

# European Critical Internet Infrastructure: past, present and future challenges



# Agenda

- Critical Infrastructures and Critical Information Infrastructures
- Large scale incidents
- Criticality of the Internet Infrastructure
- Future research: security and resilience topics

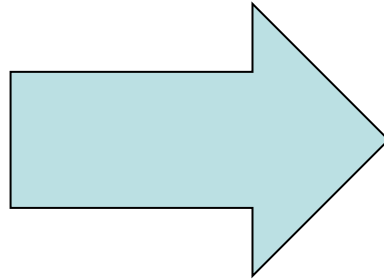
# Agenda

- **Critical Infrastructures and Critical Information Infrastructures**
- Large scale incidents
- Criticality of the Internet Infrastructure
- Future research: security and resilience topics

# Critical sectors and critical ICT assets

## Critical Infrastructures:

- Energy
- Transport
- ICT
- Finance
- Food
- Water
- Safety
- Chemicals



## Critical Information Infrastructures:

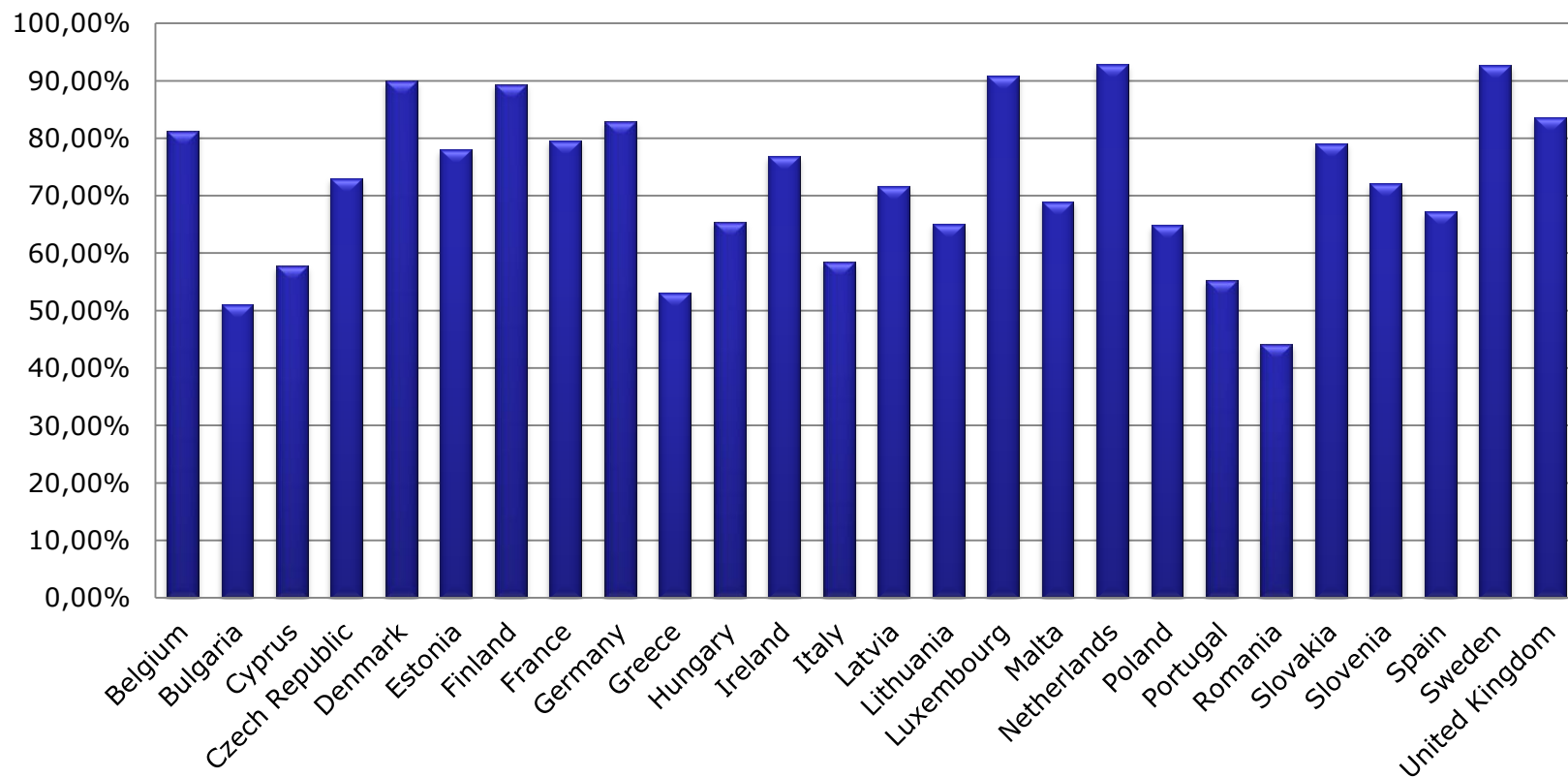
- **Telecommunications**
- Computers/software
- **Internet**
- Satellites
- Etc.

