

# Security & Continuity – A joint effort

Jaya Baloo

CISO KPN







## Why?

### ❖ Goal:

A look in our kitchen / behind the scenes

Rethink current beliefs, laws, and maybe tactics

### ❖ Starting points :

Confidentiality and Integrity can only be guaranteed in the presence of Availability

Operators have a complex mix of obligation and rights & not all operators are evil ; but they must all comply with local legal frameworks



# Increase Maturity = Improve Resilience



- BEST IN CLASS
- SMARTER, FASTER, AND BETTER THAN OUR OPPONENTS
- START SECURE; STAY SECURE; RETURN SECURE



## Joint Efforts = A state of Interdependency

### Enhancing infrastructure resilience under conditions of incomplete knowledge of interdependencies

- 1) First step is to inventorize and evaluate known interdependencies
- 2) Second step is to determine response strategy – an evaluation for how inflexible or adaptive the response can be
- 3) Final step is to put measures in place to improve both response and resiliency and methods for evolution

Good examples::

- ❖ Energy – NSTAC Example in the US
- ❖ Regional Roaming in the Netherlands
- ❖ Dutch Continuity Board

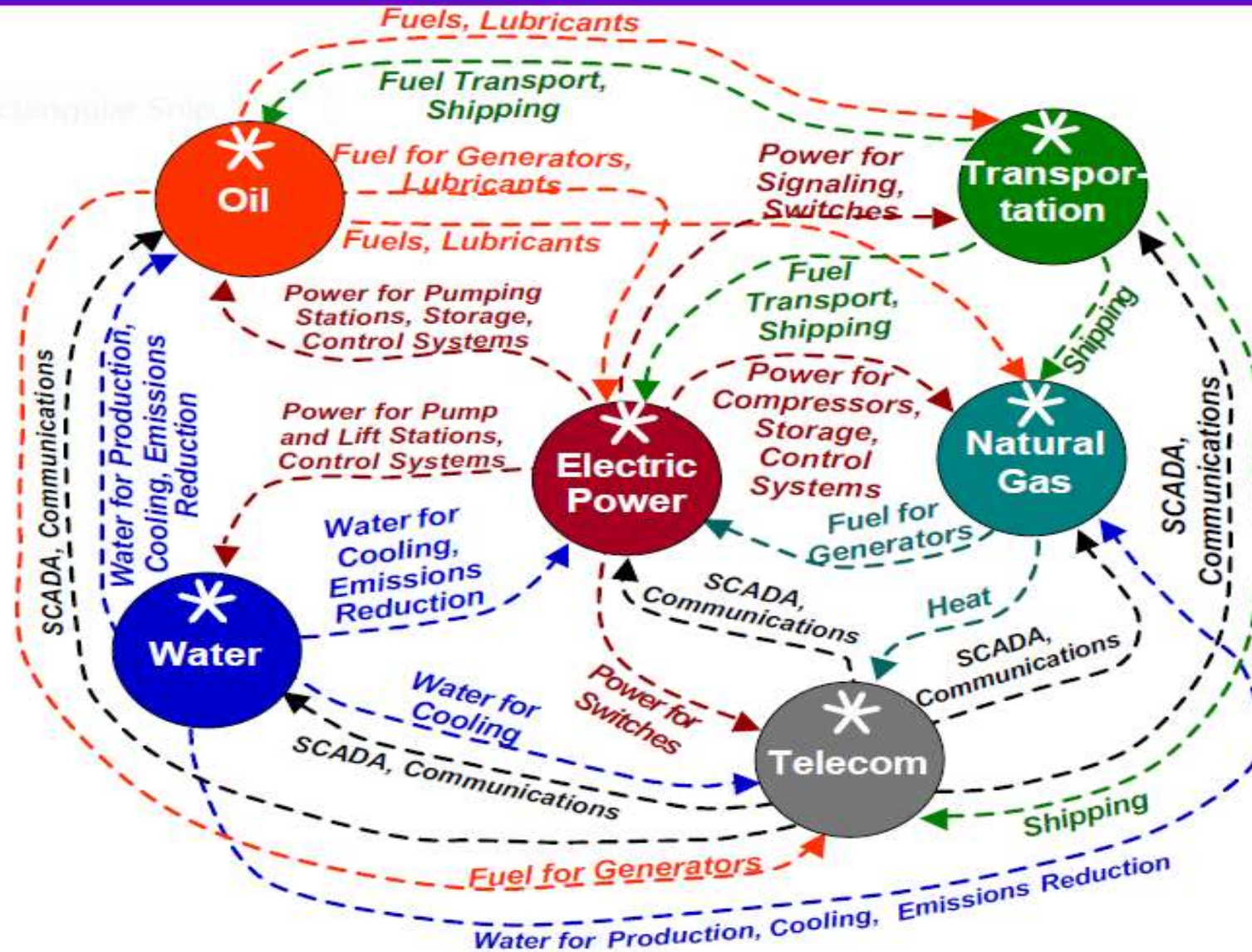


## Context :: Definition Levelling

- Physical: Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other (*electricity outage*)
- Cyber: An infrastructure has a cyber interdependency if its state depends upon information transmitted through the information infrastructure (*routing disruption*)
- Geographic: Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them (*threat ie.- earthquake*)
- Logical: Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection



# Overview of Inter -sectoral dependencies





## Example of inter dependencies within telecom sector: SS7 Signalling in Mobile Networks

### **SS7 = The nervous system of mobile networks**

- Signalling in mobile is based upon SS7
- All the information needed to operate a mobile network. User, services, session and location information
- A 300 pager with different signaling messages
- There little to no security in SS7

### **HLR = The brain of the nervous system**

- Home Location Register
  - User aware
  - Location aware
  - Service aware







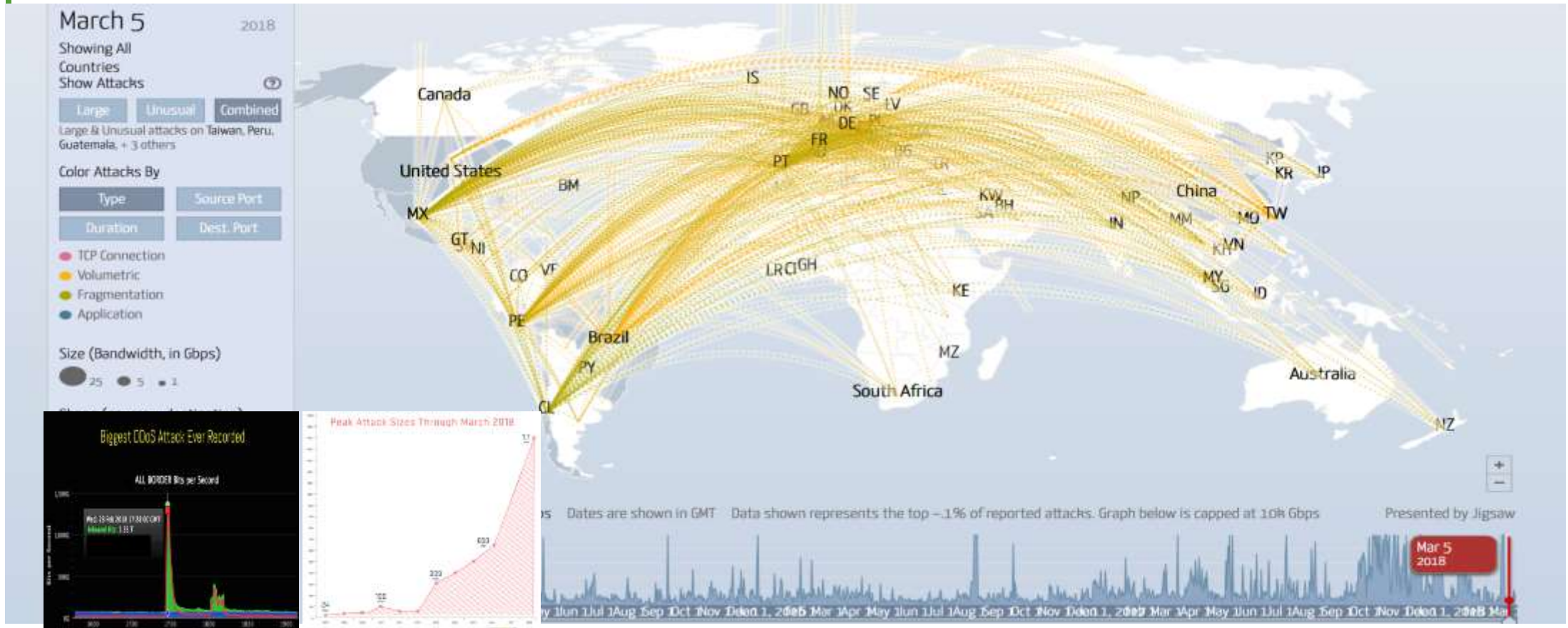
## Issues resolution through Inter-operator cooperation

