

The background of the slide is a photograph of a city skyline, likely London, with several prominent skyscrapers visible in the distance. In the foreground, there are multiple railway tracks with overhead power lines and support structures. The entire image has a blue color overlay.

# Defending Europe against DDoS in a multi-polar world



# Introduction

- Octavia de Weerd  
  - General director NBIP foundation
  - Chairwoman NL anti-DDoS-coalition

# Whois ORG-SN292-RIPE

- org-name: Stichting NBIP - [www.nbip.nl/en](http://www.nbip.nl/en)
- Independent non-profit foundation
- Sector initiative started in 2001
- Collective services for digital infrastructure providers
  - Lawful Interception and Disclosure
  - Clean Networks – [www.cleannetworks.net](http://www.cleannetworks.net)
  - DDoS Scrubbing Center – NaWas
    - Mitigation
    - Reporting
    - Research and collaboration

# Whois ORG-SN292-RIPE

- In 2013 request for anti DDoS solution
- Started POC 2013
- NaWas operational 2014 AMS-IX, NL-ix
- NaWas connected to LINX in 2019
- NaWas currently available in 9 countries in Europe

# NL-Anti-DDoS Coalition

- Cooperation on knowledge sharing about DDoS attacks (2018)
- Universities, IX's, ISP's, banks, government and corporates



[Blog](#) [News](#) [Presentations](#) [FAQ](#)

## News



### New version of the DDoS Clearing House core components

30 September 2020

SIDN Labs and SURF have released a new version of the DDoS Clearing House in a Box, a system that enables network operators to automatically

[Read More »](#)



### DDoS coalition is working together during the current DDoS attacks

4 September 2020

The website reflects coalition's joint efforts over the past two years. In recent weeks, dozens of companies in The Netherlands and Europe have been targeted

[Read More »](#)

# The applications of DDoS

- Weaponization of DDoS from the 00's onward:
  - **Mafiaboy (US, 2000):** Took out Yahoo, CNN, eBay and many others: wakeup call
  - **Spamhaus (NL/Europe, 2003):** Online beef fought with online weapons
  - **SQL Slammer (2003):** Left South Korea without internet and mobile telecoms for many hours
  - **Estonia (2007):** Civil unrest accompanied by major outages in public infrastructure
  - **Dyn, OVHcloud & Krebsonsecurity (2016)** The rise of botnets / darkweb
  - **Attacks on banks and IRS (NL, 2018):** First time critical public infrastructure had widespread fall-out in NL
  - **2022 – now:** DDoS part of hybrid warfare




## Many fear DDoS attack is repercussion for last week's exposé

The Dutch media's obsession with Russia is not accidental. Last week, Dutch newspaper [Volkskrant](#) and TV station [NOS](#) published a report claiming that the country's AIVD intelligence service compromised the computer of a hacker part of Russian-based cyber-espionage group Cozy Bear (also known as APT29).

# 2018: a turning point in The Netherlands



The screenshot shows the SIDN Labs website with a teal header. The article title is 'A proactive and collaborative DDoS mitigation strategy for the Dutch critical infrastructure'. The byline lists: Cristian Hesselman (SIDN Labs), Jeroen van der Ham (University of Twente), Roland van Rijswijk (SURFnet), Jari Santanna (University of Twente), and Aiko Pras (University of Twente). The article text begins with 'Banks and government agencies in the Netherlands repeatedly suffered from outages in the past few months as a result of relatively small DDoS attacks. This is worrisome, because DDoS attacks will only get bigger and more complex, for instance as a result of the emerging "Internet of Things". We therefore argue for a proactive and collaborative DDoS mitigation strategy for the Dutch critical infrastructure, which revolves around providers of critical'.



The screenshot shows the ComputerWeekly.com website. The article title is 'Teenager suspected of crippling Dutch banks with DDoS attacks'. The byline is 'By Tija Hofmans'. The article text begins with 'A large distributed denial of service attack on banks and other organisations in the Netherlands, first thought to emanate from Russia, is now thought to have been launched by a local teenager'. There are two CATO NETWORK advertisements on the page.



# Our servers and devices as pawns on a global chess board

- DDoS is leveraged as low-risk, high-impact asymmetric warfare tool providing plausible deniability
- DDoS campaigns with high impact tend to coincide with international diplomatic tensions, military operations, democratic elections, and critical votes
- Attacks deliberately focus on financial infrastructure, media organizations, government services, and critical utilities to maximize disruption



# Our servers and devices as pawns on a global chess board

- Hacktivist groups serve as convenient fronts for state actors while executing coordinated campaigns
- European reliance on non-European security solutions could pose a strategic risk with protection dependencies as potential geopolitical leverage points

# DDoS attack statistics Q2 2025



2292

Number of attacks



55.5 Gbps

Largest observed attack in  
bits per second this quarter



5.95 Mpps

Largest observed attack in  
packets per second this quarter

## DDoS attacks surge by 88% in March, Spain emerges as top target

Last updated: 7 May 2025

 Ernestas Nagys, Senior Journalist

Image by Cybernews.



