Security & Continuity – A joint effort

Jaya Baloo
CISO KPN


CISO

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 interdepencies
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

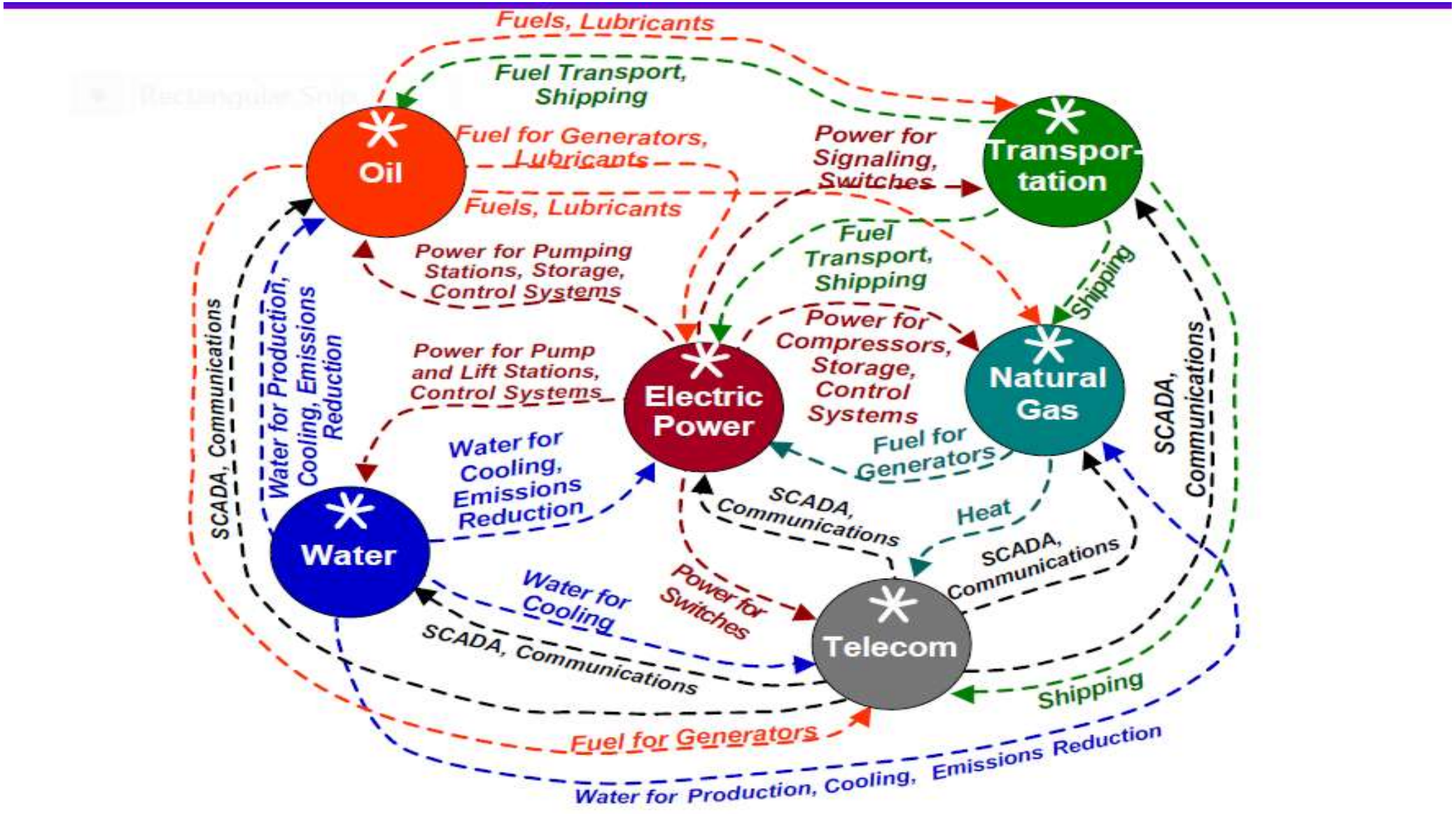
Good examples::

