“What to do to improve justified trust in using the Internet and email in the region”

Purpose of the Day
Internet Infrastructure Initiative

- **Aim:** to help build a robust, transparent and resilient internet infrastructure.

- **Rationale:** A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and increases justified trust, as it:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.

- **Offering:** this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.
Setting up Capacity building events

- Targeted at regions that are catching up
- Bringing together regional stakeholders
- Awareness raising on Open Internet Standards
- Inspiration through Good Practice Examples
- Impact through joint commitment for action
Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs
PANEL AGENDA

Intro GFCE Triple-I
Maarten Botterman

Intro: Better Use of Today’s Open Internet Standards
Hisham Ibrahim (RIPE NCC)

Inspiration from Good Practice: joint mitigation of DDOS
Aiko Pras (Professor, Twente University - via video)

Panel discussion: Increasing Trust in the use of Internet and e-mail
Kristina Hakobyan (CEO, Global AM); Yuriy Kargapolov, (Chair, ISOC IoT SIG);
Talant Sultanov (Chair, Internet Society-Kyrgyz Chapter), Bakhrom Nasirjanov
(Megafon Tajikistan)
From State-of-Practice to State-of-the-Art, together

Joint priority setting and action planning
• Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE/ISOC/Kazachstan Telecom, 25 September 2018

• Delhi, India, hosted by Indian Summerschool for Internet Governance, supported by ISOC/APNIC/Indian Govt, 12 October 2018

• Daejeon, Korea, hosted by APRICOT2019, supported by APNIC/ISOC/dotASIA, 23 February 2019
Help make the Internet more reliable in your region

1. Contribute with good practice examples to events
2. Support an event in your region as co-organizer or participant
3. Improve the reliability of Internet by taking action
Triple I is a GFCE project

www.thegfce.com

For more information contact:
maarten@gnksconsult.com
About Maarten Botterman

- More than 25 years experience with work “in the public interest”: where connected technologies touch society - internationally
- Independent analyst, strategic advisor, moderator and chairman, see for more: www.gnksconsult.com
- Currently chairing: IGF Dynamic Coalition on Internet of Things (www.iot-dynamic-coalition.org/); PICASSO Policy Expert Group (www.Picasso-project.eu), and Supervisory Board of NLnet Foundation (www.nlnet.nl.)
- ICANN Board Member (www.icann.org)
- Full CV: https://www.linkedin.com/in/botterman
- Email: maarten@gnksconsult.com
A proactive and collaborative DDoS mitigation strategy for the Dutch critical infrastructure

Cristian Hesselman¹, Jeroen van der Ham², Roland van Rijswijk³, Jair Santanna², Aiko Pras²

¹) SIDN Labs, 2) University of Twente, 3) SURFnet
Aiko Pras

Prof. Internet Security
University of Twente
The Netherlands

https://people.utwente.nl/a.pras
DDoS attacks (on the DNS)


Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)
DDoS trends

• Volume at 1+ Tbps, likely going up (Dyn @ 1.2 Tbps, GitHub @ 1.3 Tbps)

• Many widely distributed DDoS sources (Mirai: 600K, bots all over the world)

• IoT bots mutating and spreading quickly (Mirai: 75-minute doubling time)

• Easier to launch through booters/stressers (Mirai)

• Combination of direct and reflection attacks (Mirai)

• DNS increasingly a high-profile target (DNS root 2015, Dyn 2016)
The Netherlands

- DDoS attacks on Dutch critical infrastructure operators (Jan 2018)

- Estimated 40 Gbps attacks resulted in service outages at several operators

- Reactive and individual DDoS mitigation strategy

- (Commercial) DDoS protection services per critical service provider

- Person-to-person incident response communications during attacks
A proactive and collaborative strategy

• Improve information position of Dutch critical service providers by *continually and automatically* sharing *fingerprints* of actual and potential DDoS sources

• Widens view of critical service providers, enabling them to *proactively* prepare for attacks that have not hit them yet

• Information provisioning layer that *extends* existing DDoS protection services that Dutch critical service providers use and *does not replace them*

• Improve *attribution* of perpetrators and booter operators, allowing for better prosecution and increased deterrent effects

• Onboard *all* critical providers in NL (Internet, financial, energy, water, etc.)
DDoS radar (IoT example)

CSP = Critical Service Provider (e.g., a bank, ISP, or a registry)
DPS = DDoS Protection Service (e.g., Nawas or commercial such as Arbor)
Fingerprint

• Summary of DDoS traffic
  • Domain names used
  • Source IP addresses
  • Protocol
  • Packet length

• Created from traffic capture files like PCAPs

• Victim IP addresses not part of fingerprint

• Challenge: creation at high speed (10s of Gbps)
Status and next steps

• DDoS radar embraced by broad coalition of 25 players from industry (ISPs, xSPs, IXPs, banks, not-for-profit DPS) and gov’t (ministries and agencies)

• Dutch Continuity Board (DCB) acts as springboard, supported by Dutch National Cyber Security Center (NCSC-NL)

• Develop DDoS radar based on existing components, such as
  • DDoS-DB of the University of Twente (ddosdb.org)
  • NaWas’ DDoS pattern recognition system (ddos-patterns.net)

• Working groups: (1) clearing house, (2) cross-industry information sharing, (3) outreach, (4) ground rules and incident response, and (5) exercises
Longer-term

• Pilot part of an EU cybersecurity research project (CONCORDIA) + development of a blueprint “business plan” to sustainably run (national) DDoS radars

• Envisioned growth path: (1) Netherlands → Europe → global and (2) extend to “non-critical” service providers
Q&A