Incident Response for Policy Makers

An introduction

Dr. Serge Droz <serge.droz@first.org>
Chair, Board of Directors

Maarten Van Horenbeeck <marten@first.org>
Member, Board of Directors

License

Content

During this course, you will learn:

- What are **Computer Security Incident Response Teams**?
- Why are CSIRTs **essential** for the Internet?
- How **do they work together in a collaborative community?**
- What are the **basic steps in incident handling** they implement?
- **How is trust built** in the incident response community?
- How can you help your CSIRT community **mature?**

Who we are

Association of Incident Response and Security Teams

Founded in 1989

Mission

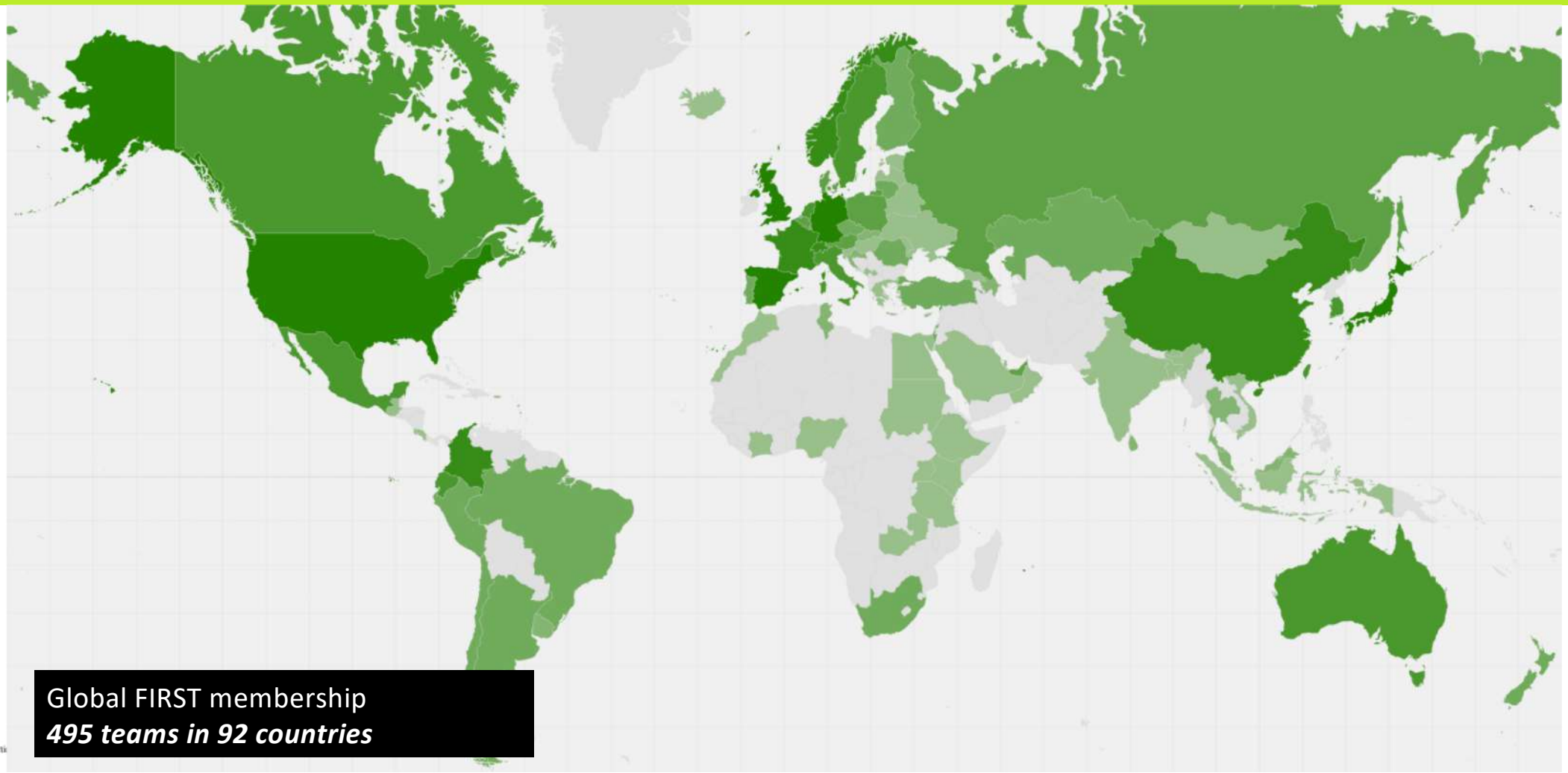
Global Coordination: In an emergency you can always find the teams you need to support you in our global community.

Global Language: Incident responders around the world speak the same language and understand each other's intents and methods.

Automation: Let machines do the boring calculations, so humans can focus on the hard questions.

Policy and Governance: Make sure others understand what we do, and enable us rather than limit us.

