Evaluating future internet technologies

Victor Reijs

SIDN Labs BYOL | Arnhem | 15 July 2019

Outline

- Aim of this BYOL…
- Scoping for today…
- IPv4/IPv6: Internet Protocol…
- Families of network technologies…
- Evaluating network technologies…
- Use cases/demonstrators…
- Brainstorm…

Aim of this BYOL

Aim of the BYOL

- Have your lunch
- Find out if we need to change the present Internet:
  - Examples, use cases, solutions, demonstrators
  - Brainstorm with you

Scoping for today

Scoping today

- Concentrate on inter-network and upto and including the network layer
  - Not looking at: software vulnerabilities of end hosts or malicious Internet content
- Multi-domain, governance, trust and deployment aspects are important from the start
- Focus on realistic/practical use cases and demonstrators
- Evaluate existing technologies using open source code and active communities with testbeds. Supported by IETF/IRTF and/or other standard/recommendation bodies
- Hands-on using an experiential approach: interconnected 2STiC testbed
- Key words: Security, stability and transparency…

Faithful transparency

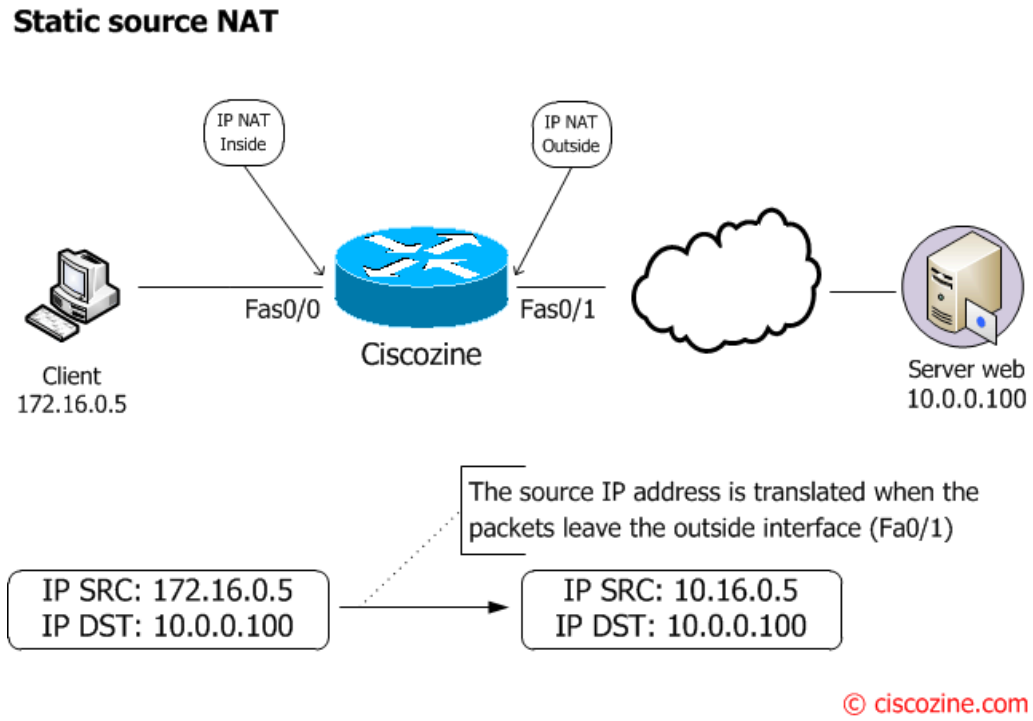
- User:
  - to provide a sense what the system is doing and why
  - to understand why one particular prediction or decision was reached
  - to feel comfortable with a prediction or decision so that they keep using the system
  - to lead into some action or behaviour
- Provider (network or service):
  - to understand how their system is working, aiming to debug or improve it
  - to facilitate monitoring and testing for safety standards
- Society:
  - to understand and become comfortable with the strengths and limitations of the system
  - to audit a prediction or decision trail, particularly if something goes wrong

SIDN LABS

IPv4/IPv6: Internet Protocol

IPV4/IPv6: Internet Protocol

- Established
- Using feature set of IPv4/IPv6 as a reference/base-line



Source: https://www.ciscozine.com/nat-and-pat-a-complete-explanation/

Lessons learnt from 40 years of networking

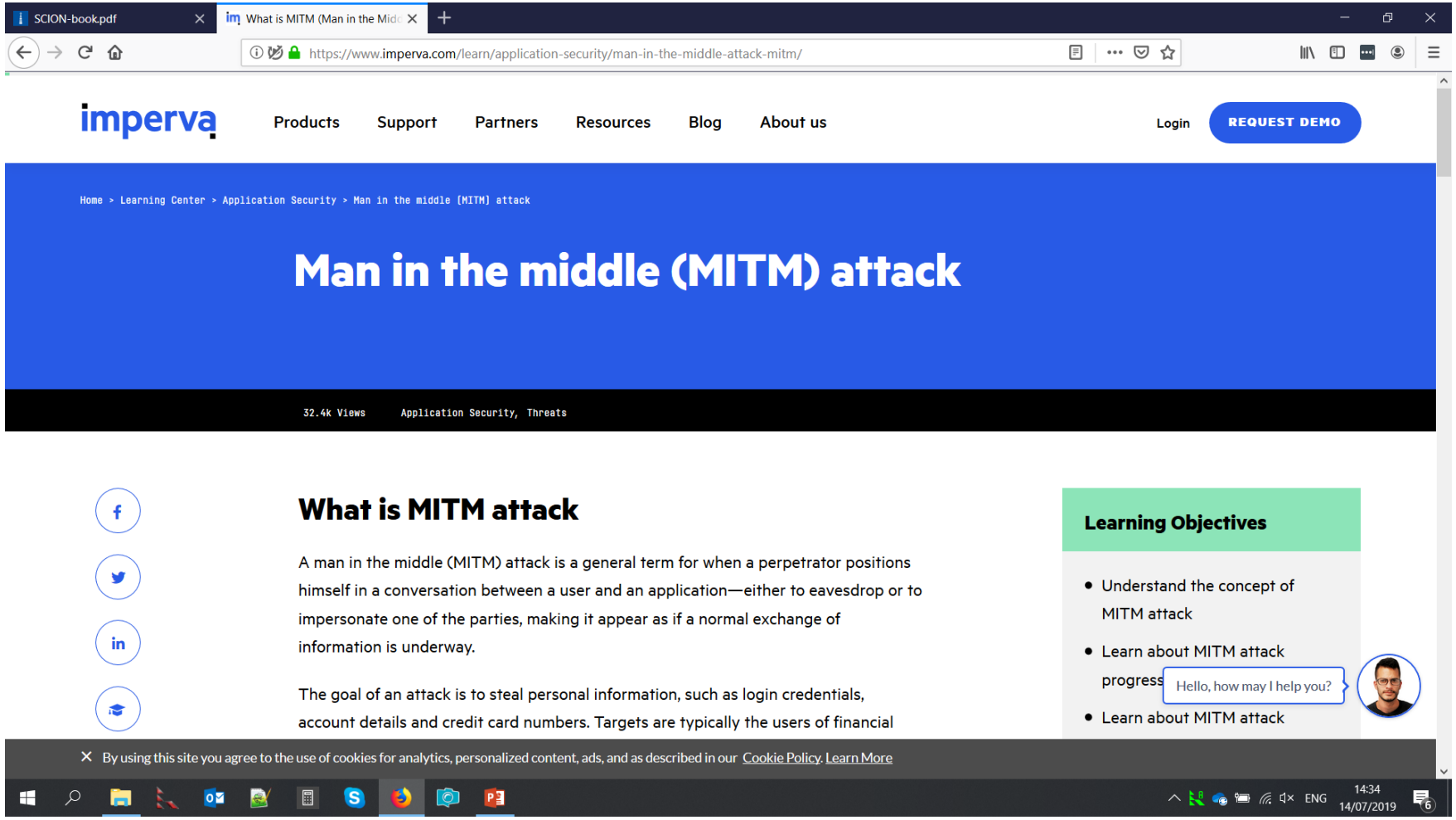
- Multipoint (“dissemination”) services are needed beside unicast services (“conversations”)
- Mobility (movement between networks) has shown to be pivotal
- Support for quality guarantees (e.g. latency guarantees for autonomous vehicles) is becoming important

- Some applications need path control and verification (e.g. evading certain jurisdictions)
- Self-determination/transparency on the use of user-data (ads, profiling, steering) is needed
- Security awareness has grown enormously and thus security service are needed (against e.g. DDoS, BGP hijacks)
- Local incidents should not have global effects (e.g. a CA compromise, BGP hijacks)

