Worldwide Security and Resiliency of Cyber Infrastructures: the Role of the Domain Name System

Dr. Igor Nai Fovino

Head of the Research Department
Global Cyber Security Center

The Global Cyber Security Center, is an International not-for-profit Foundation entirely dedicated to Cyber Security

GLOBAL CYBER SECURITY CENTER

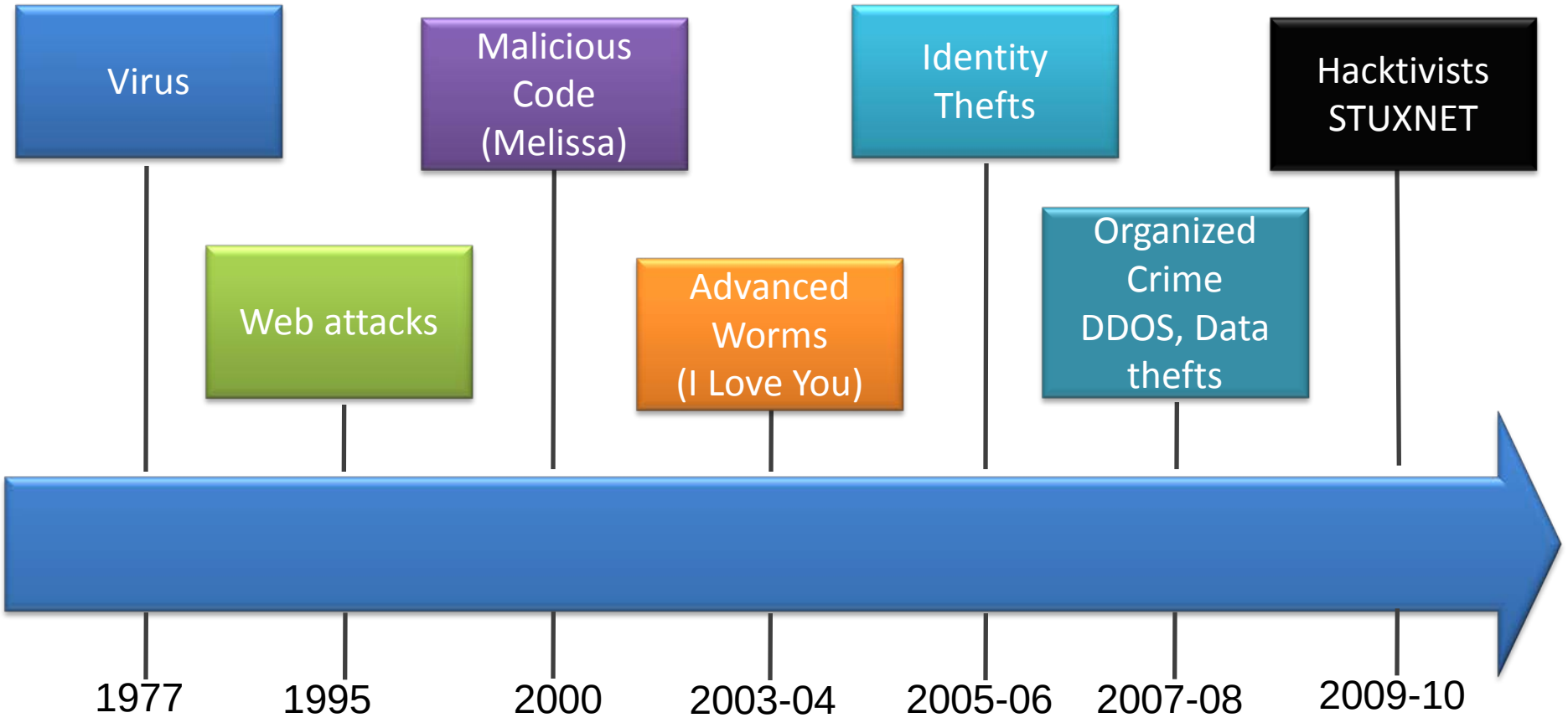
Cyber Space

The Cyber Space is composed by the global network of computers and by the devices making possible the interconnection

Modern Society is becoming more and more dependent on the Cyber-Space

Cyber-Space: new virtual world where people work, build social relations and…perpetrate crimes.

Cyber Attacks…Trends



GLOBAL CYBER SECURITY CENTER

Cyber Attacks…Trends

- Attack Speed
- Attack Complexity
- Vulnerability Discovery Speed

- Firewall permeability
- Increasing number of threats against ICT Infrastructures

- Distributed Denial of Services
- Worms
- Domain Name System Attacks
- Routers Attacks
- Advanced Persistent Threats

The Stuxnet Case

“Stuxnet is a very big project, very well planned and very well funded”.

Liam O’ Murchu, Supervisor NAM Security Response, *Symantec*

Industrial Espionage

Sabotage

Cyber War

Sony Attack

77 millions PSN User Accounts stolen

Vulnerability	A known Vulnerability on a Server
Detection	Slow Intrusion Detection
Reaction	After the Instrusion Sony nominated a CSO
Recover	Slow Recovery

Cyber attacks…a Look to The Future

Sony Attack

Operation Aurora

Stuxnet

Indian/Pakistan Cyber Army

Wikileaks

New IT Security Model

Social Networks

Smartphone

Cyber Space as a part of our daily life

Cloud/distributed computing

Smart grids

GLOBAL CYBER SECURITY CENTER

Critical Infrastructures

- Energy
- TLC
- Transport
- Chemical Plants
- Economy
- Public Health
- Public Services