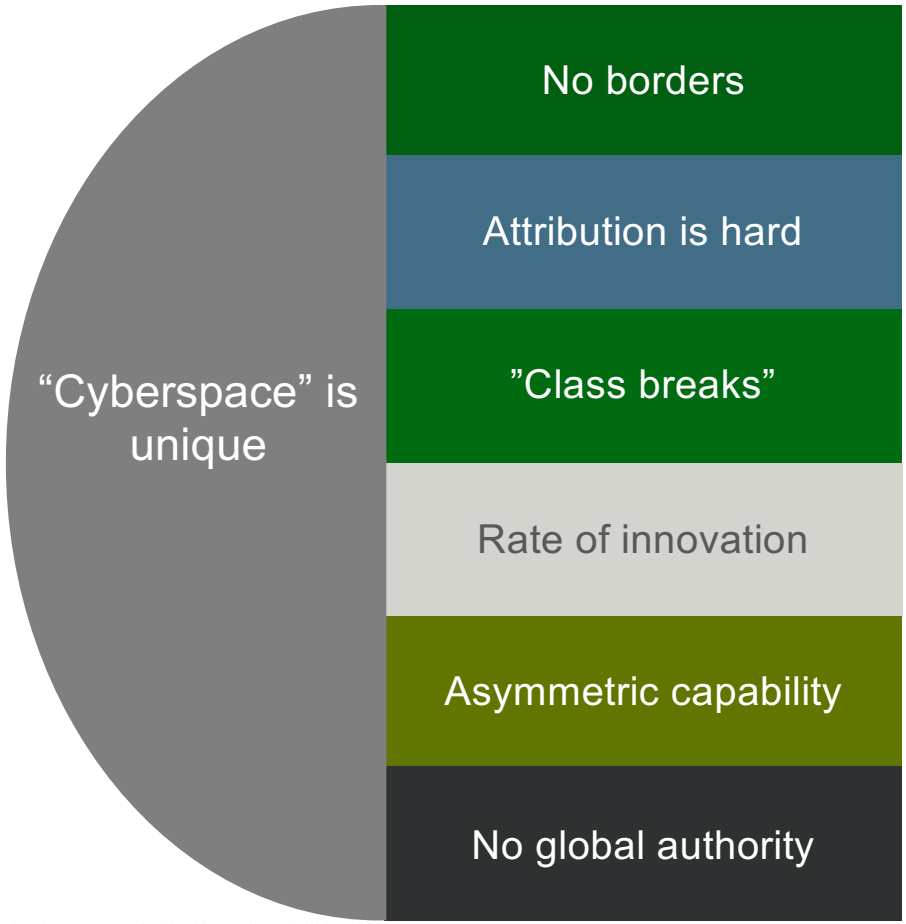
Members



Global FIRST membership
495 teams in 92 countries

Part I: Understanding the CSIRT environment

Challenges



Attacks easily expand beyond a single country, and affect others.

Most evidence is created through technical means, which are easily instrumented and not attributable.

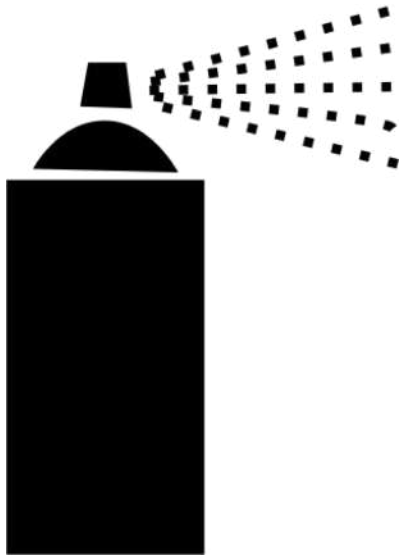
An attack can be repeated easily. No need to walk kilometers to “juggle locks”

There’s a new technology to be exploited every few weeks. Smart contracts, social media, mobile apps.

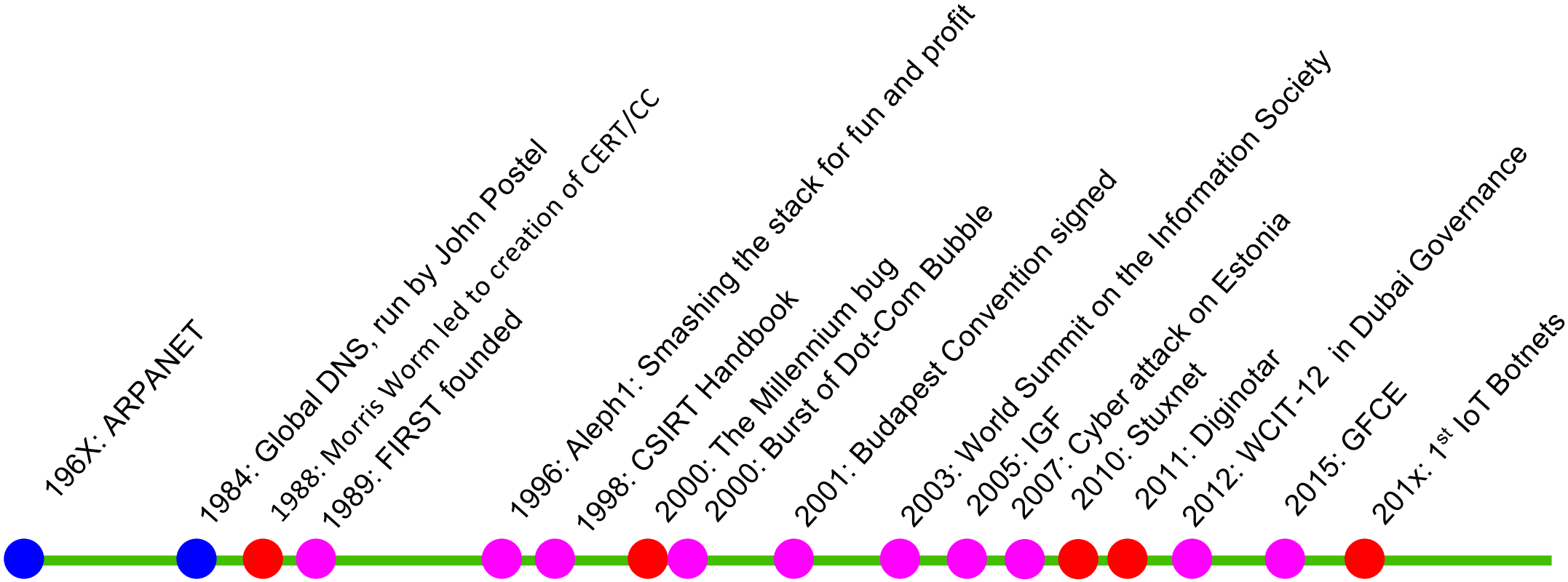
An adversary can be a state, or someone who just had a very good idea.

There’s no single authority that acts as the police officer of the internet.

