Title: Solving DDoS Attacks in the Netherlands, Europe, and Beyond by facilitating bridging solutions and stakeholders.

Distributed Denial of Service attacks exist since the beginning of the Internet. The goal of these types of attacks is to make target systems (services, devices, or even entire networks) unreachable to its intended users. Over time, these types of attacks increased in frequency and intensity. In 2011, the peak record was reported as 60Gb/s, in 2015 it was 500Gb/s, and in 2016 was 1.1Tb/s. As the dependency of our society to online service also increased, the damage cause by DDoS attacks has become extremely big. While in 2015 large corporations reported the average loss of $US410.000 per attack, in 2017 this figure increased to $US2.5M.

As an old unsolved problem, there is a large volume of academic works on DDoS attacks and hundreds of companies worldwide offering DDoS protection. For example, by the end of February 2019, Google scholar returned more than 47 thousand works on 'ddos attack'. Overall, we, as society, have been addressing DDoS attacks as a reactive approach, waiting for attacks to hit and see whether (i) our anomaly detection/mitigation solution works, (ii) our network operators are skilled enough to mitigate attacks as fast as possible, or (iii) by simply paying more to third-party companies for having more capacity or better protection. The remaining question is "why (we believe) we can solve DDoS attacks?" The answer is simply: by NOT reinventing the wheel, but, instead, facilitating filling the gaps of existing solutions and stakeholders. What we propose is a proactive approach that any stakeholder involved with a DDoS attack would get benefit.

We propose to facilitate: (1) victims, (2) network operators, and (3) network security companies to share their attack measurements and to get in return specific rules for detecting and mitigating those attack; (4) law enforcement agencies to compare attacks suffered in the society for enabling legal attribution and prosecution of attackers (and buyers of attacks); (5) network operators (specially CERT/CSIRT) getting feeds with IP addresses involved in attacks, towards cleaning misused machines from performing attacks; and (6) the academic community on getting real/fresh DDoS attack data for testing and improving their solutions.

All these proposed ideas are already working-in-progress and can be summarized in three elements: (A) a tool, available at https://github.com/ddos-clearing-house/ddos_dissector, for analyzing any type of network trace containing a DDoS attack (for example, pcap, pcapng, neflow, ipfix, sflow, and apache log), filter only the main characteristics of the attack (called 'DDoS fingerprint'), and share only the anonymized version of the filtered attack; (B) a set of tools, available at https://github.com/ddos-clearing-house/ddos_fingerprint_converters, for parsing the generic DDoS fingerprints into specific detection and mitigation technologies (for example, BGP Flowspec, eBPF, IPtables, SNORT, SURICATA, BRO, WAF, and even 'black-boxes' from private security companies); (C) a distributed database, accessible at https://ddosdb.org, for receiving, distributing, and making available ALL information on DDoS attacks (for example, filtered anonymized attack traces, DDoS fingerprints, signatures/rules for detecting/mitigating DDoS, lessons learned from network operators, and feeds for CERT/CSIRT).

The goal of this presentation for the RIPE community is threefold: (1) to give awareness to the community, (2) to collect technical and non-technical feedbacks on how to improve these ideas, and (3) to engage more organizations willingly to collaborate on solving DDoS attacks. Our presentation is divided in four parts: (1) the overall problem and idea, (2) the technical perspective followed by a 3 minutes demonstration, (3) the current deployment, coalition, and governance, and (4) the challenges and future directions, for motivating people to comment/suggest.

**These ideas were originally funded, in 2017, by SIDNfonds (an independent foundation established by the .nl ccTLD), then in 2018, these ideas were embraced by a coalition of 25 Dutch players from industry (ISPs, xSPs,IXPs, banks, not-for-profit DDoS protection providers) and gov't (ministries and agencies), facilitated by Dutch National Cyber Security Centre (NCSC-NL), and, now, in 2019, it got funded by the European Commission in a project involving 46 partners.