### Follow standards and truly work together in ops

- Anti –Spoofing = BCP 38
  - ingress filtering as a technique to ensure that incoming packets are actually from the networks from which they claim to originate
- Routing Resilience Manifesto (MANRS)
  - Provide a framework for ISPs to better understand and help address issues related to resilience and security of the Internet's global routing system
- Hierarchical Protocols – DNS; NTP ; CAs
- Upstreams embrace RPKI – BGP : DNS SEC for DNS
- NTP & use of Atomic Clocks
- Internet Abuse = Abuse –IX cooperation
- Mobile Abuse and resilience = GSMA
- Hardware & Software vendors – more a dependency than an interdependency



# When devices collude...it can escalate quickly



- Annoying DDoSs – Volumetric and Multi-Vector increase – IOT devices
- Price to hire and fire attacks is reducing and cost to defend is reaching exponential insanity



[WWW.DCBOARD.NL](http://WWW.DCBOARD.NL)



# Dutch Continuity Board

Protecting The Netherlands against DDoS attacks.

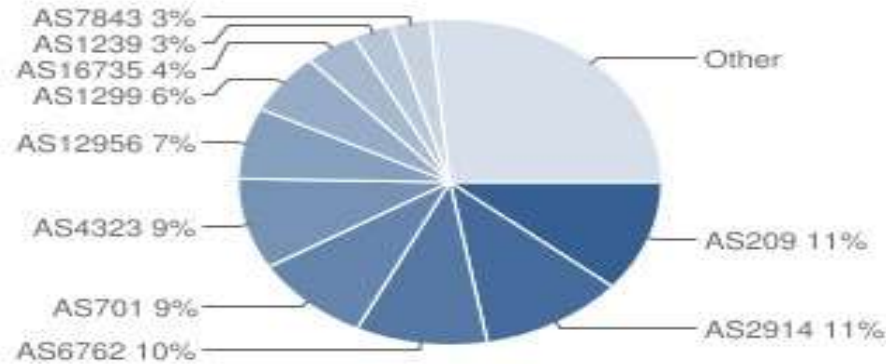
[About us](#)

[How we work](#)



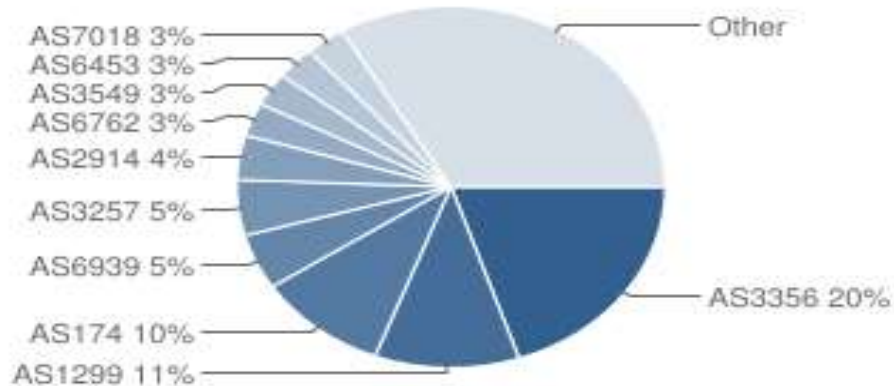
# Inter-operator cooperation -- Routing Diversity as an Asset

AS6830 IPv4 Peers



ASN	Name
<a href="#">AS209</a>	<a href="#">Qwest Communications Company, LLC</a>
<a href="#">AS2914</a>	<a href="#">NTT America, Inc.</a>
<a href="#">AS6762</a>	<a href="#">TELECOM ITALIA SPARKLE S.p.A.</a>
<a href="#">AS701</a>	<a href="#">Verizon Business/UUnet</a>
<a href="#">AS4323</a>	<a href="#">tw telecom holdings, inc.</a>
<a href="#">AS12956</a>	<a href="#">Telefonica International Wholesale Services, SL</a>
<a href="#">AS1299</a>	<a href="#">TeliaSonera AB</a>
<a href="#">AS16735</a>	<a href="#">ALGAR TELECOM S/A</a>
<a href="#">AS1239</a>	<a href="#">Sprint</a>
<a href="#">AS7843</a>	<a href="#">Time Warner Cable Internet LLC</a>