Actors



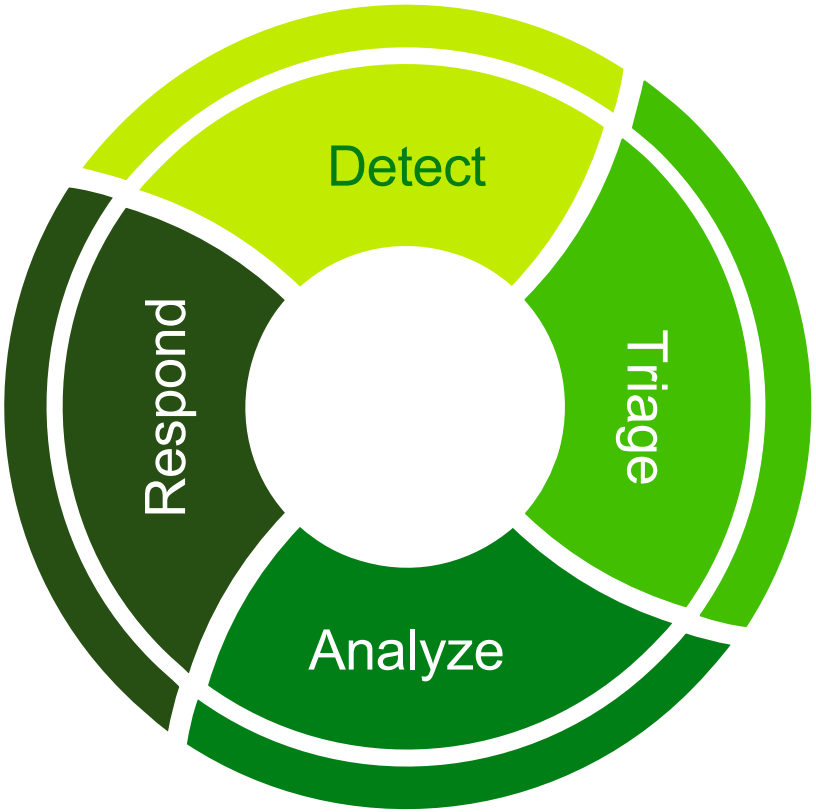
History


196X: ARPANET
1984: Global DNS, run by John Postel
1988: Morris Worm led to creation of CERT/CC
1989: FIRST founded
1996: Aleph1: Smashing the stack for fun and profit
1998: CSIRT Handbook
2000: The Millennium bug
2000: Burst of Dot-Com Bubble
2001: Budapest Convention signed
2003: World Summit on the Information Society
2005: IGF
2007: Cyber attack on Estonia
2010: Stuxnet
2011: Diginotar
2012: WCIT-12 in Dubai Governance
2015: GFCE
201x: 1st IoT Botnets


Incident Response
David Mark

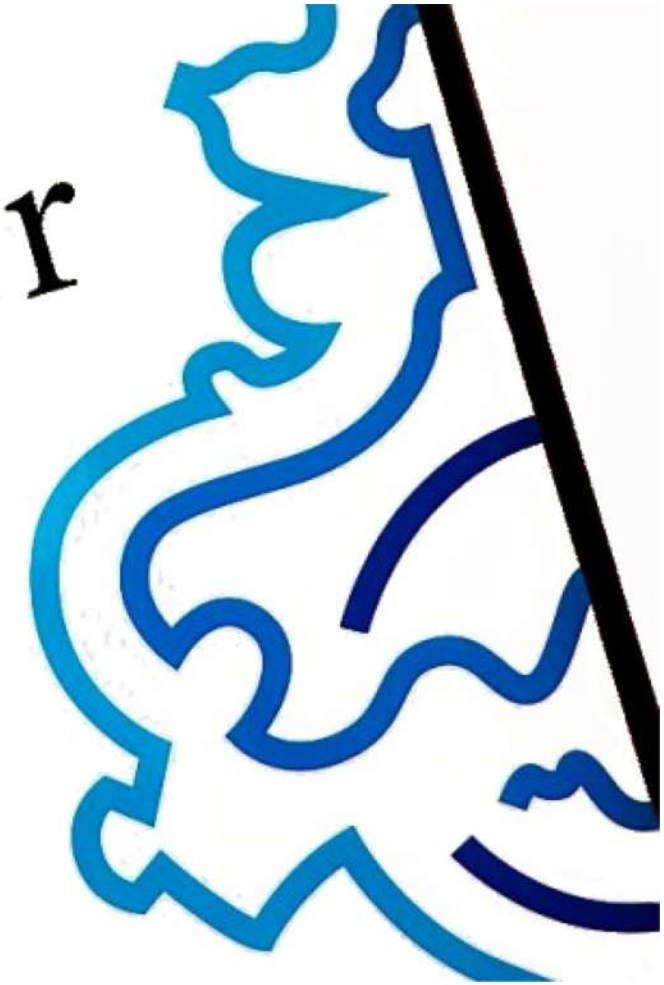
- Governance
  - Accountability and ownership
  - Legislation and policy
- Prevention
  - Security practices
  - Awareness building
- Detection
- Response

Workflow

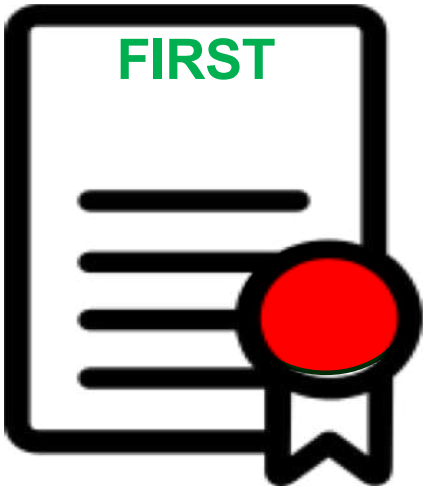


Case Study

DigiNotar



Certificates



The website delivers a certificate which
is signed by a trusted **Certificate authority**:

To verify a website the browser:
1. Asks for the certificate
2. Checks if it has been signed by a known CA
3. If ok it displays a green lock, if not a warning

Case Study: Diginotar

- Operating systems and/or browsers ship with a “trust store”, which defines who can issue digital certificates they trust
- About 150 companies are entrusted by these products
- These companies have to follow strict rules. But this has not always been enough.
- **On August 2nd, 2011, Google rolled out ”pins” to require specific companies’ certificates for Google properties.**

Case Study: Diginotar

Is This MITM Attack to Gmail's SSL ?

