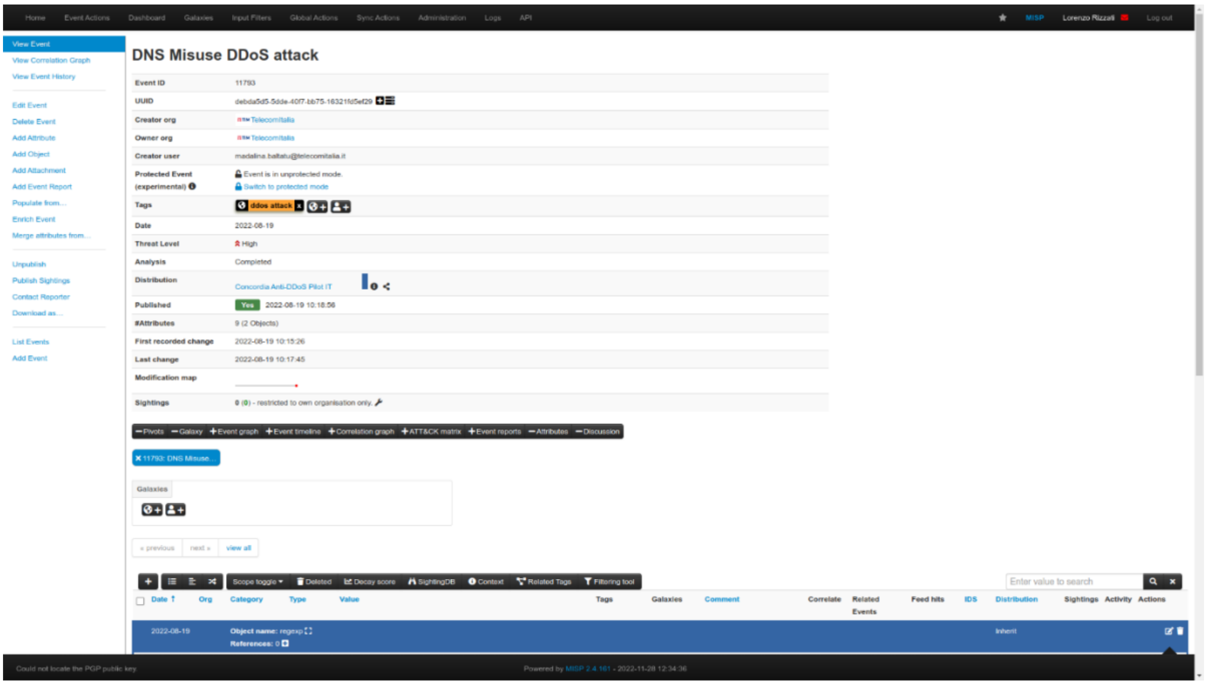
Filters: Sharinggroup: 2 ✕ | My Events | Org Events

□	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	Creator user	Date	Info
□	✓			? 11809		Amplification attack Fragmentation attack UDP validated	4943	[redacted]@unito.it	2022-08-23	[redacted]
□	✓			? 11808		Fragmentation attack Amplification attack UDP validated	4919	[redacted]@unito.it	2022-08-23	[redacted]
□	✓			? 11807		Fragmentation attack Amplification attack UDP validated	4919	[redacted]@unito.it	2022-08-23	[redacted]
□	✓	TIM	TIM	⇈ 11796		ddos attack	5	madalina.baltatu@telecomitalia.it	2022-08-19	Carpet
□	✓	TIM	TIM	⇈ 11795		ddos attack	6	madalina.baltatu@telecomitalia.it	2022-08-19	DNS M year
□	✓	TIM	TIM	⇈ 11794		ddos attack	8	madalina.baltatu@telecomitalia.it	2022-08-19	Multive
□	✓	TIM	TIM	⇈ 11793		ddos attack	9	madalina.baltatu@telecomitalia.it	2022-08-19	DNS M
□	✓	TIM	TIM	? 11700		Amplification attack Multi-vector attack TCP TCP flag attack UDP validated	40	lorenzo.rizzati@telecomitalia.it	2022-07-22	Test DD
□	✓	TIM	TIM	? 11673		ddos tlp:green	1371	lorenzo.rizzati@telecomitalia.it	2022-07-15	Transm proxy s towards
□	✓	TIM	TIM	? 11672		ddos tlp:green	2026	lorenzo.rizzati@telecomitalia.it	2022-07-15	Transm list of p attacks

Figure 25: MISP instance with DDoS fingerprints from the pilot in Italy

Starting from a fingerprint the MISP Exporter component of the converter creates a MISP event (

Figure 26) which contains the data of the fingerprint as MISP attributes or MISP objects according to the mappings defined by the project.



DNS Misuse DDoS attack

Event ID	11793
UUID	debda5d5-5dde-40f7-bb75-16321fd5ef29
Creator org	TIM Telecomitalia
Owner org	TIM Telecomitalia
Creator user	madalina.baltatu@telecomitalia.it
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	ddos attack
Date	2022-08-19
Threat Level	High
Analysis	Completed
Distribution	Concordia Anti-DDoS Pilot IT
Published	Yes 2022-08-19 10:18:56
#Attributes	9 (2 Objects)
First recorded change	2022-08-19 10:15:26
Last change	2022-08-19 10:17:45
Modification map	
Sightings	0 (0) - restricted to own organisation only.

□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
	2022-08-19		Object name: regexp References: 0										Inherit			

Could not locate the PGP public key

Powered by MISP 2.4.161 - 2022-11-28 12:34:36

Figure 26: MISP event of a DNS reflection attack

8 Exploitation of the DDoS Clearing House

8.1 DDoS Clearing House a production service

First, we are in the process of deploying the DDoS Clearing House as a production-level service in the Dutch anti-DDoS coalition, operated by NBIP. This requires some organizational change in the coalition, as the current setup is temporary by design, and only meant to run the pilot of the system. Before we deploy the system in production, we will further mature the role descriptions for the functions that are involved in running the Clearing House. This includes the database operator, in charge of hosting DDoS-DB and its data management. The deployment will also require rewriting – at least partially – the data sharing agreement that is currently in place for the pilot. Deployment as a production-level service is a natural continuation of the project after being included in the European Commission's Innovation Radar[14].

8.2 DDoS Clearing House a cyber range

Second, we will start using the DDoS Testbed as a cyber range in the Dutch anti-DDoS coalition. The testbed was originally developed to pilot the DDoS Clearing House in a representative but non-production environment. However, the distributed traffic generator was deemed useful for small-scale DDoS drills too. Hence, the testbed will be updated further, and, like the DDoS Clearing House, be deployed in production in the Dutch anti-DDoS coalition. Using the testbed, coalition members can practice their DDoS resilience on their own accord, next to the bi-yearly joint DDoS drills.

8.3 DDoS Clearing House as an internal security service

The pilot in Italy will continue its operation by sharing DDoS information internally in Telecom Italia's Security Lab and SOC. The members of the Italian pilots are also looking to expand theirs into an Italian anti-DDoS coalition.

9 Lessons learned

9.1 Collaborative DDoS mitigation is predominantly an organizational challenge

The first lesson we learned is that the problem of collaborative DDoS mitigation is much more organizationally rooted than technically. Naturally, a technical system such as our proposed DDoS Clearing House is the foundation of collaborative DDoS mitigation and a prerequisite to sharing data in the first place. However, the DDoS Clearing House, consisting of modular components, can be compared with a collection of musical instruments: they require people

[14] https://www.innoradar.eu/innovation/46297

to organize and play together to make good music. The instruments do not make the band. Hence, a solid governance model is paramount to the success of an anti-DDoS coalition.

The membership-based structure of the Dutch national anti-DDoS coalition has proven to be effective in this regard. Membership fees ensure (to an extent) participation in the coalition's activities and reduce freeloaders. The structure of working groups provides members with the ability to contribute to an area of their expertise and interest.

9.2 Keep an eye on the market while doing the research

Our second lesson learned is that long-term research projects such as need to follow changes in the market during the project. We learned that because we observed a shift in DDoS mitigation strategies over the past years. We have seen organizations move from mostly on-premises DDoS mitigation to fully outsourcing their DDoS mitigation. This brought with it a diminished sense of urgency of sharing DDoS (meta) data because organizations are no longer (or to a lesser extent) burdened with the mitigation of DDoS attacks.

Luckily, the interest in the DDoS Clearing House is still substantial. Our efforts in the Dutch anti-DDoS coalition, and the pilot in Italy have received continued interested, and have not gone unnoticed externally. Third parties have shown interest in the concept of anti-DDoS coalitions, with the DDoS Clearing House as a technical anchor point. For those organizations, this cookbook can help setting up their Clearing House and shape their coalitions. In summary, we learned it is important to keep speaking with as many stakeholders as possible, to establish expectations, requirements, and requests. The risk of losing track of these is a growing divergence between the work being done and the market needs.

