

“Internet Mapping” Project

Security and resilience of the European
communications networks



Agenda

- Previous ENISA Work
- Recent History
- 2013 Internet Mapping Project
 - Data
 - Sharing
 - Possible Developments
 - Our goal
- Examples of views
- Your feedback

Agenda

- **Previous ENISA Work**
- Recent History
- 2013 Internet Mapping Project
 - Data
 - Sharing
 - Possible Developments
 - Our goal
- Examples of views
- Your feedback

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

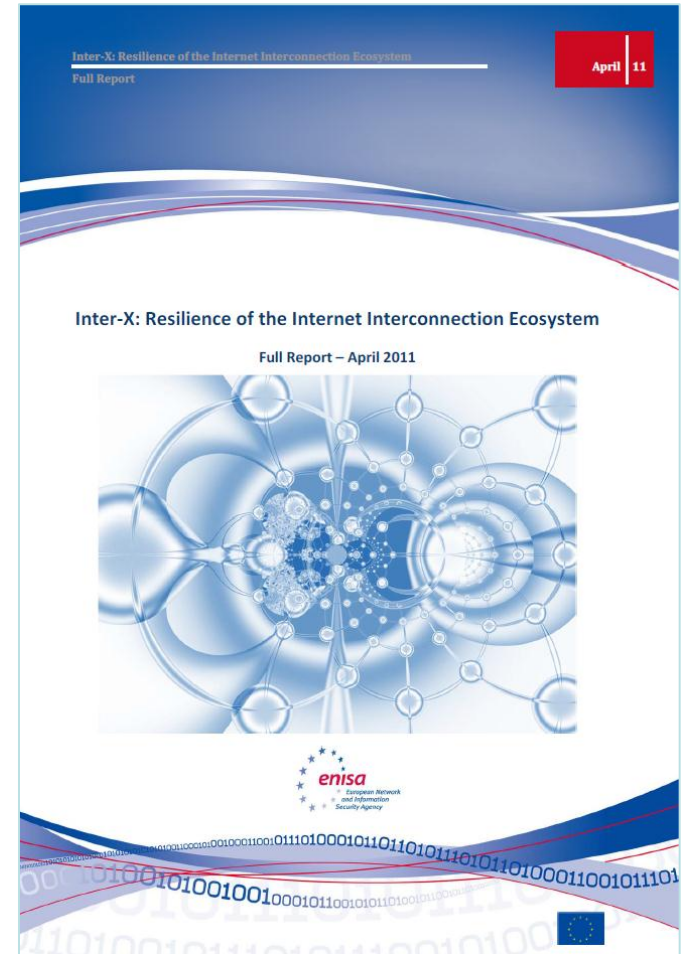
- 2010 “Secure Routing” survey
- Shows that currently there are only few security mechanisms implemented to secure internet routing on the IP layer



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

Previous ENISA Work

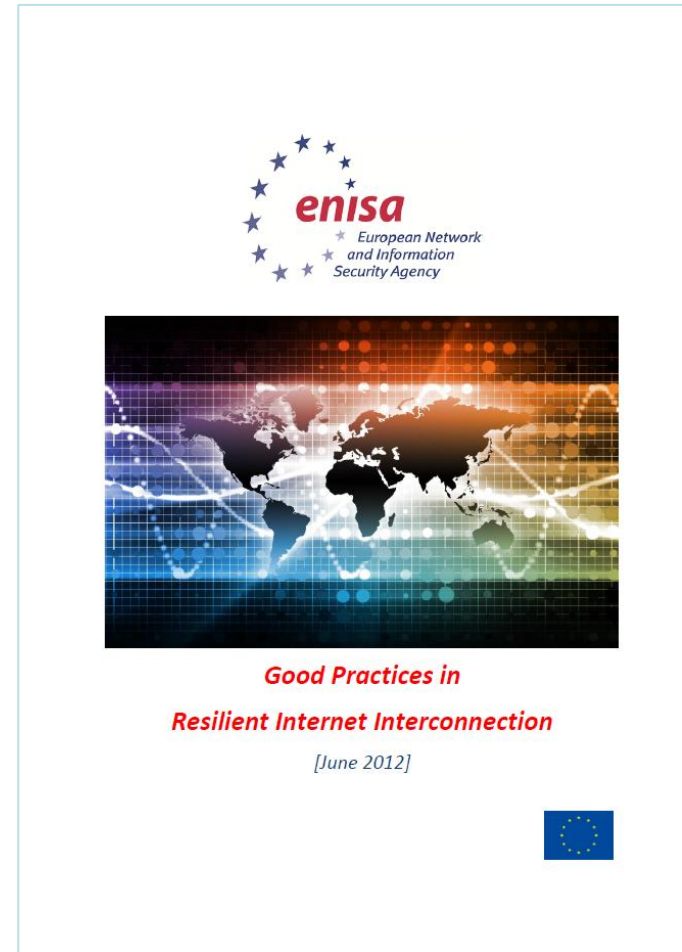
- 2010 study “Resilience of the Internet Interconnection Ecosystem” (aka “Inter-X Report”)
- Large collection of resilience aspects of interconnections on all layers
- Also contains collection of well-known incidents