by alibo 27/08/2011

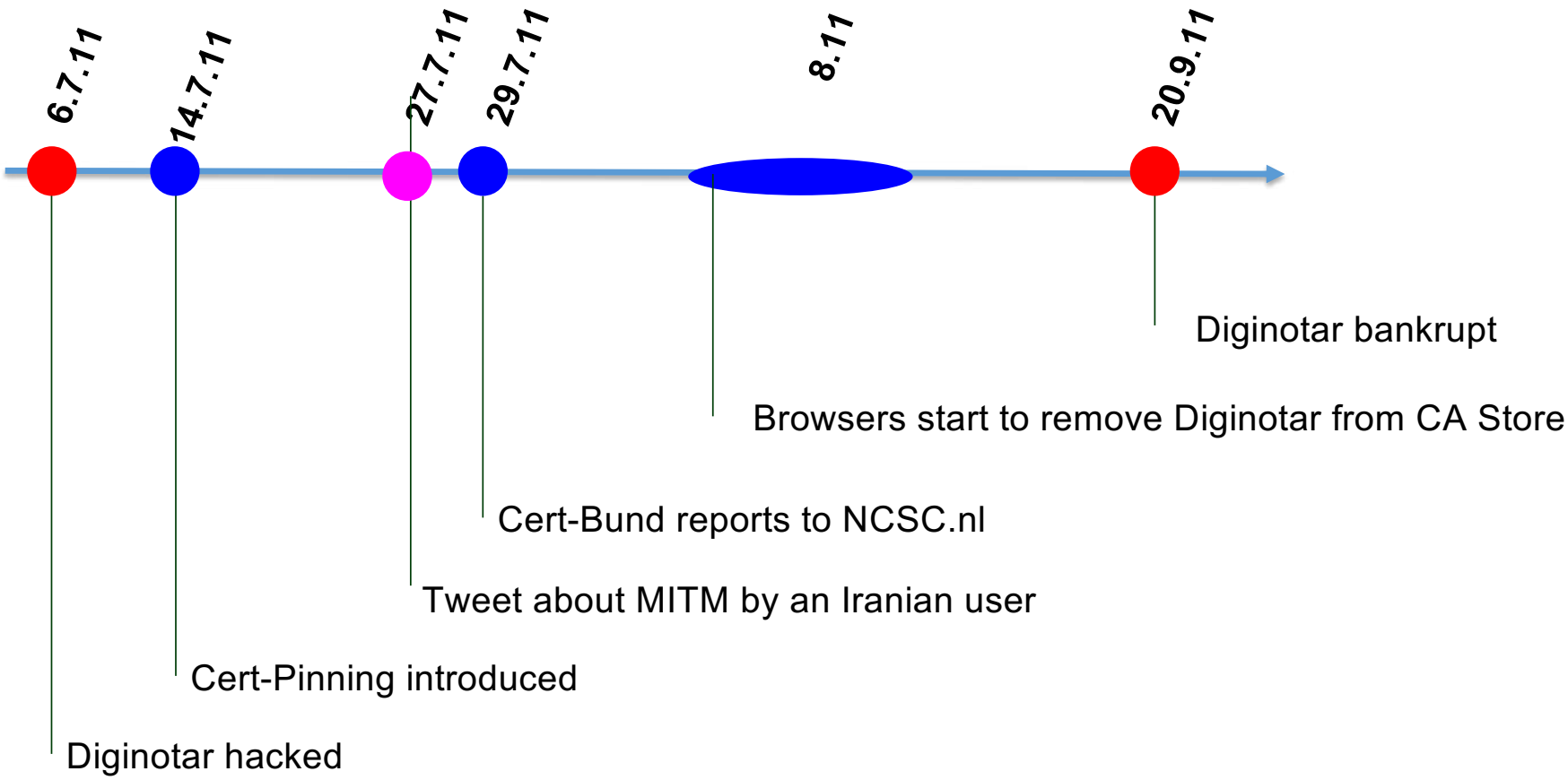
Hi,
Today, when I trid to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:
http://www.mediafire.com/?rrklb17slctityb

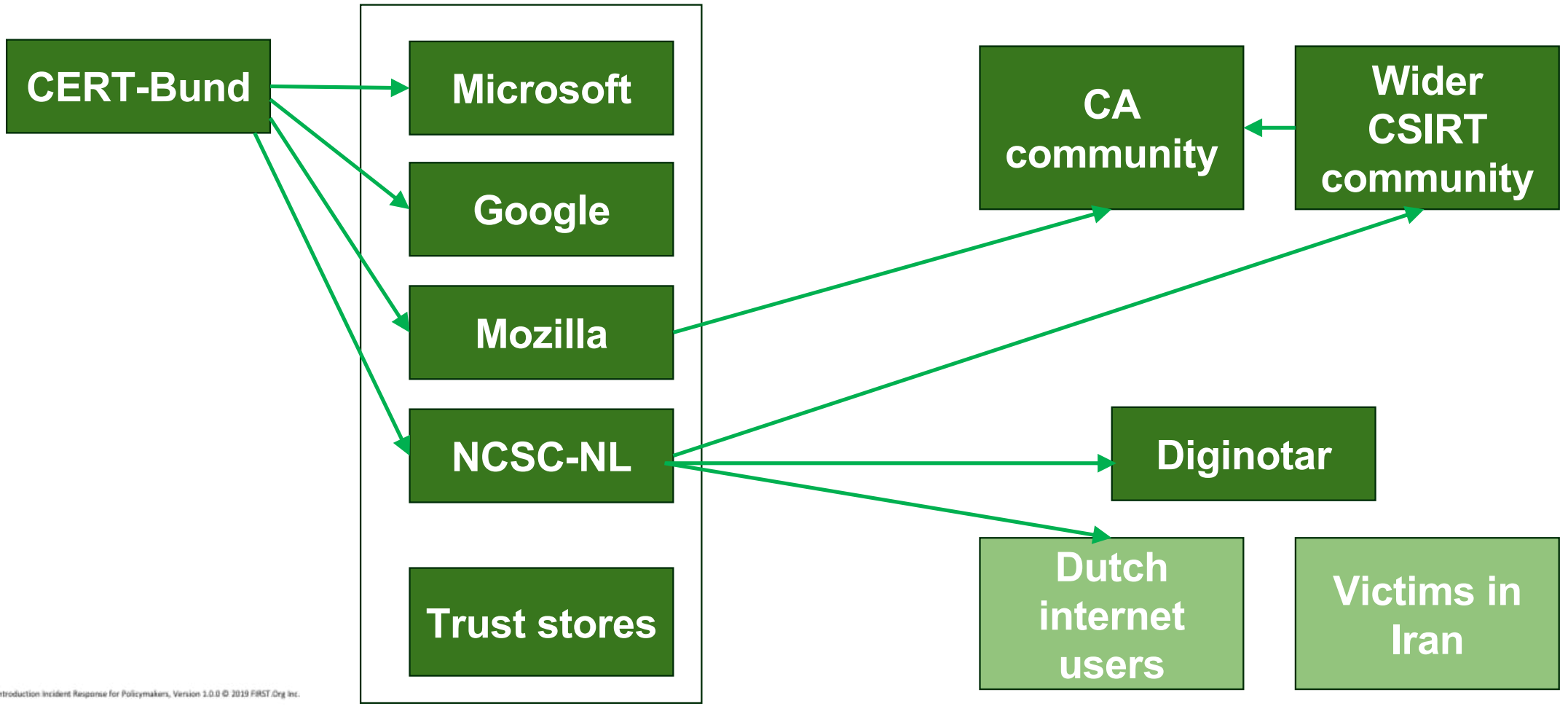
and this is text of decoded fake certificate:
http://pastebin.com/ff7Yg663

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack
(because I live in Iran and you may hear something about the story of Comodo hacker!)