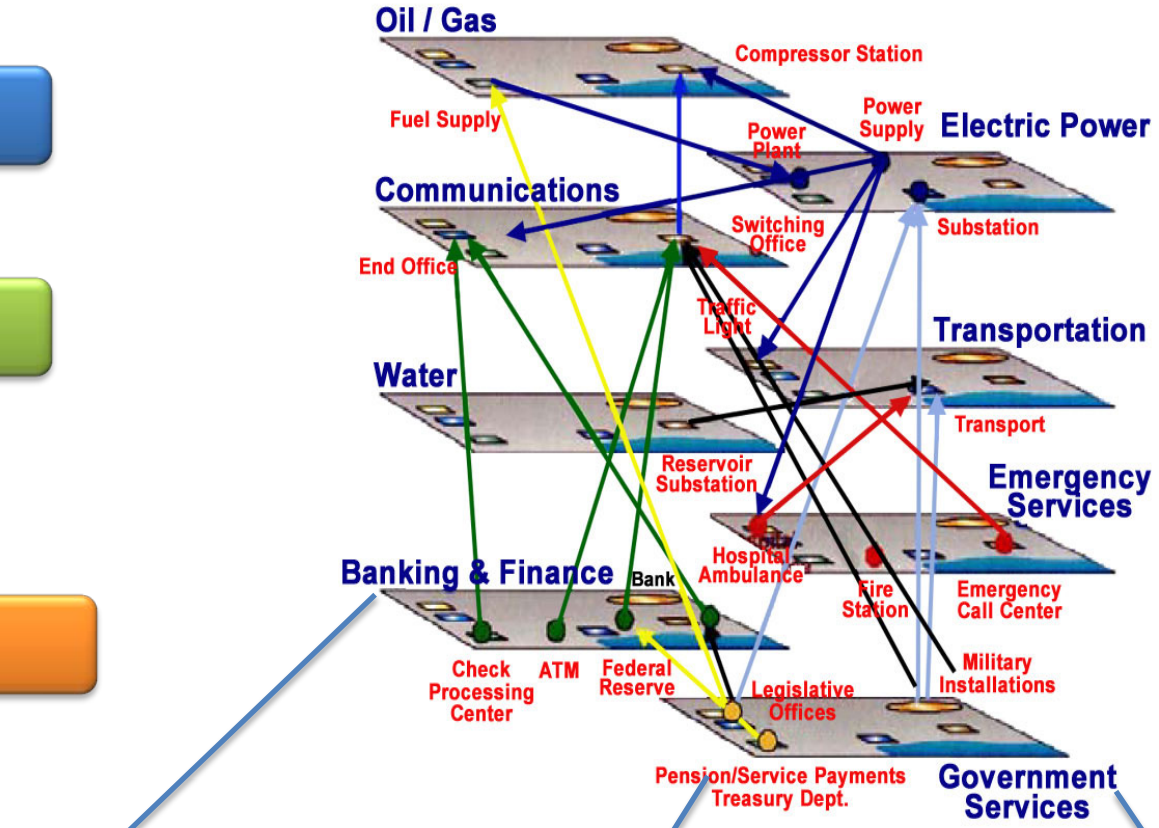
GLOBAL CYBER SECURITY CENTER

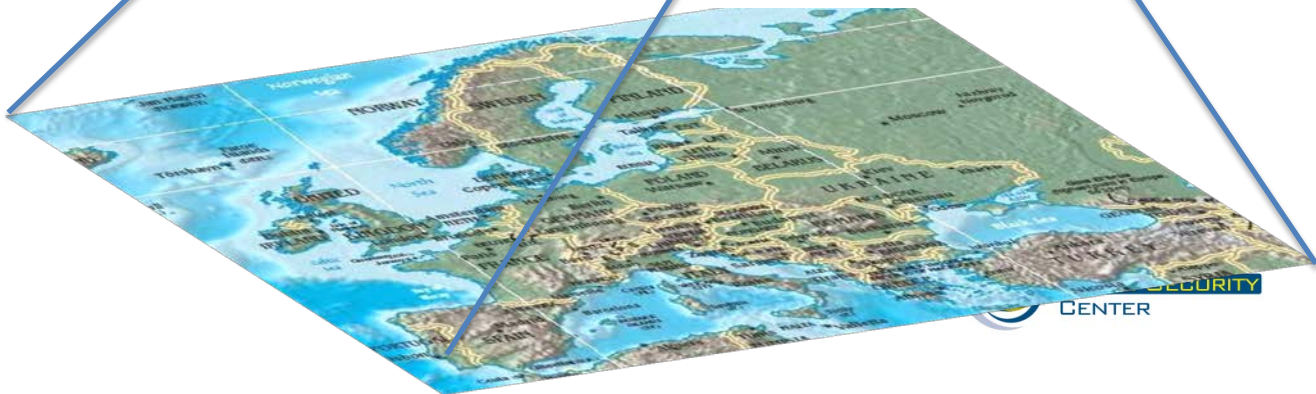
Critical Infrastructures – ICT Dependencies

