Research Vision

Paulo Esteves-Veríssimo

Univ. of Luxembourg, FSTC / SnT

paulo.verissimo@uni.lu
http://wwwen.uni.lu/
snt/people/paulo_verissimo

CritiX Lab (Critical and Extreme Security and Dependability)

Presentation to .

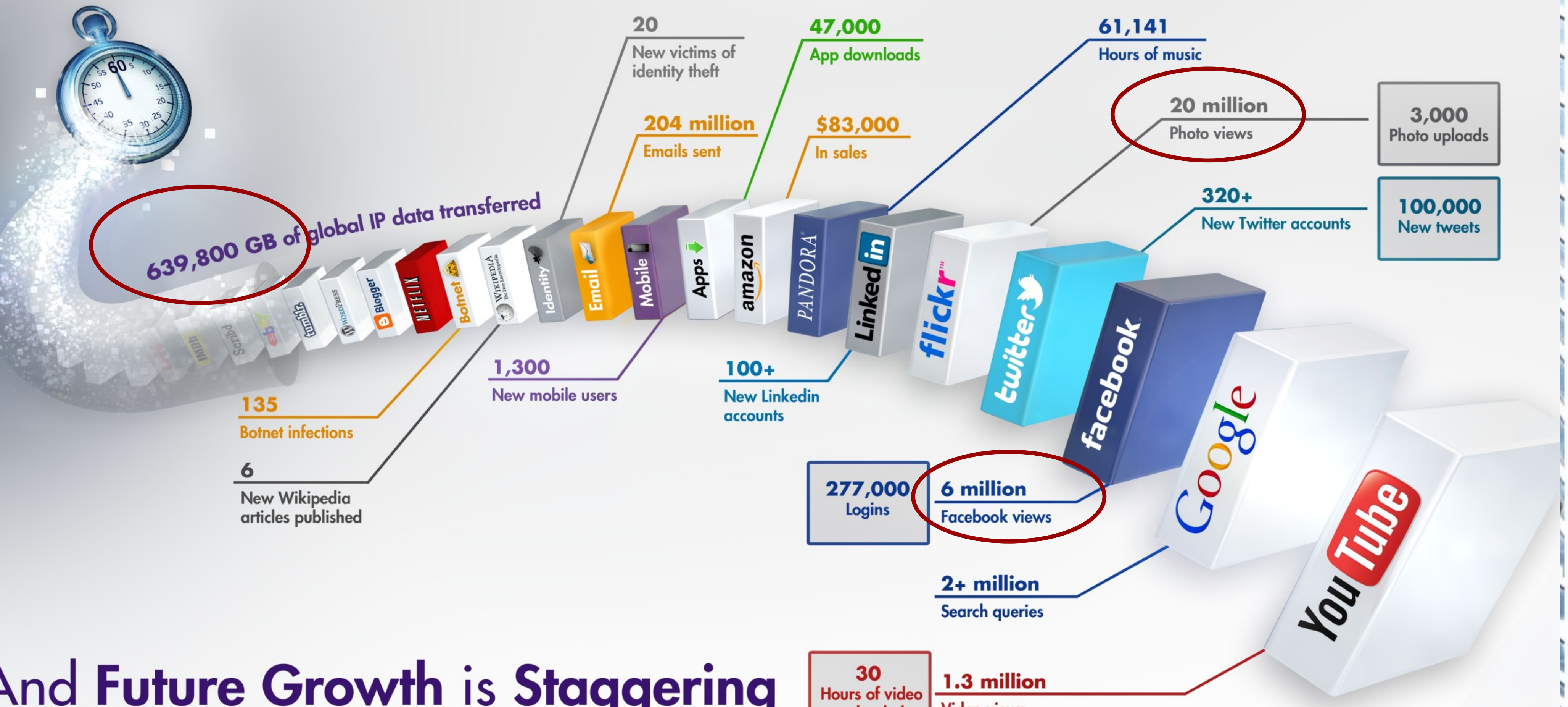
Is the world becoming net-centric?

a.k.a. INFRASTRUCTURE

Let's dare a vision of the near future

ISP
ISP
EZS1537
300 -
25
AUA356
240 -
29
DLH05X
340 -
31
GWI588
240 -
39
GOGSK
320 -
25
DLH2VY
340 -
25
LOT336
340 -
Google
RedBull
MDV

What Happens in an **Internet Minute?**



639,800 GB of global IP data transferred

20 New victims of identity theft

204 million Emails sent

47,000 App downloads

$83,000 In sales

61,141 Hours of music

20 million Photo views

3,000 Photo uploads

320+ New Twitter accounts

100,000 New tweets

135 Botnet infections

6 New Wikipedia articles published

1,300 New mobile users

100+ New Linkedin accounts

277,000 Logins

6 million Facebook views

2+ million Search queries

30 Hours of video uploaded

1.3 million Video views

And **Future Growth** is **Staggering**

Today, the number of **networked devices** =

the global population

By **2015**, the number of **networked devices** =

the global population

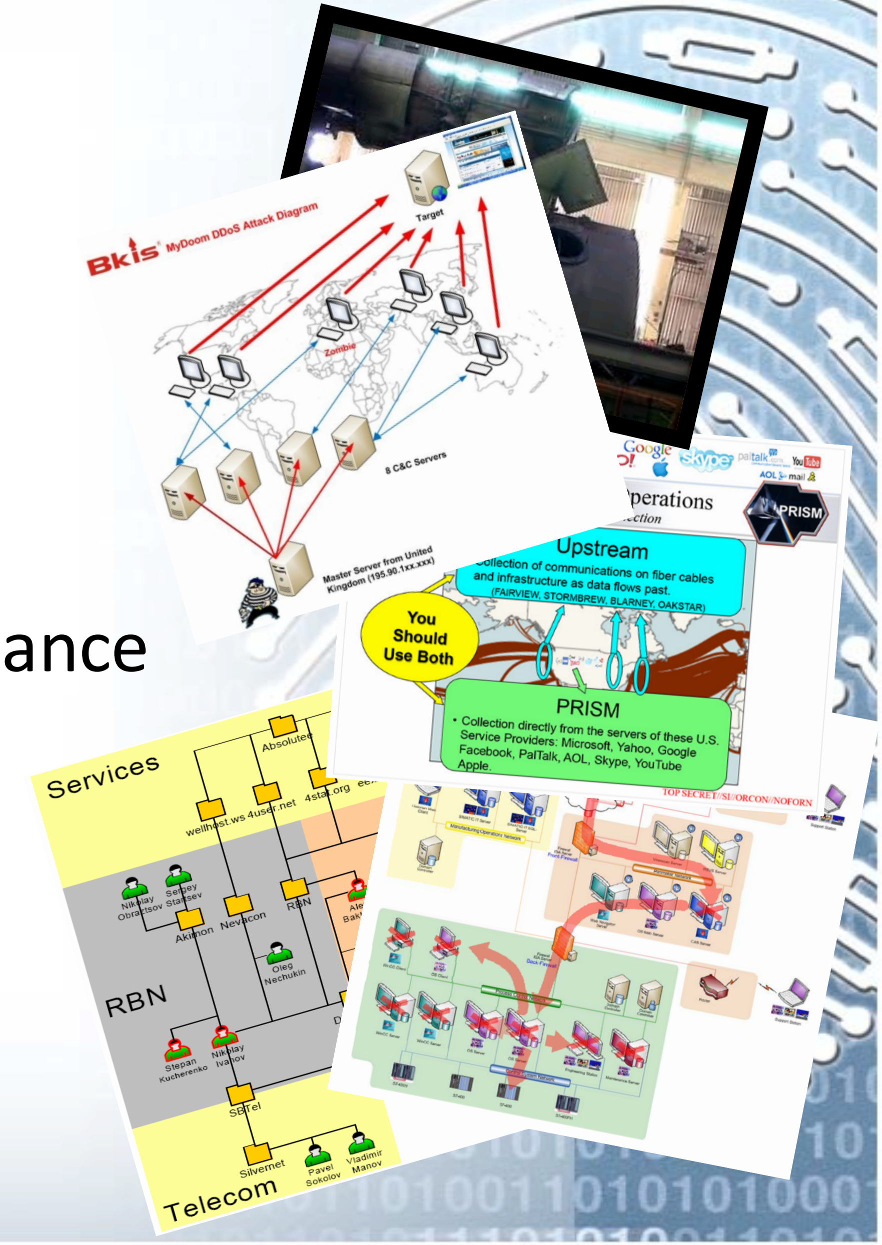
In **2015**, it would take you **5 years**