# Critical Internet Infrastructure

ICT systems that are essential for the operation of Internet:

- Physical infrastructure
- Hardware
- Protocols
- Software
- Human infrastructure

## Internet penetration – 30 June 2012



## Average number of users affected, per incident, per service (in 1000s).

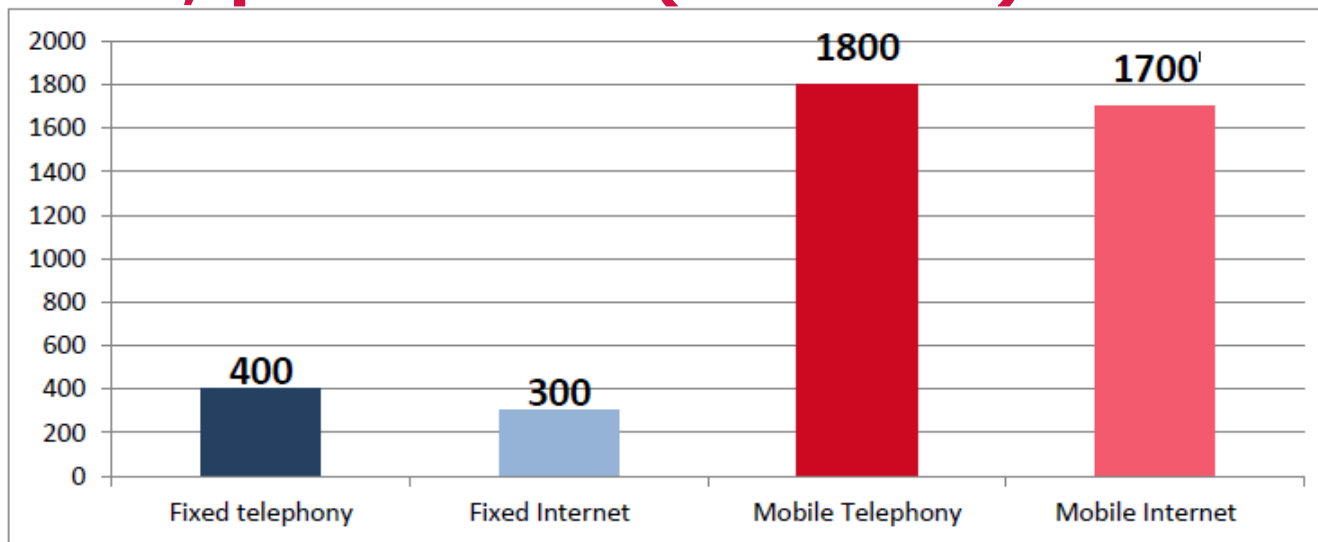
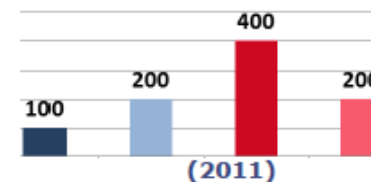


Figure 5 Average number of users affected per incident per service (1000s).



<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012>

# Agenda

- Critical Infrastructures and Critical Information Infrastructures
- **Large scale incidents**
- Criticality of the Internet Infrastructure
- Future research: security and resilience topics



## Recent History – Hurricane Sandy – October 2012

### Massive Flooding Damages Several NYC Data Centers

By: Rich Miller  
October 30th, 2012

 Like 299
  Tweet
  +1
  Share
  Print



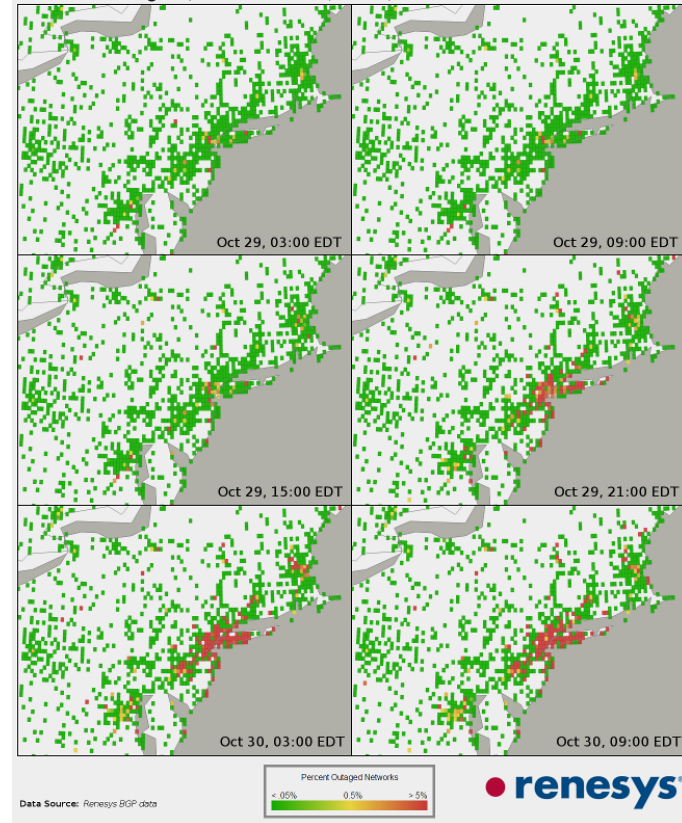
Flooding from Hurricane Sandy has hobbled two data center buildings in Lower Manhattan, taking out diesel fuel pumps used to refuel generators. A third building at 121 Varick is also reported to be without power. There were also reports of outages for some tenants at a major data hub at 111 8th Avenue, and many other New York area facilities were running on generator power amid widespread utility outages.