System of System

Emergent Services

Emergent Disservices

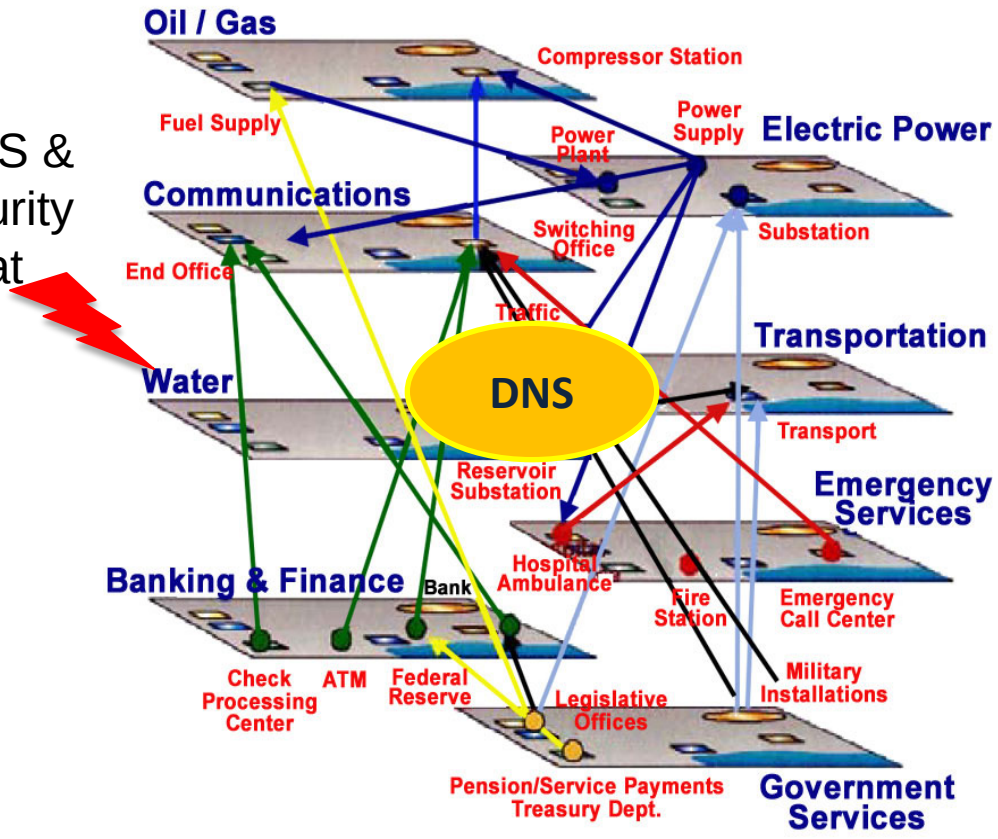




Critical Infrastructures – Domain Name System

- For decades, DNS system has operated in a reliable and robust fashion
- Community focus was on performance and availablity
- In the last years the Internet scenario changed at incredible speed

DDoS & Security threat



Massive use of Internet in Critical Infrastructures

Cloud/CDN/SOA Infrastructures

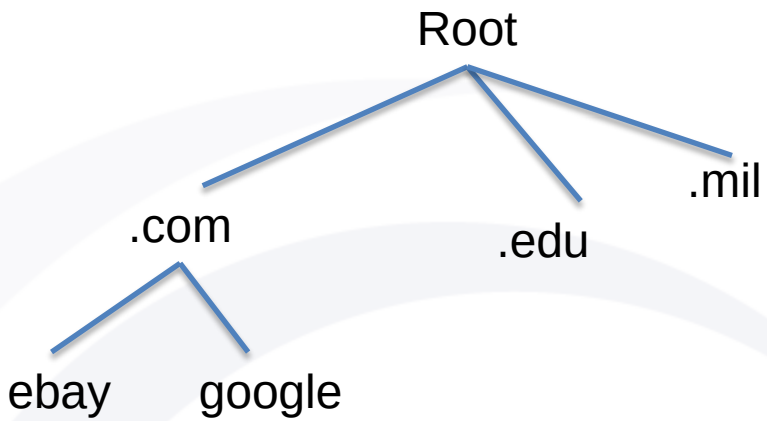
Massive increase of Emergent Pervasive Services

Centrality of DNS

Domain Name System

The Domain Name System

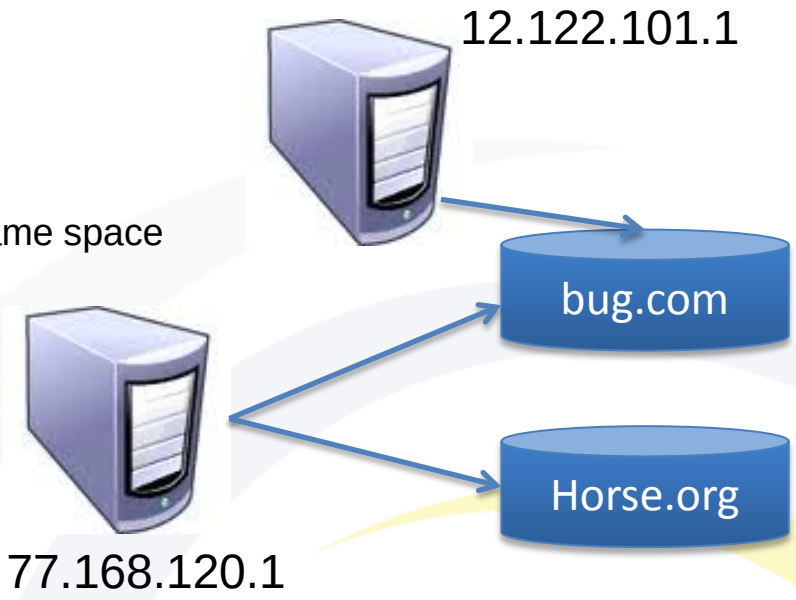
- Created in 1983 by Paul Mockapetris (RFCs 1034 and 1035)
- What Internet users use to reference anything by name on the Internet
- The mechanism by which Internet software translates names to addresses and vice versa



- A lookup mechanism for translating objects into other objects
- A globally distributed, loosely coherent, scalable, reliable, dynamic database

It is used almost every time when an user is performing some activity requiring an Internet Connection

DNS-Elements…



Servers

Name servers store information about the name space in units called “zones”

Resolvers

Name resolution is the process by which resolvers and name servers cooperate to find data in the name space.

- A name server only needs the names and IP addresses of the name servers for the root zone (the “root name servers”)
- The root name servers know about the top-level zones and can tell name servers whom to contact for all TLDs