to view all video crossing IP networks each **second**

www.intel.com/.../***internet-minute***-infographic.html

A world full of threats?

- targeted attacks and advanced persistent threats (PRISM, TAO, APT1, etc.)
- weakening and subversion of comms and computing services
- threats to privacy: mass surveillance and data collection
- sophisticated automated cyber weapons (Stuxnet, Flame, etc.)
- organised crime (RBN, etc.)

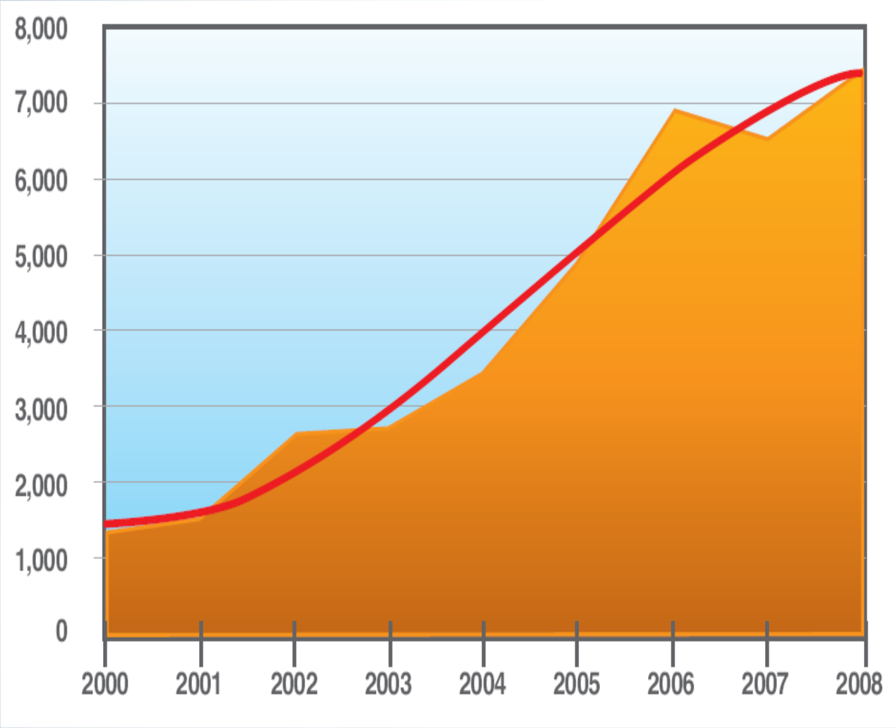


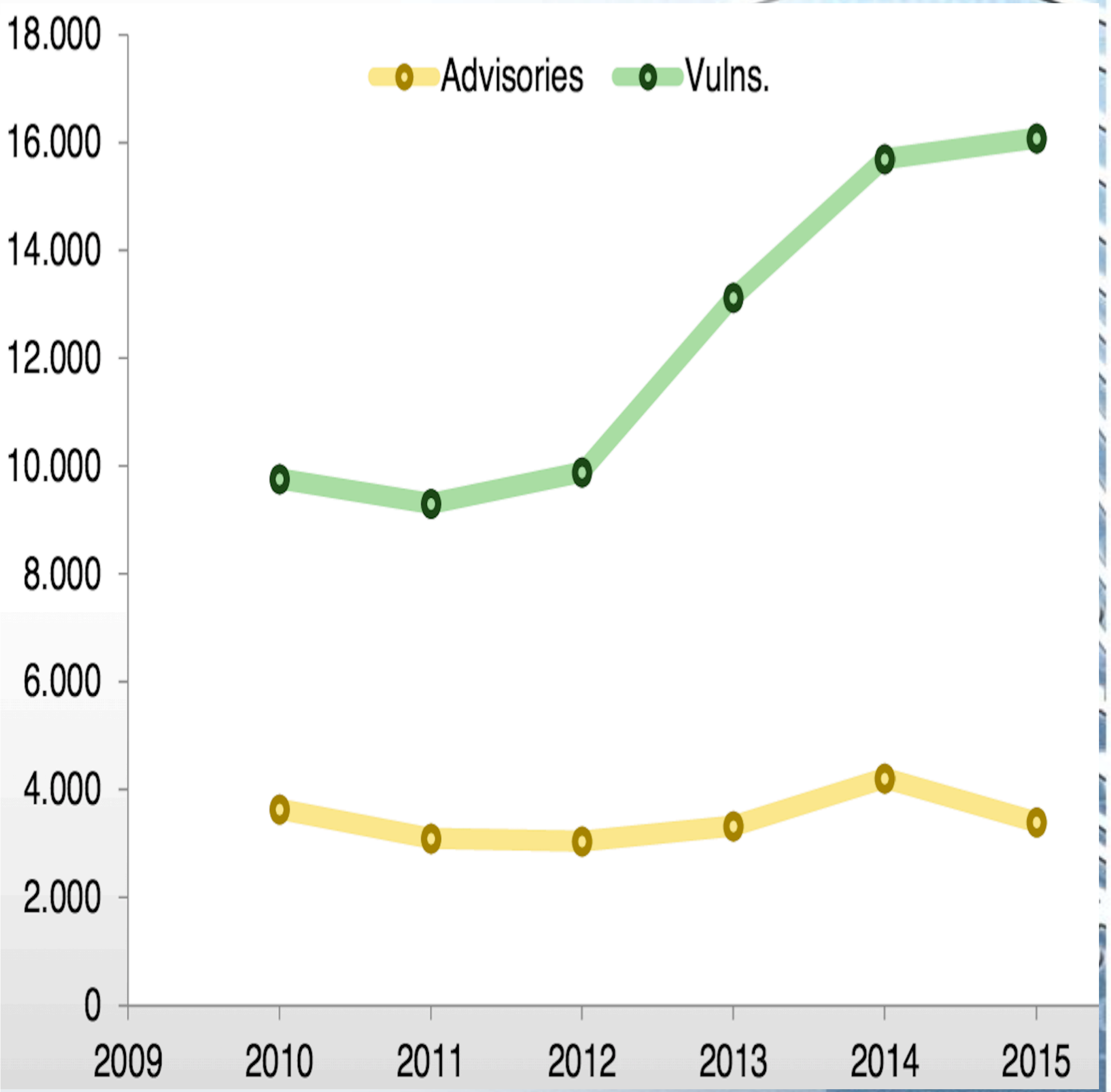
Bkis MyDoom DDoS Attack Diagram
Target
Zombie
8 C&C Servers
Master Server from United Kingdom (195.90.1xx.xxx)
Operations
PRISM
Upstream
Collection of communications on fiber cables and infrastructure as data flows past.
(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)
You Should Use Both
PRISM
• Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.
TOP SECRET//SI//ORCON//NOFORN
Services
Absolute
wellhost.ws
4user.net
4stat.org
Nikolay Obraztsov
Sergey Startsev
Akimon
Nevacon
RBN
Oleg Nechukin
RBN
Stepan Kucherenko
Nikolay Ivanov
SBTel
Silvernet
Pavel Sokolov
Vladimir Manov
Telecom