- 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 -sectortal 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

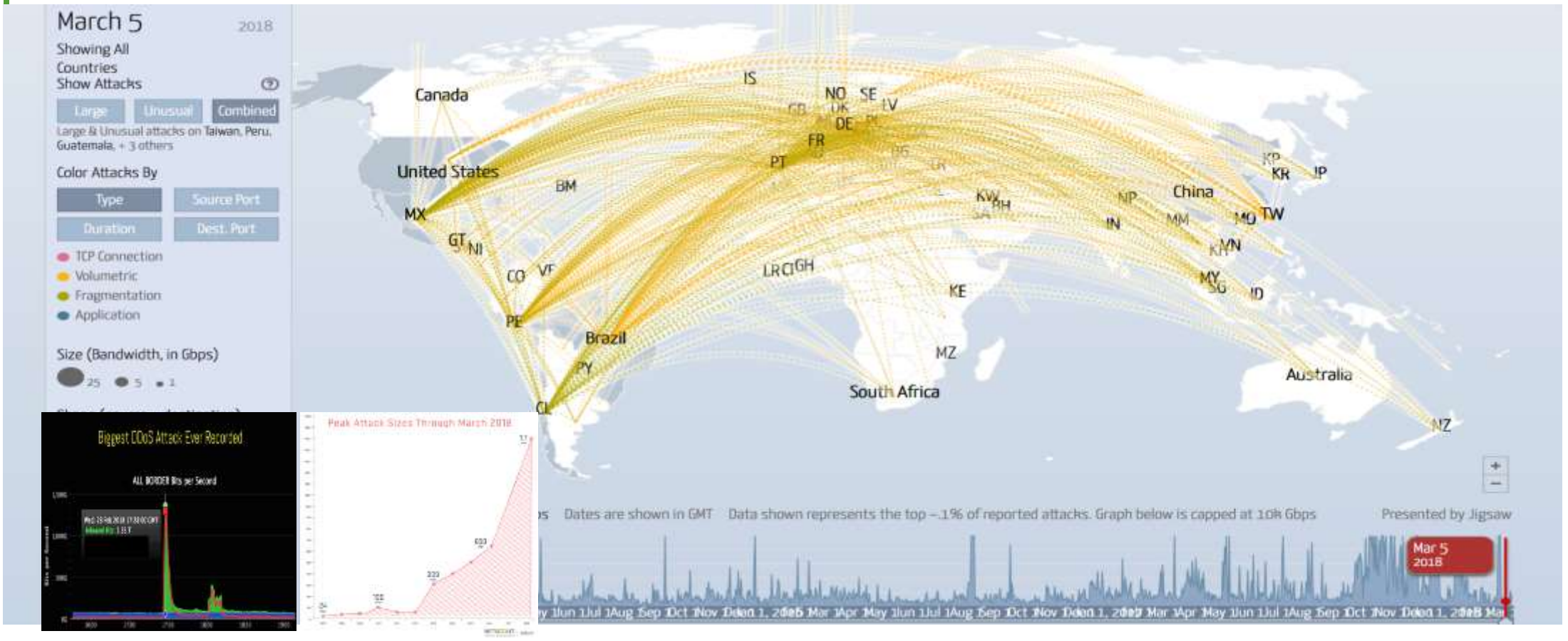
HLR = The brain of the nervous system

- 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 resilance = GSMA
- Hardware & Software vendors – more a dependency than an interdependancy