DNS-Attacks…

DNS is a Lite protocol

DNS is fairly old

…originally designed without taking in consideration security aspects

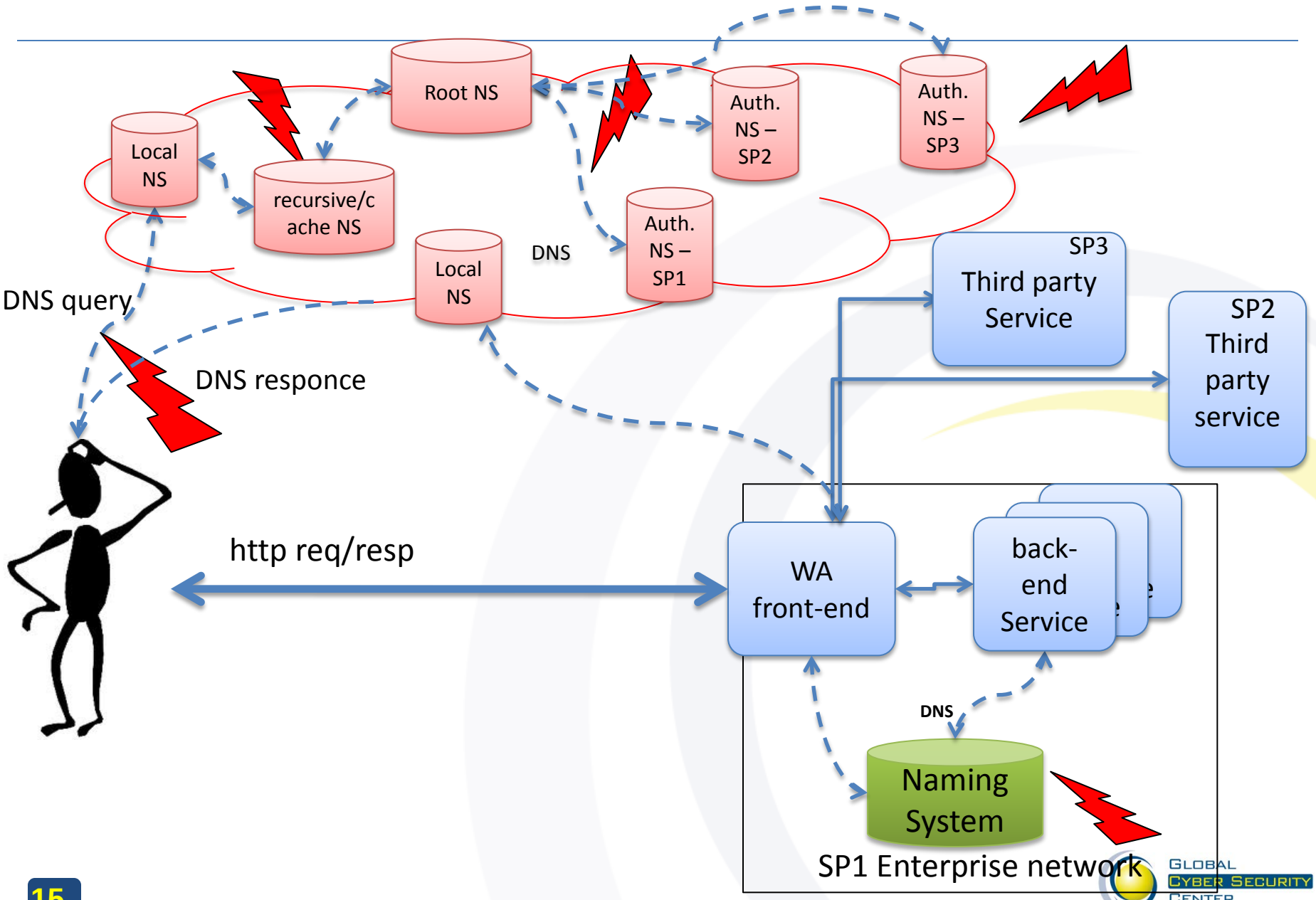
- DNS Cache Poisoning
- DNS ID Spoofing
- Client Flooding
- DNS Dynamic Update Vulnerabilities
- Information Leakage
- Compromise of DNS server's authoritative data
- DOS

DNS-SEC

DNSSEC signs the records for DNS lookup using public-key cryptography. The correct DNSKEY record is authenticated via a chain of trust, starting with a set of verified public keys for the DNS root zone which is the trusted third party

- DNSSEC does not provide confidentiality of data;
- DNSSEC does not protect against DoS attacks directly,