**NOTE:** For updates on recovery efforts on Wednesday, see our follow-up story, [New York Data Centers Battle Back from Storm Damage](#).

<http://www.datacenterknowledge.com/archives/2012/10/30/major-flooding-nyc-data-centers/>

### Hurricane Sandy

Network Outages (October 29-30, 2012)



<http://www.renesys.com/blog/2012/11/sandys-global-impacts.shtml>

## Recent History – Egypt – March 2013

### Egypt catches divers cutting Internet cable amid disruptions

 Recommend  455 people recommend this. Be the first of your friends.

CAIRO | Wed Mar 27, 2013 5:46pm EDT

(Reuters) - Egypt's coastguard caught three divers cutting through an undersea Internet cable on Wednesday, the army said, the first suggestion criminals might be involved in days of severed connections and disruptions online.

A patrol stopped a fishing boat near the Mediterranean port city of Alexandria and arrested three divers, the army spokesman said on his official Facebook page.


He did not give details of the divers' possible motive in severing the link he said belonged to Egypt Telecom, the country's monopoly landline provider.

"The armed forces foiled an attempt and arrested three divers while they were cutting a submarine cable," he said.

It was not immediately clear whether the incident was related to disruptions off Egypt reported by cable operator SEACOM last week that it said hit several lines connecting Europe with Africa, the Middle East and Asia.

<http://www.reuters.com/article/2013/03/27/net-us-egypt-internet-idUSBRE92Q1AQ20130327>

 Tweet 252

 Share 15

 Share this

 +1 43

 Email

 Print

#### Related News

Egypt needs to fix economy, strike IMF deal: Kerry  
Sat, Mar 2 2013

#### Analysis & Opinion

Target shortage feeds desperate Mideast telco M&A



<https://labs.ripe.net/Members/mirjam/mediterranean-cable-disruption-as-seen-in-ripestat>

# Recent History – Spamhaus – March 2013



HOME BLOG ABOUT US PRODUCTS AND SERVICES NEWS AND PRESS CLIENT PORTAL

## Looking at the spamhaus DDOS from a BGP perspective

Posted by Andree Toonk - March 30, 2013 - BGP instability, Hijack - 1 Comment

It's been a busy week for network engineers world wide, rerouting around broken optical links and of course the [300Gb/s DDOS attack towards Spamhaus and Cloudflare](#). This DDOS has been classified as the [largest DDOS attack ever recorded](#) and has been written about quite a bit in mainstream media.

There's been a bit of discussion about how much this DDOS actually slowed down the Internet globally. Fact is that the Internet didn't come to a halt but the large amount of new traffic that had to be handled by some of the carriers did result in congestion and significant packet loss by some of the Tier1 carriers last weekend. In this blog post we'll look at this event from the routing perspective, what effects did this have on the Internet Exchanges and we'll also look at some BGP hijacks related to this attack.

### BGP hijack affecting Spamhaus

The majority of the attack towards SpamHaus and cloudflare was a brute-force DDOS of attack. But in an attempt to affect spamhaus services different techniques were used, one of them was a BGP hijack by the alleged initiator of the attack. Greenhost.nl has a great description on [their blog](#) about how AS34109 Cyberbunker/CB3Rob (the alleged organizer of the spamhaus attack), announced a more specific route for one of the spamhaus servers: [0.ns.spamhaus.org](#) with IP address 204.16.254.40/32.