Conventional Software Vulnerabilities

ever increasing

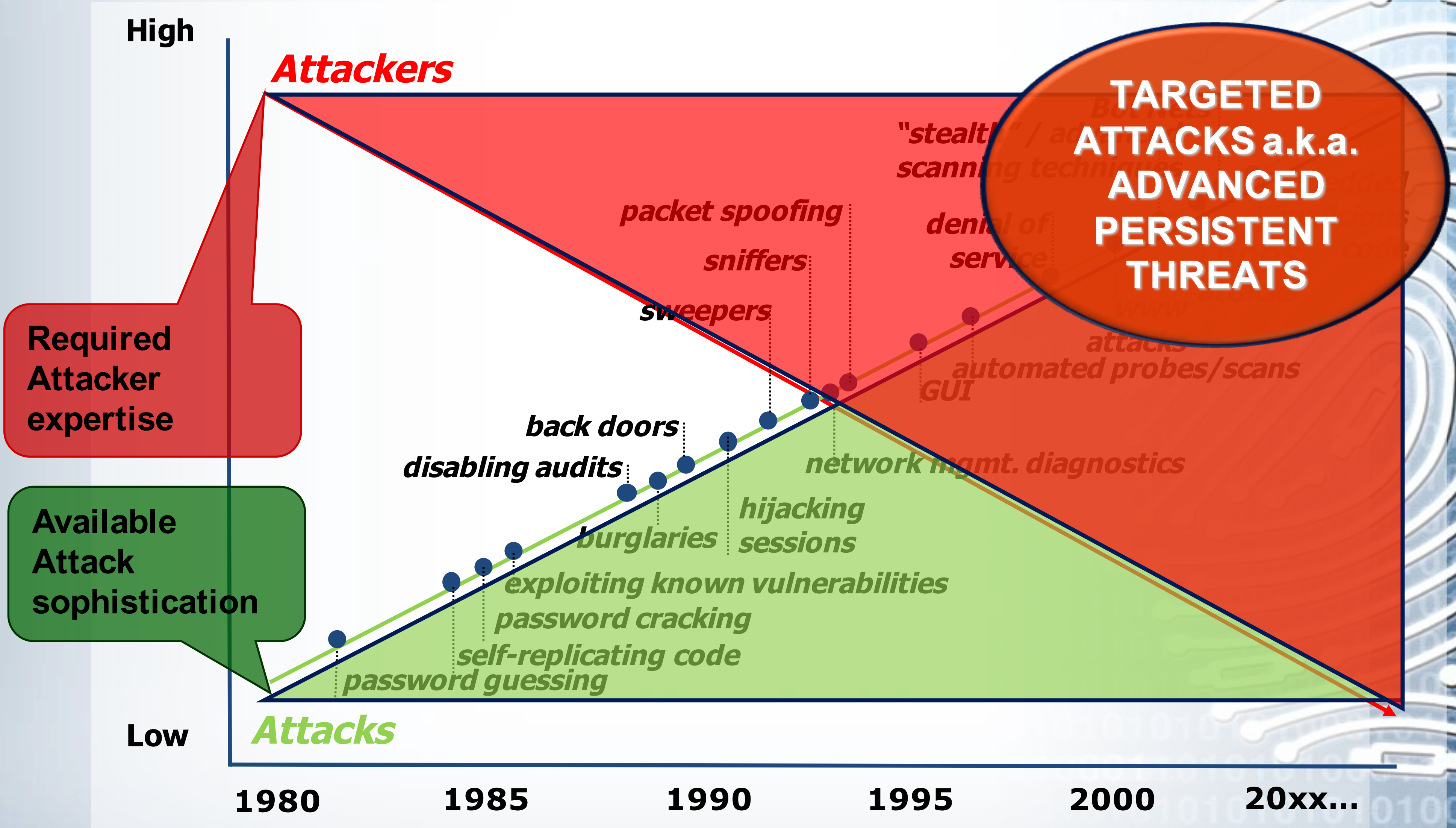
Number of new vulnerabilities per year



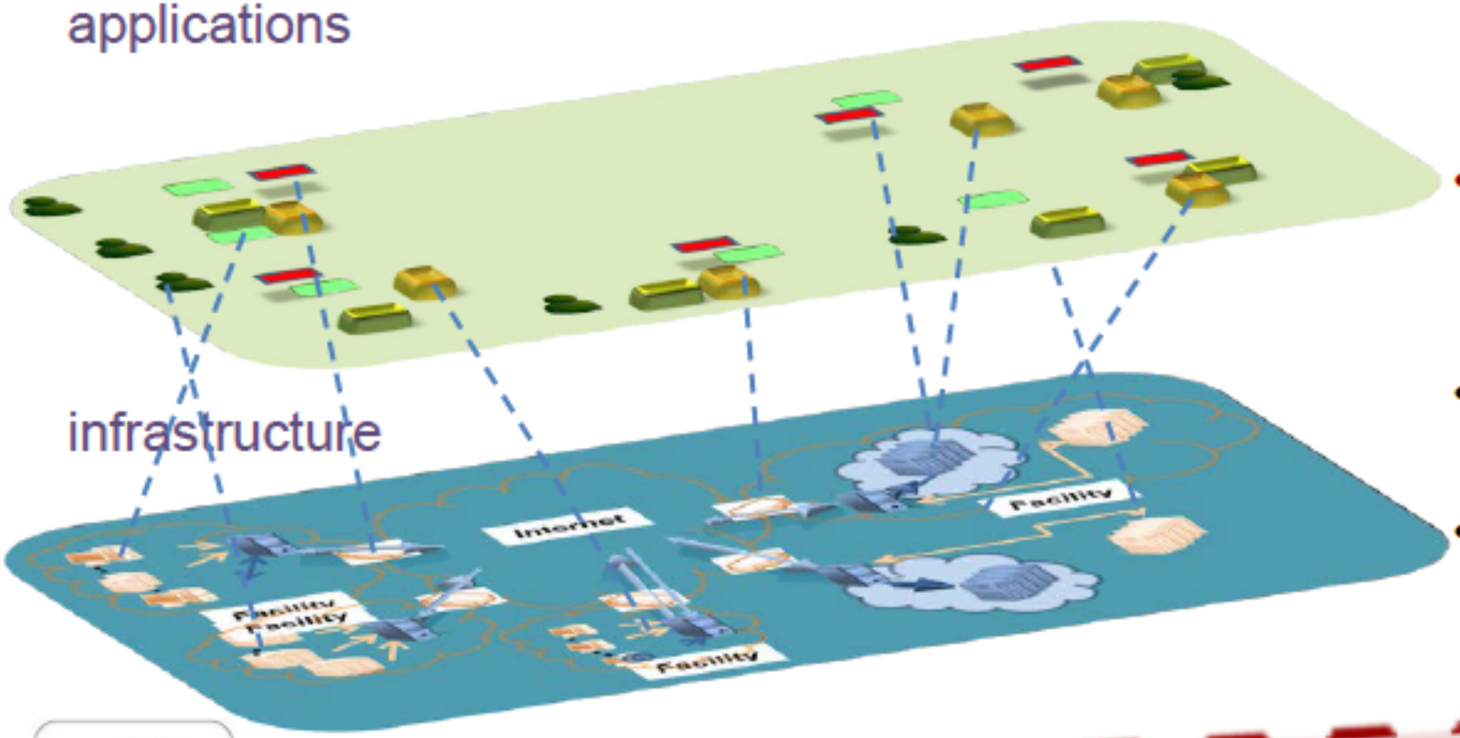


(Sources: IBM xForce, Symantec, Telexa)