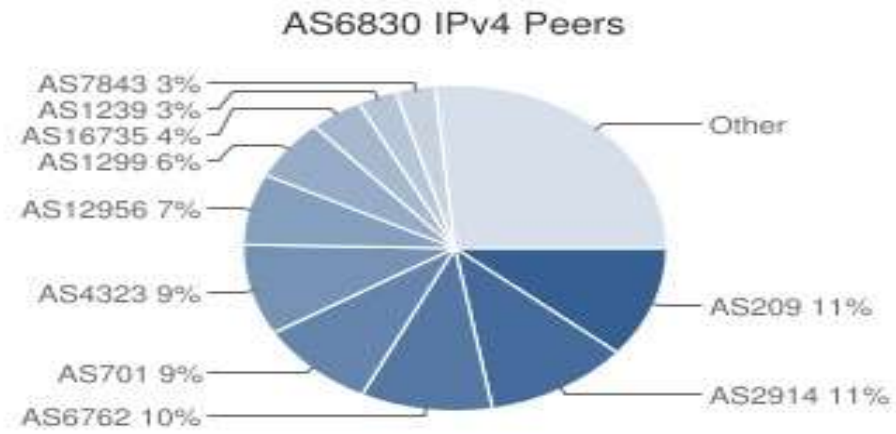
When devices collude….it can escalate quickly



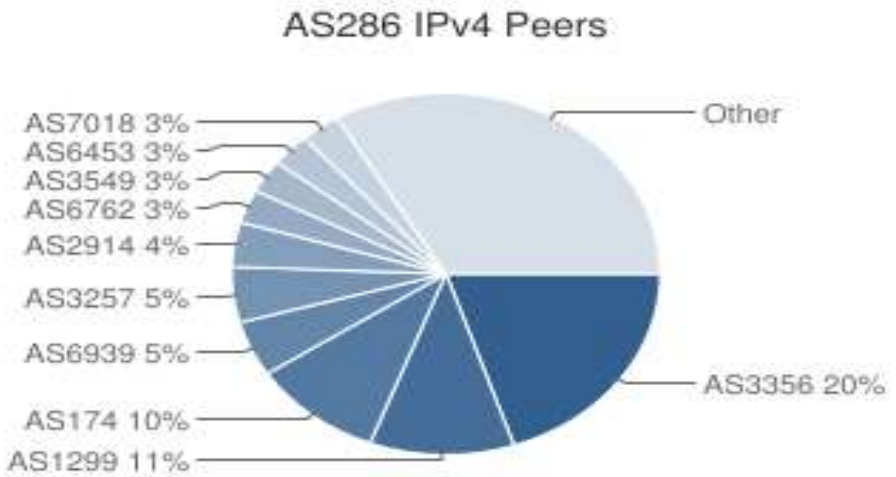
- Annoying DDOSs – Volumetric and Multi-Vector increase – IOT devices
- Price to hire and fire attacks is reducing and cost to defend is reaching exponential insanity

WWW.DCBOARD.NL

Inter-operator cooperation -- Routing Diversity as an Asset



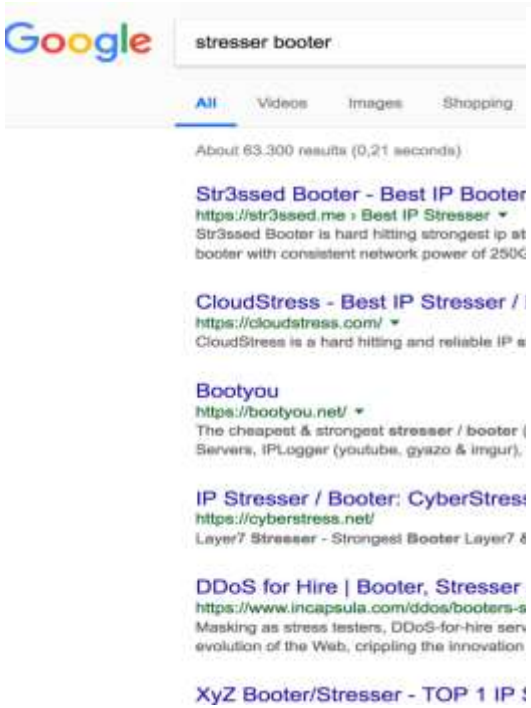
ASN	Name
AS209	Qwest Communications Company, LLC
AS2914	NTT America, Inc.
AS6762	TELECOM ITALIA SPARKLE S.p.A.
AS701	Verizon Business/UUnet
AS4323	tw telecom holdings, inc.
AS12956	Telefonica International Wholesale Services, SL
AS1299	TeliaSonera AB
AS16735	ALGAR TELECOM S/A
AS1239	Sprint
AS7843	Time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