## Latest Tweets

### Tweets

Follow

**Freedom of Info 4ALL** @ntisec 13h  
#BGP Route hijacking, till now unreported or even unnoticed. Effects can be Massive! The scale of the problem can only be estimated. #DDOS  
Retweeted by BGPmon.net  
Expand

**Andree Toonk** @atoonk 16 May  
Ooh Look, Syria added an NS record for dot SY. Hosted outside of Syria, and "not" tld.sy.  
[viewwc.generic-nic.netView](#) #DNS #internet  
Retweeted by BGPmon.  
Expand

**Frank Denis** @jedisc1

# traceroute -q1 0.ns.spamhaus.org

traceroute to 0.ns.spamhaus.org (204.16.254.40), 30 hops max, 60 byte packets

```
1  [redacted] 0.190 ms
2  [redacted] 0.394 ms
3  [redacted] 10.967 ms
4  r22.amstn102.nl.bb.gin.ntt.net (195.69.144.36) 1.961 ms
5  ae-2-r03.amstn102.nl.bb.gin.ntt.net (129.250.2.211) 3.695 ms
6  xe-3-0-3.ar1.ams3.nl.nlayer.net (69.22.139.202) 3.700 ms
7  as23352.vlan-102.ar1.ams3.nl.nlayer.net (69.22.139.123) 2.562 ms
8  ge0-4.aggrB3.ams3.nl.scn.net (205.234.220.231) 3.953 ms
9  204.16.254.40 (204.16.254.40) 2.393 ms
```

Route hijacking has happened before, such as when [Pakistan Telecom](#) started announcing itself as the route to YouTube in 2008, but it is still rather unusual.

<http://www.bgpmn.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/>

<https://greenhost.nl/2013/03/21/spam-not-spam-tracking-hijacked-spamhaus-ip/>



## Incidents as source of info

- It is straightforward to divert traffic away from its proper destination by announcing invalid routes -> youtube 2008, china 2010, Spamhaus & banking IP Hijack 2013...
- Latent bugs in BGP implementations can disrupt the system -> Cisco & RIPE unexpected attribute 2010, Juniper 2011...
- In some parts of the world a small number of cable systems are critical -> Egypt 2013
- The system is critically dependent on electrical power -> Hurricane Sandy 2012
- The ecosystem can work well in a crisis -> 9/11, japan earthquake 2011

## Potential adverse events

- Regional failure of other critical infrastructure on which the Internet depends
- Cable cut
- Natural disaster
- Coordinated attack
- Design faults



# Agenda

- Critical Infrastructures and Critical Information Infrastructures
- Large scale incidents
- **Criticality of the Internet Infrastructure**
- Future research: security and resilience topics



# Criticality of the Internet Infrastructure

- Internet of things
- M2M
- Interconnected Mobility
- Smart city
- Communications
- Enterprise networks
- E-government
- E-health



## Current issues

- The lack of good information about the state and behavior of the system
- The scale and complexity of the system
- The dynamic nature of the system



# Assessing the critical Internet Infrastructure

- Identify assets and legal frameworks
- Cross-system dependencies
- Possible point of failures not covered by private sector risk assessments
- National and European-scale complete picture



## Mapping the ecosystem

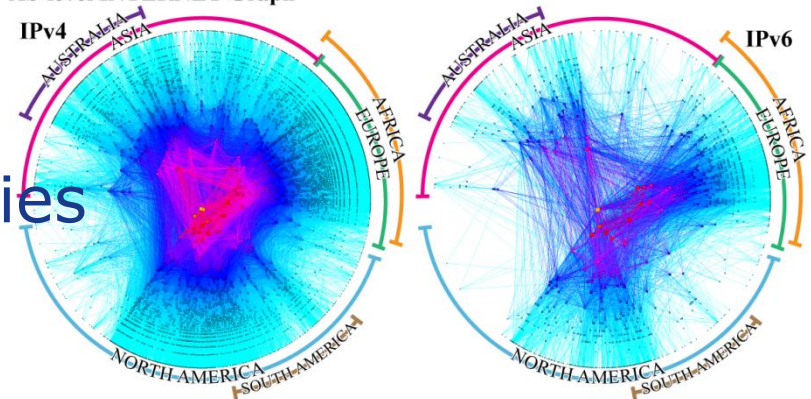
- The physical infrastructure - commercially confidential, sometimes overlap with CNI
- The routing infrastructure – hidden by design, cross borders interdependencies
- The organizational component - different legal frameworks and maturity levels

# How the Internet looks like?

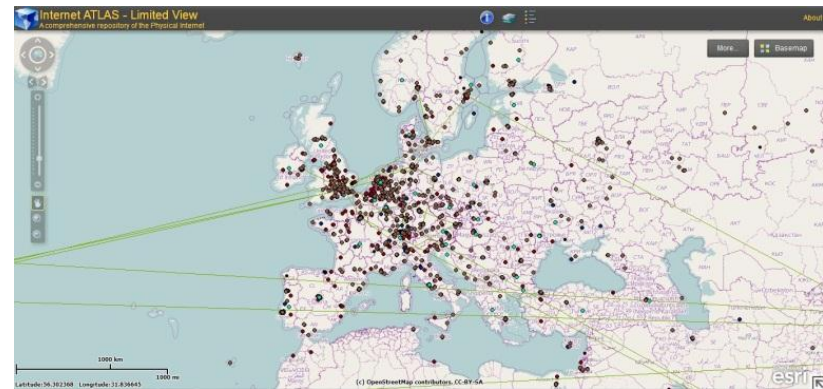
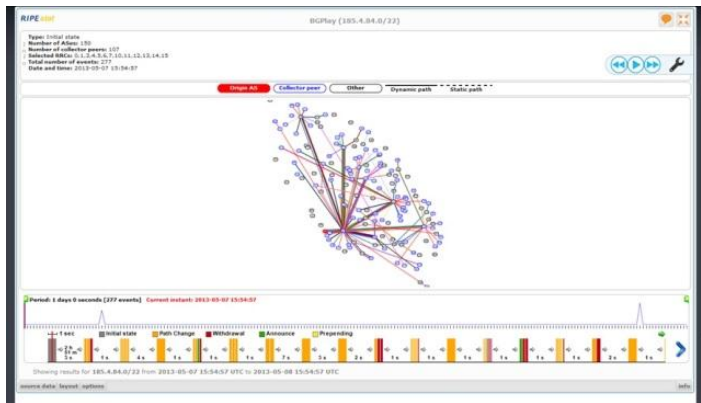
- BGP-derived maps
- AS Router-Level Topologies
- PoP-Level Topologies