Web Application scenario



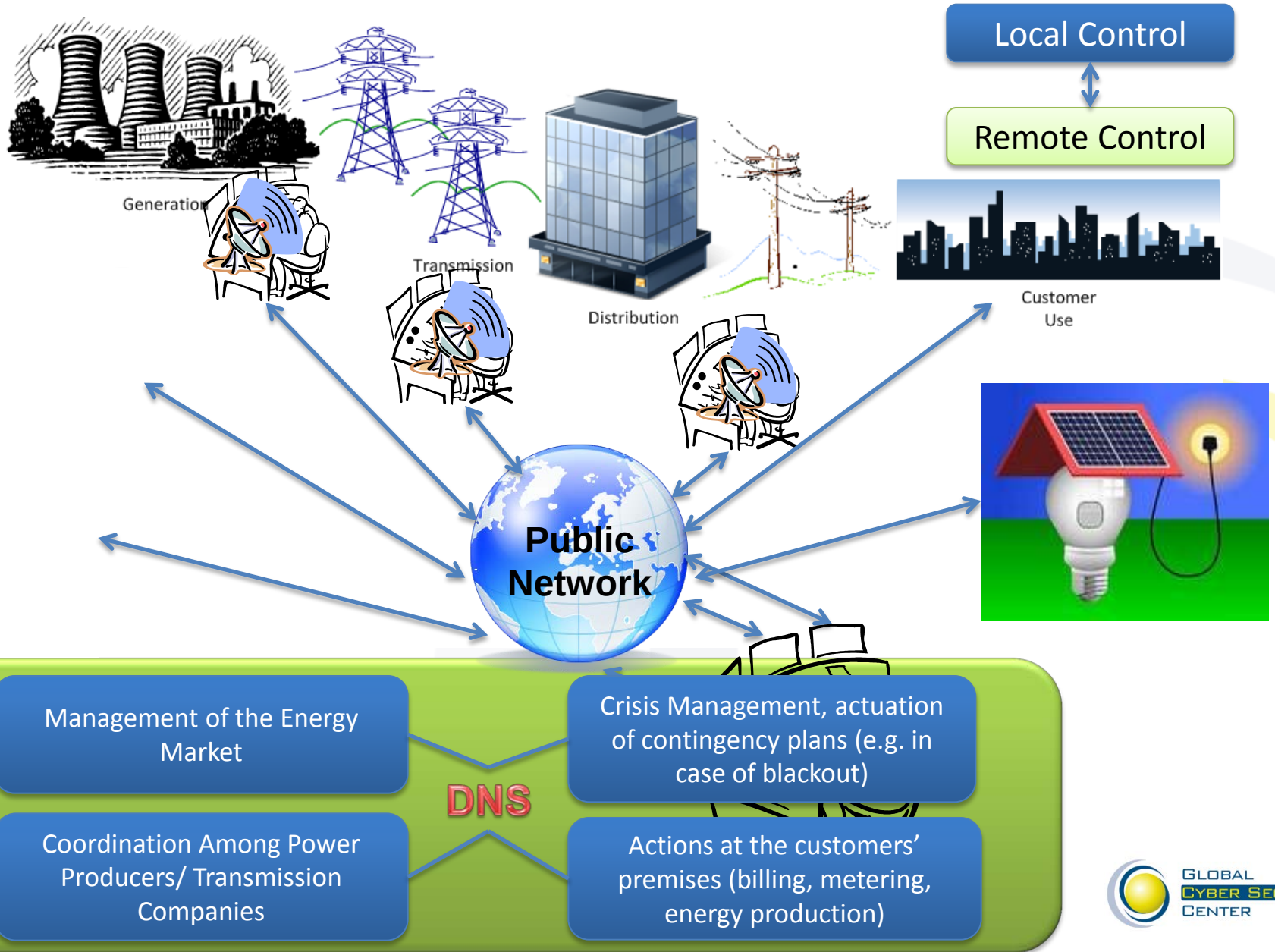
The role of the DNS in the WA scenario

- The Role of the DNS
  - To grant end-user access to web applications
  - To enable wide area distributed applications (e.g. in a service marketplace scenario)
  - To enable enterprise distributed applications

- DNS threat and their impact

Vulnerability/threat	Target	Impact
Data corruption (*e.g.* Cache poisoning, route injections, man-in-the-middle, Cache snooping)	End user	Security and resiliency level perceived by the end user
	Service provider	Capability to guarantee SLA with security and resiliency constraints
DDoS	End user	Performance perceived
	Service provider	Capability to guarantee SLA

Energy System Scenario (Upper Layer)