9.3 A modular architecture was essential for a demo-driven approach (during Covid)

The third lesson learned, touching upon the development of the technical system, is the benefit of a modular approach and well-defined interfaces for the DDoS Clearing House. It allowed to develop the various system components separately from each other, without the need to use the entire system. This allowed us to develop the system's components in parallel, while having only agreed on the interfacing between the components. As a result, we were able to develop the software in a demo-driven way, even at times of Covid.

Our demo-driven way of working involved the DDoS Clearing House holding monthly meetings, during which the status of each platform component was discussed, and plans for the coming months were gathered. The demo-driven way of working kept us engaged with each other's work, while being able to efficiently develop each component separately. Furthermore, the modularity of the software enables users to only use some of the components, while substituting their own alternatives for others. For example, in the pilot of the system in Italy, MISP was used as a platform for sharing DDoS Fingerprints, whereas in the pilot in the Netherlands, DDoS-DB was used.

9.4 Collaborative DDoS mitigation advances cybersecurity more broadly

Our final lesson learned is that forming coalitions around a specific topic – such as Anti-DDoS Coalitions – is useful not only to improve collaboration on that specific topic but also because it grows and further interconnects the network formed by all organizations and people, which communicate on many more topics concerning cybersecurity.

Since (sharing of) knowledge is an important ingredient in improving cybersecurity resilience, forming a coalition around a specific topic can influence more than just the topic itself. For example, during the (preparation of) DDoS drills in in the Dutch ADC, topics such as threat intelligence sharing platforms and safe network infrastructure are also discussed.

10 Future work

We have planned a few activities for the near future, after the CONCORDIA project comes to an end. We plan to help set up other anti-DDoS coalitions in Europe, for which this document provides a strong foundation. Our experience in the Dutch ADC and the documentation provided in this cookbook should kickstart any organization aspiring to engage in collaborative DDoS mitigation. So far, we have had two organizations from outside CONCORDIA contact us with the intention to create an anti-DDoS coalition in their respective sectors.

We will also distill this document into an article for the IEEE communications magazine to reach a broader audience. The document will summarize the technical platform specifications but focus on the interaction of technology and organizational aspects of collaborative DDoS mitigation. We plan to disseminate the article, as well as this cookbook, among interested organizations and government bodies, with the hope that they are inspired and motivated to construct their own anti-DDoS coalitions.

11 Acknowledgements

SIDN, the University of Twente, SURF, FORTH, University of Zürich, and Telecom Italia were partly funded by the European Union’s Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/

SIDN, the University of Twente, and SURF are members of the Dutch National Anti-DDoS Coalition, a self-funded public-private initiative to collaboratively protect members and the wider Internet community from DDoS attacks. Website: https://www.nomoreddos.org/en/

12 Epilogue

The DDoS Clearing House platform, this cookbook, and the appendices aim to provide enough information to set up more Anti-DDoS Coalitions in communities across Europe and the wider world. For further questions regarding the DDoS Clearing House or Anti-DDoS Coalitions do not hesitate to contact the authors of this document via thijs.vandenhout@sidn.nl or cristian.hesselman@sidn.nl.

13 References

[1] A. Feldmann, O. Gasser, F. Lichtblau, E. Pujol, I. Poese, C. Dietzel, D. Wagner, M. Wichtlhuber, J. Tapiador, N. Vallina-Rodriguez, O. Hohlfeld and G. Smaragdakis, "The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic," *ACM Internet Measurement Conference (IMC2020),* 2022.

[2] ENISA, "ENISA Threat Landscape 2021," 27 October 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. [Accessed 2022].

[3] J. M. Ceron, J. J. Chromik, J. J. Cardoso de Santanna and A. Pras, "Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands," University of Twente, Enschede, 2019.

[4] S. Herzog, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security,* vol. 4, no. 2, pp. 49-60, 2011.

[5] A. Lima, F. Rocha, M. Völp and P. Esteves-Veríssimo, "Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems," *2nd ACM Workshop on Cyber-Physical Systems Security and Privacy,* pp. 59-70, 2016.

[6] D. Leprice-Ringuet, "This 5G ambulance could be the future of emergency healthcare," 18 November 2019. [Online]. Available: https://www.zdnet.com/article/inside-the-5g-ambulance-that-could-let-doctors-treat-you-miles-from-the-hospital. [Accessed 2022].

[7] S. R. Guntur, R. R. Gorrepati and V. R. Dirisala, "Robotics in healthcare: an internet of medical robotic things (IoMRT) perspective," *Machine learning in bio-signal analysis and diagnostic imaging,* pp. 293-318, 2019.

[8] NOS, "After banks now also Tax and Customs Administration and DigiD victim of DDoS attacks," 29 January 2018. [Online]. Available: https://nos.nl/artikel/2214339-na-banken-nu-ook-belastingdienst-en-digid-slachtoffer-ddos-aanvallen. [Accessed 2022].

[9] G. C. Moura, R. d. O. Schmidt, J. Heidemann, W. B. de Vries, M. Müller, L. Wei and C. Hesselman, "Anycast vs. DDoS: Evaluating the November 2015 root DNS event," *Proceedings of the 2016 Internet Measurement Conference,* pp. 255-270, 2016.

[10] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher and Seaman, "Understanding the Mirai Botnet," *26th USENIX Security Symposium,* 2017.

[11] T. Hofmans, "Tweakers: Large-scale ddos attacks on Dutch providers take place again," 01 September 2022. [Online]. Available: https://tweakers.net/nieuws/171644/opnieuw-vinden-grootschalige-ddos-aanvallen-op-nederlandse-providers-plaats.html. [Accessed 2022].

[12] M. Keijzer, "Answers to questions by MP Weverling on DDoS attacks on Internet service providers (in Dutch)," October 2022. [Online]. Available: https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D42266&did=2020D42266 . [Accessed 2022].

[13] C. Hesselman, M. Kaeo, L. Chapin, K. Claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour and R. Rasmussen, "The DNS in IoT: Opportunities, Risks, and Challenges," *IEEE Internet Computing,* vol. 24, 2020.

[14] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials,* vol. 15, no. 4, 2013.

[15] C. Hesselman, J. van der Ham, R. van Rijswijk, J. Santanna and A. Pras, "A Proactive and Collaborative DDoS Mitigation Strategy for the Dutch Critical Infrastructure," April 2018. [Online]. Available: https://www.sidnlabs.nl/en/news-and-blogs/a-proactive-and-collaborative-ddos-mitigation-strategy-for-the-dutch-critical-infrastructure. [Accessed 2022].

[16] C. Hesselman, R. Poortinga-van Wijnen, G. Schaapman and R. Ruiter, "Increasing the Netherlands' DDoS resilience together," 9 April 2020. [Online]. Available: https://www.concordia-h2020.eu/blog-post/increasing-the-netherlands-ddos-resilience-together. [Accessed 2022].

[17] K. E. Silva, *Mitigating botnets: Regulatory solutions for industry intervention in large-scale cybercrime,* Tilburg: Tilburg University, 2019.

[18] L. Gommans, J. Vollbrecht, B. Gommans-de Bruin and C. de Laat, "The service provider group framework: A framework for arranging trust and power to facilitate authorization of network services," *Future Generation Computer Systems,* vol. 45, pp. 176-192, 2015.

[19] Robinson, Max and et al., "DefCOM: defensive cooperative overlay mesh," *DARPA Information Survivability Conference and Exposition,* vol. 3, 2003.

[20] B. Rodrigues and B. Stiller, "Cooperative Signaling of DDoS Attacks in a Blockchain-based Network," *Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos,* 2019.

[21] D. Wagner, D. Kopp, M. Wichtlhuber, C. Dietzel, O. Hohlfeld, G. Smaragdakis and A. Feldmann, "United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale," *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security,* pp. 970-987, 2021.

[22] A. Mortensen, T. Reddy and R. Moskowitz, "DDoS open threat signaling (dots) requirements," May 2019. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8612. [Accessed 2022].

[23] S. K. Fayaz, Y. Tobioka, V. Sekar and M. Bailey, "Bohatei: Flexible and Elastic DDoS Defense," *24th USENIX security symposium,* pp. 817-832, 2015.

[24] Rashidi, Bahman and C. Fung, "CoFence: A collaborative DDoS defence using network function virtualization," *12th International Conference on Network and Service Management (CNSM),* no. 12, pp. 160-166, 2016.

[25] R. Dobbins, D. Migault, S. Fouant, Moskowitz, N. Teague, L. Xia and K. Nishizuka, "Use cases for DDoS Open Threat Signaling, Internet Draft," July 2018. [Online]. Available: https://www.ietf.org/id/draft-ietf-dots-use-cases-16.txt.

14 Appendices

Note on appendix 2, 3, and 4: these are anonymized documents from the Dutch anti-DDoS Coalition which we publish with the approval of the coalition members.

14.1 Appendix 1: DDoS Fingerprint format

DDoS Fingerprints are JSON files that describe the characteristics of a DDoS attack. They are distilled from DDoS network captures using the dissector module of the DDoS Clearing House. The input to the Dissector can be NetFlow data or PCAPS.