<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>

Agenda

- Previous ENISA Work
- **Recent History**
- 2013 Internet Mapping Project
 - Data
 - Sharing
 - Possible Developments
 - Our goal
- Examples of views
- Your feedback

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



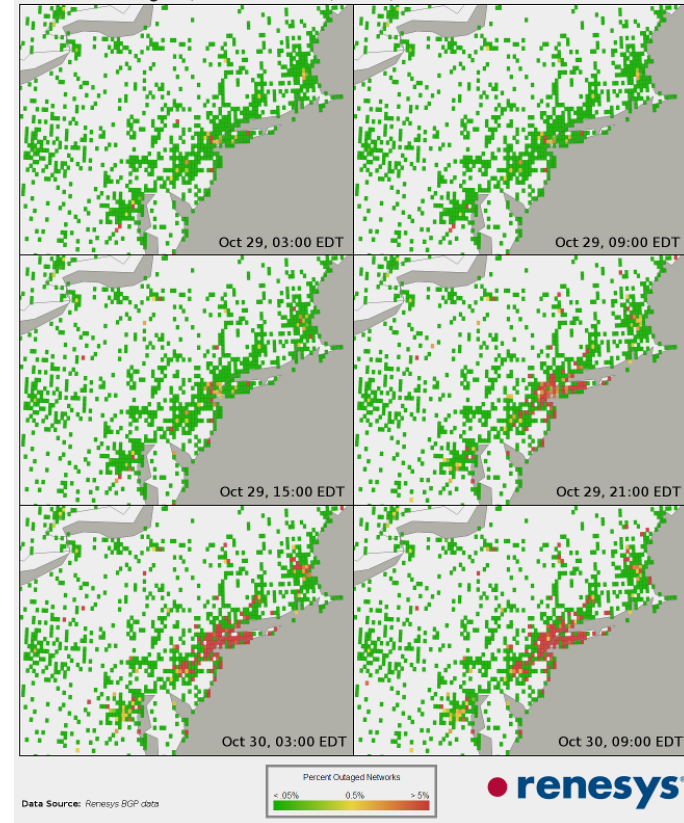
Flooding from Hurricane Sandy has hobbled two data center buildings in Lower Manhattan, taking out diesel fuel pumps used to refuel generators. A third building at 121 Varick is also reported to be without power. There were also reports of outages for some tenants at a major data hub at 111 8th Avenue, 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.net](#) [View #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
