GLOBAL CYBER SECURITY CENTER

DNSSEC Workshop

ICANN Dakar SÉNÉGAL Nº42 23 - 28 October 2011

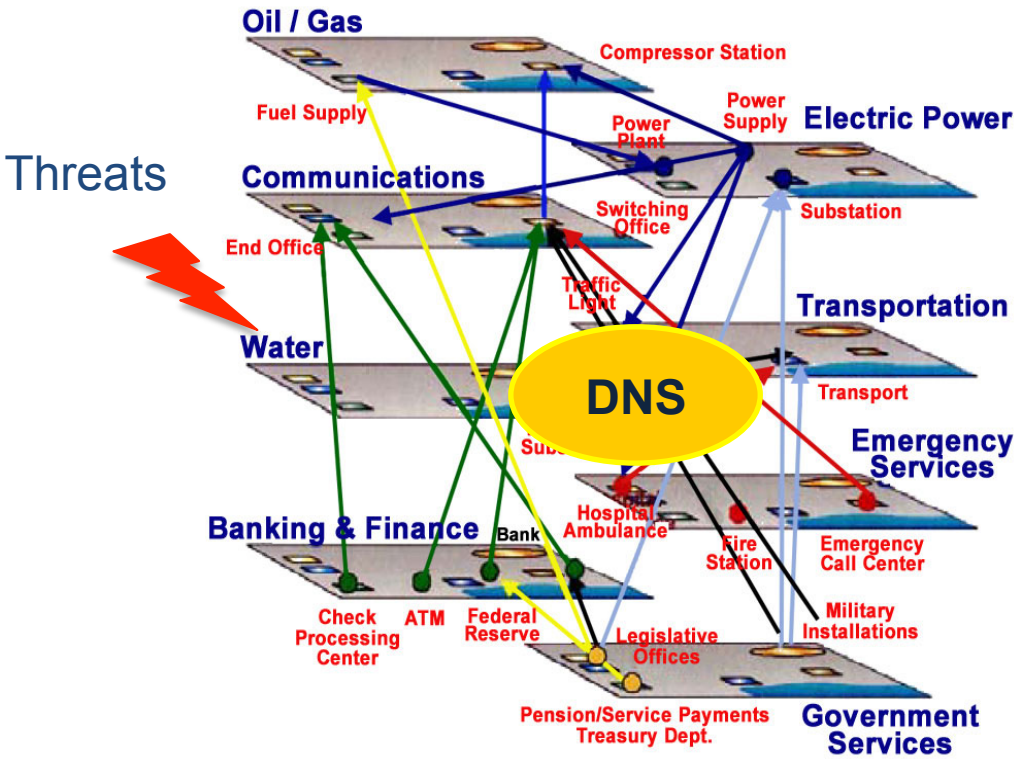
The Mensa project Measuring DNS Health and Security

