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

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

***Abstract*—Distributed denial-of-service (DDoS) attacks continue to plague the Internet and are a risk to the availability of critical digital systems that we increasingly depend on in our daily lives, such as financial services and the Internet infrastructure. To curb this problem, we propose the novel concept of an Anti-DDoS Coalition (ADC), which is a group of network operators that collaboratively increase their DDoS-readiness by (1) sharing fingerprints of the DDoS attacks they handle and (2) carrying out DDoS exercises together. The novelty of an ADC is that it combines the technical systems for both of these activities with the legal and governance means to deploy ADCs in practice. This multidisciplinary approach is unlike previous work on collaborative DDoS mitigation that focused on technology development (and largely failed).**

We make three contributions. First, we develop a multi-disciplinary blueprint for ADCs, in terms of their activities (sharing DDoS fingerprints and carrying out DDoS exercises) and supporting legal agreements and governance mechanisms. Second, we design two open-source technical systems for ADCs: a "DDoS Clearing House" for sharing DDoS fingerprints, and a "DDoS-CH Cyber Range" for carrying out small-scale DDoS exercises, both of which extend network operators' existing scrubbing services and other standard anti-DDoS measures. Third, we validate the concept of an ADC in practice with the Netherlands' national Anti-DDoS Coalition (Dutch ADC), a joint effort of 22 network operators from industry, government, and academia that are currently deploying the DDoS-CH and the Cyber Range in production.

***Index Terms*—DDoS clearing house, collaborative DDoS mitigation, DDoS fingerprints, threat intelligence sharing, anti-DDoS coalitions.**

I. Introduction

THE digitalization of societal services eases our daily lives but also introduces new risks and challenges. A common threat in the modern Internet is a so-called Distributed Denial of Service (DDoS) attack [1]. In a DDoS attack, malicious actors send a flood of network traffic toward a victim, disrupting the legitimate traffic and services running on the target system. Such disruptions are particularly crucial when the target is a critical cyber-physical infrastructure, such as energy grids, water management systems, or smart transport systems, which increasingly rely on the Internet for their communications.

Network operators can employ various layers of defense against DDoS attacks, such as DDoS scrubbing services or IP anycast. They can utilize such mitigation solutions on-premises or outsource them to a third-party provider. Outsourcing DDoS mitigation is popular because handling large attacks typically needs abundant resources and infrastructure, as well as specialized expertise. Hybrid solutions also exist where the low-profile attacks are dealt with on-premises and the more powerful ones are handled through a scrubbing service. Upstream network operators, such as Internet exchange points, can also deploy DDoS protection for their customers as they usually have high-capacity resources at their disposal.

Handling DDoS attacks this way has two downsides. First, network operators tackling DDoS attacks themselves must do so with their narrow view of the DDoS landscape and their knowledge of DDoS attacks, which may be difficult to keep current. Second, the outsourcing of DDoS mitigation has led to centralization in DDoS protection services, with currently a handful of large providers, such as Akamai and Cloudflare, dominating the market. This confines knowledge on DDoS attacks and detection and mitigation mechanisms to these companies because they are typically reluctant to share their knowledge for commercial reasons.

An alternative approach is one where network operators *collaboratively* handle DDoS attacks and learn from each other. In such setups, network operators form (cross-sectoral) communities in which they share (meta)data [2] and expertise on DDoS attacks. This allows them to increase the resilience of their networks because they learn of (new types of) DDoS attacks and mitigation procedures more quickly from their peers, which reduces the pressure on their incident response teams along with operational costs. For example, multiple Dutch banks and other organizations in the Netherlands were hit by DDoS attacks with the same characteristics one after the other within a few days in 2018 [3]. If they had been able to handle DDoS attacks collaboratively, they would have been able to share the characteristics of the attack (e.g., what protocols were being used) and subsequent targets could have prepared their networks to mitigate the attack more effectively.

While the concept of collaborative DDoS mitigation has existed for a long time [4], previous work focused solely on the technical aspects of the problem and have not shown a significant uptake. A reason behind this lag is that the legal

and organizational requirements are at least as important as the technical ones but previous initiatives did not consider them in unison.