Timeline


6.7.11
14.7.11
27.7.11
29.7.11
8.11
20.9.11
Diginotar bankrupt
Browsers start to remove Diginotar from CA Store
Cert-Bund reports to NCSC.nl
Tweet about MITM by an Iranian user
Cert-Pinning introduced
Diginotar hacked

Stakeholders



Case Study: Diginotar

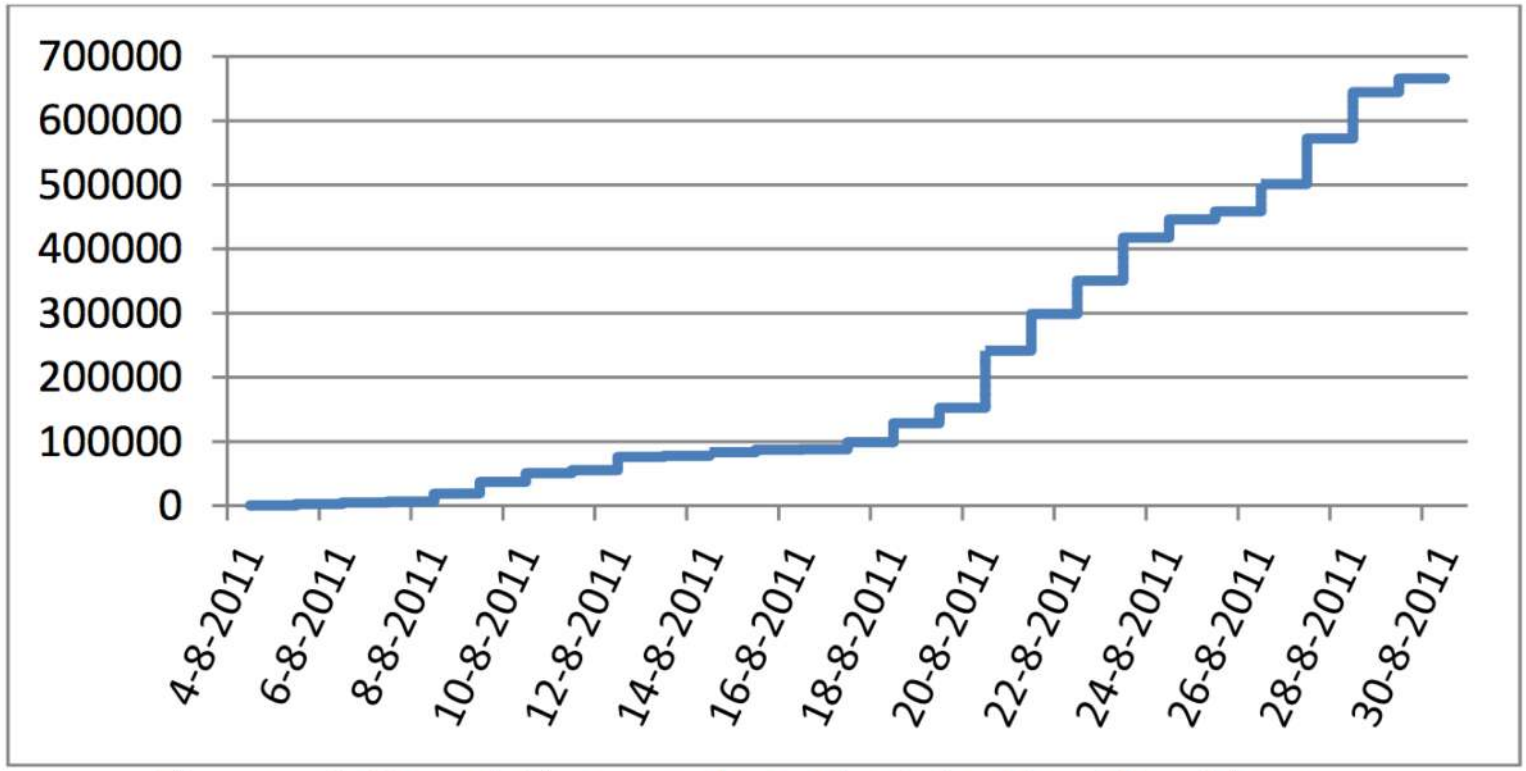


Figure 6 Cumulative number of originating IP addresses

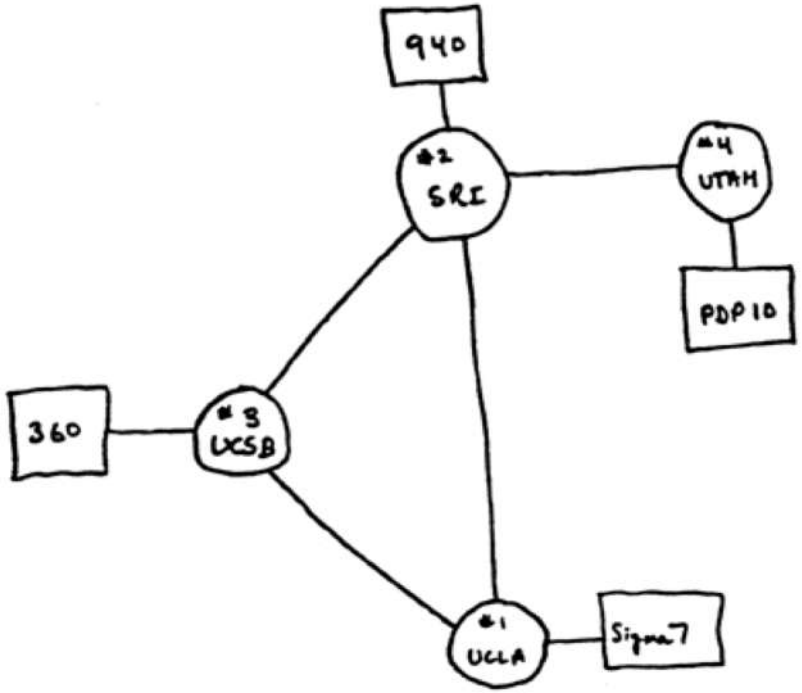
Source: Fox-IT – Black Tulip: Investigation into DigiNotar