Emiliano Casalicchio
emiliano.casalicchio@uniroma2.it

GCSEC/University of Rome Tor Vergata

26 October 2011

Motivation and concept



Massive use of Internet in Critical Infrastructures

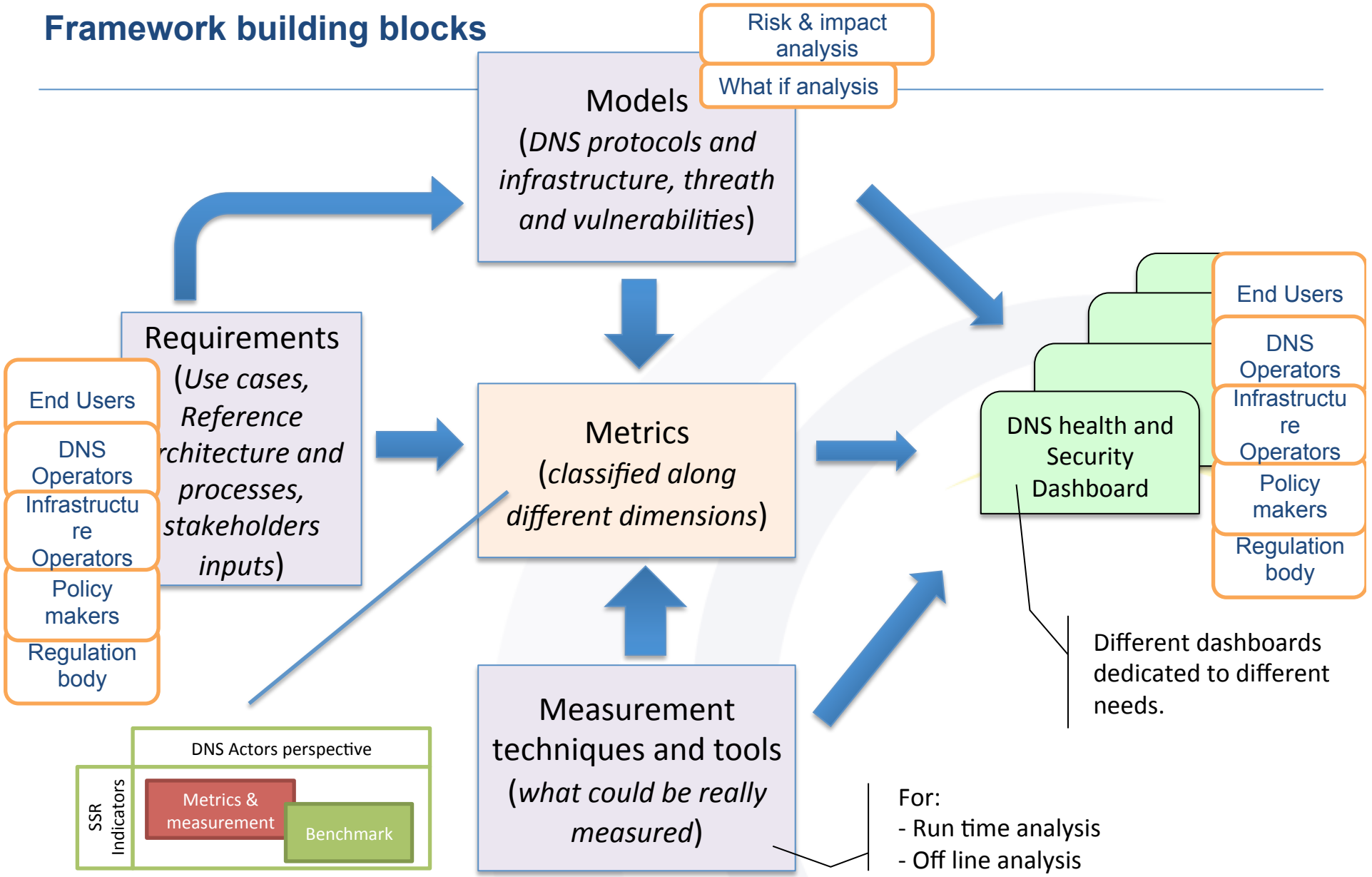
Massive increase of Emergent Pervasive Services

Centrality of DNS

Need for metrics allowing to measure DNS Health & *Security*

- I'm a critical end-user. Is the RR I use secure enough?
- Given a critical transaction, can i identify the portion of transaction security/ resiliency/performance that depend on DNS and can i quantify that part?
- Can I benchmark the security/stability level of the portion of DNS I depend on?
- Are critical process/services non functional requirements satisfied?
- DNS is robust can I improve it/can i reduce costs/ can I optimize more?

Framework building blocks



GLOBAL CYBER SECURITY CENTER

Metrics categorization and examples

29 DNS Health metrics
16 Security metrics

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

Measurement phase

How we can answer the following questions?

- Is my Recursive Resolver secure enough?
- Can I identify the “portion” of transaction security/resiliency/ performance that depend on DNS and can I quantify that part?
- Can I benchmark the security level of my RR?
- Are critical process/services **non functional requirements** satisfied? E.g.: internet of things, industrial process control, smart grid control processes
- DNS is robust can I improve it/can i reduce costs/ can I optimize more?