In this paper, we propose the concept of an Anti-DDoS Coalition (ADC), which *does* collectively consider these three different aspects: technological, legal, and organizational.

The contributions of our work are that:

- We develop a blueprint for network operators to collaboratively fight DDoS attacks by combining technical, legal, and governance constructs.
- We design two open-source technical systems for ADCs: the "DDoS Clearing House", used to share DDoS intelligence between network operators, and a "DDoS-CH Cyber Range" for carrying out small-scale DDoS exercises.
- We validate both in practice in the Dutch ADC, which is an example of a well-established ADC consisting of 22 network operators from industry, government, and academia.

The two technical systems complement network operators' existing DDoS mitigation services and do not replace them, thus providing an extra layer of security intelligence.

This paper provides an *overview* of the tools and the legal and governance structures that are required to move collaborative DDoS mitigation from the drawing board to use in practice. We therefore do not discuss each component (technical, legal, organizational) in depth. The use case we describe in this paper serves as an example of how an ADC can be set up with the blueprints we provide. For a comprehensive account of all (implementation) details, we refer to the DDoS Clearing House (DDoS-CH) Cookbook [5], which we developed under the EU's Horizon-2020 project CONCORDIA.

The remainder of this paper is structured as follows. In Section II we explore the related work on collaborative DDoS mitigation. In Section III we introduce the concept of an ADC and elaborate on their requirements. In Section IV we outline the technical systems that we design for ADCs. We discuss the validation and deployment of our work in Section V. Finally, we draw conclusions in Section VI.

II. Related Work

A fundamental drawback of the existing collaborative architectures is that they only focus on providing a technical solution. Based on our work, we learned that the legal and organizational barriers are at least as important. To the best of our knowledge, we are the first to propose and validate in practice a solution that combines these three perspectives for collaboratively mitigating DDoS attacks. We do this by introducing a technical platform, addressing legal requirements with template agreements, and implementing the platform in an operational environment.

In a recent research, Wagner et al. [6] explore the benefits of detecting and mitigating DDoS attacks based on a coordination among multiple Internet Exchange Points (IXPs). They introduce a central platform called a DDoS Information Exchange Point (DXP) to facilitate collaboration between IXPs as DDoS mitigation entities. Their work is complementary to ours, as it proposes a method to collaboratively detect and mitigate DDoS attacks across IXPs and also proposes a governance framework, though they do not validate it in practice.

The Internet Engineering Task Force (IETF) has developed DDoS Open Threat Signaling (DOTS) [7] architecture, which is a standardization effort to cope with the heterogeneity of the Internet infrastructure. DOTS aims at real-time signaling of DDoS-related telemetry data among various applications, devices, and entities involved in the detection and mitigation of a DDoS attack. At a high level, DOTS works by establishing a signaling channel between a DOTS client (e.g., a network under a DDoS attack) and a DOTS server (a centralized entity managing the mitigation) to deal with the management and coordination of DDoS attack mitigation, as well as a data channel responsible for exchanging DOTS-related configuration and policy information.

Team Cymru's Unwanted Traffic Removal Service (UTRS) [8] and DDoS peering initiated by CenturyLink and AT&T [9] are examples of technically mature BGP-based solutions for collaborative DDoS mitigation. However, they do not address legal agreements or a governance structure and have also not become widely adopted.

Another category of collaborative mitigation techniques signal DDoS-related data in a distributed way, such as through a blockchain and smart contracts [10]. Similarly, DefCOM [11] is a distributed framework that leverages an overlay network to communicate control messages.

A similar paradigm of solutions are those that rely on Software-Defined Networking (SDN) and Network Function Virtualization (NFV), which decouple the data plane from the control plane. Hameed and Khan [12] propose an SDN-based DDoS mitigation scheme that allows SDN controllers in different Autonomous Systems (ASs) to communicate attack information and efficiently filter attack traffic close to its source.

III. Anti-DDoS Coalitions

The goal of our work is to address the limitations of traditional soloistic DDoS mitigation techniques. To accomplish this, we propose the concept of an Anti-DDoS Coalition (ADC): a group of network operators collaborating to proactively increase the resilience of their infrastructures and services against DDoS attacks. We envision three types of activities for members of an ADC (see Fig. 1): Fingerprinting DDoS attacks and sharing these "DDoS fingerprints" through a so-called "DDoS Clearing House" (DDoS-CH), conducting realistic large-scale collaborative DDoS exercises to evaluate the resilience of ADC members against DDoS attacks, and sharing knowledge around DDoS.