Distinct responsibilities

- **CERT-Bund:** raise the alarm.
- **DigiNotar:** understand scope of the compromise on their end, and what type of potential impact is possible.
- **Google:** protect their customers by invalidating trust.
- **Mozilla/Microsoft:** protect customers by invalidating trust.
- **NCSC-NL:**
  - CSIRT closest to the issue, affected industry members, coordinate response.
  - Assess overall impact through source data

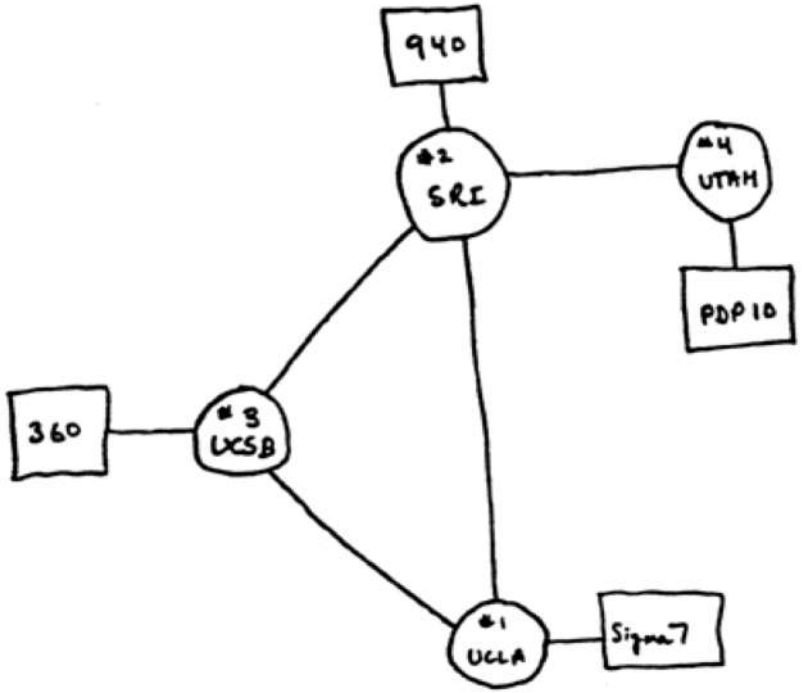

Trust
Guillaume de Germain

The Internet then and now

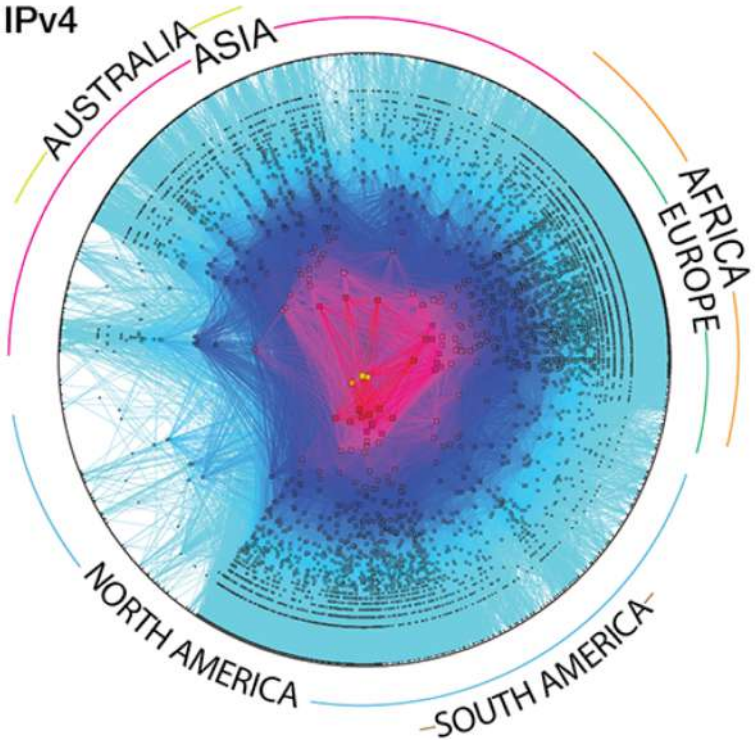


Source: https://www.darpa.mil/about-us/darpa-history-and-timeline?PP=2

The Internet then and now



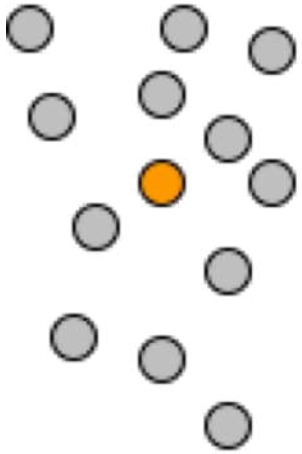
Source: https://www.darpa.mil/about-us/darpa-history-and-timeline?PP=2



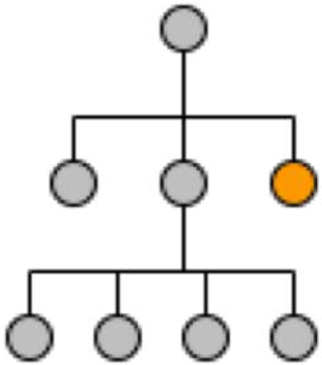
Source: https://www.caida.org/research/topology/as_core_network/2015/