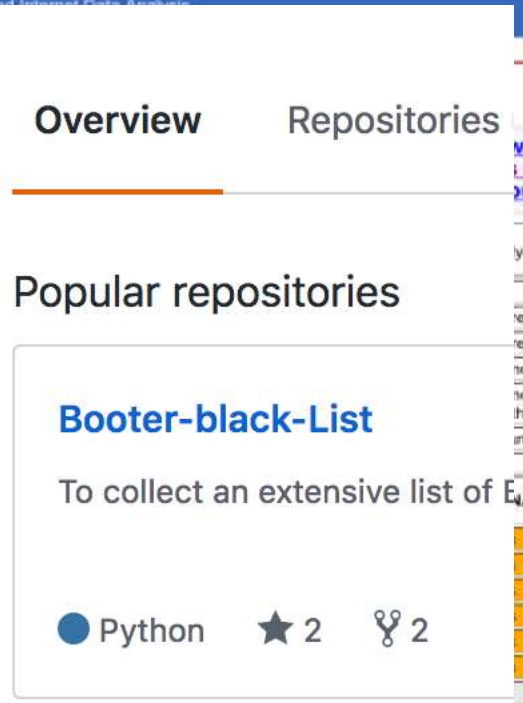


ASN	Name
AS3356	Level 3 Communications, Inc.
AS1299	TeliaSonera AB
AS174	Cogent Communications
AS6939	Hurricane Electric, Inc.
AS3257	Tinet SpA
AS2914	NTT America, Inc.
AS6762	TELECOM ITALIA SPARKLE S.p.A.
AS3549	Level 3 Communications, Inc. (GBLX)
AS6453	TATA COMMUNICATIONS (AMERICA) INC
AS7018	AT&T Services, Inc.

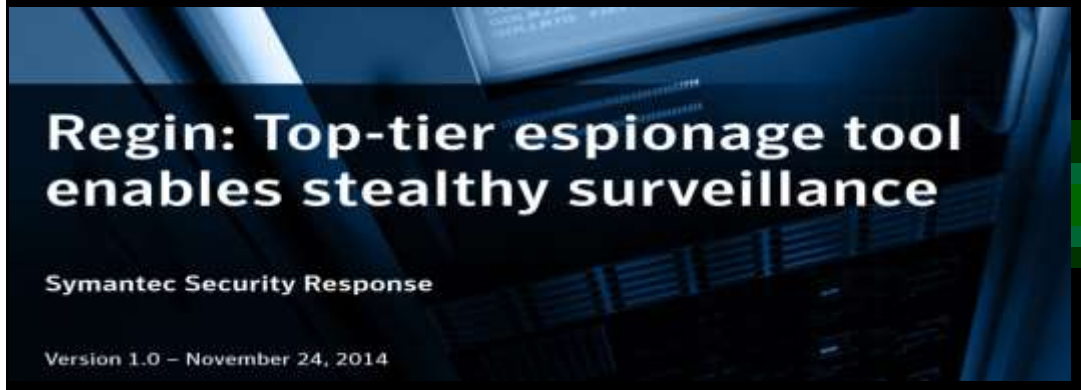
Operators have different upstream providers which broadens their view on the source of the attack