In this paper, we focus on sharing DDoS fingerprints and collaborative exercises. We briefly discuss the technical implementation of these activities and elaborate on their legal and organizational requirements.

A. ADC Members

ADCs can be a community of cross-sector network operators (e.g., financial institutions, government agencies, telecommunications providers, ISPs), or sector-specific network operators (e.g., financial institutions across EU Member States).

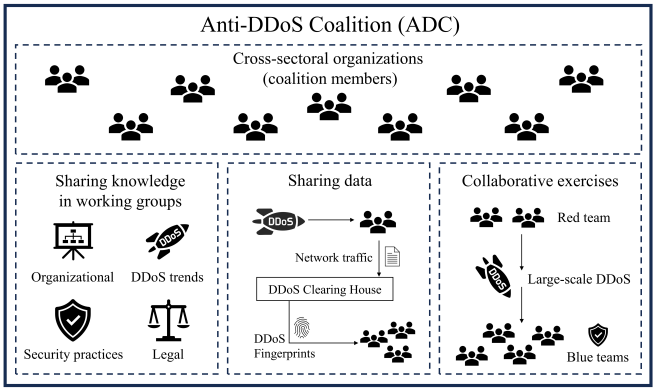

Fig. 1. An anti-DDoS coalition and its activities. Our work focuses on sharing DDoS fingerprints and collaborative exercises.

Additionally, network operators may be a member of several ADCs at the same time (e.g., a cross-sector national ADC and a multi-national sector-specific ADC).

An ADC is also open to network operators who themselves are not directly a target of DDoS attacks. For example, DDoS mitigation providers that are willing to share their knowledge and metadata about the attacks they handle and law enforcement agencies that would like to use the DDoS metadata for digital forensics and investigation of cybercrime. We leave the latter scenario as future work because it will require additional accuracy and integrity measures, such that DDoS fingerprints may be used in court.

B. Sharing DDoS Fingerprints

The network operators in an ADC generate fingerprints of the DDoS attacks targeted at them and share them with other network operators in the ADC. A DDoS fingerprint is a JSON file that summarizes the key features of a DDoS attack such as source IP addresses, source and destination ports, protocols and services, time, and duration of the attack, thus describing the different attack vectors that make up a DDoS attack. Fig. 2 shows an example of a DDoS fingerprint that we generated using the Dissector tool (see Section IV-A1), with traffic from the DDoS-CH Cyber Range (see Section IV-B). Fingerprints help ADC members learn of new (types of) DDoS attacks that have not hit them yet and evaluate whether their deployed defensive measures are suitable to handle these attacks. This allows network operators to widen their perspective on the DDoS landscape, which is important because DDoS attacks are very dynamic and attackers continually change their attack vectors to bypass countermeasures. Also, in the case of sequential DDoS attacks, other ADC members receive an early warning for attacks that might be underway.

Fig. 3 zooms in on the "Sharing data" activity in Fig. 1. It shows the fingerprint information flow in an ADC with three service provider members (SP1, SP2, SP3). In this example, DDoS attack `A` hits SP2, which generates a fingerprint (`FP(A)`), such as the one shown in Fig. 2, and shares it through a DDoS-CH with other network operators in the ADC (SP1 and SP3). Based on the shared fingerprint, SP1 and SP3 can deploy filtering rules (R1 and R3) in their infrastructure


```
{
  "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
}
```


Fig. 2. Example fingerprint of a UDP flood DDoS attack.