## Partner content

**Making Surgery Less Dangerous** ✓

Making Surgery Less Dangerous: Is Automation Really the Answer?

by Partner content by a third party

## Editor's choice



founded in 1614 - top 100 university

[Onderwijs](#) • [Onderzoek](#) • [Maatschappij/bedrijven](#) • [Alumni](#) • [Nieuws](#) • [Over ons](#) •[Over ons](#) • [Actueel](#) • [Nieuws](#)

### The knotty issue of holding countries responsible for cyberattacks

The Record.

RecordedFuture News

[Leadership](#) • [Cybercrime](#) • [Nation-state](#) • [Elections](#) • [Technology](#)

PRESIDENTIAL CANDIDATE GEORGE SIMON LED THE FIRST ROUND OF VOTING ON SUNDAY. IMAGE: ALLIANCE FOR THE UNION OF ROMANIAN VIA WIKIMEDIA COMMONS (CCO)

Daryna Antoniuk

May 5th, 2025

[Elections](#) • [Government](#)[Leadership](#) • [News](#)[News Briefs](#)

### Russian hackers target Romanian state websites on election day

A Russian-linked hacktivist group known as NoName057(6) claimed responsibility for cyberattacks on several Romanian websites over the weekend, as voters headed to the polls to elect a new president.

## PRESS RELEASE

## DDoS Attacks Rising Faster in EMEA than Anywhere Else, According to New Akamai Report

Since 2019, only the EMEA region has experienced a continual rise in DDoS attack events, region even overtaking North America.

United Kingdom - London | June 04, 2024

Cybercrime file image - Credit: [Bendering](#), [www.altpress.de](#), [Christoph Scholz](#), [Flickr](#), [Wikimedia Commons](#) - License: CC-BY-SA[POLITICS](#) • [TECH](#) • [CYBERATTACK](#) • [DDoS ATTACKS](#) • [DDoS](#) • [DUTCH COURT SYSTEM](#) • [MORE TAGS](#)

THURSDAY, 4 MAY 2023 - 18:22

SHARE THIS:  
[f](#) [x](#) [in](#) [g+](#) [v](#)

### Dutch government websites struggling with cyberattacks possibly from Russian hackers

Cyberattacks, potentially originating from Russian hackers, have been causing difficulties for Dutch government websites on Thursday. The Dutch court system's website, Rechtspraak.nl, was grappling with a distributed denial-of-service (DDoS) attack. The website of the Dutch Senate was also difficult to access on Thursday. The attacks coincided with Ukrainian President Volodymyr Zelenskyy's visit to the Netherlands, where he made his first official stop since fleeing Russia.

UPDATE: vineri, 29 aprilie 2022, 09:07

## Val de atacuri cibernetice în România. Vizate mai multe instituții, între care Guvernul și Ministerul Apărării / Atacurile, revendicate de hackerii pro-ruși de la Killnet

Adrian Vasilache • [HotNews.ro](#)[Share](#)

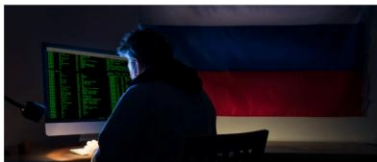
NEWS • CYBERSECURITY AND DATA PROTECTION

### Dutch party websites attacked as EU vote kicks off

The cyberattacks were claimed by a pro-Russian hacker group called HackNet.

## Pro-Russian hackers NoName hit Germany with DDoS Attacks

Last updated: 25 April 2025

 Ernestas Nagys, Senior Journalist

## Partner content

**Making Surgery Less Dangerous** ✓

Making Surgery Less Dangerous: Is Automation Really the Answer?

by Partner content by a third party

© 27 May 2025

So how should we respond?

Probably not like this:

*“the harmless DDoS myth”*

The impact of a DDoS attack is limited and often symbolic. [...] In many cases, the impact of a DDoS attack is limited.”

*-Quote by a government official in response to recent DDoS attacks*

# But is it?

“The impact of a DDoS attack is limited and often symbolic. [...] In many cases, the impact of a DDoS attack is limited.”

*-Quote by a government official in response to recent DDoS attacks*

# What is to be done?

- We should debunk the ‘Harmless DDoS myth’ wherever it matters, instead put DDoS in a broader narrative
- We should reframe DDoS resilience as a collective responsibility instead of an individual responsibility for individual organisations
- We need to work on a pan-European framework for DDoS readiness
- The goal should be to deny the opportunity to disrupt our societies with DDoS



# Building a European DDoS defense network: what you can do

- Use and contribute to tools that are already available, such as the DDoS fingerprint database
- Implement MANRS
- Implement RPKI
- Prioritize abuse detection and mitigation

# What we could start with collectively

- Scale successful models like the NL anti DDoS coalition throughout Europe
- Develop open-source DDoS mitigation tools with European funding and governance
- Create a DDoS resilience framework: individual actions and compliance enhances collective resilience
- Fund academic research specifically targeting next-generation European security solutions



# Thank you

- Questions?
- Want to collaborate or exchange ideas? Contact [bureau@nbip.nl](mailto:bureau@nbip.nl)