Fingerprints generated from PCAP data may contain more detailed characteristics than those generated from NetFlow files, but their overall structure is the same. Each fingerprint contains summary statistics of the entire attack, such as average bits/s, duration, and number of packets. Each fingerprint also contains an array of *attack vectors* that each describe one of the vectors that make up the given attack. Fingerprints have at least one attack vector. Examples of attack vectors are DNS amplification, TCP SYN Flood, NTP amplification, etc. Each attack vector describes the traffic that belongs to that vector and includes information like source IP addresses, targeted ports, and IP protocol. When a fingerprint is uploaded to DDoS-DB some additional fields are added.

The following fields are defined for fingerprints generated from NetFlow data. Fingerprints generated from PCAPs will not include the fields related to the number of flows. Additional fields that can be extracted from PCAP files are listed after these.

The datatype Map<?, Float> refers to a map of values to their corresponding fraction of traffic. E.g.: http_method: {"GET": 0.85, "POST": 0.15}

Summary statistics

Field name	**Description**	**Datatype**
attack_vectors	Array of attack vectors that make up this attack (see below)	Array of objects
target	IP address or subnet of the attack target, or “Anonymous” (when uploaded to DDoS-DB)	String
tags	Tags assigned to this attack, e.g., “Amplification attack”, “Multi-vector attack”, “TCP SYN flag attack”	Array of strings
key	MD5 hash digest of the fingerprint, used as identifier and as file name of the fingerprint	String
time_start	Timestamp of the start of the attack (time zone local to the attack target)	DateTime
time_end	Timestamp of the end of the attack (time zone local to the attack target)	DateTime
duration_seconds	Duration of the attack in seconds	Integer
total_flows (only from Flow files)	Total number of flows in the attack capture	Integer
total_megabytes	Total volume of the attack in megabytes (MB)	Integer
total_packets	Total number of packets in the attack	Integer
total_ips	Total number of unique source IP addresses from which attack traffic originated	Integer
avg_bps	Average number of bits/s during the attack	Integer
avg_pps	Average number of packets/s during the attack	Integer
avg_Bpp	Average number of Bytes per packet	Integer

Attack vectors (excluding additional fields from PCAPs)

Field name	Description	Data type
service	Name of the service used in this attack vector, determined by the source port and protocol. e.g., UDP port 53 -> DNS. Or: “Unknown service” or “Fragmented IP packets” for the vector of packet fragments that cannot be assigned to another vector	String
protocol	IP protocol, e.g., TCP, UDP, ICMP	String
fraction_of_attack	The fraction of the entire DDoS attack that this attack vector makes up ∈ [0, 1], calculated from total bytes, not taking into account the vector of packet fragments (null)	Float or null
source_port	Source port of this attack vector if the source port in combination with protocol is associated with a specific service (e.g., UDP/53 -> DNS), if not - see destination_ports	Integer or “random”
destination_ports	List of outlier destination ports (if any) with the corresponding fraction of the traffic, or “random”. e.g. {“443”: 0.65, “80”: 0.35}. (The keys are strings because of the JSON format)	Map<String, Float> or “random”
tcp_flags	List of outlier TCP flags (if any) with the corresponding fraction of the traffic, e.g., {“…A….”: 0.987}. Null if the protocol is not TCP, or there are no outliers.	null or Map<String, Float>
nr_flows (only from Flow files)	Number of flows that contribute to this attack vector	Integer
nr_packets	Number of packets in this attack vector	Integer
nr_megabytes	Number of megabytes sent through this attack vector	Integer
time_start	Timestamp of the start of the attack vector: the first flow of this attack vector (time zone local to the attack target)	DateTime
duration_seconds	Duration of this attack vector in seconds (last timestamp - first timestamp)	Integer
source_ips	Array of unique IP addresses that sent traffic to the target on this attack vector (truncated in the preview, and in the overview on DDoS-DB), the JSON file contains all IP addresses	Array of strings

Added in DDoS-DB

Field name	Description	Data type
submitter	user account that submitted the fingerprint to DDoS-DB	String
submit_timestamp	Timestamp of the upload (UTC)	String
shareable	If this fingerprint can be shared with other users / other DDoS-DB instances	Boolean
comment	Comment added to the fingerprint	String

Additional fields added from PCAP data

PCAP files contain the packets themselves, and thus allow the extraction of more detailed fields for various attack vectors. The following fields are added to fingerprints generated from PCAP files or added to specific attack vectors.

All PCAP fingerprints

Field name	Description	Data type
ethernet_type	The protocol encapsulated in the ethernet frame (more details)	Map<String, Float> or “random”
frame_len	length of ethernet frame in bytes	Map<Integer, Float> or “random”

IP-based attack vectors (most)

Field name	Description	Data type
fragmentation_offset	fragmentation_offset of packets	Map<Integer, Float> or “random”
ttl	Time to live	Map<Integer, Float> or “random”

DNS attack vectors

Field name	Description	Data type
dns_query_name	query name of the DNS request (domain name)	Map<String, Float> or “random”
dns_query_type	Query type (e.g., A, TXT, AAAA, ANY)	Map<String, Float> or “random”

HTTP(S) attack vectors

Field name	Description	Data type
http_uri	URI of the HTTP request	Map<String, Float> or “random”
http_method	HTTP request method (e.g., GET, POST)	Map<String, Float> or “random”
http_user_agent	User agent string	Map<String, Float> or “random”

NTP attack vectors

Field name	Description	Data type
ntp_requestcode	NTP request code	Map<Integer, Float> or “random”

ICMP attack vectors

Field name	Description	Data type
ICMP type	ICMP type (e.g. Echo)	Map<String, Float> or “random”

14.2 Appendix 2: Pilot agreement Dutch ADC (Translated)

Disclaimer: this appendix is translated from Dutch. It is of no legal significance in this document and is solely included as informational resource.

AGREEMENT REGARDING pilot DDOS CLEARING HOUSE NL

THE PARTIES,

Stichting Internet Domeinregistratie Nederland, located at Meander 501, 6825 MD in Arnhem, represented in this matter by Cristian Hesselman, hereinafter referred to as "SIDN"

AND

<Full name>, located at <address>, represented in this by <name>, hereinafter referred to as "Participant"

TAKING INTO ACCOUNT THAT,

A. Parties cooperate in the context of the "DDoS Clearing House NL" project, in order to better prepare for DDoS attacks.
B. SIDN is the registry for domain names with the extension .nl and strives for a reliable, safe, and accessible .nl, DNS and internet infrastructure.
C. SIDN is prepared to take on the management of the Database.
D. Participant <short description of what kind of organization Participant is, from which the logic of participation in the project is evident (see B as an example)>.
E. The participant is prepared to fulfill the obligations under this agreement.
F. Parties wish to make the following agreements in that context.

HEREBY AGREE AS FOLLOWS,

1. DEFINITIONS

    1. The "Project" means the cooperation between the Parties in the context of the pilot for the purpose set out in Article 3 and is entered into for a period of six months (with an automatic extension of three months at a time until the Project Group has decided that the Project is terminated) from the signing of this Agreement.
    2. The "Database" means DDoS fingerprints stored at SIDN that are accessible to the members of the Project Group.
    3. The "DDoS fingerprints" are aggregated summaries of previous DDoS attacks that have occurred, analyzed by the Dissector, consisting of source IP addresses, source port numbers, target port numbers, protocol specific properties and the start time and duration of the DDoS attack.
    4. The "Project Group" refers to all parties participating in the Project.
    5. The "Agreement" means this Agreement.

2. SUBJECT

    1. This Agreement applies to the cooperation between the Parties in the context of the project.

3. PURPOSE OF THE PROJECT

    1. The purpose of the Project is to allow the Project Group to gain experience in maintaining a centralized Database that facilitates the automated detection of DDoS attacks based on the DDoS fingerprints using the Dissector script and to use DDoS fingerprints to investigate and structurally improve the usability and effectiveness of such a central database. The parties contribute to the Project in good faith and free of charge with the aim of achieving the goal.

2. The Participant provides information about DDoS attacks in the form of DDoS Fingerprints. The Participant runs the most recent version of the Dissector to create Fingerprints from DDoS traffic before uploading it to the Database. Raw network traffic in the form of PCAPs or Flow dumps are not shared.
3. SIDN will include this data in the Database, after which other Participants can consult the data by logging in to the Database with their own account.
4. During the Project, participation in the Project Group will be carefully limited to a small group selected members who are only admitted to the Project Group with the consent of all other members.

4. RESPONSIBILITIES

   1. SIDN is responsible for the management and adequate security of the Database in accordance with the requirements of applicable law and this Agreement.
   2. Given that this is a free service in the context of a pilot, SIDN will make reasonable efforts to make and keep the Database available to all Participants and to prevent the loss of data in the Database.
   3. SIDN is not only an administrator, but also a Participant. In its role as a Participant, SIDN has the same rights and obligations as the other Participants under this Agreement.
   4. The participant is responsible for the correctness and lawfulness of the data that it contributes to the Database.
   5. Both parties are responsible for the lawful use of the Database.

5. LIABILITY

   1. A Party is liable for damage resulting from its own actions contrary to the provisions of this Agreement.
   2. Parties are not obliged to pay compensation for reputational damage under this Agreement.