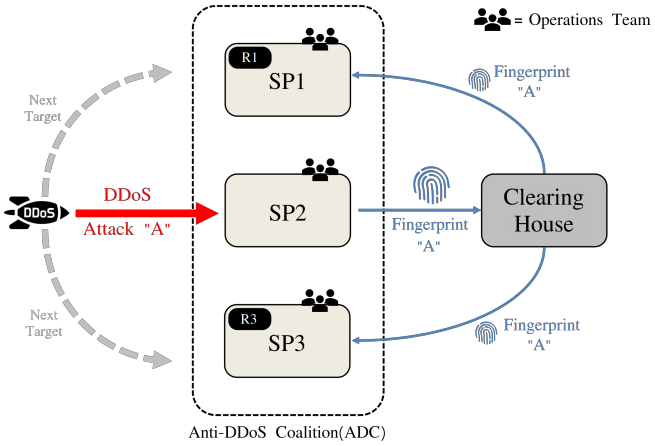

Fig. 3. Anti-DDoS Coalition DDoS fingerprint information flow.

to block similar attack traffic if it targets them later on. Receiving attack fingerprints in advance helps the operations teams of member network operators to make decisions before they are overloaded and under pressure to mitigate the attack. Because the fingerprints contain sensitive information, such as IP addresses, we require data sharing agreements to share

them across organizations (see Section III-D).

C. Collaborative DDoS Exercises

An ADC facilitates large-scale collaborative DDoS exercises, during which its members practice their resilience to DDoS attacks in realistic attack scenarios, such as volumetric attacks (Tbps-levels of traffic), and application-layer attacks.

We distinguish between four roles during the exercises: Red Team, Blue Team, Observer, and Coordinator. These are established common practices for cyber security tests, such as penetration testing internal networks or applications. The Red Team made up of employees of participating network operators, is responsible for coming up with an attack plan and carrying out the attacks at the time of the exercise. Blue Teams are the defending teams of each ADC member – they do not know in advance which attacks will be targeted at them. Besides these two main roles, there is a team of Observers who evaluate the exercises on site. The Red Team and at least one Blue Team representative of each network operator are present in person to facilitate communication. Lastly, every participating ADC member appoints one Coordinator, who oversees the exercise from their network's point of view.

D. Legal Agreements and Governance

An ADC needs several agreements to manage various "assets", such as the fingerprints in the DDoS-CH. Examples are data sharing agreements for sharing DDoS fingerprints through the DDoS-CH, membership rules that network operators need to adhere to (e.g., regarding the confidentiality of data), and agreements to waive liability for potential damage caused in DDoS exercises.

A well-defined governance model outlining responsibilities, powers, and duties is necessary to guarantee the cohesion of an ADC. This includes a governance body that oversees its members' participation, a funding model for the ADC (e.g., member contribution and funds distribution), the process for new network operators to join the ADC, and managing the coalition's assets such as the DDoS-CH.

One of the challenges in cross-operator collaborations is to establish mutual trust. With mutual trust, governance can be based on unanimous decision-making, but this may become ineffective as ADCs grow to dozens of members. As ADCs grow, personal trust among coalition members must shift to impersonal trust in the procedures and governance mechanisms of the coalition [13].

We developed templates for ADC governance and legal agreements, which are publicly available in the appendices 2-8 of the DDoS Clearing House Cookbook [5].

IV. Technical Systems of an ADC

In this section, we provide an overview of the two technical systems that we designed for ADCs: the "DDoS Clearing House", used to share DDoS fingerprints between network operators, and a "DDoS-CH Cyber Range" for carrying out small-scale DDoS exercises. The technical details of both systems are described in the DDoS Clearing House Cookbook [5].

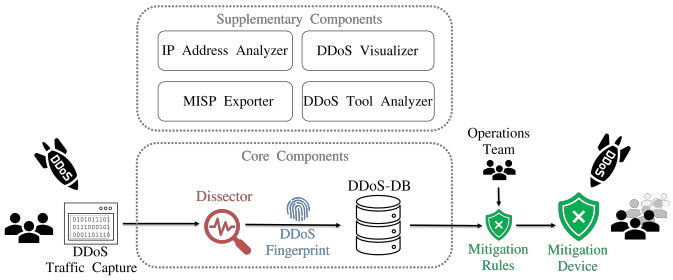

Fig. 4. The DDoS Clearing House schematic overview.

A. DDoS Clearing House

One of the cornerstones of an ADC is a DDoS-CH. This is a platform through which ADC members share fingerprints of DDoS attacks that hit their infrastructure.