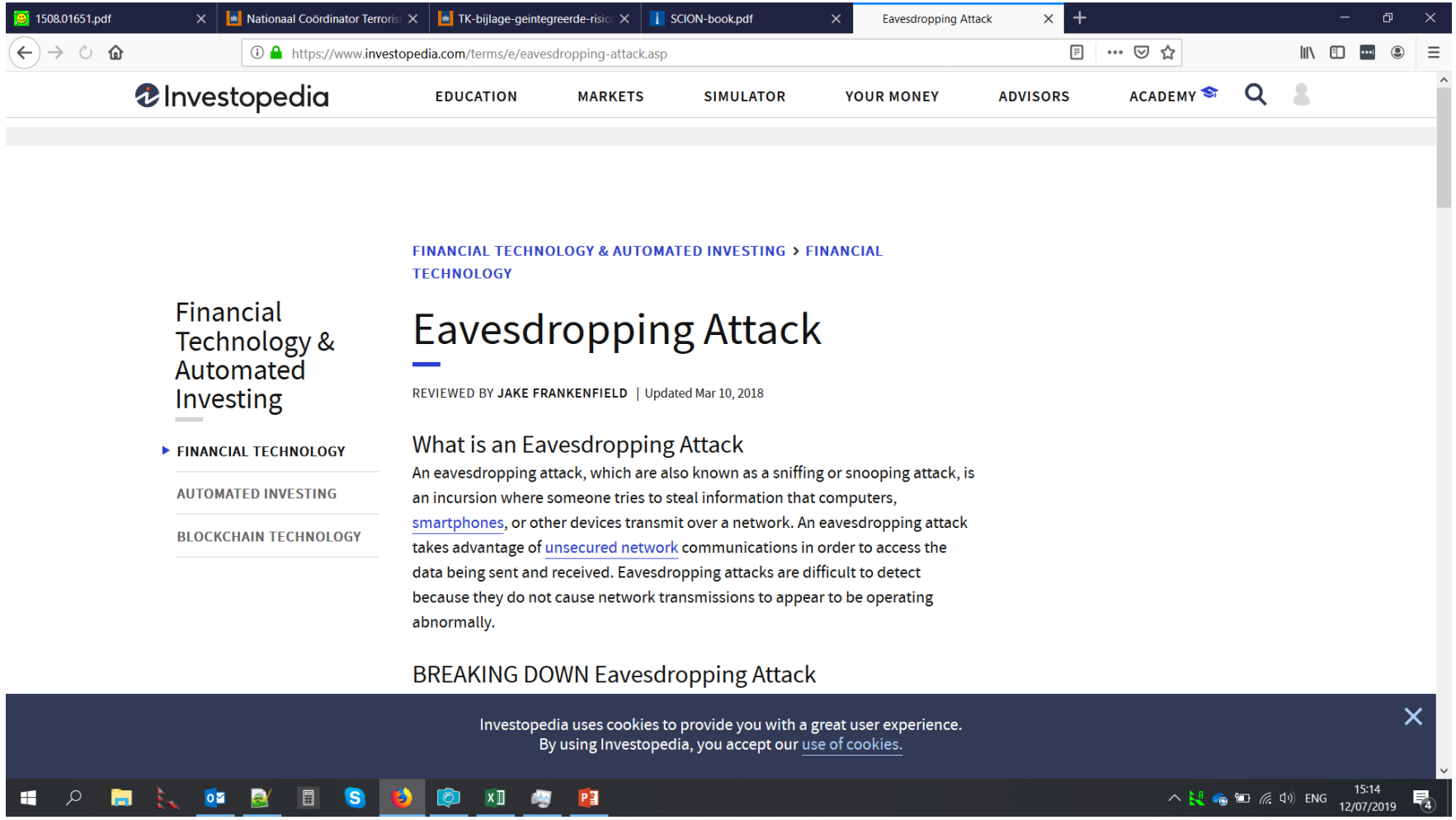
SIDN LABS

Some threads

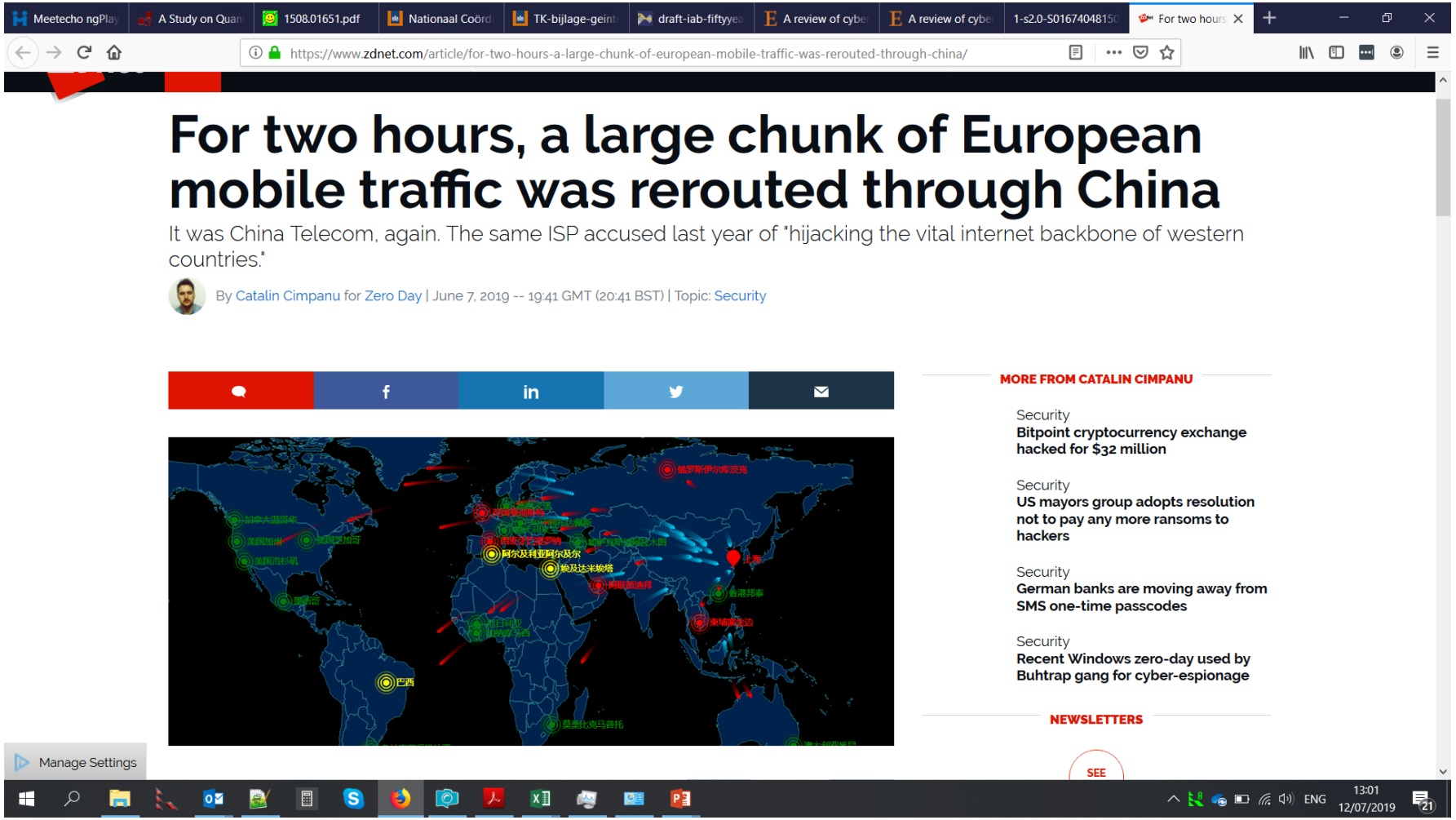
Man in the middle



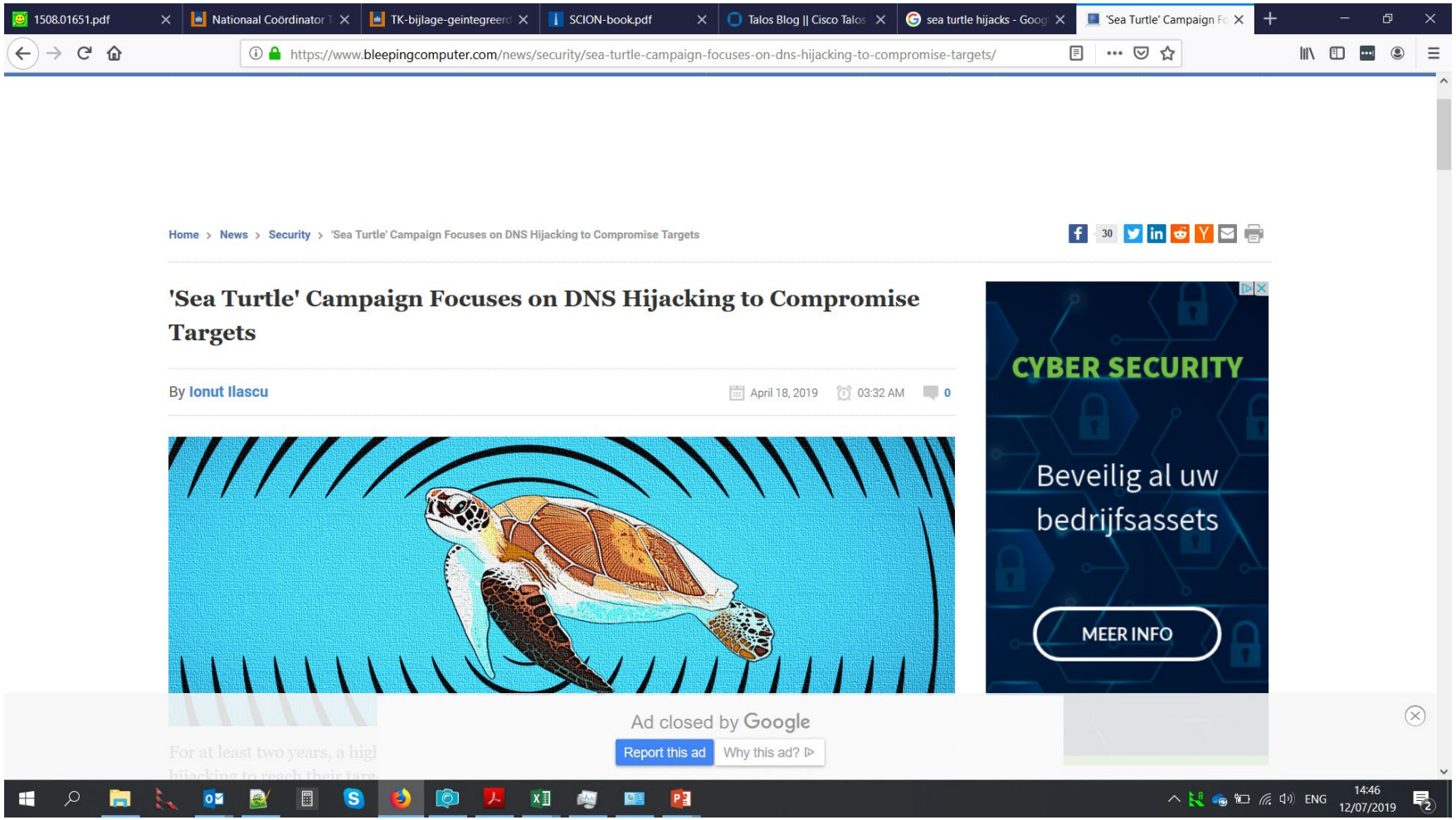
Eavesdropping



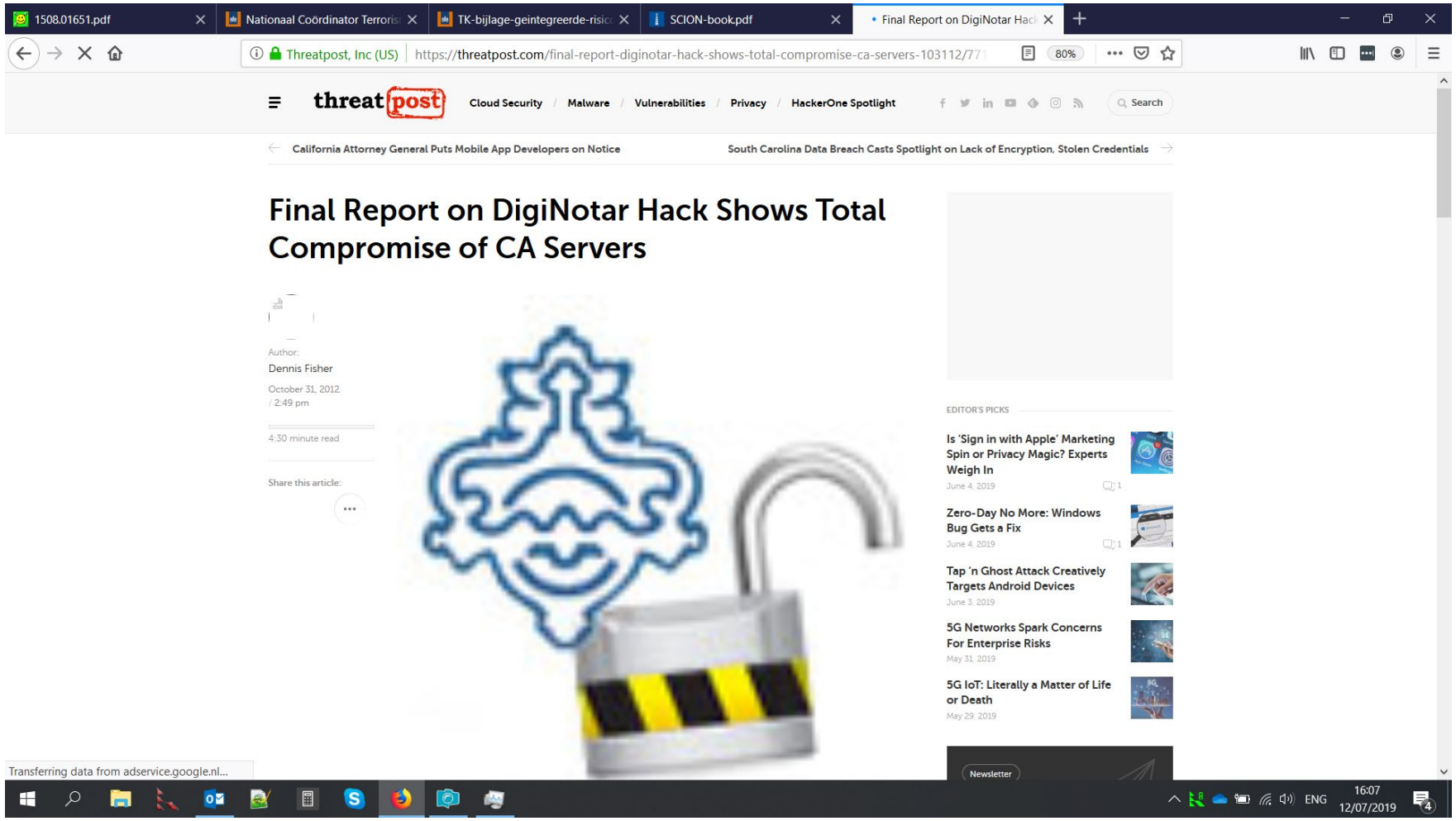
Prefix hijack



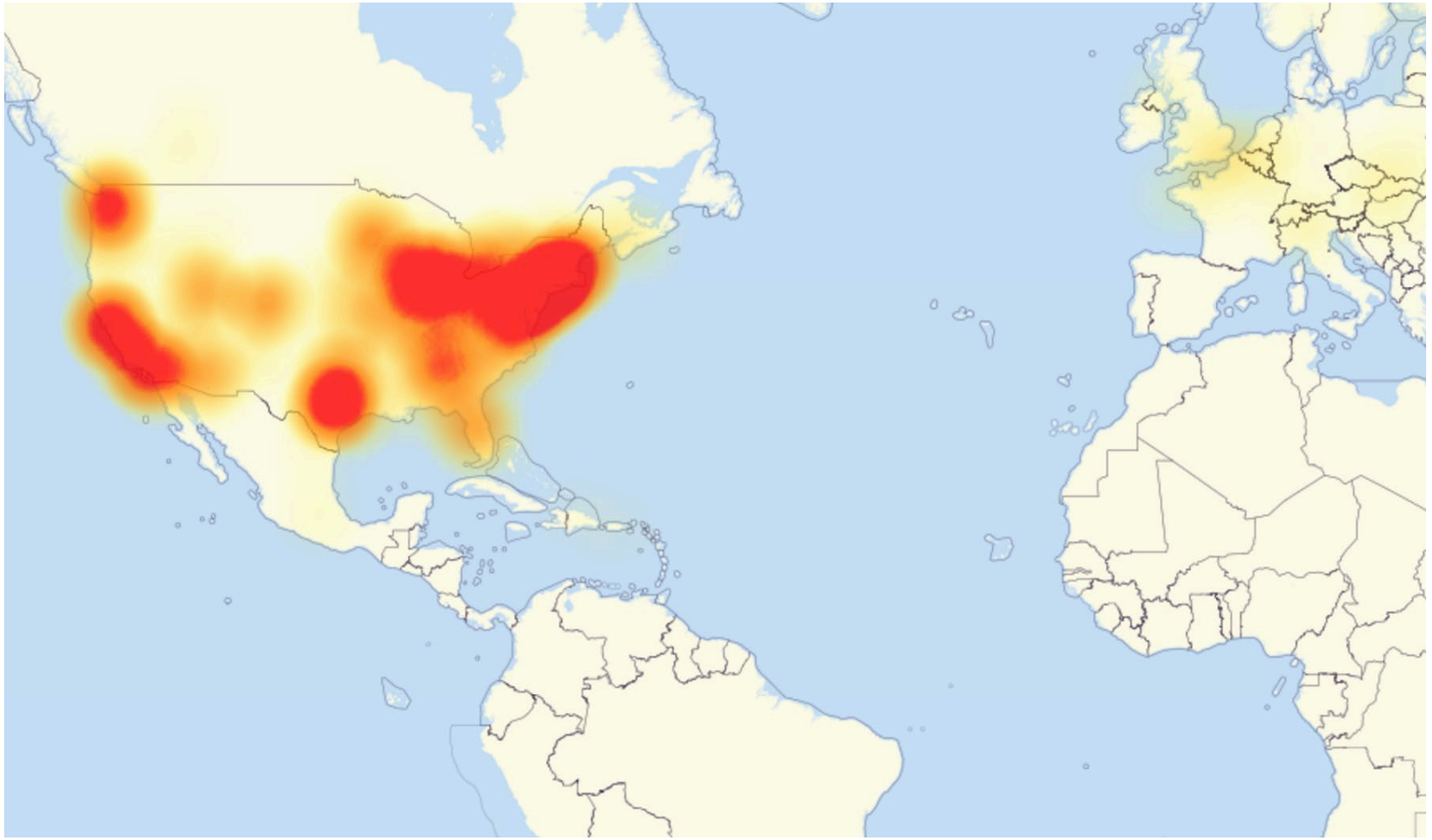
DNS hijacking



Forged TLS

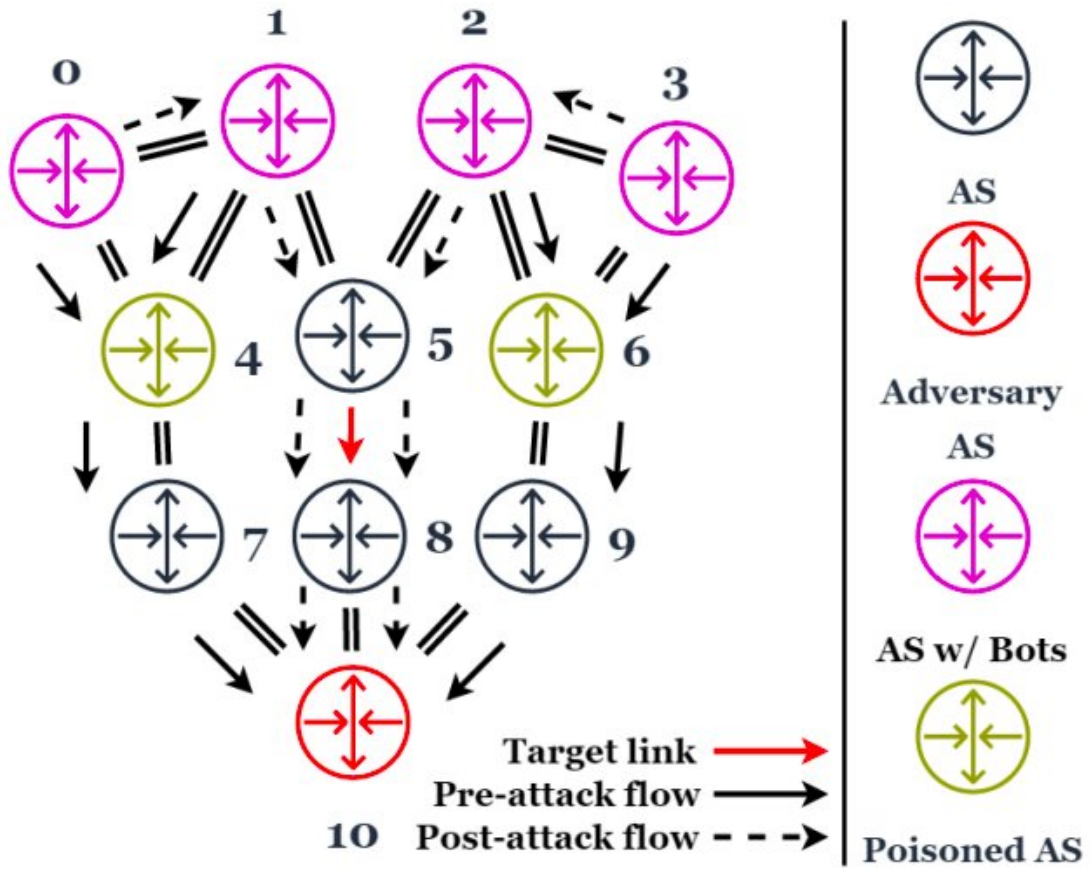

1508.01651.pdf
Nationaal Coördinator Terroris
TK-bijlage-geintegreerde-risic
SCION-book.pdf
Final Report on DigiNotar Hac
Threatpost, Inc (US)
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77
80%
threatpost
Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne Spotlight
Search
California Attorney General Puts Mobile App Developers on Notice
South Carolina Data Breach Casts Spotlight on Lack of Encryption, Stolen Credentials
Final Report on DigiNotar Hack Shows Total Compromise of CA Servers
Author:
Dennis Fisher
October 31, 2012
/ 2:49 pm
4:30 minute read
Share this article:
EDITOR'S PICKS
Is 'Sign in with Apple' Marketing Spin or Privacy Magic? Experts Weigh In
June 4, 2019
Zero-Day No More: Windows Bug Gets a Fix
June 4, 2019
Tap 'n Ghost Attack Creatively Targets Android Devices
June 3, 2019
5G Networks Spark Concerns For Enterprise Risks
May 31, 2019
5G IoT: Literally a Matter of Life or Death
May 29, 2019
Newsletter
Transferring data from adservice.google.nl...
ENG
16:07
12/07/2019