6. CONFIDENTIALITY AND ACCESS

   1. SIDN will only grant access to the Database to Participants of the Project Group after SIDN has agreed to the same obligations as those included in this Agreement.
   2. Parties treat all data from the Database as strictly confidential and ensure that persons they give access to the Database are contractually bound by an obligation to maintain the confidentiality of what comes to their knowledge unless such information was already known or was already publicly available.
   3. SIDN only grants access to (information in) the Database to investigating officers and -services, such as the police, if and insofar as SIDN is required to do so by virtue of a statutory provision. This provision does not apply to investigative services that have been admitted to the Project Group as participants. SIDN will inform the Participant to whose DDoS fingerprint(s) an investigation request applies if this SIDN is permitted under applicable law.

7. PROTECTION OF (PERSONAL) DATA

   1. Parties use the Database exclusively for the purpose of the Project, as set out in Article 3 of this Agreement and not for any other purpose.
   2. The Parties will comply with the obligations under the General Terms and Conditions during the implementation of the Project. The Data Protection Regulation (the “AVG”), the AVG Implementation Act and the Telecommunications Act, if and insofar as these laws apply to a Party.
   3. Parties are jointly responsible, as referred to in Article 26 of the GDPR, for the processing of personal data in the Database, together with the other participants of the Project group. This joint responsibility only applies when the information is included in the Database. Until then, the responsibility within the meaning of the GDPR lies with the Participant.
   4. If a security breach occurs at SIDN, as a result of which confidential information becomes known to persons outside the Project Group, SIDN will immediately report this to the

Participant. If required, SIDN will report such a breach to the supervisory authority. The participant is responsible for reporting to the data subject, if required.

5. In the event that data subjects exercise their rights under Chapter 3 of the GDPR, the Party receiving the request will try to handle the request itself, or if it is not able to do so independently, enlist the help of the other Party or another participant of the Project Group. Parties are obliged to cooperate with each other and the other participants of the Project Group in handling such requests.
6. Both Parties are themselves obliged to inform the data subjects about the processing as provided for in the context of the Project.

8. SECURITY

1. SIDN will ensure that appropriate technical and organizational security measures are taken to secure the Database.
2. SIDN restricts access to the IP addresses of Participants that have been included in a whitelist and Participants gain access based on a username in combination with a password.
3. The security rules are established through the governance, as set out in Article 9 of this Agreement.
4. The Participant adheres to the security regulations when using the Database.

9. GOVERNANCE

1. Parties participate in regular consultations with the other participants of the Project Group. Within this consultation, all developments regarding the Project are discussed.
2. The Project Group preferably decides unanimously regarding all matters that concern the entire Project Group. If a decision cannot be reached unanimously after a good faith attempt has been made to reach unanimity, a proposal shall be passed by majority vote.
3. Decisions of the Project Group may not conflict with the provisions of the Agreement.
4. This Agreement may be amended within governance if all members of the Project group unanimously vote in favor of an amendment. A simple majority is not sufficient for an amendment to the Agreement. In that case, the contracts of all members of the Project Group will be changed in the same way. The change will only take effect if the change is in writing and signed by all members of the Project Group.

10. AUDIT

1. The Participant has the right to carry out an inspection of the associated documentation with and the facilities that SIDN uses to manage and secure the Database.
2. SIDN will provide the Participant with the cooperation that is reasonably required in an inspection such as referred to in Article 10.1.
3. If another participant of the Project Group in the 12 months prior to the request until an inspection has carried out a comparable inspection or has it carried out by an independent expert, SIDN may suffice by sharing the results of that other participant of the Project Group with the Participant.
4. The Participant is obliged to share the results of an inspection at SIDN's request with another participant of the Project Group, except for the results of the inspection that only pertain to the Participant himself.

11. TERMINATION

1. A Party is free to terminate participation in the Project at any time, with immediate effect.
2. In the event of termination by the Participant, SIDN will ensure that all data submitted by the Participant is removed from the Database within seven days after termination, if the Participant so requests.
3. In the event of termination by SIDN in its role as manager, SIDN will ensure that all data in the Database will be deleted within fourteen days.

4. In the event of termination, SIDN will facilitate that the Participant receives a copy of the data it provided to the Database.

12. CHANGES

1. This contract may be amended by mutual agreement of the Parties or through the arrangement in Article 9.4. Changes apply in all cases to all Participants so that the same conditions always apply to all Participants.

13. APPLICABLE LAW AND JURISDICTION

1. This Agreement is governed by Dutch law.
2. Any disputes arising from or related to this Agreement will be submitted to the exclusive jurisdiction of the court in Amsterdam.

Signed <name>	SIDN
at	at
on	on
________________________	________________________
<name>	Cristian Hesselman

14.3 Appendix 3: Governance regulations Dutch Anti-DDoS Coalition (Translated)

Disclaimer: this appendix is translated from Dutch. It is of no legal significance in this document and is solely included as informational resource.

GOVERNANCE REGULATIONS
ANTI-DDOS COALITION

Article 1. Status of the regulations

1.1 These Rules (the "**Rules**" and each Article of these Rules: an "**Article**") are the Rules of the Anti-DDoS Coalition (the "**ADC**").

1.2 These Rules were adopted by the Plenary Meeting of the ADC referred to in Article 3.1 by decision taken on 14 September 2021 (the "**Adoption Date"**).

1.3 These Rules constitute an appendix to each cooperation agreement entered by <facilitator>, with its registered office at <address>, registered in the Trade Register under number <number>, for the purpose of building and supporting the ADC, enters on an individual basis with companies and institutions (each such cooperation agreement: a "**Cooperation Agreement**" and each of <facilitator>'s counterparts under the Cooperation Agreements: a "**Participant**").

1.4 The Cooperation Agreements aim (among other things) to:

(a) the Participants make available to the ADC financial resources, manpower and delegates as members of the bodies of the ADC; and

(b) <facilitator> and the Participants shall carry out and perform their duties and obligations under the Cooperation Agreements in accordance with a consultative structure with the Participants.

The purpose of these Regulations is to specify the consultation structure referred to under (b) of this Article 1.4.

Article 2. Participants

2.1 The ADC consists of Participants

2.2 The Plenary Meeting shall, on the proposal of the Core Team, both as referred to in Article 4, determine the policy for the admission of new Participants. This policy is determined in such a way (i) that the ADC is an open association, (ii) that the ADC is composed in a proper, balanced manner and in line with its objective, and (iii) that there is transparency regarding what is required from companies and institutions as Participants.

2.3 The admission policy referred to in Article 2.2 may be amended by the Plenary Meeting at the proposal of the Core Team.

2.4 The Plenary Meeting shall decide on the admission of a Participant in accordance with the admission policy referred to in Article 2.2.

2.5 <facilitator> shall only enter into a Cooperation Agreement with a new Participant if the Plenary Consultation has decided to do so in accordance with Article 2.4.

2.6 <facilitator> will only exercise a power under a Cooperation Agreement to terminate that Cooperation Agreement (and the cooperation with a Participant) if the Plenary Meeting has decided to do so.

2.7 The Participants existing at the time of the Adoption Date are listed in **Annex I** (forming an integral part of the Cooperation Agreement), together with the date on which they became Participants.

Article 3. Cooperation Agreement

3.1 The Cooperation Agreement shall be a standardized agreement concluded in accordance with a model to be adopted by the Plenary Assembly.

3.2 The Plenary Meeting is authorized to amend the model referred to in Article 3.1. This amendment can only take place in agreement and with the consent of <facilitator>.

3.3 The Plenary Meeting is authorized to decide in individual cases that a Cooperation Agreement is entered into in deviation from the model referred to in Article 3.1. Reasons must be given for such a decision.

Article 4. Organization of the Anti-DDoS Coalition

4.1 The Anti-DDoS Coalition consists of the Plenary Consultation Committee, the Core Team, Working Groups and Project Groups, and the individual Participants.

4.2 The Plenary Consultation is the decision-making body of the Anti-DDoS Coalition ('Plenary Consultation').

4.3 The Plenary Meeting consists of one or more decision-maker representatives of the Participants.

4.4 In the Plenary Consultation, Participants, considering the advice of the Core Team, take decisions on policy, strategy, and the determination and allocation of financial resources.

4.5 The Plenary Meeting shall decide on the accession of new Members upon the advice of the Core Team and subject to the terms and conditions for accession as described in Appendix 4 *(not included in this document)*.

4.6 A decision of the Plenary Meeting on the matters described in Article 2.2 shall be taken by majority vote.

Article 5. The Core Team is the executive committee of the Anti-DDoS Coalition ('Core Team').

5.1 The ADC has a core team (the "Core Team").

5.2 The Core Team is responsible for the organization and operation of the ADC, achieving the ADC's objectives.

5.3 The Core Team should behave according to the directions of the Plenary Consultation.

5.4 The Core Team has a coordinating function towards the Working Groups and Project Groups.

5.5 The Core Team is responsible for overseeing <facilitator>'s management of the ADC's finances, subject to Article 10.2.