Fig. 4 depicts a schematic overview of the DDoS-CH and its components, which covers the "Clearing House" block in Fig. 3. The DDoS-CH consists of two core components: the Dissector and the DDoS DataBase (DDoS-DB). It also comes with four supplementary components, meant to enrich the services of the DDoS-CH. For brevity, we only discuss the Dissector and DDoS-DB in this paper and refer to the DDoS Clearing House Cookbook [5] for a discussion on the supplementary components. We designed the DDoS-CH in such a way that ADCs can choose which components they want to use and which they want to leave out of their setup. We publish the open-source code of DDoS-CH components on GitHub [14].

The focus of our work is to enable the use of our technical systems in any operational environment. In the development of the techincal systems we considered the interoperability of components and their building blocks and valued their open-source availability. Concretely, the technical novelty is its generic, modular, and customizable implementation, making it usable by many ADCs, each imposing different policies, and by many network operators, each running different network implementations.

1) Dissector: The Dissector generates DDoS fingerprints (see Fig. 2) by inspecting samples of DDoS network traffic. The Dissector can work with packet captures or network flows (e.g., NetFlow, IPFIX) to facilitate deployment in different network setups. The Dissector looks for outliers in the traffic traces by inspecting various features such as source port and network protocol, and summarizes them in distinct attack vectors. DDoS fingerprints can be uploaded to an instance of DDoS-DB and/or MISP, to simplify use by network operators already using MISP.

To comply with the policy defined by the governance of an ADC, operators may choose to anonymize the target of the attack.

2) DDoS-DB: DDoS-DB is the repository that stores DDoS fingerprints. We designed DDoS-DB so that it can be run in a centralized or decentralized setup, depending on an ADC's requirements. For example, each network operator in an ADC can run their own instance of DDoS-DB with one central

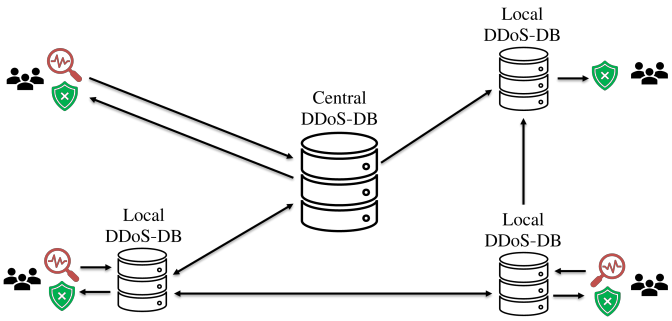

Fig. 5. An example of a hybrid deployment of DDoS-DB.

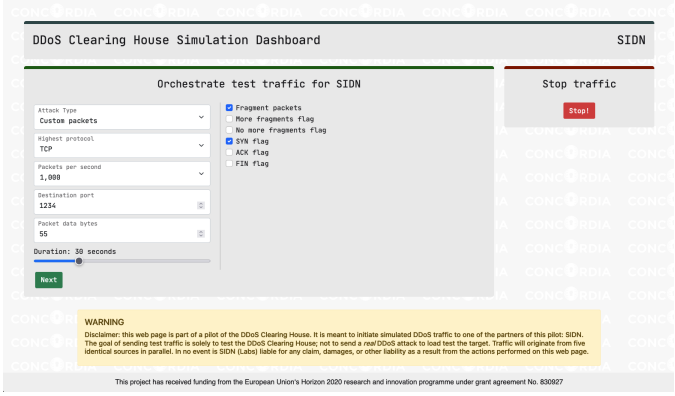

Fig. 6. DDoS-CH Cyber Range dashboard.

coalition instance for sharing. Instances of DDoS-DB can synchronize with each other to exchange fingerprints.

An ADC may also opt for a fully decentralized deployment model in which each member hosts their own instance of DDoS-DB that shares fingerprints with other DDoS-DB instances at other network operators in a peer-to-peer way. Fig. 5 visualizes an example hybrid topology and zooms in on the "DDoS-DB" component in Fig. 4. In the example, some network operators exchange fingerprints peer-to-peer, while others synchronize with a central DDoS-DB instance. Each network operator is in charge of their own data, and they choose exactly what information they (do not) share with the rest of the coalition. This lowers the bar to deployment in production.