CAIDA's IPv4 & IPv6 AS Core  
AS-level INTERNET Graph

Archipelago  
Jan 2013



Copyright 2013 UC Regents. All rights reserved.



# Agenda

- Critical Infrastructures and Critical Information Infrastructures
- Large scale incidents
- Criticality of the Internet Infrastructure
- **Future research: security and resilience topics**

# Metrics and Measurement

- More data:
  - Incident Investigation
  - Network Performance
  - Resilience
- Accurately measure:
  - the structure of the Internet
  - structural properties of the Internet in a changing provider ecosystem

## Policy research

- Common terminology
- Understanding legal frameworks and markets
- Harmonizing approaches
- Define toolset and best practises
- Information sharing frameworks
- Integrated applied research

# Vulnerability research

- Devices
- MPLS
- BGP
- RPKI
  - RPKI-based origin validation
  - Path validation
- DNS
  - DNSSEC

# Risk assessment frameworks for Internet Infrastructures and depending infrastructures

- Mission critical components
- Operational impact analysis
- Disaster recovery plans
- Operational exercises



## Emerging topics

- Integrated inventories (GIS, routing, performance)
- AR and gesture recognition for visualization of complex systems
- Real time monitoring
- Automated tools for impact assessment and scenario identification
- Federation of CI and CII early warning systems