5.6 The Core Team monitors compliance with the Cooperation Agreement and the agreements made in the Working Groups and reports to the Plenary Meeting.

5.7 The Core Team advises the Plenary Meeting on the accession of new Participants in accordance with the accession conditions as described in Appendix 4 *(not included in the current document)*.

Article 5. Composition of the Core Team and appointment and dismissal of members of the Core Team

5.1 The Core Team has one chair, one treasurer, one relationship manager, one secretary.

5.2 The Plenary Meeting determines the composition of the Core Team and may add additional members.

5.3 Members of the Core Team are elected for two years by a majority vote of the Plenary Meeting. Parties whose personnel act as members of the Core Team shall ensure that the member in question is available for at least 2 hours a week (unpaid). If a Party whose personnel serve as members of the Core Team terminates the collaboration agreement in accordance with Article 4 of the collaboration agreement, the Plenary Meeting shall appoint a substitute member for the Core Team.

5.4 Only natural persons may be appointed as members of the Core Team.

5.5 Members of the Core Team are appointed by the Plenary Meeting.

5.6 A member of the Core Team may be dismissed at any time by the Plenary Meeting.

5.7 Members of the Core Team shall not be remunerated for their work at the expense of the ADC, except for the Secretary.

Article 6. Division of tasks and decision-making of the Core Team

6.1 The Core Team appoints a chairperson, a treasurer, and a relationship manager from among its members. The secretary is appointed by <facilitator>.

6.2 The Core Team shall meet as often as a member of the Core Team deems appropriate.

6.3 A member of the Core Team may only be represented at the meeting by another member of the Core Team by written proxy. The requirement of a written power of attorney is fulfilled if the power of attorney is recorded electronically.

6.4 Each member of the Core Team shall have one vote. The secretary has no voting rights. All decisions shall be taken by an absolute majority of the votes cast, provided that consensus is always sought. If the votes are tied, the proposal shall be rejected.

6.5 Decision-making of the Core Team may take place outside a meeting, provided that all members of the Core Team have agreed to this method of decision-making and the votes are cast in writing or electronically.

6.6 The Secretary shall keep a record of the decisions taken. The notes are available for inspection by the Participants, either electronically or otherwise.

6.7 The Plenary Meeting may subject decisions of the Core Team to its approval. Such decisions must be clearly defined and communicated to the Core Team in writing. The requirement of written communication is fulfilled if the communication is recorded electronically.

Article 7. Working and Project Groups

7.1 Working and Project Groups are set up by the Plenary Meeting and focus on the performance of tasks defined by the Plenary Meeting for the benefit of the Anti-DDoS Coalition ('Working Groups', 'Project Groups' or 'Working and Project Groups').

7.2 Work and Project Groups are self-managing and operate independently within the limits of agreed budgets and agreements made with the Plenary Meeting.

Article 8. <facilitator>

8.1 <facilitator> provides the secretary to the ADC. The secretary supports the Plenary Consultation, the Core Team, the Working and Project Groups and their chairs.

8.2 <facilitator> manages the finances of the ADC, overseen by the Core Team.

8.3 <facilitator> is not authorized to represent ADC. <facilitator> enters legal acts on behalf of ADC in its own name, on behalf of ADC.

8.4 <facilitator> is authorized to enter legal acts on behalf of the ADC insofar as these are explicitly stated in the adopted annual plan as referred to in Article 17.1 or are approved separately by the Core Team.

8.5 Entering into legal acts for the account of the ADC for which the value exceeds the amount of EUR <amount> and which are not explicitly mentioned in the adopted annual plan as referred to in Article 17.1 requires the approval of the Plenary Meeting.

8.6 Notwithstanding Articles 10.4 and 10.5, <facilitator> is independently authorized to decide on entering legal acts for the account of the ADC insofar as the value thereof, assessed on a case-by-case basis, does not exceed EUR <amount> and the aggregate value of all the legal acts entered into pursuant to this Article 10.6 during a calendar year does not exceed EUR <amount>.

Article 9. Plenary consultations

9.1 The ADC has a general assembly (the "**Plenary Assembly**").

9.2 The Plenary Consultation is responsible for overseeing (i) the execution of the tasks of the Core Team and the Working and Project Groups, (ii) general matters within the ADC.

Article 10. Meetings of the Plenary Assembly

10.1 The Core Team shall convene a meeting of the Plenary Consultation as often as it deems appropriate, or when a meeting of the Plenary Consultation should be held according to these Rules of Procedure.

10.2 At the written request of at least five Participants, the Core Team is obliged to convene a meeting of the Plenary Consultation on a date no more than four weeks after submission of the request.

10.3 Participants will be called to the Plenary Meeting by a member of the Core Team.

10.4 Notice of a Plenary Meeting shall be given by email to the address of each Participant made known by them to the Core Team for this purpose.

10.5 The notice shall state the subjects to be discussed and the place and time of the meeting. Matters not stated in the notice of the meeting may be announced in a supplementary notice.

10.6 Notice of a Plenary Meeting shall be given no later than the seventh day before that of the meeting.

Article 11. Chair, Secretary, minutes, and record of decisions of the Plenary Meeting

11.1 The Plenary Meeting shall appoint a chairperson, a natural person, from the ranks of the Participants.

11.2 The chairman of the Plenary Meeting shall preside over its meetings. However, the chairman of the Plenary Meeting may, even if he is present at the meeting, designate another person to chair in his place. In the absence of the Chair of the Plenary Meeting, without having appointed another to chair the meeting, the members of the Core Team present at the meeting shall appoint one of them to chair the meeting. In the absence of all members of the Core Team, the meeting itself shall appoint its chairman. The secretary of the Core Team shall also act as such at Plenary Meetings. In the absence of the secretary of the Core Team, the chair shall appoint the secretary.

11.2 The secretary of the meeting shall keep minutes of the proceedings at the meeting. Minutes shall be adopted at the next meeting.

11.3 The Secretary shall keep a record of the decisions taken. The notes are available for inspection by the Participants, either electronically or otherwise.

Article 12. Right of assembly and access to Plenary Sessions

12.1 All Participants shall have access to and the right to speak at Plenary Meetings. All Participants are entitled to exercise voting rights. The main contact person of the Participant is initially the voting representative from the Participant. In the absence of the main contact person, the main contact person shall pass on the name of his or her replacement when cancelling the Plenary Meeting.

12.2 All Core Team members have access to Plenary Consultation meetings.

12.3 A Participant may grant a written proxy to another Participant to cast his vote. The requirement of written proxy is fulfilled if the proxy is recorded electronically.

12.4 The chairman of the meeting shall decide on the admission of other persons to the meeting.

Article 13. Voting and decision-making in Plenary deliberations

13.1 At the Plenary Meeting, each Participant shall have one vote.

13.2 All decisions for which no greater majority is prescribed in these Rules of Procedure shall be taken by an absolute majority of the votes cast.

13.3 The chairman shall determine the manner of voting, on the understanding that, if one of the persons present with voting rights so requires, voting on the appointment and dismissal of persons shall take place by closed, unsigned ballot papers.

13.4 If in a vote on the election of persons no one obtains an absolute majority of the votes cast, another free vote shall be taken. If, in that case too, no one obtains an absolute majority of the votes cast, repeat voting shall take place until either one person obtains an absolute majority of the votes cast or a vote is taken between two persons and the votes are tied. In the event of a further ballot, not including a new free ballot, a vote shall always be taken between the persons voted for in the preceding ballot except for the person who received the smallest number of votes in the preceding ballot. If the lowest number of votes have been cast for more than one person in the preceding ballot, lots shall be drawn to decide which of those persons may no longer be voted for in the next ballot. If the votes are equally divided between two persons, lots shall be drawn. However, if the votes are tied in a vote between two persons who have been placed on a list of candidates, the person who appears first on the list of candidates shall be appointed. If the votes are tied in another vote, the proposal shall be rejected.

13.5 Decisions of Participants may be taken outside a meeting, provided that all Participants have agreed to this method of decision-making and the votes are cast in writing or electronically. The votes are considered to have been cast in writing or electronically if the decision stating how each of the Participants voted is recorded in writing or electronically.

Article 14. Annual plan, Annual report, and quarterly reports

14.1 By [November 1], the Core Team shall prepare the annual plan with associated budget for the following calendar year (the "**Annual Plan**").

14.2 The Annual Plan shall be adopted by the Plenary Meeting, at a meeting held for that purpose within [one] month of its establishment.

14.3 Each member of the Core Team and the Chairs of the Working and Project Groups shall prepare a quarterly report on their work within [four] weeks of each calendar quarter.

14.4 The form and content of the quarterly reports as referred to in Article 17.3 shall be determined by the Plenary Meeting.

14.5 Within [three] months after the end of a calendar year, the Core Team shall prepare an annual report on the affairs of the ADC and the progress of its work, including the balance sheet and statement of income and expenditure with explanatory notes (the "**Annual Report**").

14.6 The Annual Report shall be adopted by the Plenary at a meeting held for that purpose within [one] month after the Annual Report has been prepared.