We implemented DDoS-DB using a MongoDB database and a Django web application. In the web application, users can browse and search for fingerprints based on attack characteristics. An authenticated API enables network operators to upload fingerprints from the Dissector to DDoS-DB and synchronize it with other instances of DDoS-DB or MISP.

B. DDoS-CH Cyber Range

Cyber ranges are platforms that simulate cyber threats in a realistic and controlled way to train cyber security professionals. The DDoS-CH Cyber range enables network operators to run smaller-scale DDoS exercises at their own convenience, next to the cross-operator large-scale exercises organized by an ADC (see Section III-C). The Cyber Range is a web-based dashboard through which users can customize their attack traffic (e.g., by choosing from a number of well-known predefined DDoS traffic patterns) and launch these attacks from a few Virtual Machines (VMs) distributed across the world on a cloud platform. Fig. 6 shows the DDoS-CH Cyber Range dashboard.

We configured the VMs in such a way that they are limited to sending only up to 2Mbps of Internet traffic. This is enough for users to notice incoming attack traffic and practice its mitigation by generating and sharing the attack fingerprint, but too little to bring down a target network or induce any strain on the networks of upstream providers.

Importantly, participants on the Cyber Range each get their credentials to their own dashboard, from which they can only send DDoS traffic to themselves. This avoids the necessity of waiver agreements between network operators, as are required for large-scale exercises (see Section III-D).

V. Validation with the Dutch ADC

In this section, we elaborate on the validation of the concept of ADCs and the DDoS-CH in practice. The Dutch ADC is a well-established, cross-sectoral, national anti-DDoS coalition. It consists of 22 network operators of critical infrastructure from the Netherlands, including ISPs, IXPs, banks, and government bodies. We also ran a pilot with the DDoS-CH in a smaller ADC in Italy, for which we refer to the DDoS Clearing House Cookbook [5].

A. Clearing House Deployment

We validated the DDoS-CH in a pilot with six members of the Dutch ADC: NBIP (a Dutch non-for-profit scrubbing service provider), SIDN (the operator of .nl top-level domain), KPN (large ISP in the Netherlands), the University of Twente, the National Payments Association, and the Dutch Tax and Customs Administration. Together they form a representative delegation of the entire coalition, with members from academia, industry, and government.

The goal of the pilot was to: (1) enable us to further improve the technical system, and (2) show the members of the Dutch ADC the maturity of the platform and the viability of sharing DDoS fingerprints using it.

During a period of three months, NBIP created 269 DDoS fingerprints from real DDoS attacks they handled with their scrubbing service. They shared these fingerprints with the other pilot participants through DDoS-DB, who could then use the information to obtain a better view of the DDoS landscape. We also used the fingerprints extensively in this period to further develop the Dissector.

The DDoS-CH is currently being deployed as a production-level service for the members in the Dutch ADC, hosted and managed by NBIP.

B. Joint DDoS Exercises

The Dutch ADC hosts large DDoS exercises twice a year, coordinated by the Dutch Tax and Customs Administration.

The motto for the exercises is "test your anti-DDoS measures before others do it for you".

To prepare network operators in the Dutch ADC for real DDoS attacks, the exercises aim to reproduce real DDoS attacks as accurately as possible. The Red Team (see Section III-C) therefore constructs custom relevant DDoS attacks for each participating network operator, targeting particular services, websites, and networks they host. The Red Team sends large traffic volumes of hundreds of Gbps to participating members. More often than not, at least one participant experiences real downtime as a result. Thus, to limit the impact on users, the exercises are carried out at night on the weekend. Providers of large network infrastructure capable of sending out such large volumes of traffic volunteer their services to act as a DDoS source to enable the exercises for the coalition. Examples are SURF, the operator of the Dutch national research and education network, and Nikhef, the National Institute for Subatomic Physics.

After an exercise, participating network operators discuss results and improve their DDoS resilience measures to be better prepared for real attacks. For example, the Dutch Tax and Customs Administration has lately been targeted with DNS PRSD (Pseudo Random Sub Domain) DDoS attacks, which they could mitigate effectively because they had practiced this in one of the exercises. Furthermore, during exercises, they found design flaws in their perimeter which they could address before they were exploited by malicious actors.

More details about the setup and execution of the exercises are available in our presentation at Black Hat Europe [15].