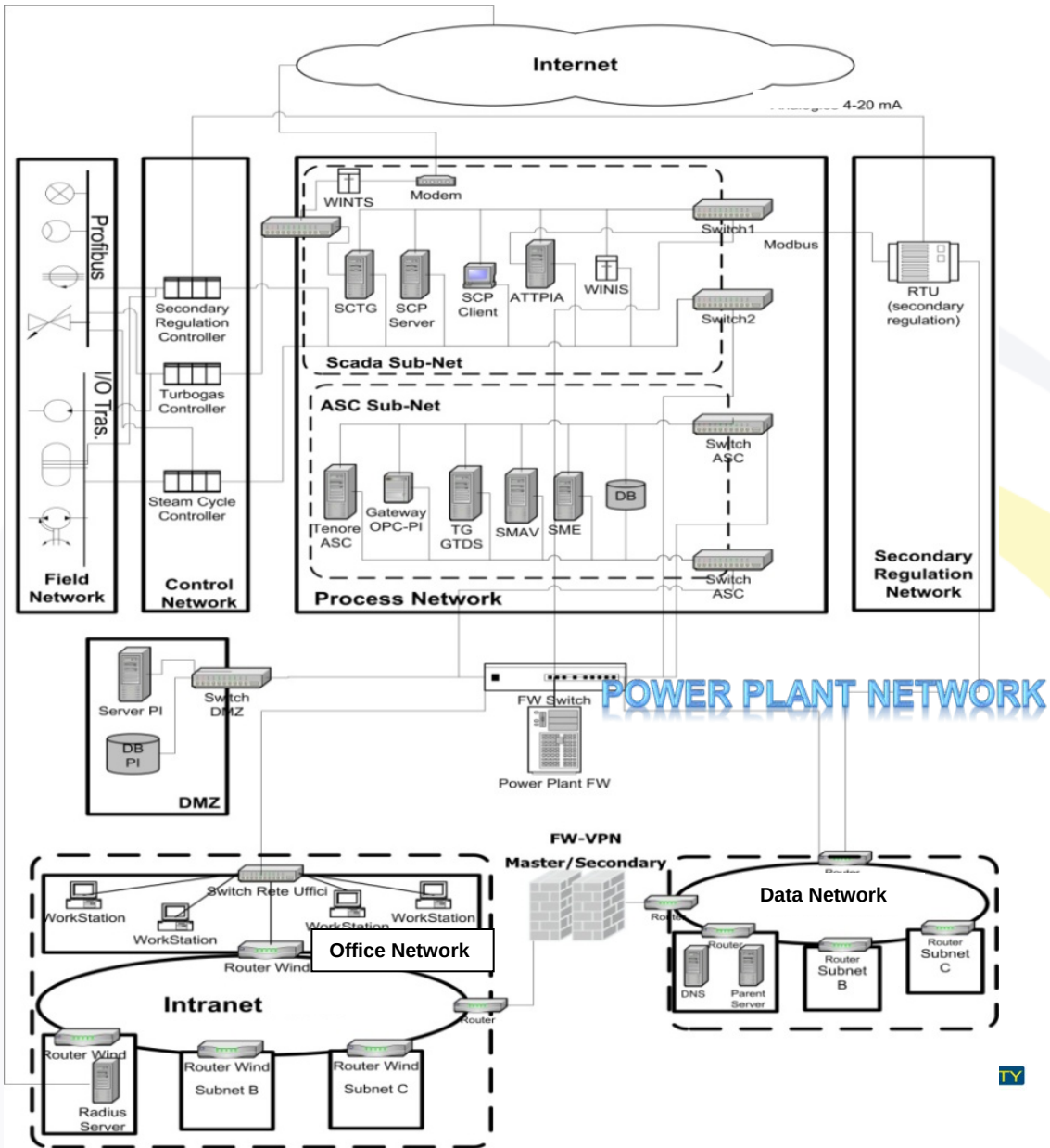


GLOBAL CYBER SECURITY CENTER

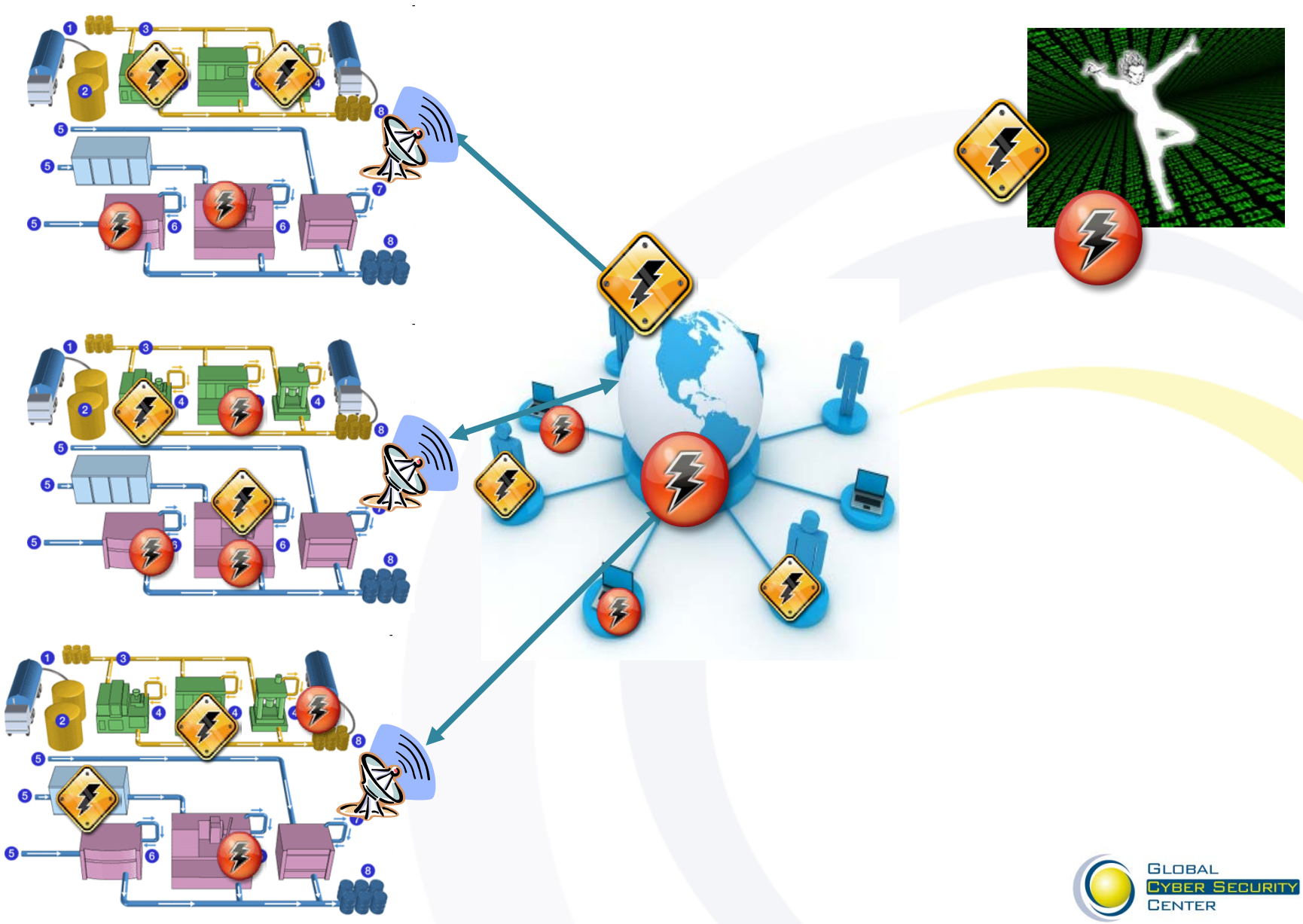
Energy System Scenario (Lower Layer)

- Remote operator Specialized Operations
- Access to Diagnostic Services
- Delivery of data to second level SCADA Svr.
- Delivery of control command to second and first level SCADA Svr.
- Third party remote Maintenance Operations
- Primary and Secondary Regulation
- Primary and Secondary Regulation

DNS



…Smart Grids…



…Needs…

Proceed in the deployment of DNSSEC

Create Information Sharing Centers for the security of the DNS

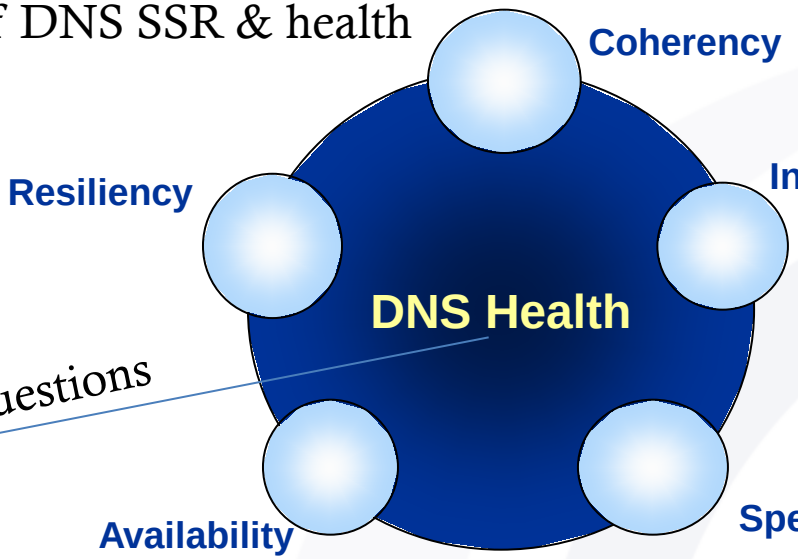
Start a discussion at international level on the definition of policies helping in improving the DNS Security and Stability