14.7 The Annual Plan, the quarterly reports referred to in Article 17.3 and the Annual Report are made available to the Participants, either electronically or otherwise, within one week of their preparation.

14.8 The adopted Annual Plan and Annual Report are available for inspection by the Participants, either electronically or otherwise.

Article 15. Secrecy

15.1 Each Participant, each member of a body of the ADC, and any other person involved with the ADC by or under these Bylaws is required to exercise due discretion, and, where confidential information is involved, confidentiality, with respect to all information and documentation obtained during his position or involvement, except to the extent the person is compelled to disclose by law or regulation.

15.2 For the application of Article 18.1 - without prejudice to the general application of Article 18.1 - these Regulations, the Collaboration Agreements, the Annual Plans, the quarterly reports referred to in Article 17.5 and the Annual Report are confidential documentation.

Article 16. Residual competence

The Plenary Consultation shall have all powers not assigned in these Rules to other bodies of the ADC.

Article 17. Amendment

17.1 The Plenary Meeting may amend these Rules of Procedure by decision.

17.2 The Plenary Meeting may, in exceptional cases, declare a provision of these Rules of Procedure to be inapplicable. Reasons shall be given for such a decision.

Article 18. Applicable law and competent court

18.1 These Regulations and their interpretation are governed by Dutch law.

18.2 Disputes arising in connection with these Regulations, including disputes about the existence and validity thereof, shall be settled by the competent court in The Hague.

14.4 Appendix 4: Dutch ADC membership agreement (translated)

Disclaimer: this appendix is translated from Dutch. It is of no legal significance in this document and is solely included as informational resource. In its daily operations, the Dutch anti-DDoS coalition is supported by a facilitating organization (anonymized with <facilitator> in the following document).

MEMBERSHIP AGREEMENT BETWEEN [PARTICIPANT] AND ANTI-DDOS COALITION represented by <facilitator>

Undersigned:

[PARTICIPANT] hereinafter referred to as "......", with its registered office at ...... and having offices at the ...... in ...... , legally represented by Mr/Mrs [NAME], [FUNCTION]
and
<facilitator>, hereinafter referred to as "<facilitator>", having its registered office and principal place of business in <address>, legally represented by <contact>
Individually referred to as "Party" and collectively referred to as "Parties".

Taking into account that Parties wish to record that:

- [PARTICIPANT] [PARTICIPANT GENERAL DESCRIPTION].

- <Facilitator general description>.

- <facilitator> for the construction and support of the Anti-DDoS Coalition [hereinafter: "ADC"] has offered to run the secretariat.

- [PARTICIPANT] has indicated that he wants to actively participate in ADC and that he also wants to make a financial and/or in-kind contribution to this.

- The parties have made further agreements about this, which they wish to record in this agreement.

- <facilitator> has concluded this agreement on an individual level with various participants. The Participants (hereinafter referred to as "Participants") are appointed to the list of Participants set forth in Annex 1 to this Agreement.

- The Anti-DDoS Coalition is a neutral non-profit platform that focuses on combating, preventing, remedying and analyzing DDoS attacks in order to increase Dutch and European autonomy and increase resilience to DDoS attacks. ('Anti-DDoS Coalition').

- Parties to this Agreement wish to establish the mutual rights and obligations that apply within the cooperation as individual Parties ("Cooperation Agreement").

- The Annexes to this Agreement shall form an integral part of this Cooperation Agreement.

- The parties to this Cooperation Agreement wish to clarify the manner of cooperation, including decision-making.

- Capitalized terms have assigned the meaning to these terms in this Cooperation Agreement.

Agree as follows:

1. PARTICIPATION ANTI-DDOS COALITION

1.1 All Participants have equal rights and obligations. A Party becomes a Participant of the Anti-DDoS Coalition after signing this agreement and performing obligations in article 1.3. Upon signing, the new Participant agrees to what is stipulated in this Cooperation Agreement and all Annexes attached thereto.

1.2 Participants are expected to actively participate in the cooperation. Each Participant shall submit at least one candidate to one or more working groups and shall have a representative authorized representative in the Plenary Consultation. Participation in a Working Group takes place in consultation with the Core Team and the relevant Working Group. Participants will give each other the support that can reasonably be required of them for the cooperation in the Anti-DDoS Coalition.

1.3 Participants are obliged to:

a) Payment of the annual financial contribution determined in the Plenary Consultation in accordance with agreements in the Regulations (Annex 2) for the Anti-DDoS Coalition. Payment shall be made within thirty (30) days of receipt of an invoice drawn up for this purpose. <facilitator> is entitled to send the relevant invoice after signing this agreement. Or

b) Making the contribution as agreed with the Plenary Consultation in accordance with what is stipulated in the 'Conditions exception satisfaction financial obligation of Participants as included in Appendix 5.

1.4 Without prejudice to the provisions regarding confidentiality [Article 7] and personal data [Article 8], each Party is obliged to all information that is important for cooperation in the Anti-DDoS Coalition for the proper execution of this Cooperation Agreement, or of which it can reasonably suspect that this information for the Anti-DDoS -Coalition is or may be important to provide directly to the other Parties in the Anti-DDoS Coalition.

2. OBLIGATIONS OF <facilitator>

Setting up and maintaining processes:

- Coalition and office support activities: <facilitator>, in collaboration with the Core Team of the ADC, will carry out secretarial and coalition support work for the Plenary consultation, the Core Team, the work and project groups and its chairmen.

- Reporting and accountability: <facilitator>, with the core team and in collaboration with the work and project groups, will report to the Plenary consultation and account for what has been agreed in the plenary consultation.

- Contractual agreements: <facilitator> will make agreements within the limits of the annual budget about, for example, the hiring of products and services in accordance with the Regulations (Appendix 3).

- Budget accountability and invoicing: From the facilitating role, <facilitator> is responsible for the budget towards the Plenary consultation and carries out the invoicing towards the Shareholders on behalf of the coalition.

- <facilitator> carries out these obligations within the framework of the annual budget and in accordance with the agreed governance as elaborated in the ADC Governance Regulations and in accordance with its mandate from the Governance Regulations (Appendix 3).

3. MUTUAL RIGHTS AND OBLIGATIONS – COOPERATION

1. The parties shall refrain from conduct and/or actions as a result of which the good name of the other party and the parties involved in the construction and support of ADC (as referred to in Appendix 1) can be discredited.

2. Na termination of this agreement, for whatever reason, Parties will no longer be permitted to exercise rights that anyone can derive from this agreement in any way.

4. DURATION AND TERMINATION

4.1 This Cooperation Agreement is entered into at the time of signature for the remaining period of the relevant calendar year. Payment or delivery of the contribution required under Article 1.3.a will be settled to rato over the remaining period.

4.2 Participation in the Anti-DDoS Coalition by individual Parties will be tacitly renewed after the end of the relevant calendar year, unless the Party has terminated the Membership in writing to the Core Team 3 months prior to the expiry of the Cooperation Agreement.

4.3 Each Party may terminate the Cooperation Agreement prematurely by written notification (also by e-mail) to the Core Team with due observance of a notice period of 1 month. Termination does not release the Party concerned from the already promised or paid financial contribution as referred to in Article 1.3(a) (no right to a refund).

4.4 The Core Team may terminate theappointment of a Party in writing if the Party concerned fails to fulfil its obligations under this Cooperation Agreement. The Core Team will inform the Party concerned in writing of an intention to terminate, after which the Party in question has 30 days to still fulfil its obligation, unless compliance is no longer possible. In addition, the <facilitator> and/or the participant may terminate the agreement with immediate effect in the following cases:

- the other party is declared bankrupt or has applied for suspension of payment.
- the other party is dissolved or liquidated.
- the other party performs or fails to perform acts because of which the good name of the other party is seriously discredited, unless these acts or omissions cannot be blamed on the other party.

4.5 The parties are entitled to suspend the agreement or agreements affiliated with it in the context of ADC, without further notice of default, to suspend it in whole or in part with immediate effect or to dissolve it in writing, without being obliged to pay any compensation, if there is a question of the independence of the other party being at stake. in the event of continuation of this agreement or related agreements, unless the relevant Party(ies) are able to take measures within a reasonable period of time in such a way that the independence of the other party can be guaranteed, all this as far as possible within the laws and regulations and / or (internal) independence rules.

4.6 Parties are obliged to inform the other party without delay of changes because of which Parties no longer comply with the provisions of the Preconditions for the accession of new participants.

5. **LIABILITY**

5.1 In principle, each party bears its own liability. Third parties must turn to the legally liable party with any claims and claims. Any claims by third parties that are addressed to <facilitator> and that are related to the execution of this agreement and the accompanying annexes, will – if these claims lead to legally established liability – be borne by all participants involved in the agreement with regard to the financial consequences, unless the harmful act or omission is attributable to <facilitator>.

6. **EXTERNAL COMMUNICATION**

6.1 Unless there is a situation as included in Article 6.2 of this agreement, the Parties will not mention each other in external (advertising) communications without the prior written consent of the Party concerned.