DDoS/Botnet attack: Dyn DNS using IOT devices

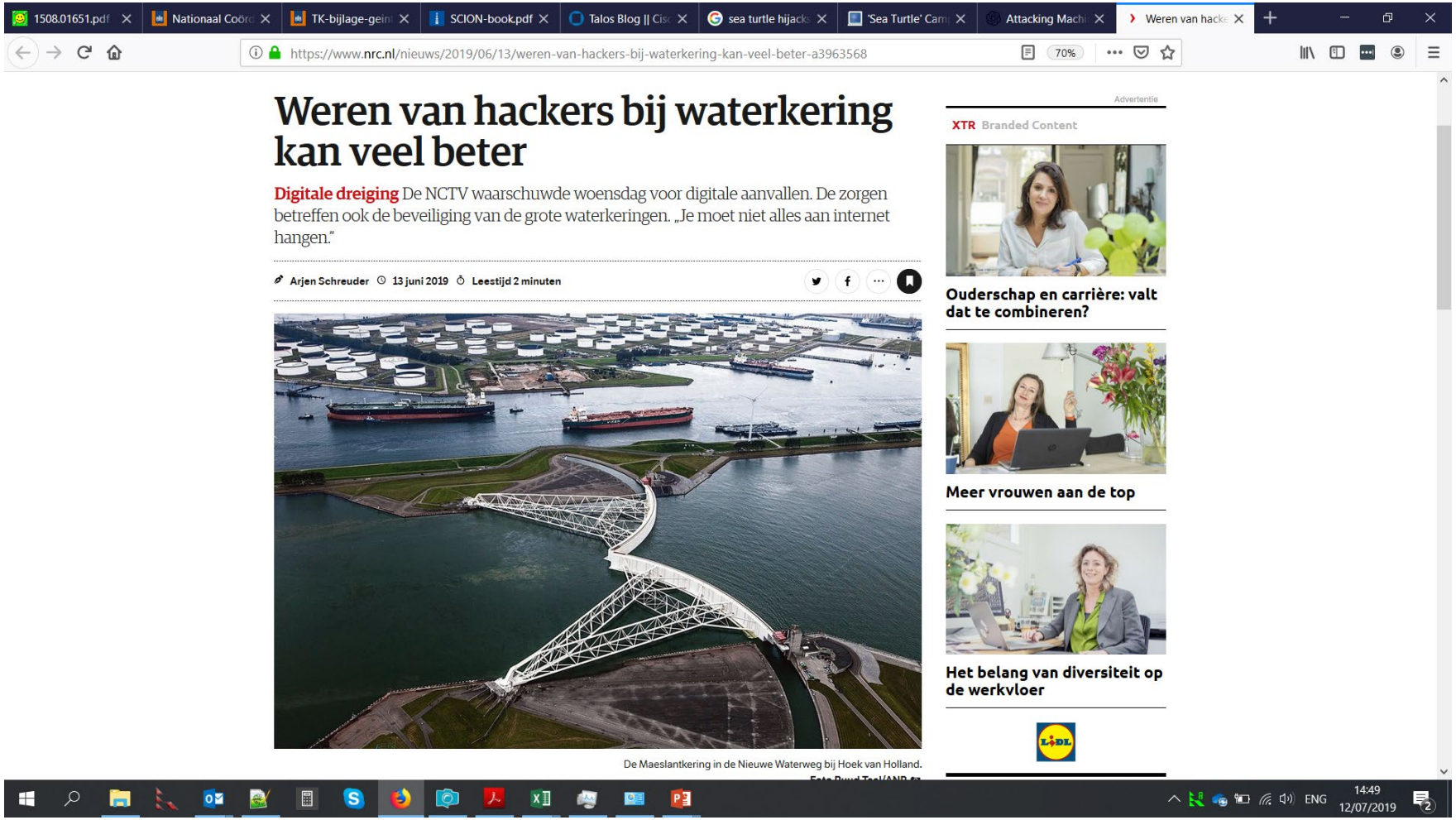


Source: https://en.wikinews.org/wiki/Distributed_malware_attacks_Dyn_DNS,_takes_down_websites_in_US

Compromised AS': Maestro attack

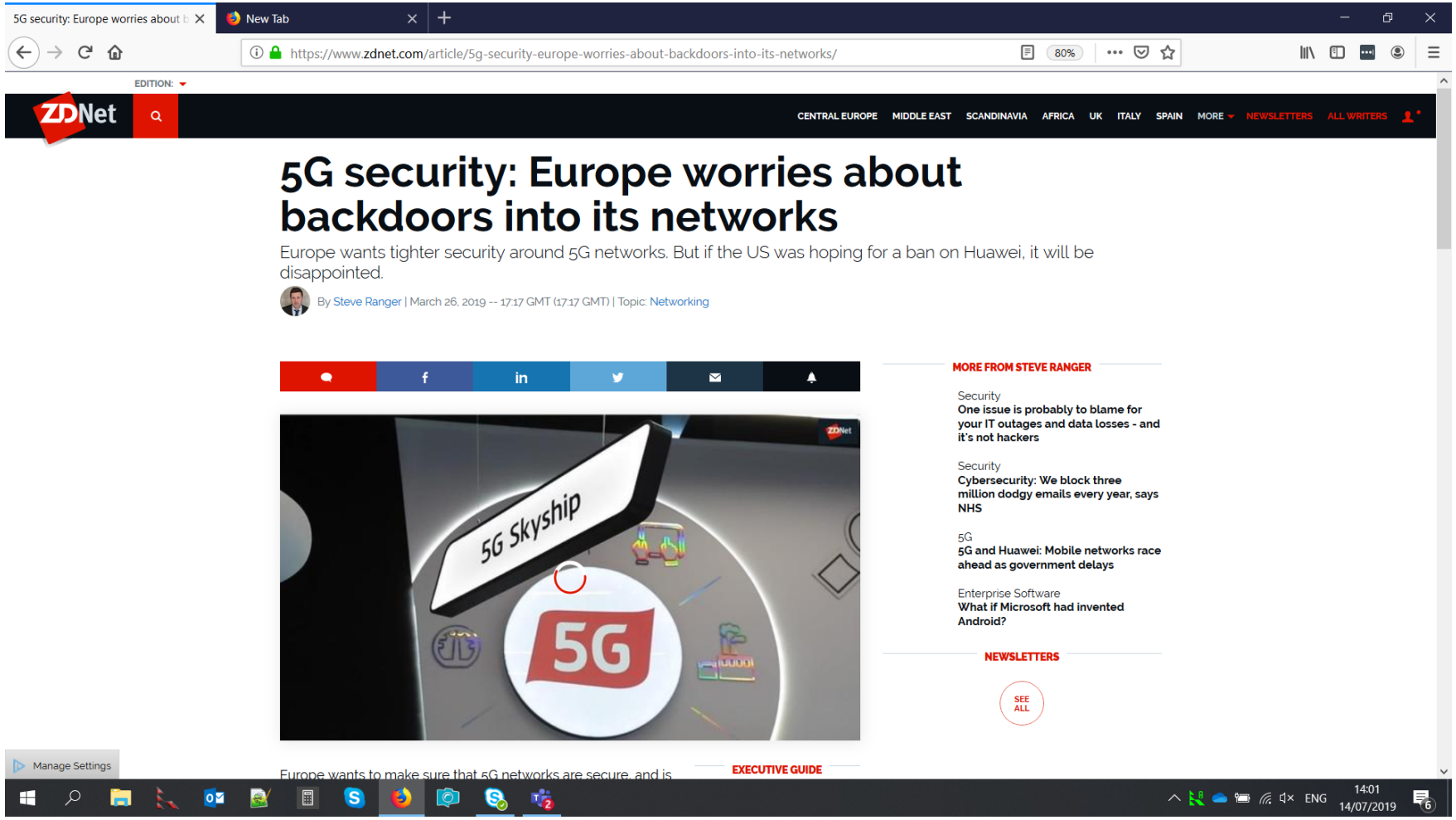


Control network security (SCADA/ICS/IOT)