Models of Governance

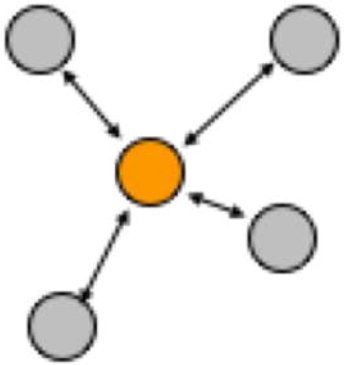
Market



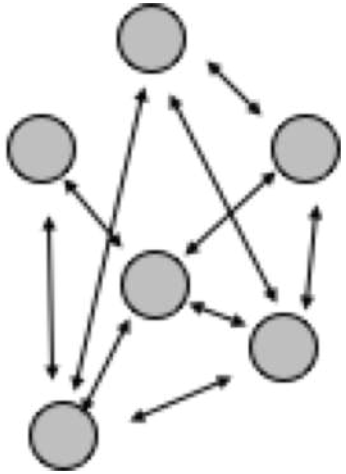
Hierarchy



Collaboration



Network



Network Governance

*Governance [is achieved] through relatively **stable** cooperative relationships between three or more legally autonomous organisations **based on horizontal**, rather than hierarchical coordination, recognizing one or more network or collective goals*

The late **Elinor Ostrom** receives the 2009 economic sciences Nobel prize for her groundbreaking work: “Governing the Commons”.

Source: https://commons.wikimedia.org/wiki/File:Nobel_Prize_2009-Press_Conference_KVA-31.jpg

Effective network collaboration requires **trust** and a **common goal**.

If either is missing collaboration is not possible.


FIRST Events
Annual Conference
Symposia
TCs
Training Courses
Outreach
Building Trust: Global events August 2017-2018

Trust inhibitors

- **Hidden Agendas**
- **Placing the CERT in the wrong spot**
- **Sanctions**

Trust inhibitors

- **Placing the CERT in the wrong spot**

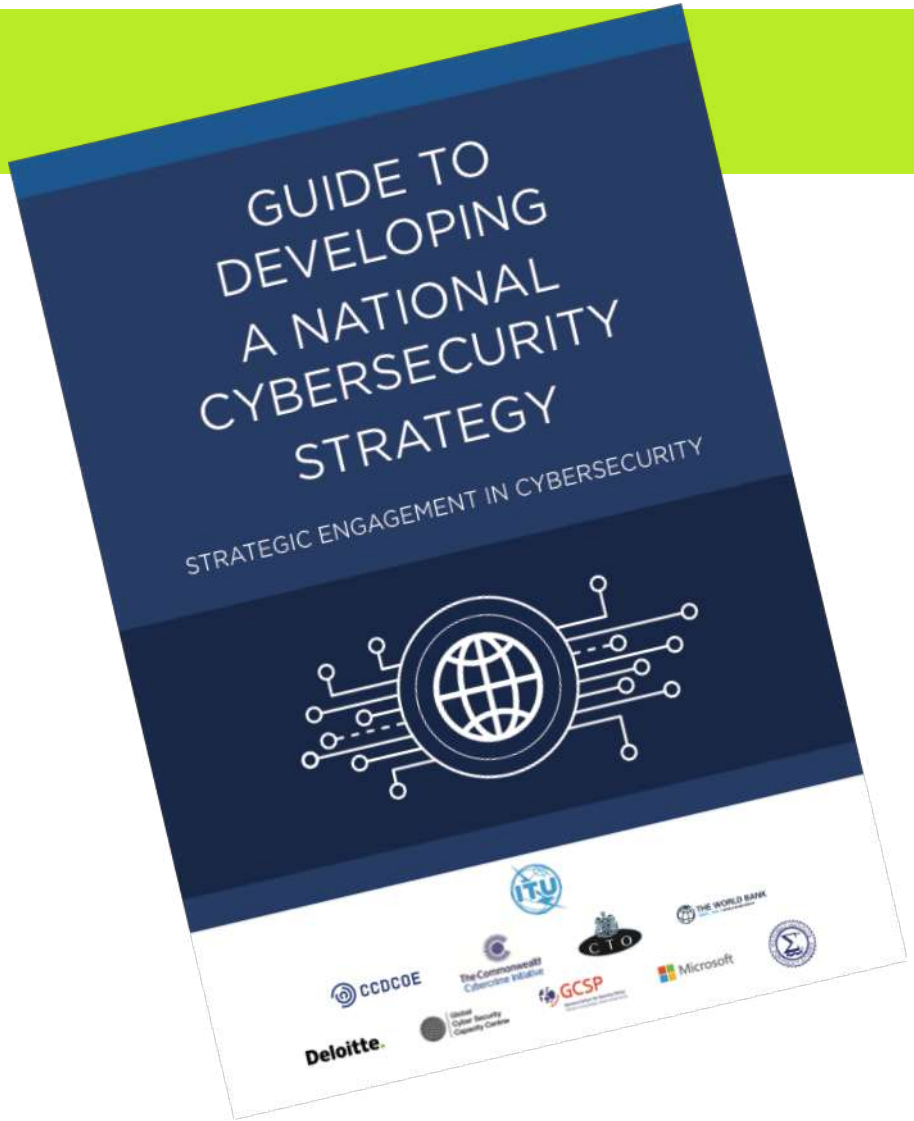
  (k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. **A State should not use authorized emergency response teams to engage in malicious international activity**.