C. Legal & ADC Governance

The NL-ADC co-developed and used the templates for the legal agreements outlined in Section III-D. For example, they used the waiver agreement template for their collaborative DDoS exercises.

The Dutch ADC is governed by a so-called "core team" with an elected chair and two other representatives of participating network operators, who are elected by the ADC's members. The Dutch ADC contracted a support organization (ECP) to act as a legal anchor point and to oversee the various legal agreements required for the functioning of the coalition (see Section III-D).

The Dutch ADC has quarterly plenary meetings in which representatives of all coalition members gather. During plenary meetings, the coalition shares experiences and makes organizational decisions by voting, for example on the admittance of new members or changes in managerial positions.

The detailed work takes place in five working groups, including "Legal Affairs" (supports the other working groups with legal advice and requirements), "Clearing House" (governs the further development and deployment of the DDoS-CH in the Dutch ADC), and "Exercises" (prepares and runs the bi-yearly large-scale DDoS exercises and manages the DDoS-CH Cyber Range). Each of the working groups meets on a monthly basis to discuss any updates relevant to their task and report to the entire coalition during the plenary meetings.

The governance of the NL-ADC is expressed in internal policy and requirements, which are implemented through the relevant working groups in the technical systems. For example, the NL-ADC chose the centralized deployment model, which is realized by the Clearing House working group by hosting a central DDoS-DB instance.

VI. Recommendations & Future Work

We proposed the novel concept of an Anti-DDoS Coalition (ADC), which enables groups of network operators to collaboratively and proactively combat DDoS attacks and form an additional layer of security on top of existing mitigation facilities such as scrubbing services. We discussed the activities ADCs engage in and proposed two technical platforms to support them: the DDoS Clearing House and DDoS-CH Cyber Range. We showed the viability of our approach by validating it with the Dutch national ADC, which involves 22 network operators and has engaged in collaborative DDoS mitigation since 2019. The DDoS-CH is currently being deployed at NBIP as a production-level service for the members of the Dutch ADC.

Based on our work, we formulate four recommendations. The first is that researchers and system designers should consider their technical work on collaborative DDoS mitigation in unison with the design of a suitable governance model and clear and simple (data sharing) agreements. We found this is key for the concept to work in practice, because it is as much a legal and organizational endeavor as it is technical, as exemplified by the Dutch ADC.

Second, we recommend that researchers and system designers work in multidisciplinary teams with experts on DDoS attacks, operational practices, legal matters, and governance constructs. For example, we introduced the legal experts in the Dutch ADC to the types of information the DDoS-CH would exchange. As a result, they delivered a less complex and less conservative data sharing agreement than initially.

Our third recommendation is that researchers develop initiatives for collaborative DDoS mitigation in close interaction with participating network operators to understand the operators' requirements. For example, we found out the members of the Dutch ADC did not want to disclose the IP addresses of DDoS targets in their networks for legal reasons.

Finally, we recommend a new ADC to start with a limited group of network operators and grow from there, for example by starting with a pilot with a few interested parties as we did with the Dutch ADC. This allows ADC members to build up trust and fine-tune the legal agreements and governance model before going to a larger production phase.

Our future work is to finish transferring our knowledge to the Dutch ADC so they can further promote the creation of more ADCs in other communities. At the time of writing, the Dissector is being further matured at Delft University of Technology, and the Dutch Tax Authority is extending the Cyber Range with attack presets specifically made for members of the Dutch ADC. The Dutch ADC also recently set up a new working group to explore the use of fingerprints in criminal investigations.

ACKNOWLEDGMENTS

This work was partially funded by the European Union's Horizon 2020 Research and Innovation programme under project CONCORDIA (grant agreement No 830927), and the GÉANT GN5-1 programme.

We thank our CONCORDIA partners for their contribution: Mattijs Jonker (University of Twente), Paolo De Lutiis and Lorenzo Rizzati (Telecom Italia), Christos Papachristos (FORTH), and Bruno Rodrigues (University of Zürich).

Additionally, we extend our gratitude to the members of the Dutch anti-DDoS coalition for their participation, in particular Octavia de Weerdt (NBIP) and Martijn Peijer (Dutch Tax Administration).