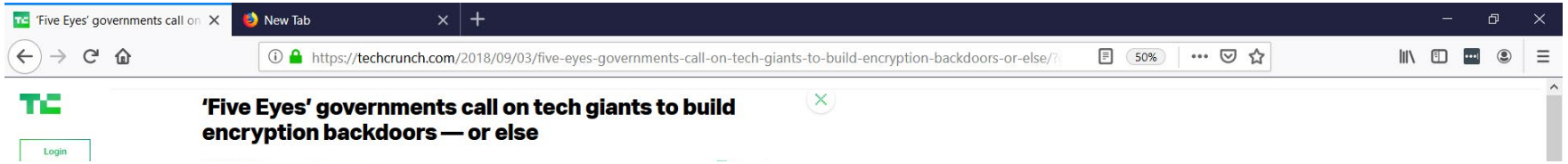


IP/MAC address spoofing

Backdoors: governments worry about backdoors



Backdoors: governments demand backdoors



8983/19

LIMITE

CT 45
COSI 97
CATS 67
ENFOPOL 213
TELECOM 202
CYBER 144

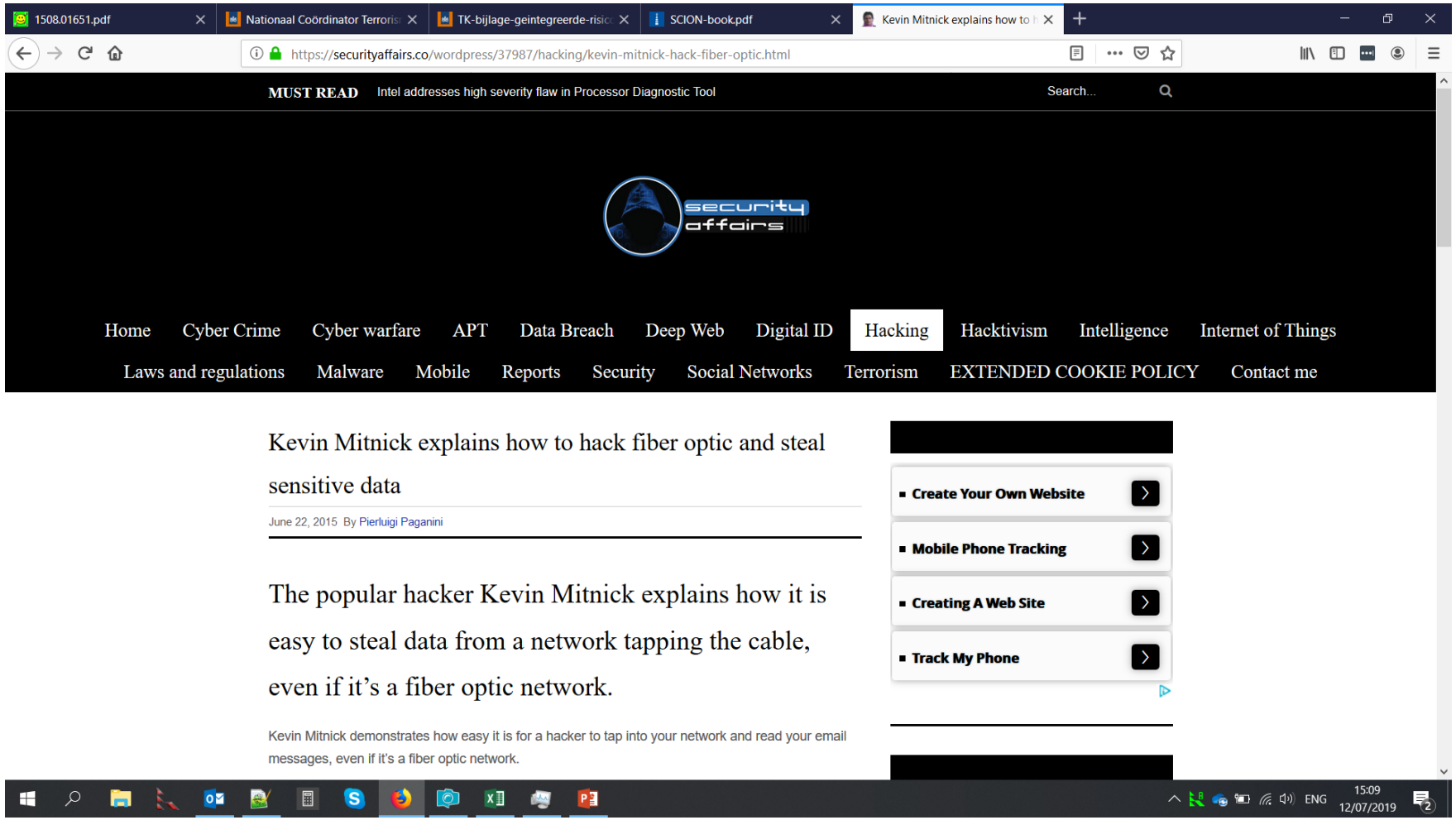
NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	**Law enforcement and judicial aspects related to 5G**

https://www.nporadio1.nl/reporter-radio/onderwerpen/507473-het-5g-netwerk-onder-de-loep

SIDN LABS

Physical access



Families of network technologies

How clean is clean slate?

- Can the new technology be introduced in a phased way (dual stack or in the core network and still have the existing technology in access network)
- How does it integrate with the established technology (in this case IPv4/IPv6)?
- Is one prepared (in the long term) to change/remove the established technology?
- Do application's APIs need to be changed?
- How developed (TRL levels) are implementations of the new technologies?

internet technology families

- Packet/bit based
  - Established (IPv4, IPv6)
  - Link/physical layer
    - Intermittent and high latency connectivity
    - Mobility
    - Fundamentally different communication physics
  - Programmability
    - PHB networking
    - Network virtualisation
    - Shaping industry structure
    - Services in the network
  - New network design principles
    - Minimum need for global unique identifiers
    - Regionality
    - Architecture for change (SCION)
    - Conceptual clarity (RINA)
- Information based
  - Performance increase due to objects
  - Information centric networking (NDN)

SIDN LABS

Evaluating network technologies

Evaluation guidelines (1/2)

- Needs of society
  Support society development, secure, utility, trust, ecology, privacy
- Generality
  Unknown future, look at all layers, modularity
- Longevity
  Evolvable, adaptable, flexibility, solving a (imminent) problem, transition planning, KISS
- Services
  Type of services, design, expressive power, control by end nodes, transparency

Evaluation guidelines (2/2)

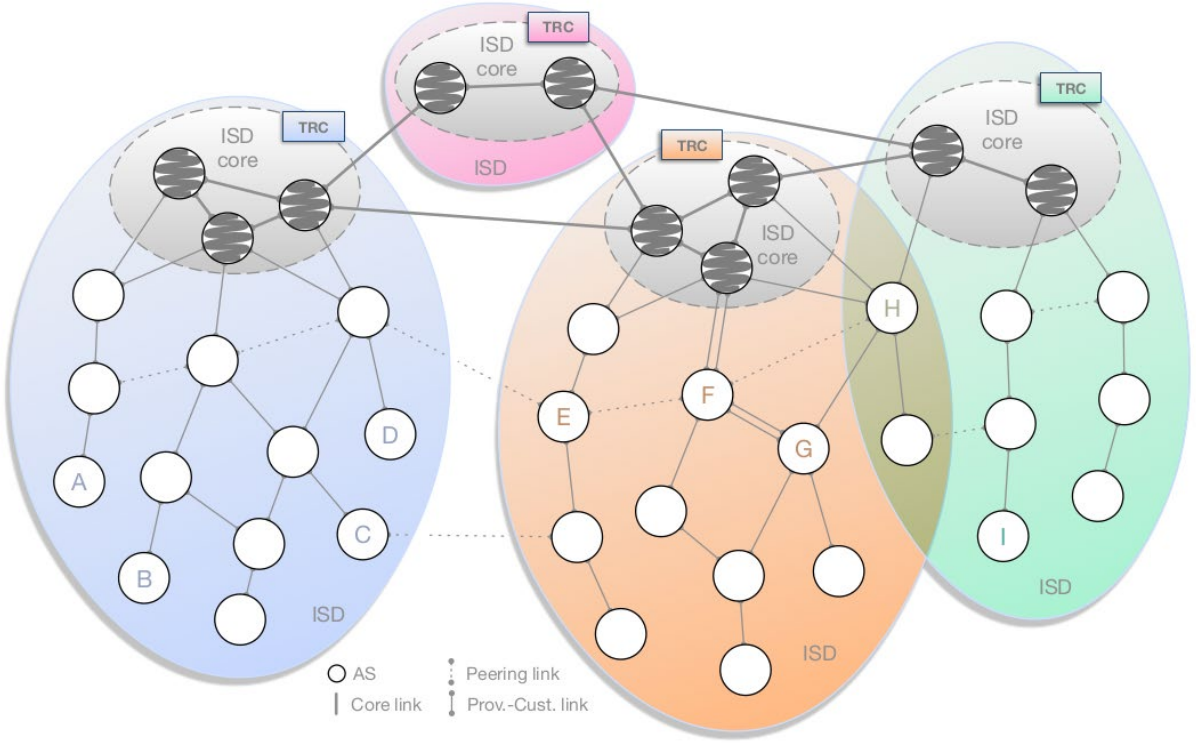
- Naming and/or addressing
- Control and management: FCAPS
  Fault, Capacity, Accounting, Performance (Stability) and Security
- Economical viability
  Deployable, fitness for purpose, involved stakeholders, vendors.
  TCO
- Solving threads
- Supporting our demonstrators

Technologies planned to be evaluated

- SCION: Stability, Control and Isolation on Next-generation networking…
- RINA: Recursive InterNetwork Architecture…
- NDN: Named Data Networking…

SCION: Stability, Control and Isolation on Next-generation networking

- Architecture for change
- In first instance about one-to-one communication



Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

SCION principles

- Scalability
  - packet-carried forwarding state
  - hierarchical design
- Control
  - ISPs decide available paths
  - endhost selects path

Transparency

- Isolation
  - isolation domains (failure stay with one)
  - built-in DDoS protection