Trust inhibitors

- **Sanctions**

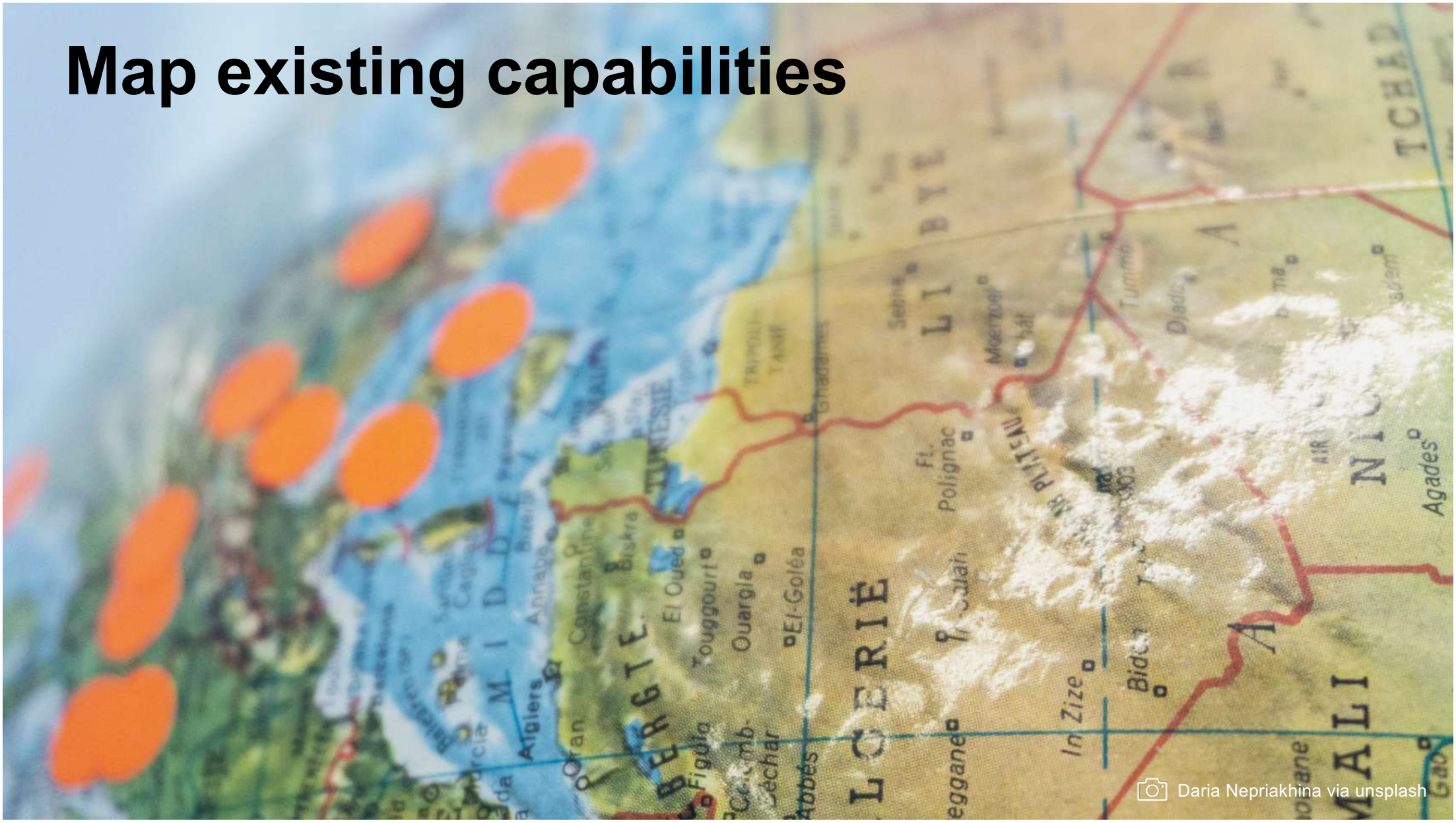

Part II: Developing a CSIRT community

What do you want to achieve?



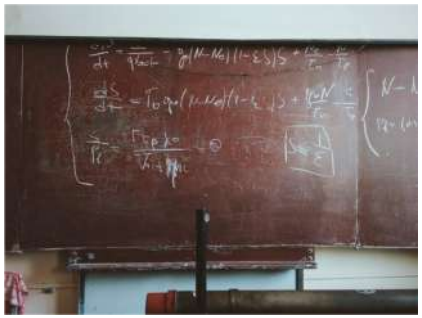
- Protect government assets
- Protect critical Infrastructure
- Resilience of the economy
- Cyber hygiene
- Help citizens

Map existing capabilities



Typical players

ISPs



Research Networks

Registries

Private sector

Example: Large Events

“You absolutely must have everyone on board!”

Cristine Hoepers (CERT.br)

“The Brazilian effort was successful because they had so much practice in collaboration.”

Jacomo Picollini (Team Cymru)

National CSIRT

Better: A CSIRT with a national responsibility.

- Government CERT
- Registry
- NREN

But one **CSIRT of last resort**

Non-state CSIRTs

Example: Microsoft Security Response Center

Maturing CSIRTs

Maturity

Handle incidents

Meet and Greet

Engage

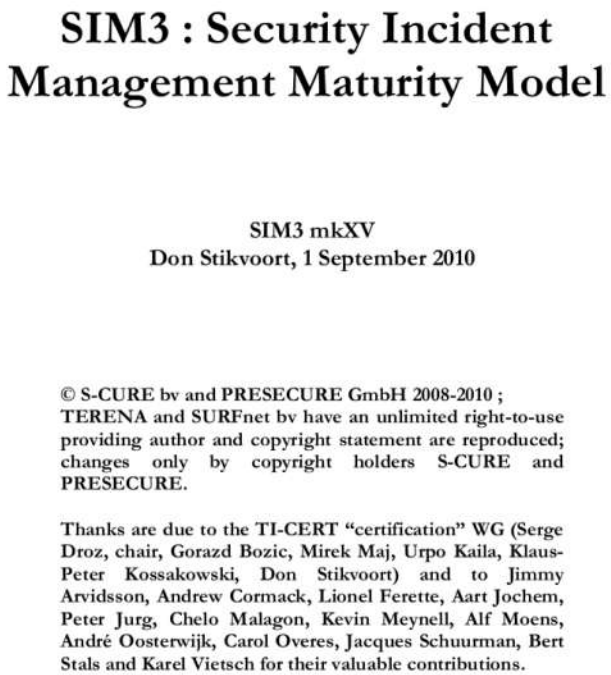
SIM3

Security Incident Management Maturity Model

Measures four groups of parameters
1. Organisational
2. Human
3. Tools
4. Processes

at 5 levels
1. Not available
2. Implicit
3. Explicit internal
4. Explicit formal
5. Controlled

See also
https://www.thegfce.com/initiatives/c/csirt-maturity-initiative



SIM3 : Security Incident Management Maturity Model

SIM3 mkXV
Don Stikvoort, 1 September 2010

Thanks are due to the TI-CERT "certification" WG (Serge Droz, chair, Gorazd Bozic, Mirek Maj, Urpo Kaila, Klaus-Peter Kossakowski, Don Stikvoort) and to Jimmy Arvidsson, Andrew Cormack, Lionel Ferette, Aart Jochem, Peter Jurg, Chelo Malagon, Kevin Meynell, Alf Moens, André Oosterwijk, Carol Overes, Jacques Schuurman, Bert Stals and Karel Vietsch for their valuable contributions.


FIRST™
Improving Security Together