# Network Infrastructure Security and Resilience

*Communication networks  
are the building blocks of the information society*



# Food For Thought

*370 millions of Internet users at 30 June 2012*

*500 millions of potential users*

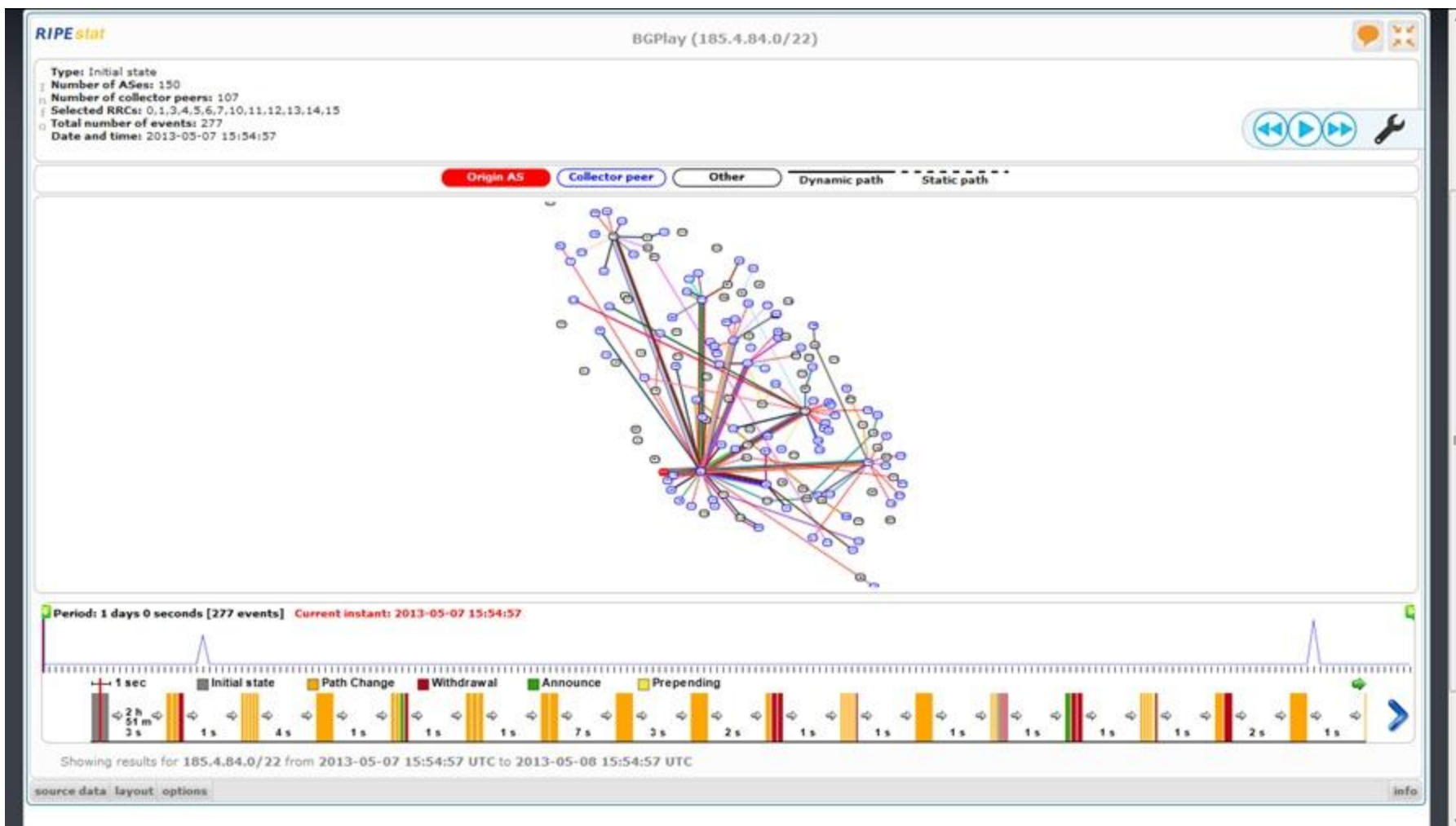


# Thank you

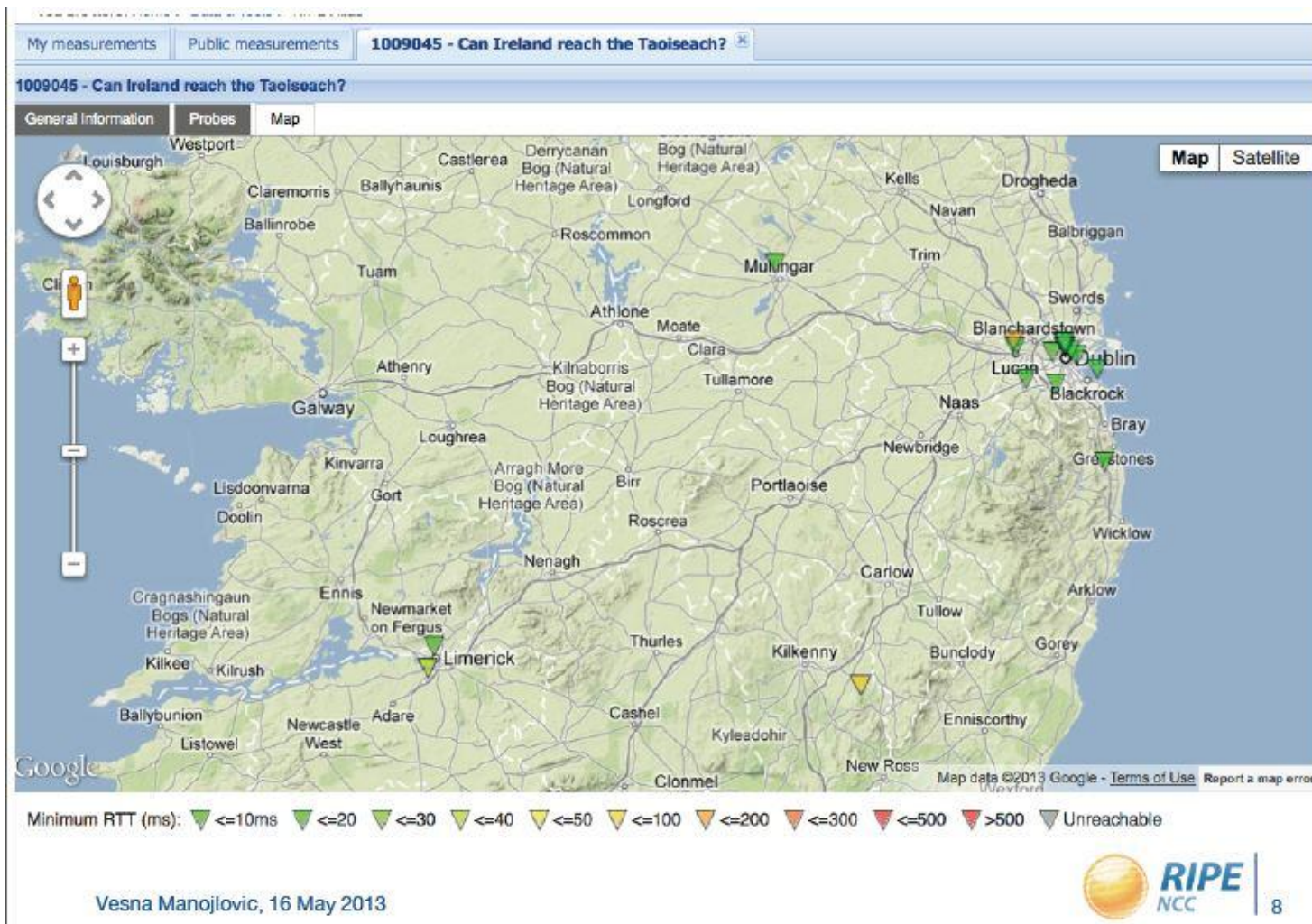