Security

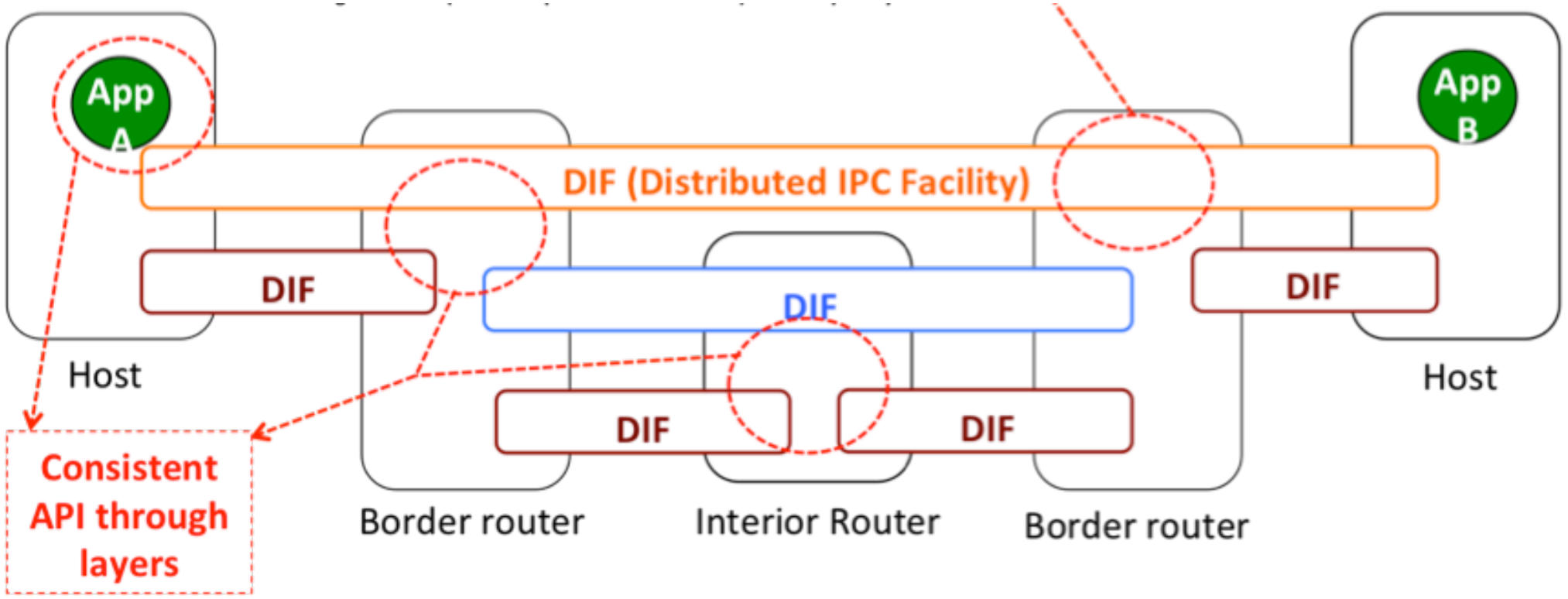
- On Next-generation networks
  - new control plane & data plane (replaces IP + BGP)
  - endhost-controlled multipath for free

Stability

SIDN LABS

RINA: Recursive InterNetwork Architecture

- Framework for conceptual clarity
- SCION can be a RINA DIF



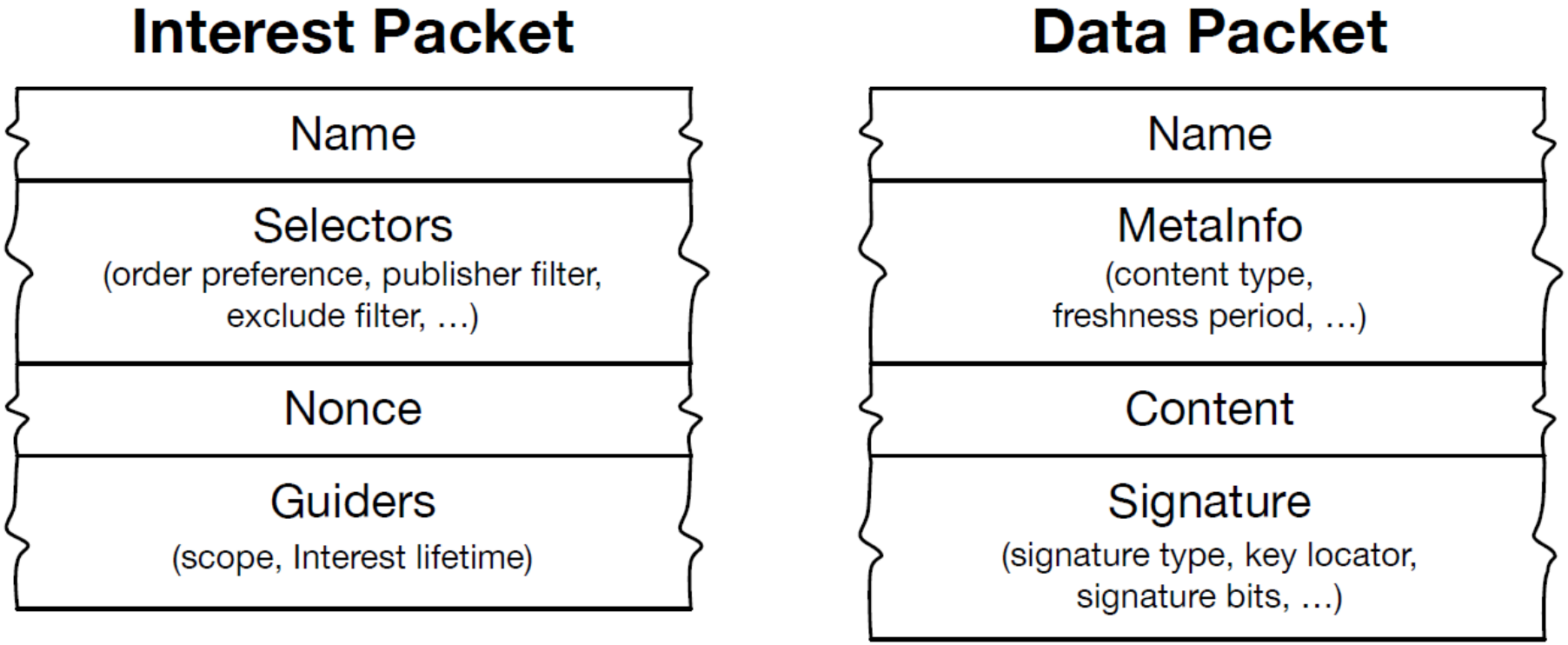
Source: http://ict-arcfire.eu/index.php/rina/

RINA framework principles

- Structure
- Protocol design
- Naming, addressing and routing
- Mobility and multi-homing
- Quality of Service, resource allocation, congestion control
- Security
- Network Management
- Path-aware networking
- New routing + forwarding architecture
- Provable security: Protocol + Code
- Heterogeneous trust model
- Built-in DDoS defence mechanisms

NDN: Named Data Networking

- Information centric networking
- One to one communication is somewhat problematic



Source: By NDN Consortium - named-data.net, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=35288191

NDN principles

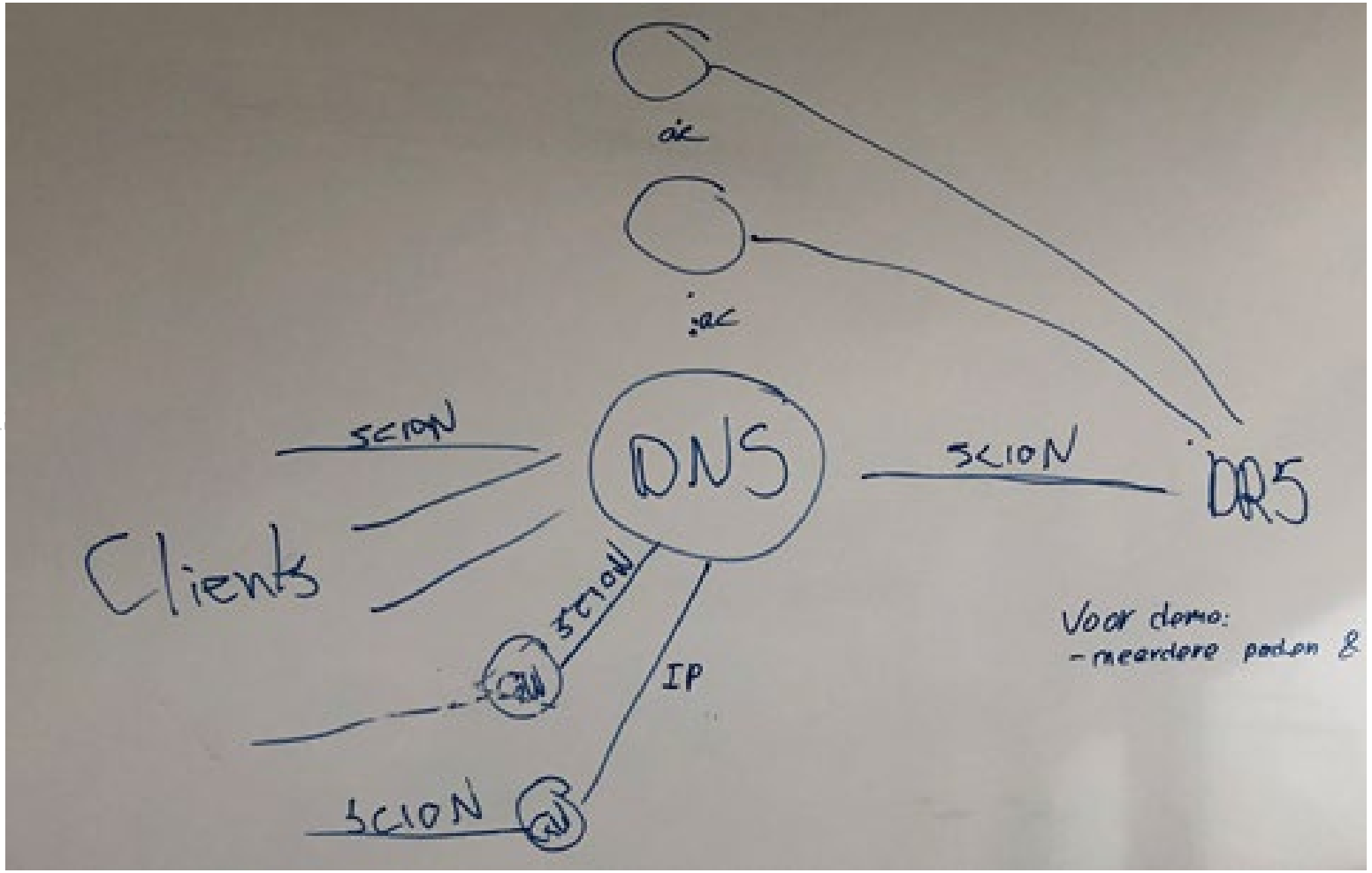
- Evolvement from existing host-centric to data-centric
- Authentic: a valid/cryptographic name-to-content binding
- Trustworthy: reputable or trusted origin
- Not specifically a Delay/Disruption-Tolerant Network