```

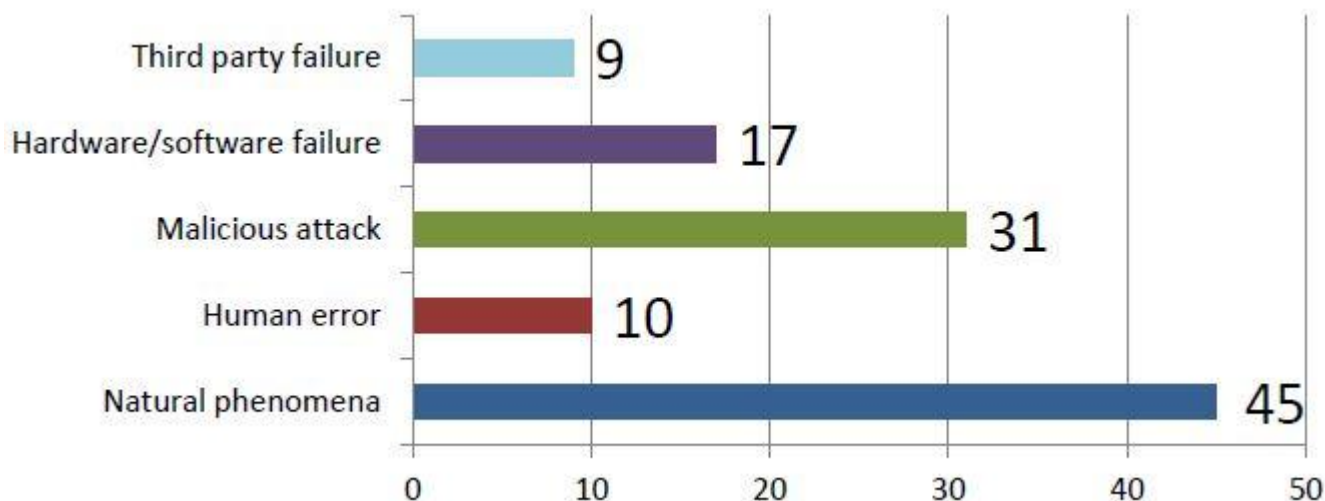
Route hijacking has happened before, such as when [Pakistan Telecom](#) started announcing itself as the route to YouTube in 2008, but it is still rather unusual.

<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/>



Average duration of incidents per root cause category in hours in Europe in 2011



On average incidents caused by natural phenomena lasted longest (45 hours).

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011/at_download/fullReport

Agenda

- Previous ENISA Work
- Recent History
- **2013 Internet Mapping Project**
 - Data
 - Sharing
 - Possible Developments