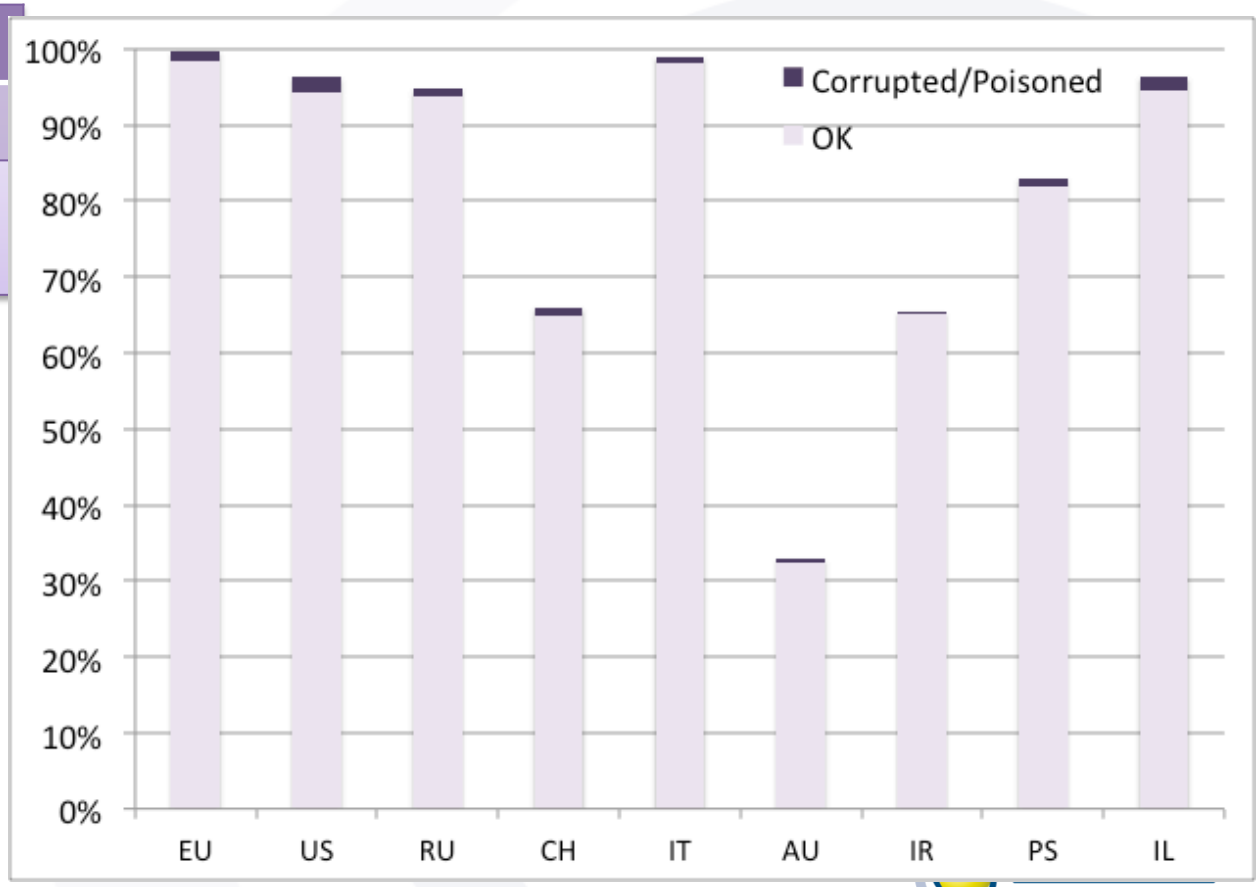
To start … two metrics

- Cache poisoning “probability”
- DNSSEC queries Speed/Size

Cache poisoning prob. evaluation: Base measurement

- 6000 queries
- 3 Resolvers for each country
- Average values with an error 0.04% < $\frac{\sigma}{\sqrt{n}}$ < 0.18%