6.2 With this agreement, the parties grant each other the right to use the name and logo of the other Party, insofar as it concerns activities and resulting publications about ADC. In doing so, Parties must always observe the conditions as set by the other Party for the use of the name and logo, and the name and logo will only be used for the purpose of this agreement.

6.3 After termination of this agreement for whatever reason, Parties are no longer permitted to use the name and logo of the other Party.

7. **SECRECY**

7.1 Confidential Information means any information of a Party or a third party that reasonably qualifies as confidential (Confidential Information).

7.2 A Party shall: (i) use the Confidential Information of another Party only for the purpose for which it was provided; (ii) not making available to third parties; and iii) only to persons who need the Confidential Information to carry out (activities arising from) this Cooperation Agreement.

7.3 The limitations in Article 7.2 do not apply: (i) to information that has become public without breach of a confidentiality obligation; (ii) to information that can be demonstrated that a Party already had access to that information before it was provided by the other Party, unless that information was prepared by the first Party for the benefit of the other Party; (iii) to information that can be demonstrated to have been independently developed; or (iv) to Confidential Information the disclosure of which is permitted under Section 7.4.

7.4 A Party may disclose Confidential Information of the other Party pursuant to a court order or instruction from a competent regulator if: (i) measures are in place that protect the reasonable interests of the other Party; (ii) the first Party shall notify the other Party in order to give the other Party the opportunity to act against the order or instruction, unless this is not permitted by that order, instruction or applicable law; and (iii) the first Party informs the court or competent supervisory authority of the confidential nature of the information. A Party may also disclose Confidential Information of the other Party if it has specific rules regarding the disclosure of information and those rules require it to disclose, provided that the Party disclosing the Confidential Information first seeks advice from the other Party.

7.5 The obligations under this Article 7 shall remain in full force and effect at the end of the Cooperation Agreement.

8. **PERSONAL DATA**

8.1 In principle, no personal data will be processed under this Agreement. If personal data are nevertheless processed in the execution of this Agreement (in the future), the Parties involved will draw up further agreements regarding the processing of Personal Data and record them in a separate agreement.

9. **INTELLECTUAL PROPERTY RIGHTS**

9.1 The parties do not transfer any intellectual property rights in the context of this Cooperation Agreement.

9.2 If, in the context of the implementation of this Cooperation Agreement, two or more Parties jointly develop products or services on which Intellectual Property Rights will be based, the Parties will jointly become entitled parties to these Intellectual Property Rights. The parties will not transfer the associated rights to third parties without the consent of the other Party(ies) or exercise their rights jointly in good faith.

9.3 The parties indemnify each other against claims by third parties due to infringement of the intellectual property rights of those third parties.

10. **BACK-TO-BACK**

<facilitator> concludes this cooperation agreement with all ADC participants and will impose the rights and obligations arising from this agreement on all participants and other parties involved in the construction and support of ADC. <facilitator> is responsible for organizing the cooperation within ADC and in that role will oblige all parties involved to comply with the rights and obligations included in this agreement.

11. **OTHER PROVISIONS**

11.1 No general or specific conditions or stipulations of one of the Parties apply to this Cooperation Agreement.

11.2 The Amendment to this Cooperation Agreement (Annex 2) is an integral part of this Cooperation Agreement. In the event of any conflict between the provisions of the Agreement and the Cooperation Agreement, the provisions of the Cooperation Agreement shall prevail.

11.3 Termination or dissolution of the Cooperation Agreement does not release the Parties from the provisions with regard to confidentiality and liability.

11.4 Deviations from this Cooperation Agreement due to individual or bilateral agreements between the Parties are not possible. Changes to this Cooperation Agreement are only possible with the unanimous consent of the Plenary Consultation and by means of a written record, in accordance with the provisions of Article 17 of the Rules of Procedure.

11.5 All amounts referred to in this agreement are exclusive of VAT.

11.6 This agreement is governed by Dutch law. Disputes arising from or related to this agreement will be submitted for resolution to the competent court in The Hague.

Thus agreed and drawn up in duplicate

at [PLACE]

on [DATE]

<facilitator> [PARTICIPANT]

…………………………………………………………

14.5 Appendix 5: DDoS drill waiver (Translated)

Disclaimer: this appendix is translated from Dutch. It holds no legal significance and is solely included as informational template. The document was signed between two coalition members (anonymized with <XXX> and <YYY> respectively). Sensitive information has been anonymized or removed.

Subject: Consent to the execution of a simulated (Distributed) Denial of Service attack
(hereinafter (D)DoS) by <XXX>.

Date: <date>

Subject: (D)DoS attacking the infrastructure of <XXX> via the infrastructure of <YYY>

<XXX>

and

<YYY>
both separately and jointly:
"Party" or "Parties"

considering that:

- there is a signed agreement between <YYY> and <XXX> (ON2013) (hereinafter: the Agreement)
- it has been agreed in the Agreement that it is permitted that <XXX> (D)DoS perform tests (or have them performed) on certain internet-related services of <XXX>, being web services, application(s) and/or IT infrastructure(s) that may be owned/used by <YYY>.
- the Agreement states that <YYY> will cooperate with this
- in addition to the Agreement, the Parties agree to this indemnification Agreement as it is necessary for the performance of this (D)DoS test for <XXX> to:
    - test for; or
    - certain parts of certain web services, application(s) and/or IT infrastructure(s) of <XXX> that may be owned and/or used by <YYY>

agree as follows:

1. The (D)DoS test is performed by <XXX>and in close consultation with <YYY>, on <date> <time>.

2. The <YYY> contact person, the <position>, must be informed in writing by the contact person of <XXX>informed at least 48 hours prior to this date about final scope, final target systems and other relevant information (insofar as it may deviate from what has been agreed in this document).

3. In the event of unforeseen circumstances, all parties involved in the (D)DoS, including <XXX> and <YYY>, reserve the right to stop the execution of the planned test, and therefore this permission, by means of a notification to the Tax Authorities. If reasonably possible, the Parties will consult on this before definitive discontinuation.

   <XXX> contact person must provide contact details so that, at the request of <YYY>, the present test work can be stopped without delay. In this case, the parties can enter joint consultation about other dates/times.

4. The tests shall be conducted on or from an appropriate subnet as set out in Section 10 of this Safeguard Agreement. Any changes to this must be made known to the other Party at least 48 hours prior to the

execution of the (D)DoS test.

5. by signing this indemnification agreement, <YYY> expressly authorizes <XXX> and any third parties engaged by <XXX> for the performance of a (D)DoS test as described in this indemnification agreement or otherwise agreed in response to this indemnification agreement. Other previously agreed (contractual) agreements between
<YYY> and <XXX> explicitly do not apply to the execution of the (D)DoS test as described in this indemnification agreement. This consent is valid after signing this indemnification agreement for the dates/time referred to in Article 1, unless the Parties jointly agree on other dates/times as a result of and in accordance with Article 1 and/or Article 3.

6. The possible (D)DoS scenarios that will be executed are limited to attacks related to the primary targets:

FQDN	IPv4 address	IPv6 address
example.nl	...	...

Excluded are:

- Attacks / exploitation of (known) vulnerabilities that are known in advance to make the aforementioned services offered unreachable and / or can have such an impact on the infrastructure of <YYY>, this at the discretion of <YYY>
- During the test period to create (D)DoS volume attack may from the participants, who use the anti-DDoS service from the ON2013 contract, collectively at no time more than <?>Gbps amounts where the following condition applies:
  1. Only one <?>Gbps attack for 1 participant is allowed at a time.
  2. Anticipating the attack of <?>Gbps or higher with a maximum of <?>Gbps, the first 5 minutes should be started with a volume of max <?> Gbps (for <?>Gbps/<?>Mpps switch to NaWas).
  3. It must also first be verified that the NaWas mitigation is enabled and only then may a maximum of <?>Gbps attack capacity be sent.
  4. When the attack has stopped (and runs/ran through NaWas), the mitigation of Nawas must then be terminated by <YYY>.
  5. Participant must not disable the BGP peers towards <YYY> when NaWas is enabled.
  6. It is required for <XXX> that the NaWas test of <date> runs correctly due to the higher attack capacity (max <?>Gbps).
  7. For the participant <ZZZ> a maximum of an attack volume of <?> Gbps may be applied (this customer does not yet use NaWas).

- The following bandwidths are allowed:
  - Between <time> the participants who use the anti-DDoS services from the ON2013 contract may not jointly exceed <?>Gbps at any time with due observance of the above conditions.
  - Between <time> hours, the participants who use the anti-DDoS services from the ON2013 contract may not work together at any time

7. Any changes to the above attack patterns will be clearly described in the final plan of attack and in the (draft) report, of which <YYY> will receive a copy upon request. Social engineering is not part of the research without the explicit permission of
<YYY>.