SIDN LABS

Use cases/demonstrators

Use cases/demonstrators

- Existing IP services
  - DNS (2019 KPI)
  - AMS-IX
- IOT/ICS related
  - Intelligent Transport System
  - SCADA/ICS
  - Rijkswaterstaat
  - Smart girds
- Transactions
  - Banks
  - Customs



Use cases/demonstrators

- Existing IP services
  - DNS (2
  - AMS-I
- IOT/ICS
  - Intellig
  - SCADA
  - Rijksw
  - Smart g
- Transact
  - Banks
  - Customs

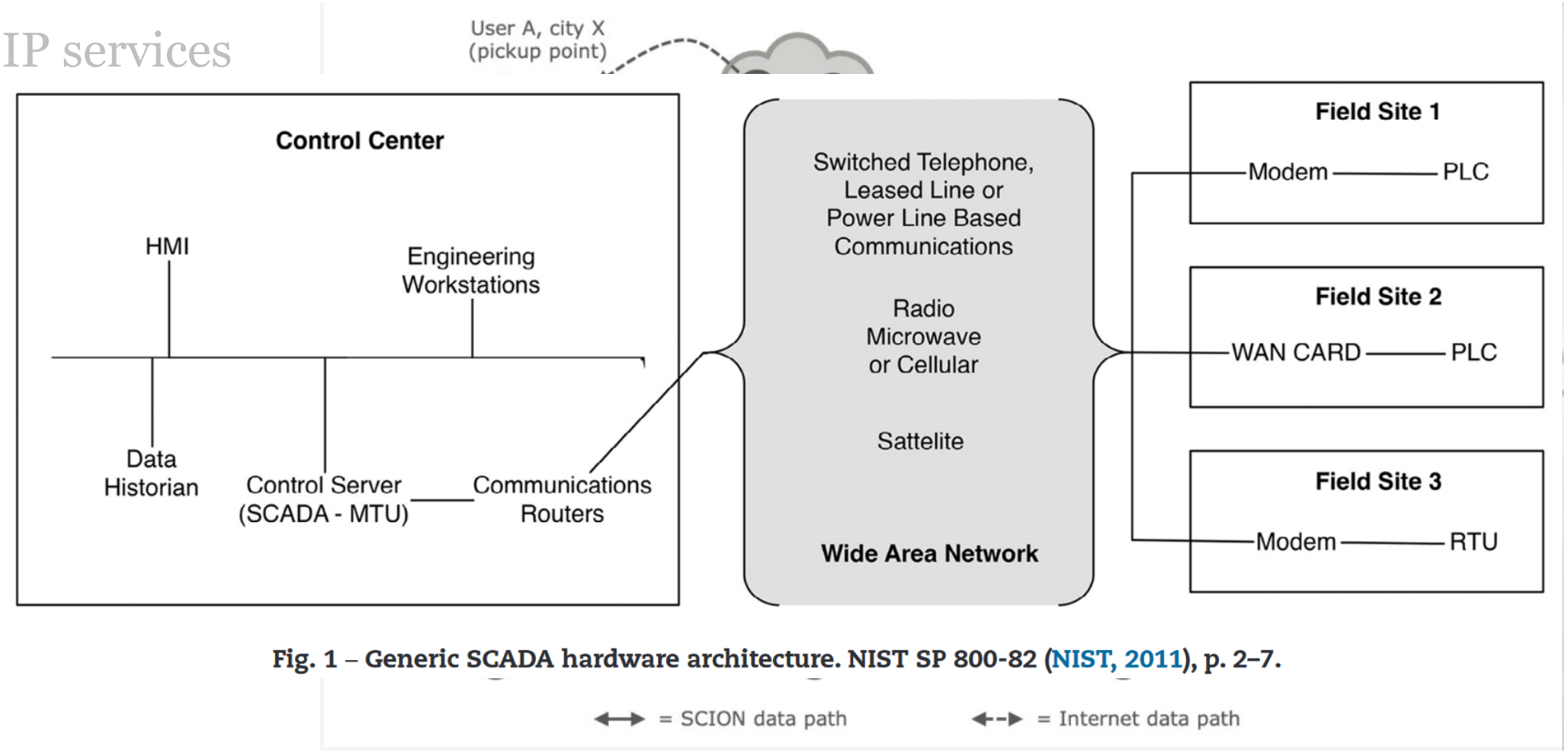


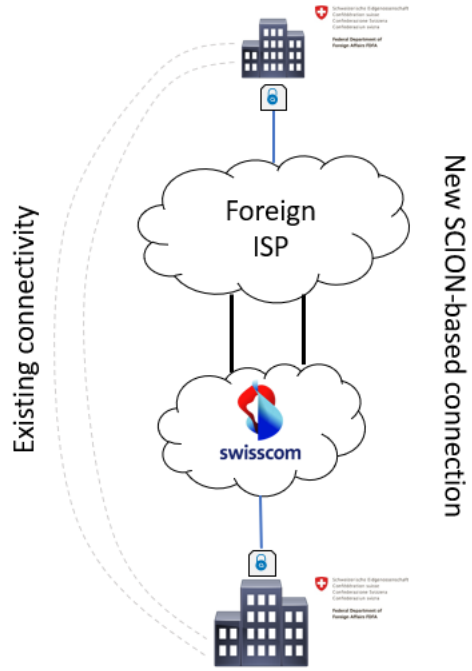
Fig. 1 – Generic SCADA hardware architecture. NIST SP 800-82 (NIST, 2011), p. 2–7.

Use cases/demonstrators

- Existing IP services
  - DNS (2019 KPI)
  - AMS-IX
- IOT/ICS related
  - Intelligent Transport Syste
  - SCADA/ICS
  - Rijkswaterstaat
  - Smart girds
- Transactions (betalings v
  - Banks
  - Customs

Use Case 2: Connecting Swiss Embassies to Bern

- **The Challenge:**
  - Secure and alternative connection between one of the most important Embassies and its headquarters
- **The solution:**
  - SCION Connection via 2 Service Providers as managed service
- **The results:**
  - Latency improved over existing connectivity
  - Interdomain-Failover tests successful
  - SCION connection replaced existing connections as default path



anapaya systems

SIDN LABS

Brainstorm

Brainstorm

- Do you have other threads?
- Do you know other future network technologies?
- How should we evaluate future network technologies?
  - Availability of STOP function, society need (China, Europe, USA, company, et.)
- Do you have other examples of use cases?
  - Filesharing, videostreaming
  - Understand demands of user groups.
- What is the preference: add functionality to IP or introduce a future network technology?
- Should this future network technology replace IP?
- What if we broaden this to the whole stack?
  - Providers: network providers and service providers

Volg ons

SIDN.nl

@SIDN

SIDN

Thanks for your attention!

www.sidnlabs.nl | stats.sidnlabs.nl

Victor Reijs, victor.reijs@sidn.nl