Attack sophistication vs. attacker expertise



(Source: Adapted from Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009, November 2002. (CERT) platforms and applications

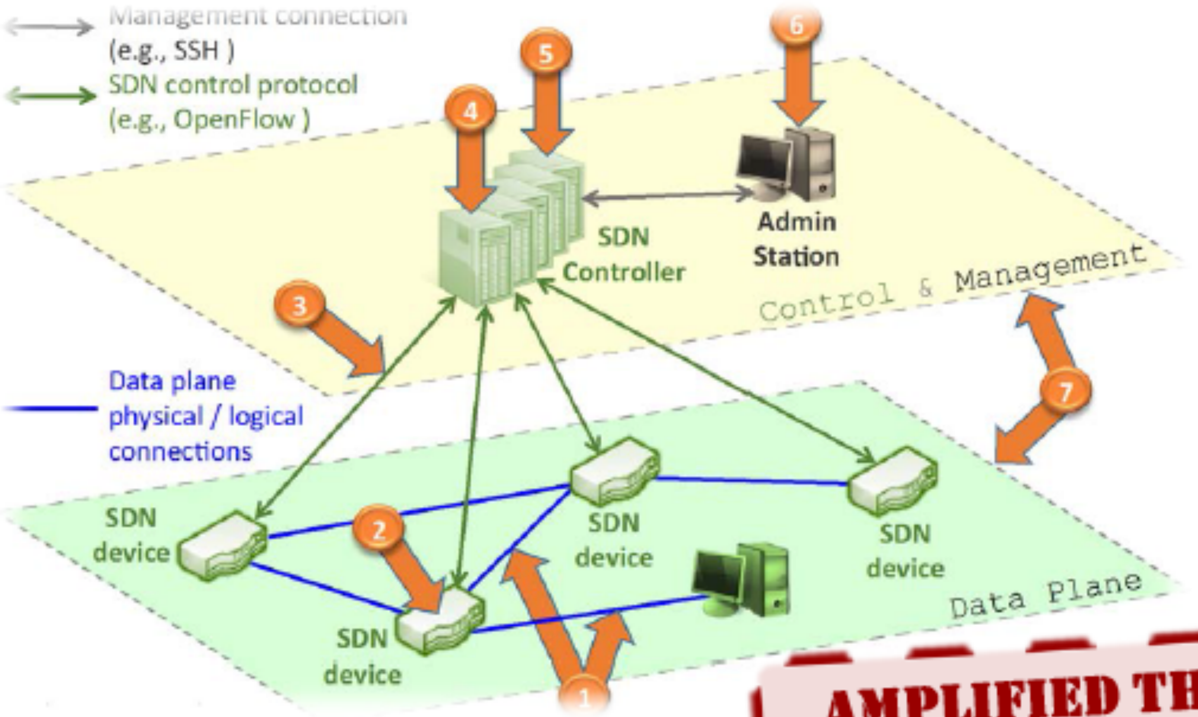


infrastructure

- short-term and dynamic dev/test/deploy cycle
- weak separation between both layers
- long-term and stable dev/test/deploy cycle
- good Sec&Dep

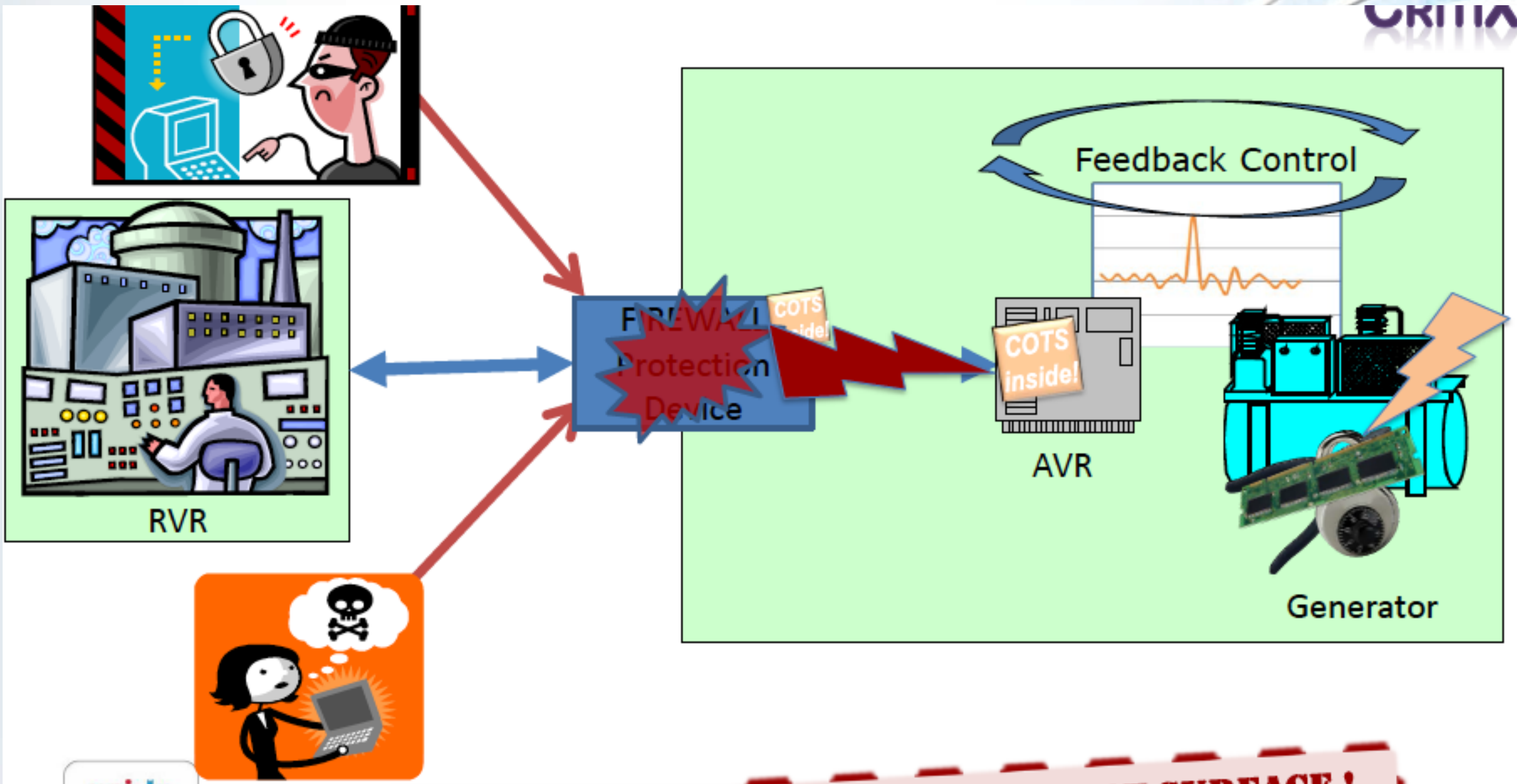
AMPLIFIED THREAT SURFACE !