 - Our goal
- Examples of views
- Your feedback

2013 Internet Mapping Project

- “CIIP relevant” sectors:
 - Banking
 - Energy
 - Logistics
 - Health
- Understanding your national Internet infrastructure can be of help in avoiding and responding to outages and malicious attacks

2013 Internet Mapping Project: Data

- Address IP routing layer first
- Not all relevant information can be easily deduced from a routing table snapshot (e.g. private peerings, backup routes)
- Additional information may be available based on NDA

2013 Internet Mapping Project: Sharing

- Baseline set of results could be shared and compared
 - within a defined community such as CERTs
 - under appropriate NDA
- Learn lessons to improve the overall situation in Europe

2013 Internet Mapping Project: Possibilities for Further Developments

- Extend the view to include e.g.
 - Bandwidth
 - Physical layer
 - Data centres
- Provide a platform to host the “public” part of the analyses set

2013 Internet Mapping Project: Our goal

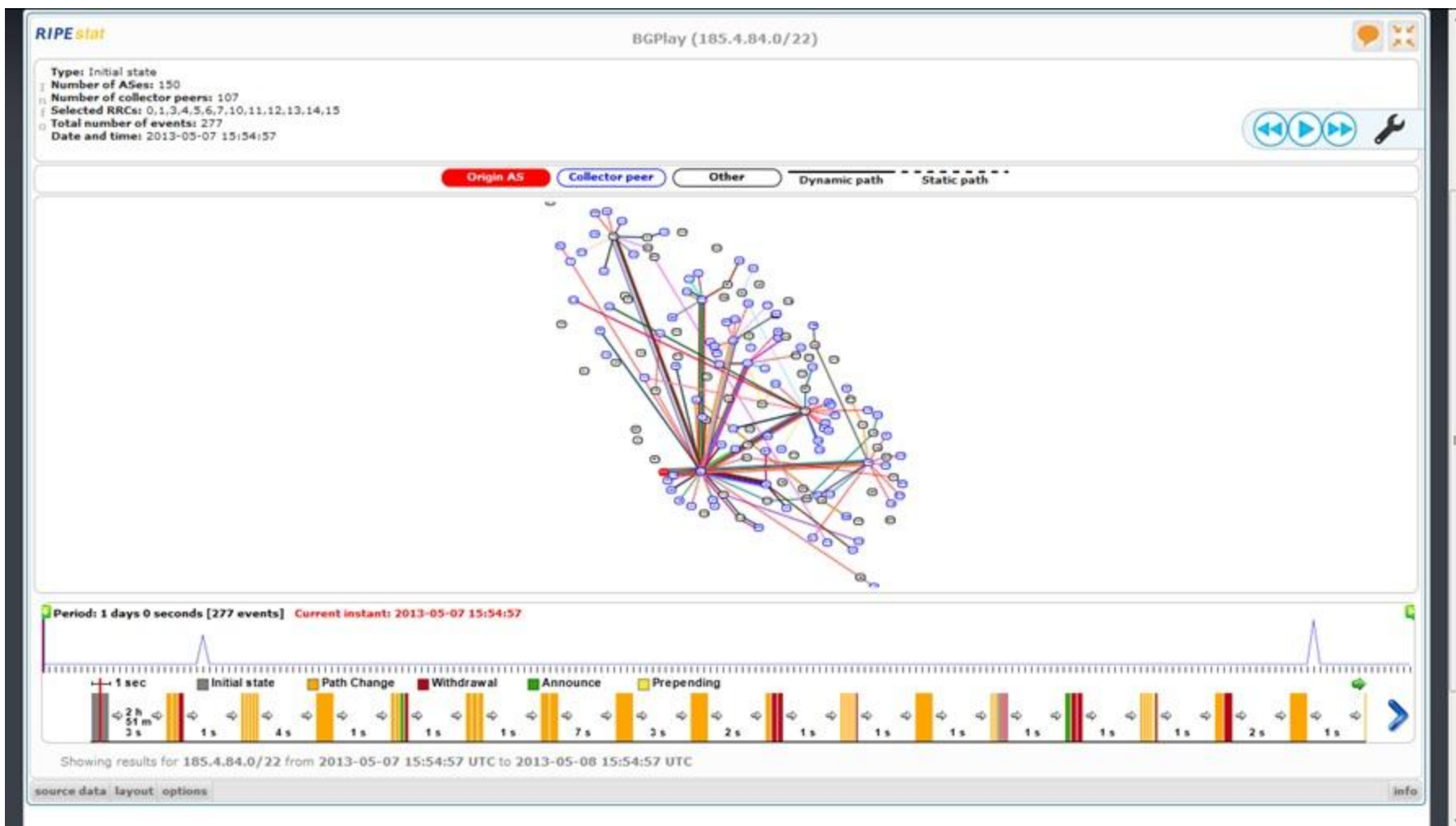
- framework and a step-by-step guide to assess and map “your country Internet infrastructure”
- recommendations to enhance resilience of the Internet infrastructure in your country and EU
- Help you
 - mapping the infrastructure of your constituency
 - responding to this kind of incidents and outages