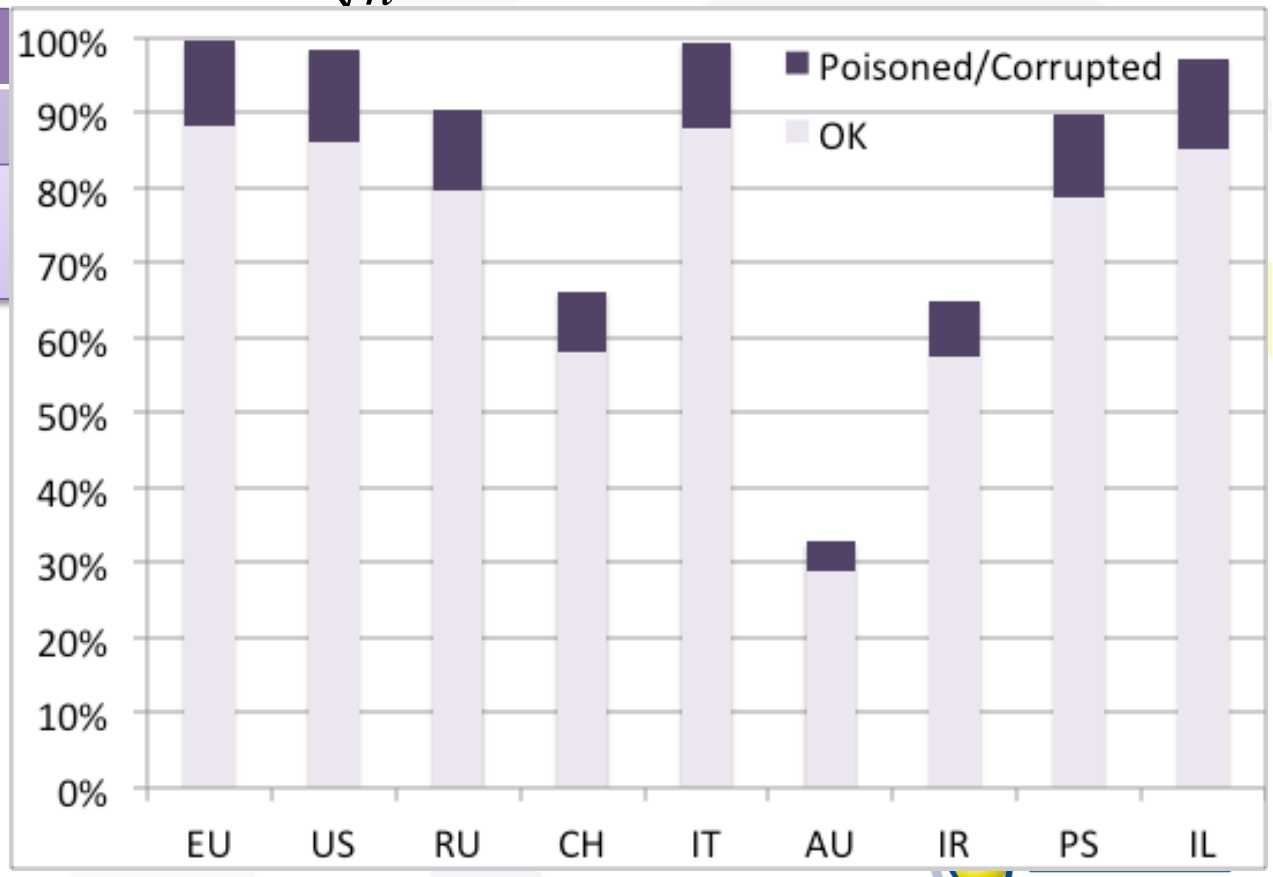
TOTAL	
OK	72.35%±0.327%
Corrupted/ Poisoned	1.00%±0.067%