- ironically, causes of concern lie in SDN's main benefits:
  - *network programmability and control logic centralization*
  - *smaller diversity*
  - *new threats that did not exist before or were harder to exploit*



[Kreutz et al., HotSDN'13]

AMPLIFIED THREAT SURFACE !



RVR

FIREWALL Protection Device

COTS inside!

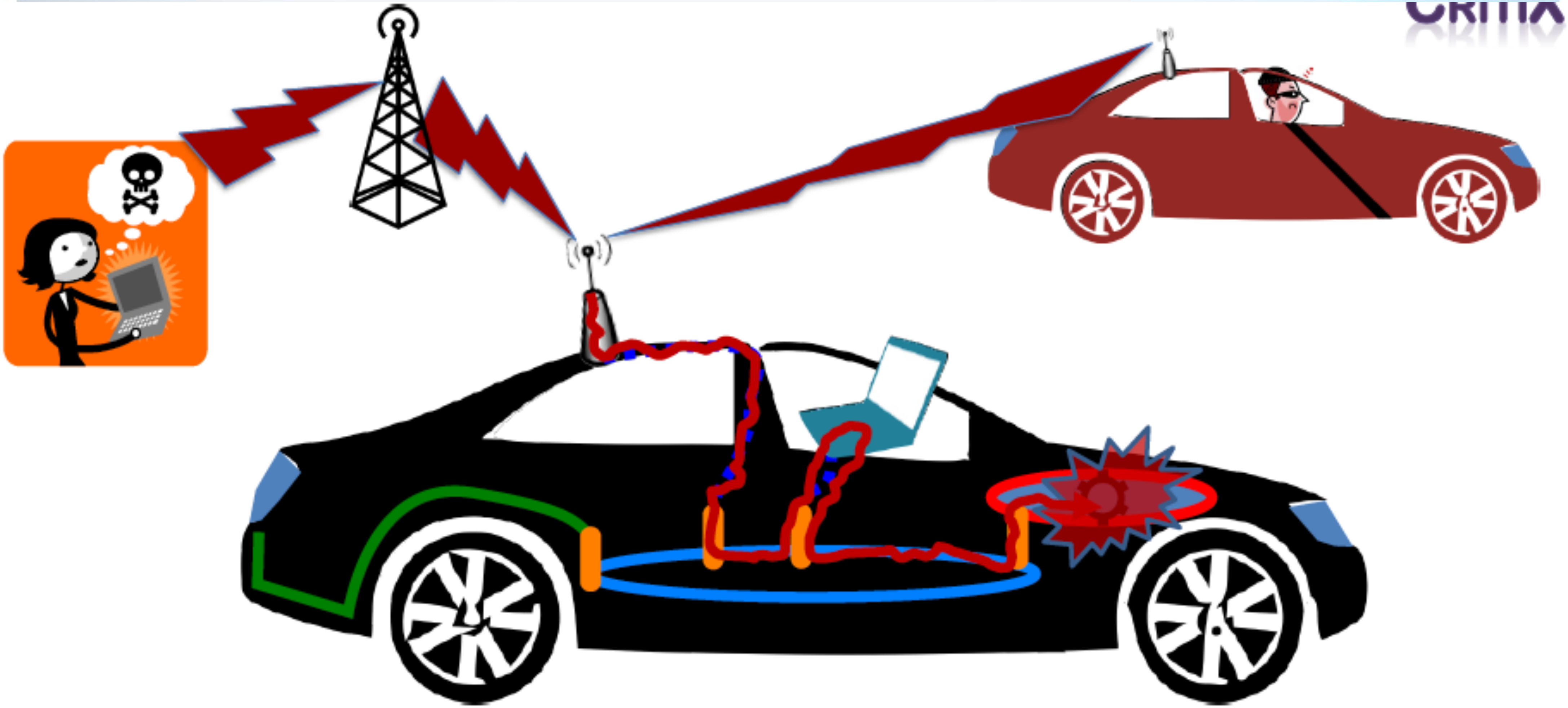
Feedback Control

COTS inside!

AVR

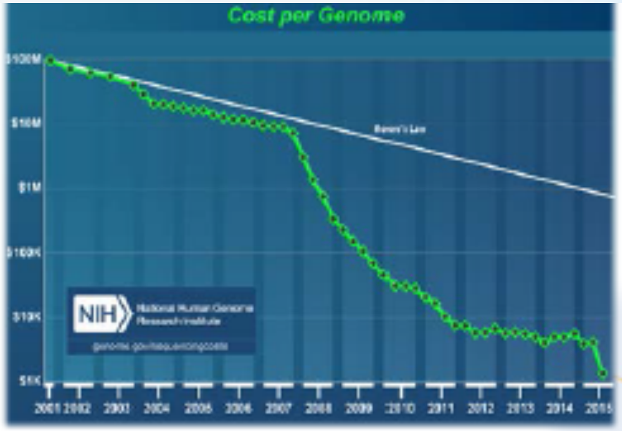
Generator

AMPLIFIED THREAT SURFACE !



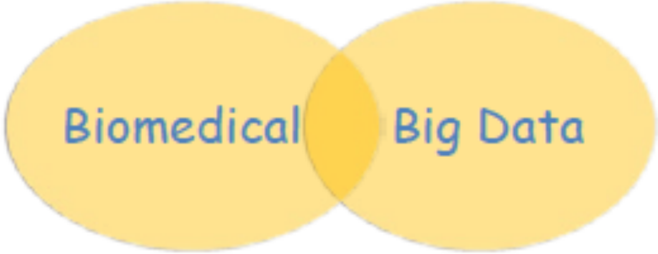
AMPLIFIED THREAT SURFACE !

- Due to Next Generation Sequencing, we will soon be generating more genomic data than we can currently securely store and process



- Handling terabytes of information has become the norm for genomics, but trend is to scale up.

- This brings cloud and big data analytics onto the agenda, challenging the secure storage and analysis of such data, e.g. use of clouds


Biomedical
Big Data

AMPLIFIED THREAT SURFACE !