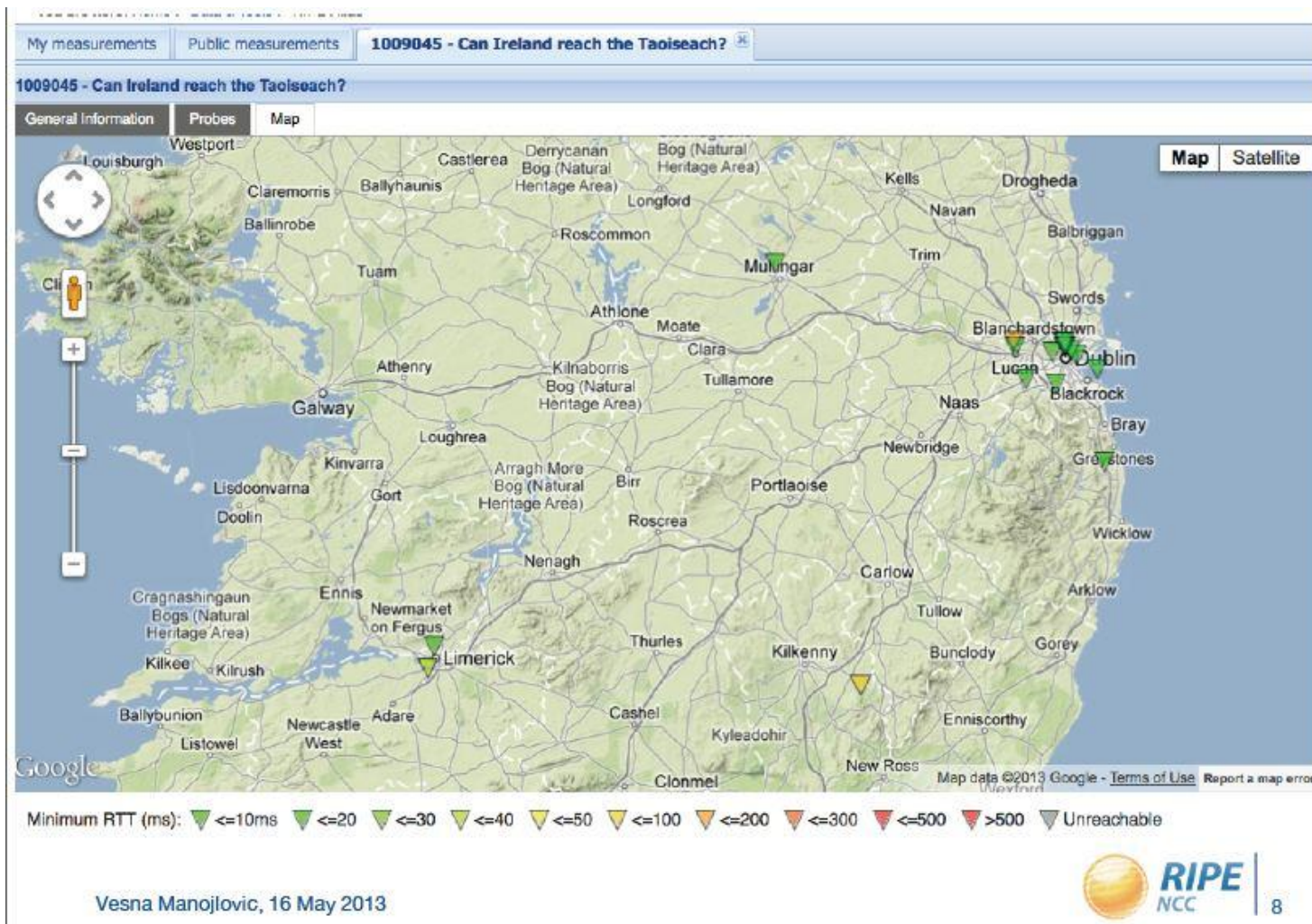
2013 Internet Mapping Project: Your feedback

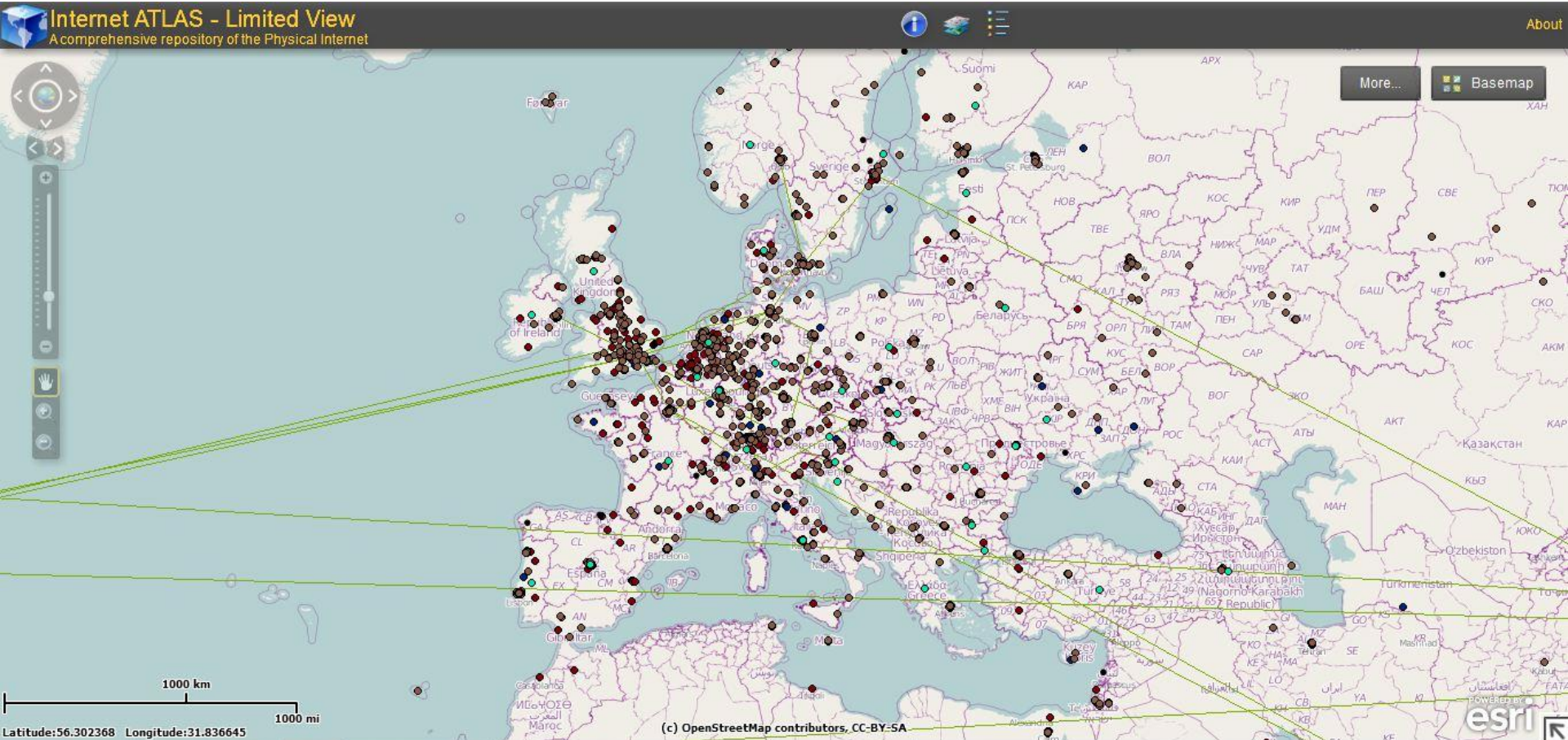
- the existing works and relevant data sources you would like to see in this study
- what do you think you need to know about your national Internet interconnections and constituency
- what do you think you need to collaborate with the other partners (CERTs, LEA, etc.) while facing these kind of outages and incidents

Agenda

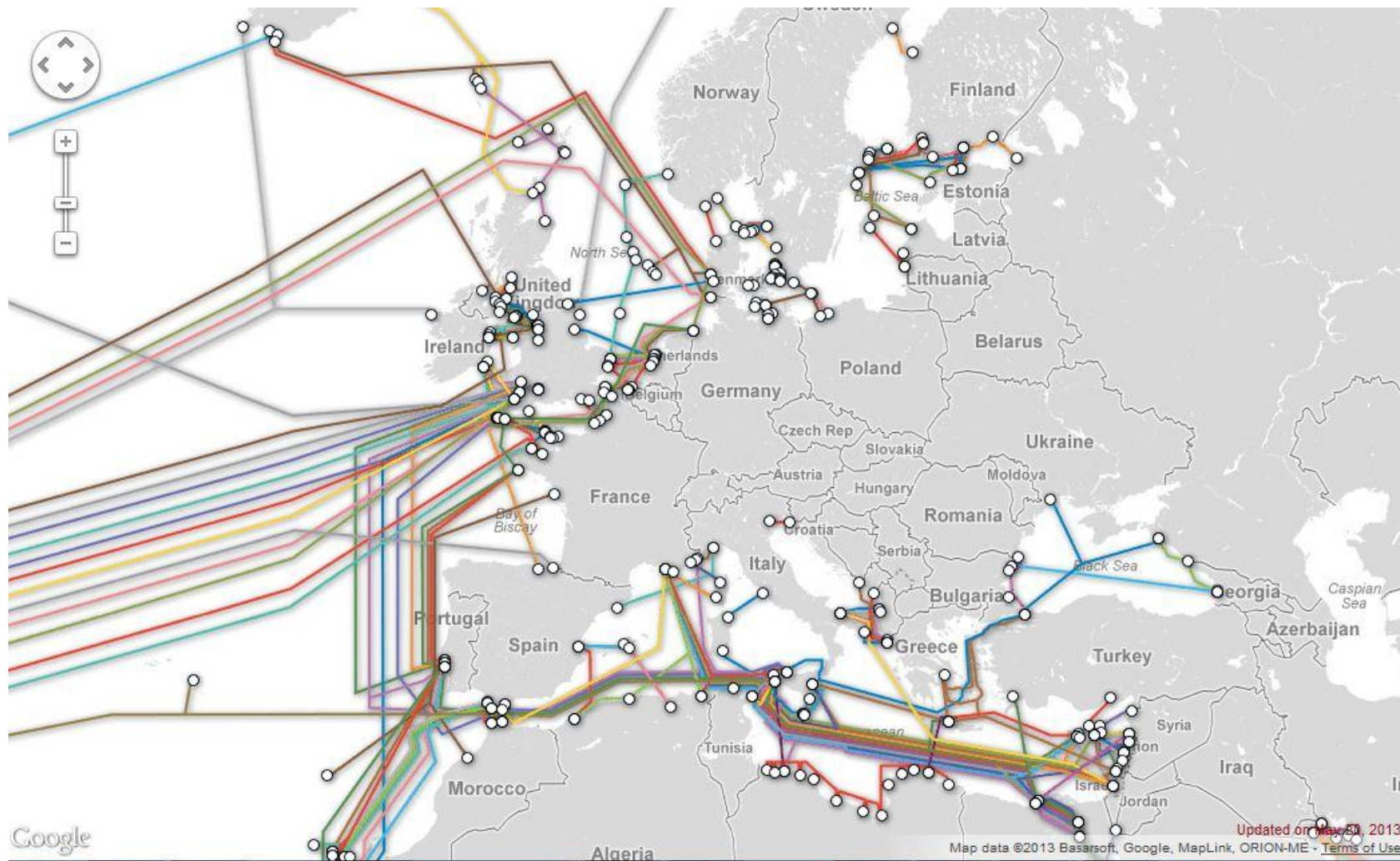
- Previous ENISA Work
- Recent History
- 2013 Internet Mapping Project
 - Data
 - Sharing
 - Possible Developments
 - Our goal
 - **Examples of views**
- Your feedback







Telegeography submarine cable map



Telegeography Internet Exchanges map



Agenda

- Previous ENISA Work
- Recent History
- 2013 Internet Mapping Project
 - Data
 - Sharing
 - Possible Developments
 - Our goal
- Examples of views
- **Your feedback**

2013 Internet Mapping Project: Your feedback

- the existing works and relevant data sources you would like to see in this study
- what do you think you need to know about your national Internet interconnections and constituency
- what do you think you need to collaborate with the other partners (CERTs, LEA, etc.) while facing these kind of outages and incidents

Thank you

Rossella Mattioli

rossella.mattioli@enisa.europa.eu

Thomas Haeberlen

thomas.haeberlen@enisa.europa.eu