Rossella Mattioli

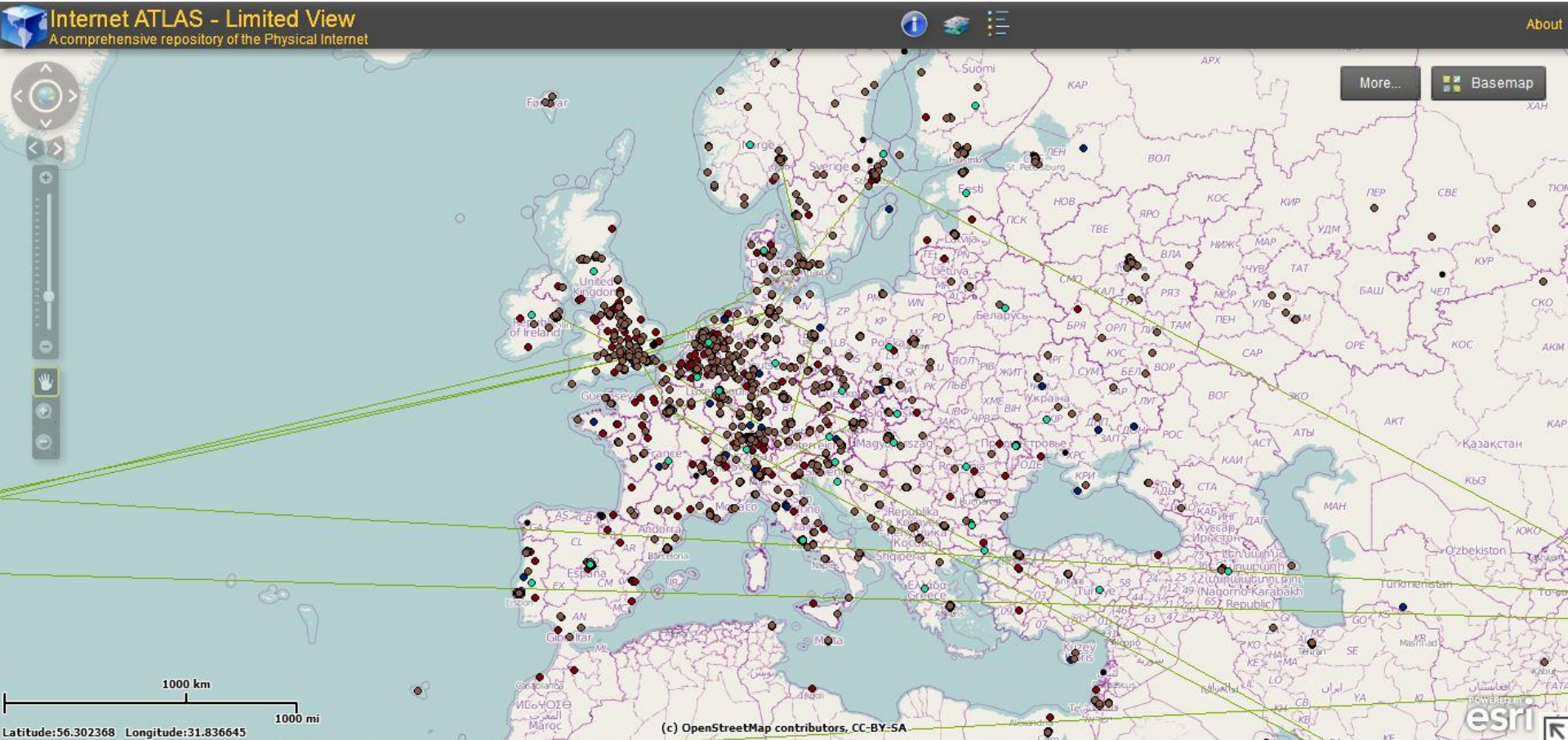
[rossella.mattioli@enisa.europa.eu](mailto:rossella.mattioli@enisa.europa.eu)











## Previous ENISA Work

- 2010 “Secure Routing Technologies” report
- Gives an overview of available technologies and proposed solutions to secure routing