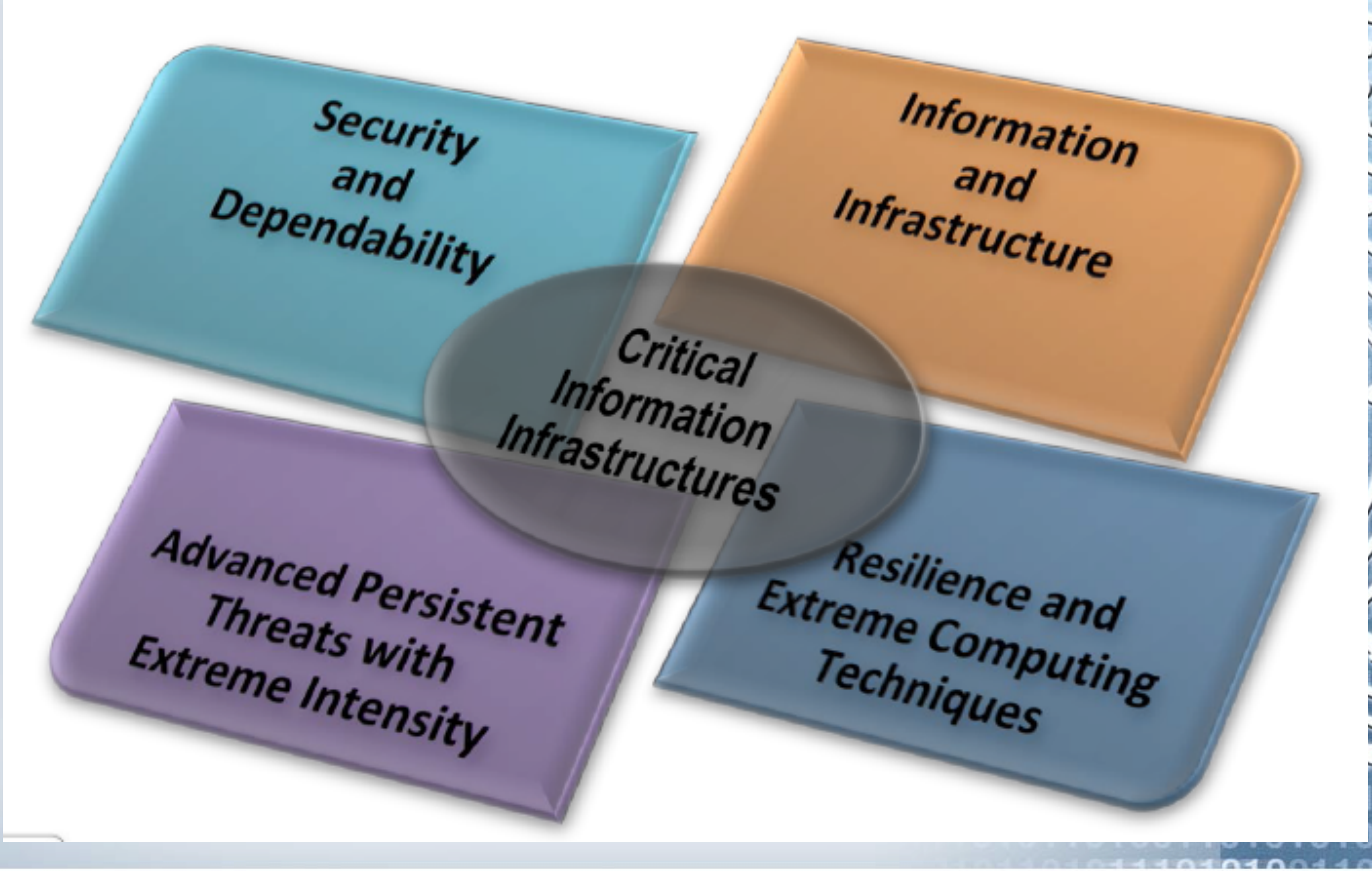
CritiX research vision

CRITIX - Critical and Extreme Security and Dependability Research Lab

Research enablers for the next generation of protection

- *Critical Security and Dependability:*
  - information infrastructures under advanced persistent threats
- *Extreme Computing:*
  - CSE pushed to the extremes of functional and non-functional properties
- *Architecting and designing for resilience:*
  - accidental and malicious faults; protection in an incremental way; automatic adaptation

Meeting the Challenges of Critical Dependability and Security



Security and Dependability

Information and Infrastructure

Critical Information Infrastructures

Advanced Persistent Threats with Extreme Intensity

Resilience and Extreme Computing Techniques

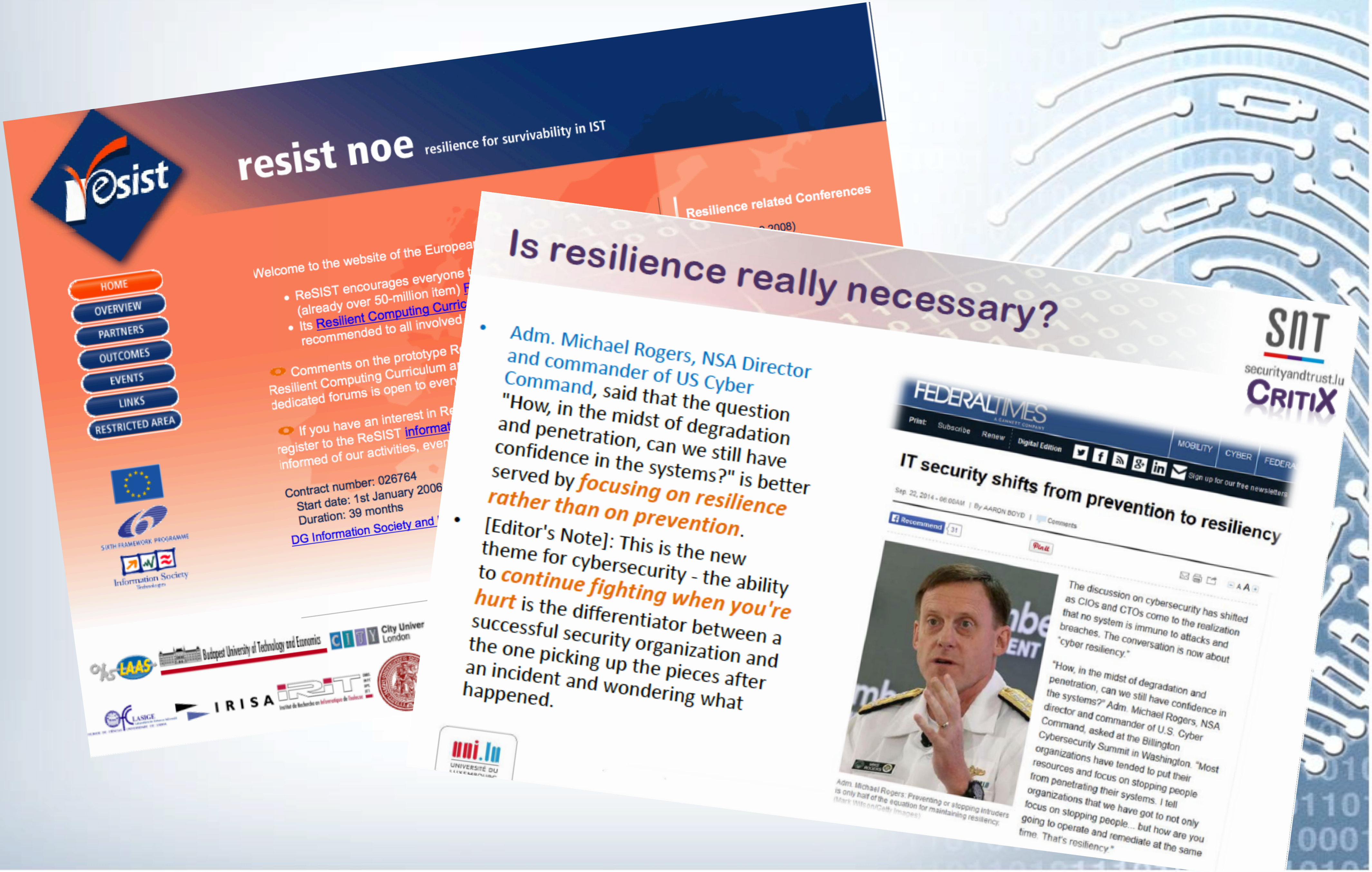
Architecting and designing for resilience

- comprehensive approach to those threats, from first principles: *“build defence in”*

- simultaneously coping with accidental and malicious faults
- provide protection in an incremental way
- automatically adapt to a dynamic range of severity of threats

- seek unattended and perpetual operation

Is resilience really necessary?