AS286 IPv4 Peers



ASN	Name
<a href="#">AS3356</a>	<a href="#">Level 3 Communications, Inc.</a>
<a href="#">AS1299</a>	<a href="#">TeliaSonera AB</a>
<a href="#">AS174</a>	<a href="#">Coqent Communications</a>
<a href="#">AS6939</a>	<a href="#">Hurricane Electric, Inc.</a>
<a href="#">AS3257</a>	<a href="#">Tinet SpA</a>
<a href="#">AS2914</a>	<a href="#">NTT America, Inc.</a>
<a href="#">AS6762</a>	<a href="#">TELECOM ITALIA SPARKLE S.p.A.</a>
<a href="#">AS3549</a>	<a href="#">Level 3 Communications, Inc. (GBLX)</a>
<a href="#">AS6453</a>	<a href="#">TATA COMMUNICATIONS (AMERICA) INC</a>
<a href="#">AS7018</a>	<a href="#">AT&amp;T Services, Inc.</a>

Operators have different upstream providers which broadens their view on the source of the attack



# SHUT IT DOWN – If we know – we must act!

Google search results for "stresser booter".

About 63,300 results (0,21 seconds)

- Str3ssed Booter - Best IP Booter**  
<https://str3ssed.me> - Best IP Stresser  
 Str3ssed Booter is hard hitting strongest ip at booter with consistent network power of 250G
- CloudStress - Best IP Stresser /**  
<https://cloudstress.com/>  
 CloudStress is a hard hitting and reliable IP a
- Bootyou**  
<https://bootyou.net/>  
 The cheapest & strongest stresser / booter | Servers, IPLogger (youtube, gyszo & imgur),
- IP Stresser / Booter: CyberStres:**  
<https://cyberstress.net/>  
 Layer7 Stresser - Strongest Booter Layer7 &
- DDoS for Hire | Booter, Stresser**  
<https://www.incapsula.com/ddos/booters-a>  
 Masking as stress testers, DDoS-for-hire serv evolution of the Web, crippling the innovation
- XyZ Booter/Stresser - TOP 1 IP :**



CAIDA Center for Applied Internet Data Analysis

Search CAIDA DONATE

PROJECTS FUNDING

Overview Repositories

Download FAQ |  
 by AS Results by Country Results by Provider  
 route |

show non-remediated spoofing Change filters

**Spoof status key**

received.  
 received, but the source address was changed en route.  
 not received, but unspoofed packet was.  
 not received, but unspoofed packet was.  
 this IP block indicates a switch from allowing spoofing to blocking it.  
 unspoofed packet was received.

**Booter-black-List**

To collect an extensive list of E

Python ★ 2 🍷 2

AS	Spoof Private	Spoof Routable	Adjacency Spoofing	Results
AS	rewritten	received	/8	<a href="#">Report</a>
AS	rewritten	received	/8	<a href="#">Report</a>
AS	rewritten	received	/8	<a href="#">Report</a>
AS	rewritten	received	/29	<a href="#">Report</a>
AS	blocked	received	/8	<a href="#">Report</a>
AS	rewritten	received	none	<a href="#">Report</a>
AS	blocked	received	/8	<a href="#">Report</a>
AS	rewritten	received	/8	<a href="#">Report</a>
AS	rewritten	received	none	<a href="#">Report</a>

646342 | 2018-10-01 07:19:36 | 17 138 138 v/24 | 67868 JETISIX.AS | nld (Netherlands) |



# Hardware & Software caught in the balance of global conflict







10

01

0100010

belgacom

**Regin: Top-tier espionage tool enables stealthy surveillance**

Symantec Security Response

Version 1.0 – November 24, 2014



1





## Sound Advice

- Results show that a strategy of constructing redundant interdependencies may be the most robust option for a financially constrained infrastructure operator.
- Cumulative effect of marginal gains in the cyber realm:
  - Identify and stop vulnerabilities, malware, and abuse
  - Deploy robust and secure protocols
  - Limit hierarchical uncertainties by signing information and creating backup paths and redundancy
  - Embrace diversity but with proportionality in regards to simplicity
  - Distributed architecture is a truly internet model



# Use the Security Life Cycle vigorously across the information security and continuity domains



# Our Mission



**Our mission** is to keep KPN reliable & secure and trusted by customers, partners and society

How we will do so :

- Use the **prevent-detect-respond-verify** security life cycle vigorously across the information security and continuity domains as defined by the KPN Security Policy (KSP)

What we will achieve :

- Delivering secure **products & services** to our customers
- Providing **thought leadership** in the field of security.





**In time of peace prepare  
for war.**

Publius Flavius Vegetius Renatus



**THANK YOU!**  
Questions? Comments? Stuff?

[Jaya.baloo@kpn.com](mailto:Jaya.baloo@kpn.com)

@jayabaloo