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





Hardware & Software caught in the balance of global conflict



belgacom

GCHQ

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

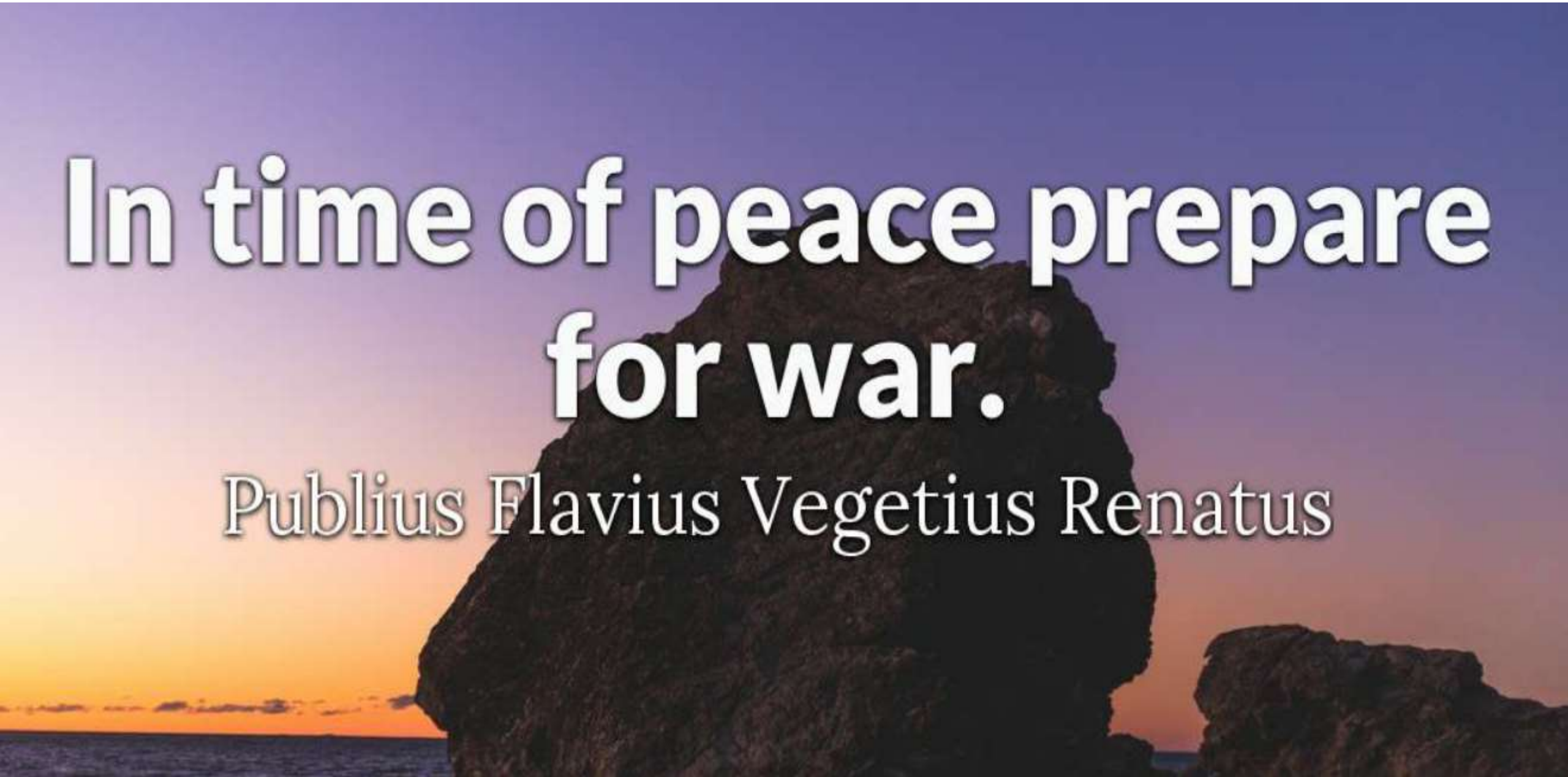
Our mission is to keep KPN reliable & secure and trusted by customers, partners and society

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

@jayabaloo