Welcome to the website of the Europea

- ReSIST encourages everyone t (already over 50-million item) R
- Its Resilient Computing Curric recommended to all involved

Comments on the prototype R Resilient Computing Curriculum a dedicated forums is open to every

If you have an interest in Re register to the ReSIST informat informed of our activities, even

Contract number: 026764
Start date: 1st January 2006
Duration: 39 months

DG Information Society and

Is resilience really necessary?

- Adm. Michael Rogers, NSA Director and commander of US Cyber Command, said that the question "How, in the midst of degradation and penetration, can we still have confidence in the systems?" is better served by ***focusing on resilience rather than on prevention***.
- [Editor's Note]: This is the new theme for cybersecurity - the ability to ***continue fighting when you're hurt*** is the differentiator between a successful security organization and the one picking up the pieces after an incident and wondering what happened.

IT security shifts from prevention to resiliency

Sep. 22, 2014 - 06:00AM | By AARON BOYD | Comments

The discussion on cybersecurity has shifted as CIOs and CTOs come to the realization that no system is immune to attacks and breaches. The conversation is now about "cyber resiliency."

"How, in the midst of degradation and penetration, can we still have confidence in the systems?" Adm. Michael Rogers, NSA director and commander of U.S. Cyber Command, asked at the Billington Cybersecurity Summit in Washington. "Most organizations have tended to put their resources and focus on stopping people from penetrating their systems. I tell organizations that we have got to not only focus on stopping people... but how are you going to operate and remediate at the same time. That's resiliency."

Adm. Michael Rogers: Preventing or stopping intruders is only half of the equation for maintaining resiliency. (Mark Wilson/Getty Images)

Designing and architecting for resilience

1.	we want systems to operate through faults and attacks in a seamless manner, in an automatic way	Preventing and Tolerating Faults and Intrusions
2.	we want systems to endure the fact that operating conditions and environments are everyday more uncertain and/or hostile	Handling Incremental Threat Severity
3.	we want systems to be deployed in unattended manner	Resisting Continued Threats
4.	we want systems to attain very high levels of assurance	Validating and Assessing Assumptions and Mechanisms

(P. Verissimo, M. Correia, N. Neves, P. Sousa, "Intrusion-Resilient Middleware Design and Validation", in Information Assurance, Security and Privacy Services, ser. Handbooks in Info Systems. Emerald, May'09)

A methodic approach to modular and distributed resilient computing

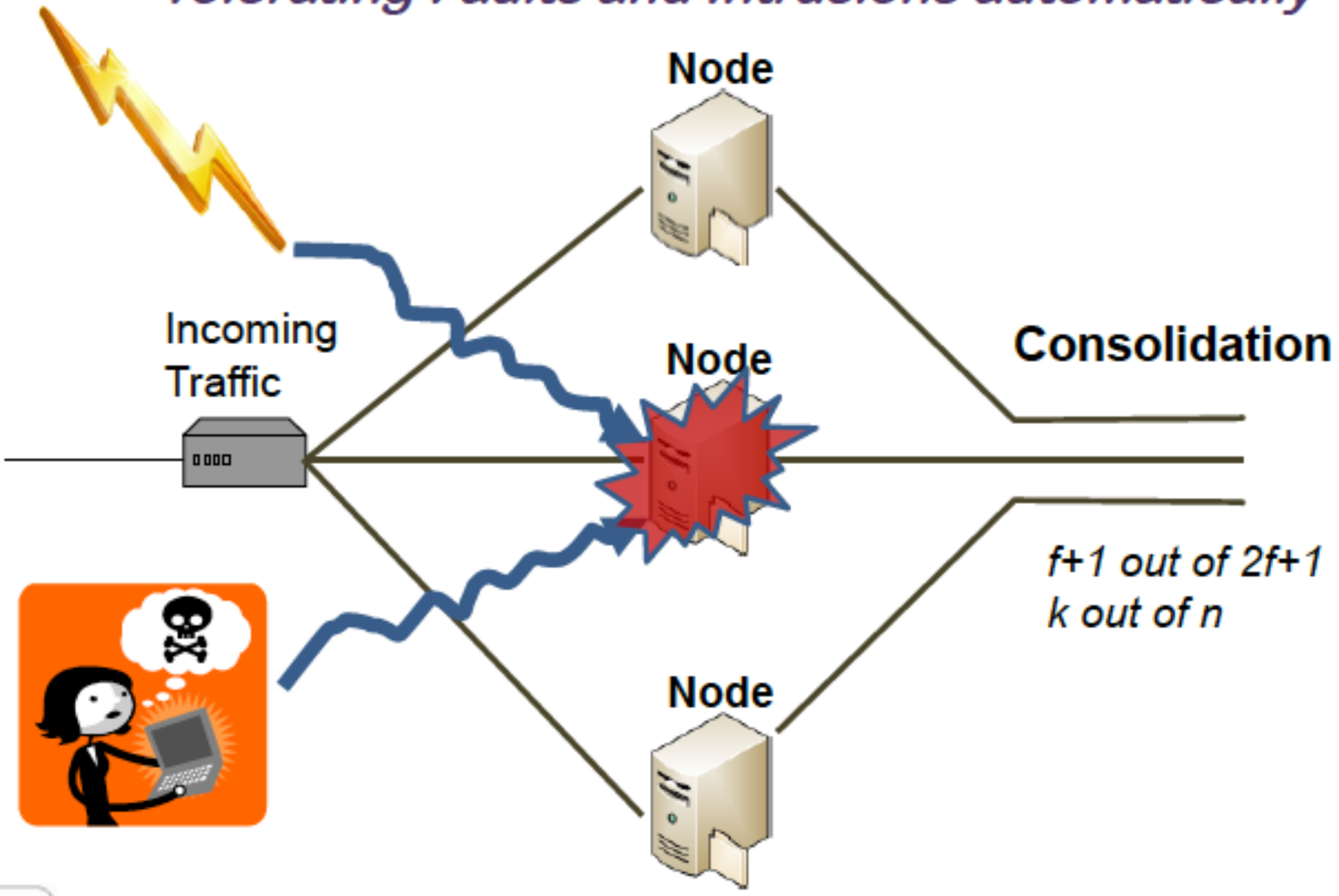
- Fault and intrusion tolerance, or automatic security and dependability
- Handle increasing threat severity
- Resist continued threats

- Divide-and-conquer to beat extreme threats
- Hybrid models and architectures
- Ultra-reliable trusted components
- High-confidence vertical verification
- Privacy- and integrity-preserving data processing

Fault and Intrusion Tolerance (FIT)