REFERENCES

[1] Cloudflare, "What is a DDoS attack?" https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/, accessed on 15 July 2023.

[2] J. Berkes and A. Wick. (2017) DDoS Defense for a Community of Peers. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=497970. Presentation, FloCon. Accessed on 15 July 2023.

[3] Reuters, "Dutch tax office, banks hit by DDoS cyber attacks," https://www.reuters.com/article/us-netherlands-cyber-idUSKBN1FI1LM, accessed on 15 July 2023.

[4] 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, pp. 2046–2069, 2013.

[5] T. van den Hout, C. Hesselman, R. Poortinga, R. Yazdani, M. Jonker, C. Papachristos, P. De Lutiis, M. Baltatu, and B. Rodrigues, "DDoS Clearing House Cookbook, CONCORDIA Deliverable D3.6," https://ddosclearinghouse.eu/cookbook, 2022, accessed on 15 July 2023.

[6] 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," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 970–987.

[7] A. Mortensen, T. Reddy, and R. Moskowitz, "RFC 8612: DDoS Open Threat Signaling (DOTS) Requirements," https://www.rfc-editor.org/info/rfc8612, May 2019.

[8] Team Cymru, "Unwanted Traffic Removal Service," https://www.team-cymru.com/ddos-mitigation-services, accessed on 18 January 2024.

[9] CenturyLink and AT&T, "Bi-Lateral Security Management Framework (a.k.a. DDoS peering)," https://pc.nanog.org/static/published/meetings/NANOG71/1447/20171003_Levy_Operationalizing_Isp_v2.pdf, accessed on 18 January 2024.

[10] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in *Security of Networks and Services in an All-Connected World: 11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security*. Springer, 2017, p. 16–29.

[11] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A Framework for a Collaborative DDoS Defense," in *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*. IEEE, 2006, pp. 33–42.

[12] S. Hameed and H. A. Khan, "Leveraging SDN for Collaborative DDoS Mitigation," in *2017 International Conference on Networked Systems (NetSys)*, 2017, pp. 1–6.

[13] L. Gommans, J. Vollbrecht, B. Gommans-de Bruijn, 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.

[14] "DDoS Clearing House," https://github.com/ddos-clearing-house, accessed on 15 July 2023.

[15] K. Lovink and M. van Ulden, "How We Organize Large-Scale DDoS Exercises in the Netherlands," https://www.blackhat.com/eu-22/briefings/schedule/index.html#how-we-organize-large-scale-ddos-exercises-in-the-netherlands-28542, 2022, accessed on 15 July 2023.

Ramin Yazdani received his M.Sc. degree in Electrical Engineering from the University of Twente in 2019. He is currently a PhD student at DACS (Design and Analysis of Communication Systems) research group at the University of Twente, the Netherlands. His main research interests are network measurements, DDoS, and DNS.

Thijs van den Hout is a research engineer at SIDN Labs, the R&D department of the .nl ccTLD registry. He has a Master's degree in Artificial Intelligence. His focus is the application of machine learning techniques to increase the safety of the Internet, for example through abuse detection. He chairs the Clearing House working group in the Dutch anti-DDoS coalition.

Remco Poortinga - van Wijnen is team lead Security - Technology at SURF, the cooperative association of Dutch educational and research institutions in the Netherlands and operator of the Dutch National Research and Education Network (NREN). He has a Master's degree in Electronic Engineering (University of Twente 1997). His focus is the application of technology and services in order to improve the cybersecurity resilience of R&E institutions.

Karl Lovink is the Technical Lead of the Security Operations Center (SOC) of the Dutch Tax and Customs Administration. He completed the post-graduate course Judicial Expert at Leiden University, holds several GIAC certificates, and furthered his knowledge in the field of ICT and security through courses such as Splunk, Taranis, and Information Technology Architecture. He chairs the Exercises working group in the Dutch anti-DDoS coalition.

Cristian Hesselman directs SIDN Labs, the research arm of SIDN, the operator of the Netherlands' national top-level, .nl. His research focuses on increasing the trustworthiness of the Internet, for instance, through large-scale infrastructure measurements and the design of secure future networks. He is also a part-time professor at the University of Twente, the Netherlands.