<http://www.enisa.europa.eu/act/res/technologies/tech/routing>



## Previous ENISA Work

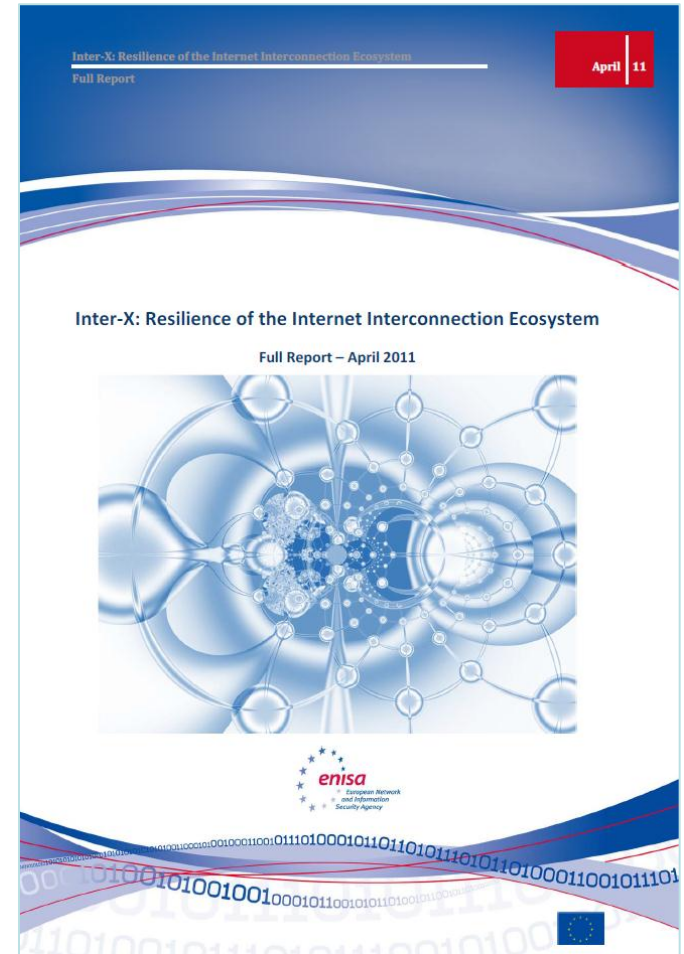
- 2010 “Secure Routing” survey
- Shows that currently there are only few security mechanisms implemented to secure internet routing on the IP layer



<http://www.enisa.europa.eu/act/res/technologies/tech/routing>

## Previous ENISA Work

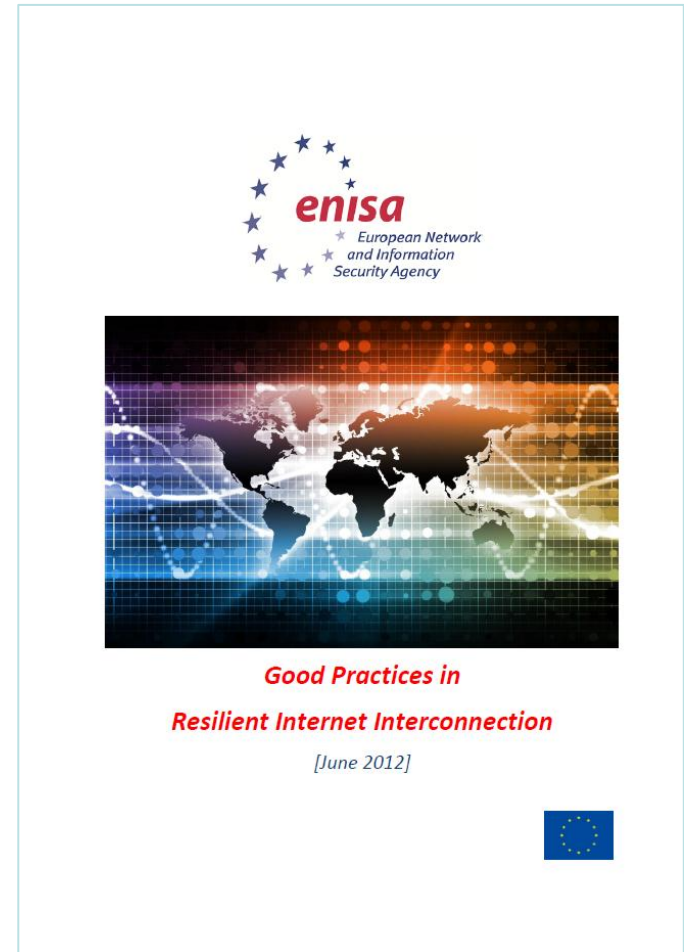
- 2010 study “Resilience of the Internet Interconnection Ecosystem” (aka “Inter-X Report”)
- Large collection of resilience aspects of interconnections on all layers
- Also contains collection of well-known incidents



<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx>

## Previous ENISA Work

- 2011 report “Good Practices in Resilient Internet Interconnection”
- 15 good practices and 11 recommendations for enhancing resilience of internet interconnections
- Recommendation 10: ***Develop techniques to accurately measure the structure of the Internet***



<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/resilience-of-interconnections/report>