8. <XXX> hereby declares that they (and parties acting on its behalf) will exercise restraint and professionalism in the execution of the (D)DoS test, in such a way that no intentional/reasonably foreseeable damage will be caused to <YYY> systems and/or components that are part of the <YYY> services and/or data thereon from <YYY> and/or its customers. In the event of a possible discussion about the level of professionalism exercised, <YYY> will assess the level of professionalism whether or not on the basis of a third party to be hired by <YYY>

9. <XXX> is liable for damage suffered by <YYY> arising from the aforementioned (D)DoS test to the (production) environment of <YYY>, insofar as that damage results from (I) an attributable shortcoming in

the execution of the obligations under the underlying indemnification letter (see also article 8 regarding degree of professionalism), and /or (II) unlawful act. This only applies during the agreed test period (see also article 1), unless the damage reveals itself later.

10. The locally present <YYY> contact person and/or the <YYY> NMC (tel.<tel>) present locally (during the test) will be informed as soon as possible if serious security risks have been discovered, continuity has demonstrably been disrupted and/or access to information has been obtained.

    The (D)DoS attack will be carried out from systems with the following IP addresses or subnet:

Network provider	ASH	subnet
Name	AS numbers	IP ranges

11. <YYY> reserves the right to adjust the scope and/or underlying route and/or to change it during the execution of the (test) work. If reasonably possible, <YYY> will do this in consultation with the tax authorities.

12. During test work, the <YYY> ICT infrastructure and/or (custom) applications and/or web services must remain unchanged. Substantial changes in the attack patterns to be carried out and/or nature of attack can only be made in mutual coordination. Deviation by <XXX> to the attack patterns to be carried out, this can lead to additional work and any costs that <YYY> <XXX> may charge.

13. <XXX> will, if possible, make screen prints or other types of evidence for <YYY> to substantiate any findings and /or information if this is mentioned in the (draft) report. The (draft) report to be drawn up provides sufficient insight into the way in which the test was completed, including a digital audit trail.

14. At the request of <YYY> <XXX> will make available a draft report prior to a final report and/or in any case the passages relating to the target systems attributed to it/ belonging to it.

15. All information and data that are exchanged between and exchanged or of which the Parties become aware, including software & infrastructure, preparatory material, and trade secrets, will be treated as confidential by the other Party.

    The parties will make every effort to prevent information regarding incidents from being traceable to one or more party(s) involved in the (D)DoS test.

    The parties undertake not to disclose information and data relating to this simulated (D)DoS attack to third parties without the written consent of the other Party, unless and insofar as they are obliged to do so under any legally binding judicial provision. In the latter case, <YYY> will be informed by <XXX> where possible and vice versa.

16. The parties will explicitly oblige their staff and other persons involved to comply with this obligation of confidentiality.

17. This Agreement is governed by Dutch law.

By signing this agreement, the Participant and <XXX> indicate that they have taken note of the above and that they are committed to it. This agreement must be signed and returned to the tax authorities.

Thus, agreed on <date>, recorded on five pages of text and signed in duplicate.

On behalf of <XXX>	On behalf of <YYY>
______________________________	______________________________
<name> Position <XXX>	<name> Position <YYY>

14.6 Appendix 6: Testbed working arrangements

DDoS Clearing House testbed, working arrangements between SIDN and [PARTNER]

SIDN and [PARTNER] hereby agree to the following:

DDoS Clearing House
The DDoS Clearing House is a system that enables organisations to share measurements of the DDoS attacks they handle in the form of "DDoS fingerprints", which can be used to proactively mitigate the same DDoS attack at another target. The DDoS Clearing House does not replace DDoS mitigation services like scrubbers but is a shared facility that provides an additional layer of security on top of existing solutions.

DDoS Clearing House testbed
The DDoS Clearing House distributed testbed (testbed) is a realistic simulated environment that mimics an actual deployment of the DDoS Clearing House. It enables the participants in the testbed to test the technical components of the Clearing House in a controlled way by sending small volumes of test traffic *to themselves*. This test traffic represents a DDoS attack (but is not one) and enables a "DDoS victim" to create a DDoS fingerprint of the simulated DDoS attack and share it with other collaborators in the testbed. Participants that act as potential victims can use these fingerprints to test to what extent they can proactively mitigate the same DDoS attack if they were to become a victim at a later stage. The test traffic can go up to at most 5MB/s, which by today's standards is a negligible amount of traffic.

The testbed consists of the DDoS Clearing House components, deployed by the testbed participants, and a traffic generator. The traffic generator produces the test traffic through five (5) virtual machines distributed throughout the world (source machines), hosted on a cloud platform. The testbed has an online dashboard through which participants can instruct the source machines to send customised traces of DDoS test traffic. The traffic generator can only send traffic from the source machines to a testbed participant that requested to receive that traffic through the dashboard. Participants cannot use the traffic generator to send traffic to other testbed participants. The traffic generator is managed by SIDN.

Participants can tweak technical details of the test traffic, such as the number of packets per second, protocols, and flags. The traffic generator is limited to sending 1.000 packets per second with no more than 1.000 bytes of content per packet. With five source machines this amounts to a maximum of 5MB/s of traffic being sent to the participant that requested to receive the traffic, which is a volume insufficient to negatively affect any contemporary network.

The testbed will not involve the exchange of PII because the only IP addresses from which data originates are those of the five source machines that the traffic generator uses.

Role of [PARTNER] in the testbed
[PARTNER] will provide an IP address of a "target machine", so it can play the roles of both actual and potential DDoS "victim" in the testbed. By signing these working arrangements, [PARTNER] confirms that the target machine cannot affect any of [PARTNER]'s production services or other essential facilities in any way.

Neither SIDN nor [PARTNER] shall be liable to the other for damages arising out of and/or relating to these working arrangements and/or the associated activities, except for damages resulting from the malicious action or wilful recklessness of SIDN or [PARTNER].

[PARTNER] and SIDN are both partners in Task 3.2 of the CONCORDIA project, where the DDoS clearing House and its testbed have been developed.

Applicable law
These working arrangements are governed exclusively by Dutch law.
Any dispute that may arise concerning these working arrangements or its fulfilment will be referred to the competent court of law in Arnhem, the Netherlands.

Signed:
SIDN

Signature: ___________________

Name: ___________________

Position: ___________________

Date: ___________________

Signed:
[PARTNER]

Signature: ___________________

Name: ___________________

Position: ___________________

Date: __________________

14.7 Appendix 7: Database operator role description

Database operator

The database operator is the participant responsible for managing the DDoS-DB instance for the Dutch Anti-DDoS Coalition. This role description describes the responsibilities and requirements of the database operator.

Responsibilities:

- Keeping the DDoS-DB instance of the coalition available for the participants and solely for the participants.
- Ensure a valid TLS certificate on the domain name.
- Keeping the DDoS-DB instance up to date with the latest version of the stable code on GitHub and implementing any security patches in a timely manner.
- Manage participant user accounts and add or remove accounts as needed.
- Keep data from the DDoS-DB safe and make encrypted backups of it on a weekly basis.
- Securing and monitoring the network in which DDoS-DB is located.
- The DDoS-DB authority is hosted by a Dutch hosting provider who are connected to the Clean Networks Platform and have signed the code of conduct for abuse control.

Requirements:

- A server to run DDoS-DB and the web server (min. 4GB RAM, 100GB storage).
- A technical contact person who is responsible for solving problems regarding the accessibility, safety, and technical operation of the service. Is the point of contact for technical questions.
- An organizational contact person (can be the same as the technical contact person) who is responsible for the purchase and conclusion of new participants and the signing of agreements. Is the point of contact for organizational questions.
- Is a financially healthy party
- Participation in the *clearinghouse* working group.

14.8 Appendix 8: Testbed operator role description

Testbed operator
The testbed operator is the participant responsible for managing the DDoS Testbed. Participants can use the DDoS Testbed to perform DDoS exercises on a smaller scale on their own when they feel it is necessary. As a result, they are not dependent on the large-scale biennial DDoS exercise for small exercises.

The DDoS testbed sends DDoS traffic of your choice from multiple machines at the same time. The traffic can only be sent to the participant requesting the traffic, so not to other participants. As a result, no mutual indemnities are necessary. This role description describes the responsibilities and requirements of the testbed operator.

Responsibilities:

- Keeping the testbed accessible for the affiliated participants and only for these participants. Affiliated participants sign a disclaimer with the testbed operator.
- Ensure a valid TLS certificate on the domain name of the dashboard.
- Keeping the testbed up to date with the latest version of the stable code on GitHub and implementing any security patches in a timely manner.
- Add new participants after signing the agreement. From application to access must take up to a week.
- Remove former participants from the platform when the agreement expires.

Requirements:

- A server running the testbed dashboard.
- Multiple servers that function as "attack nodes" where the DDoS traffic comes from. These machines are under our own management. The maximum bandwidth of the machines is fixed in advance in the safeguard. Participants can always choose to send less traffic to themselves. The testbed may send *a maximum of* 10Gb/s traffic to the target.
- DDoS traffic must be stoppable at all times at the touch of a button.
- A technical contact person who is responsible for solving problems regarding the accessibility, safety, and technical operation of the service. Is the point of contact for technical questions.
- An organizational contact person (can be the same as the technical contact person) who is responsible for the purchase and conclusion of new participants and the signing of agreements and indemnities. Is the point of contact for organizational questions.
- Is a financially healthy party
- Participation in the *Practicing* working group.