Cache poisoning prob. evaluation: With injected poisoned records

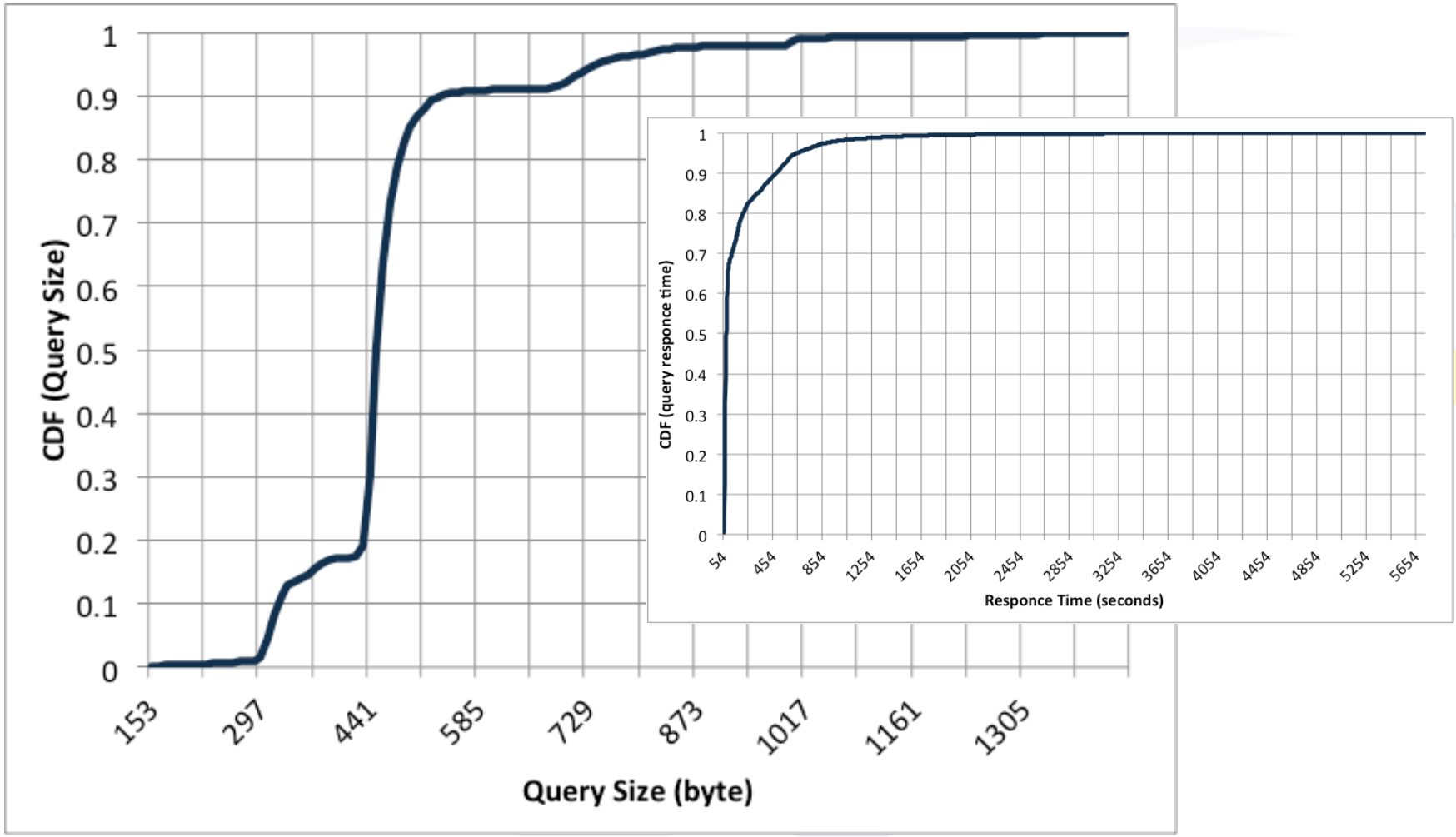
- 6000 queries
- 10% randomly injected poisoned records
- 3 Resolvers for each country
- Average values with an error 0.16% < $\frac{\sigma}{\sqrt{n}}$ < 0.65%

TOTAL	
OK	72.35%±0.190%
Corrupted/ Poisoned	9.88%±0.333%



Speed: DNSSEC queries size

- 22000 DNSSEC queries



GLOBAL CYBER SECURITY CENTER

GLOBAL CYBER SECURITY CENTER

Preliminary project results are available at:

http://www.gcsec.org/content/dns-security-and-stability

Project team (past and present)

Doug Brent
E.Casalicchio
M.Caselli
David Conrad
Joao Damas
Igor Nai Favino
Maria Luisa Papagni

Advisory Board

Johan Irhén
Jim Galvin
Steve Crocker

Thank you!

emiliano.casalicchio@uniroma2.it