Define a Framework allowing to measure the DNS Health

DNS-CERT

…DNS Health…

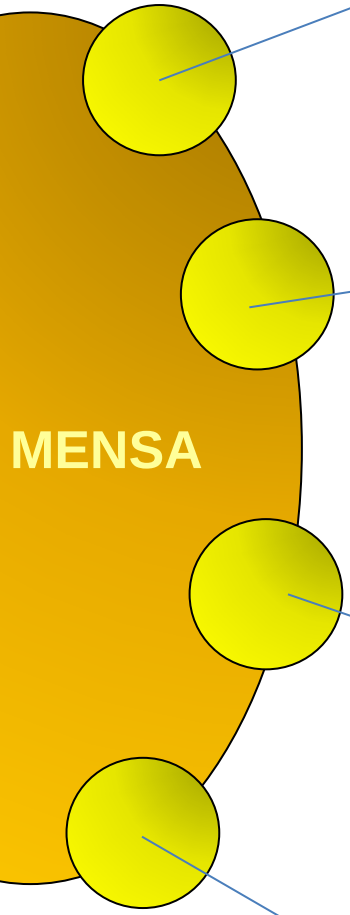
- Many actors, including ICANN, have already begun a deep discussion about the concept of DNS SSR & health



Open Questions

- Need for a Stable and open Framework for Measurements & Benchmarking
- Identification of proper metrics for measuring the Health properties
- Definition of a multiperspective interpretations map for different DNS Actors (Root server operators, non root auth., clients)
- Aggregation and comparison of measurement

The Mensa Initiative



It will build on and evolve from the strong foundation already established by interested community members in ICANN-sponsored fora

To design a multi-perspective framework for the measurement and benchmarking of the DNS SSR level.

To support risk analysis, what-if analysis and impact analysis of changes to the DNS infrastructure as well as DNS policy-making.

To refine the current concept of DNS SSR and to enhance the awareness among the "critical" end-users of the DNS

Metric categories

- Vulnerability
  - Repository Corruption
  - System Corruption
  - Denial of Service
  - Protocol issues
  - Data Disclosure

Main DNS vulnerabilities

- Security

The ability of the DNS to limit or protect itself from malicious activity

- Resiliency

The ability of the DNS to effectively respond and recover to a known, desired, and safe state when disruption occurs

Summary of Vulnerability Metrics

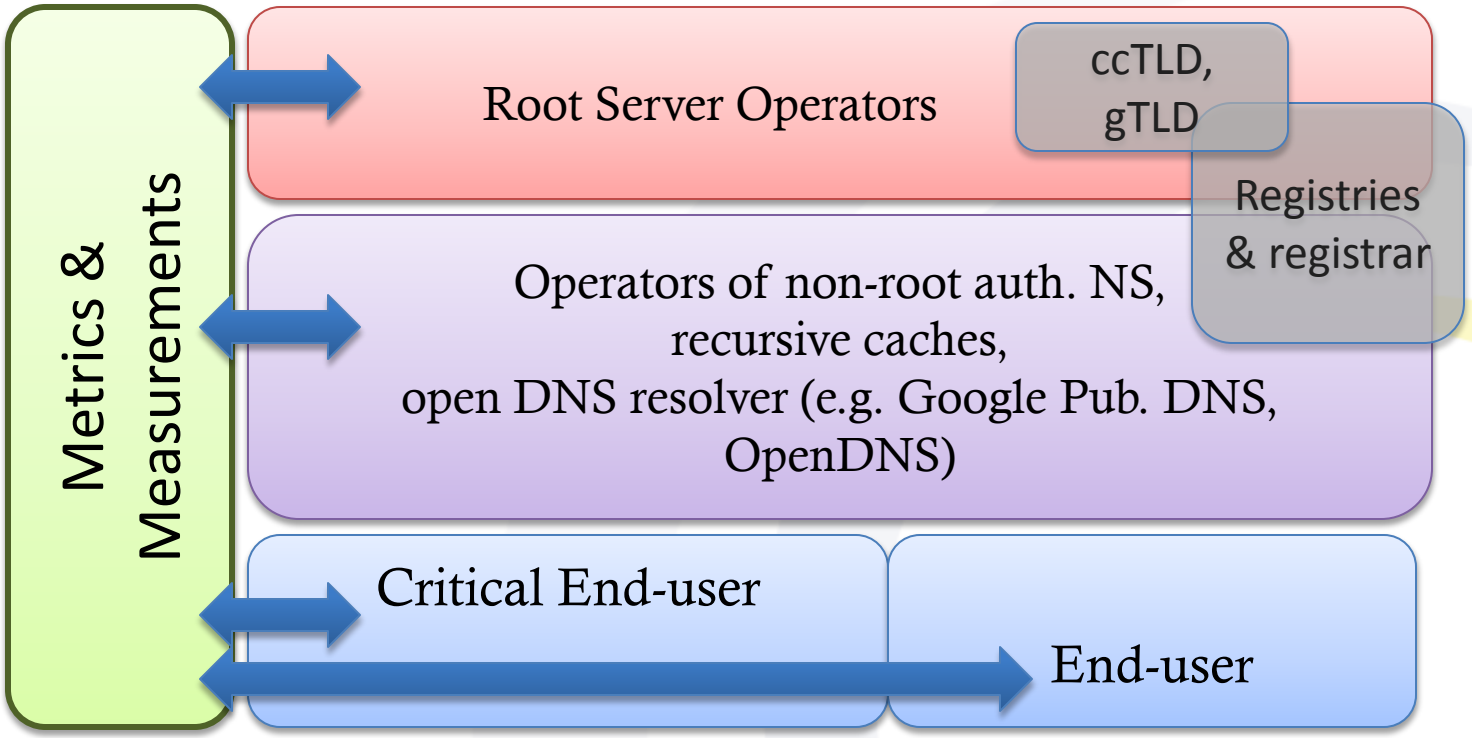
Specific for DNS

Metric categories		Example of Measures
Vulnerability	Repository Corruption	Data Staleness, NS Parent/Child Data Coherence, Glue inconsistencies, Zone inconsistencies
	System Corruption	NXDOMAIN Redirection, NS Data Registration Correctness
	Protocol Issues	Cache Poisoning (percentage, probability, rate), cache poisoning rate, DNS Spoofing/Open Recursion, Zone Transfer failure
	Denial of Service	DoS rough effectiveness, Geographical DOS Effectiveness, Zone transfer transaction speed, network performance, server performance, Rate of repeated queries

Summary of Security and Resiliency Metrics

Metric categories	Example of Measures
Security	Attack surface, attack deepness, System Immunity level, attack escalation speed, Downtime impact, MTTR, Vulnerability density, Loss Expectancy, Adjusted Risk,
Resiliency	Mean Time to Incident Discovery, Operational mean time between failures, Operational Availability, Operational reliability, Fault Report Rate, Incident rate

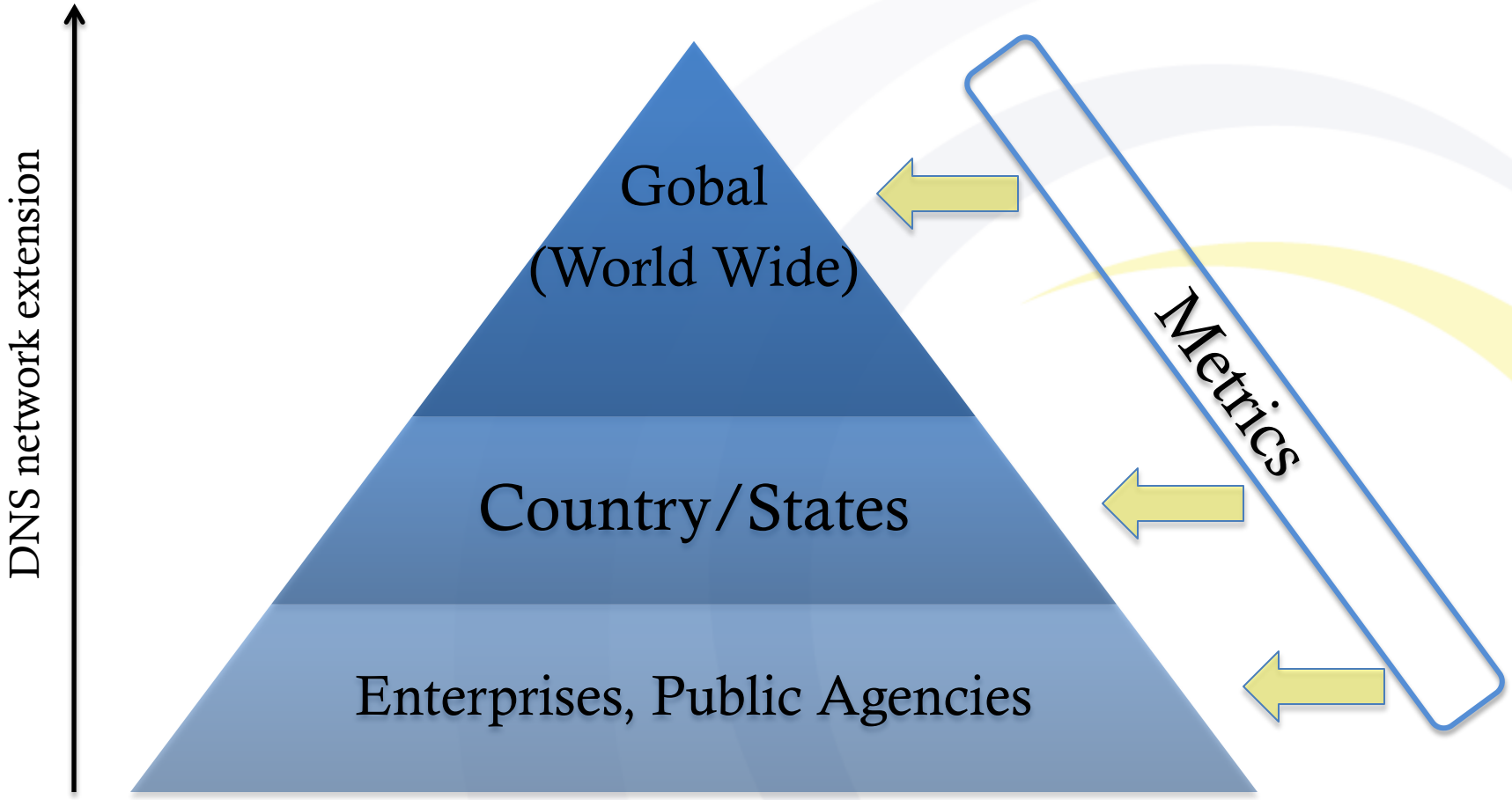
Multi-perspective framework



M&M should provide the **right point of view** for each DNS actor

Multi-perspective framework

Indicators should be appropriate for different network extensions



Policies

Defining a minimum level of QoS to be guaranteed by the operators

Forcing the adoption of certain best practices among the Critical End-Users

Regulating the Management of DNS Activities and Incidents

Information Sharing

CERT

CERT:

A group of people in an organization who coordinate their response to breaches of security or other computer emergencies such as breakdowns and disasters.

The DNS CERT is a community function to ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS.

Conclusions

Attacks to the DNS system can be used to indirectly damage critical infrastructures

The DNS is today not perceived as an important element by end-users and critical users

The DNS must be, indeed, considered a Critical Infrastructure

- Policies
- Assessment Frameworks
- Protocol enforcement
- Information Sharing

GCSEC, in collaboration with ICANN and DNS-OARC will organize in October 2011, in Rome The first international workshop on DNS-Health and Security

(see for details www.gcsec.org)

GLOBAL
CYBER SECURITY
CENTER

Thank you!