An abstract solution

Tolerating Faults and Intrusions automatically



Node

Incoming Traffic

Node

Consolidation

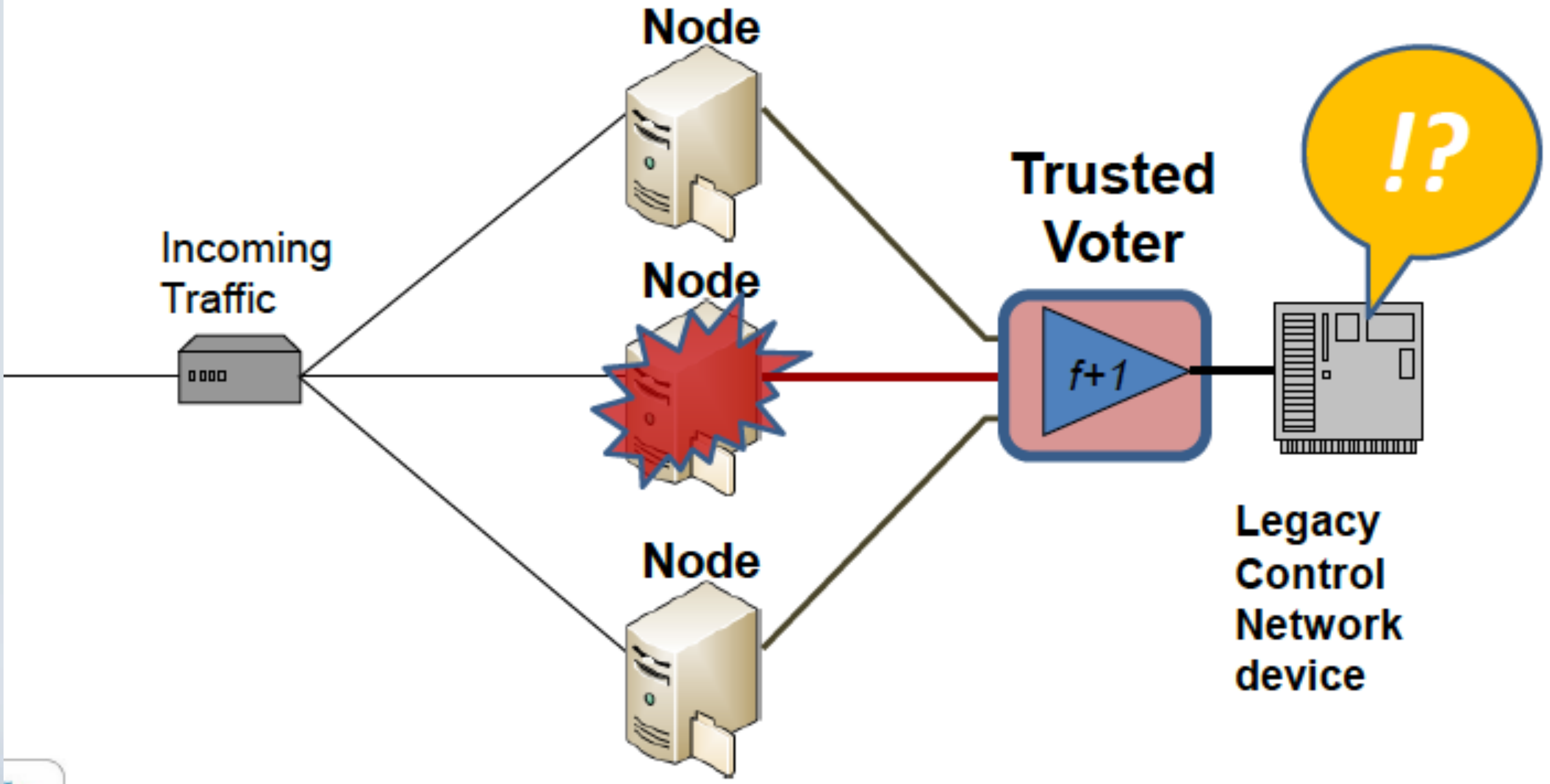
Node

f+1 out of 2f+1
k out of n

f – max. number of faulty replicas (f=1 in this example)

Fault and Intrusion Tolerance (FIT)

Handling legacy systems



Node

Node

Node

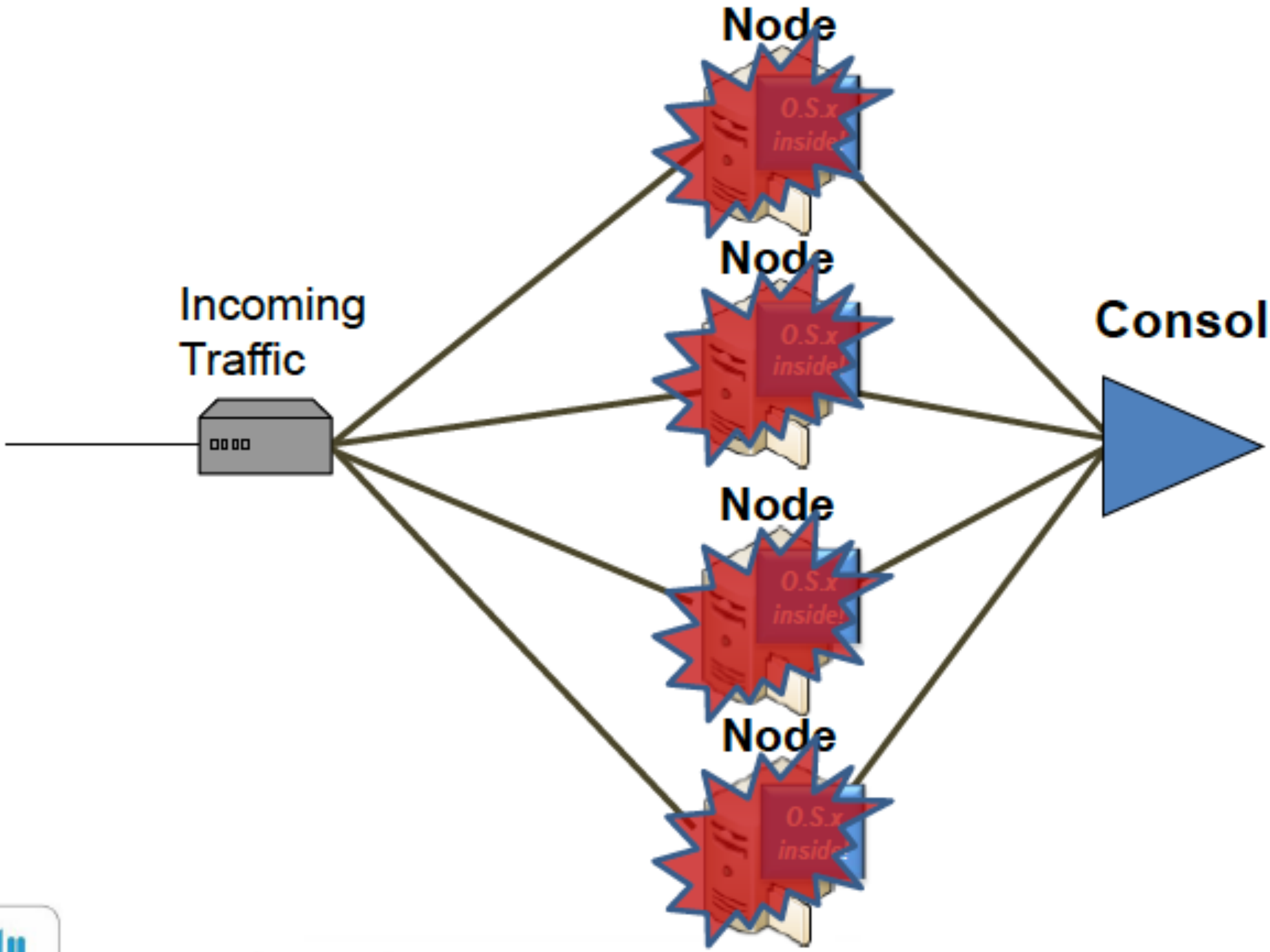
Incoming Traffic

Trusted Voter

Legacy Control Network device

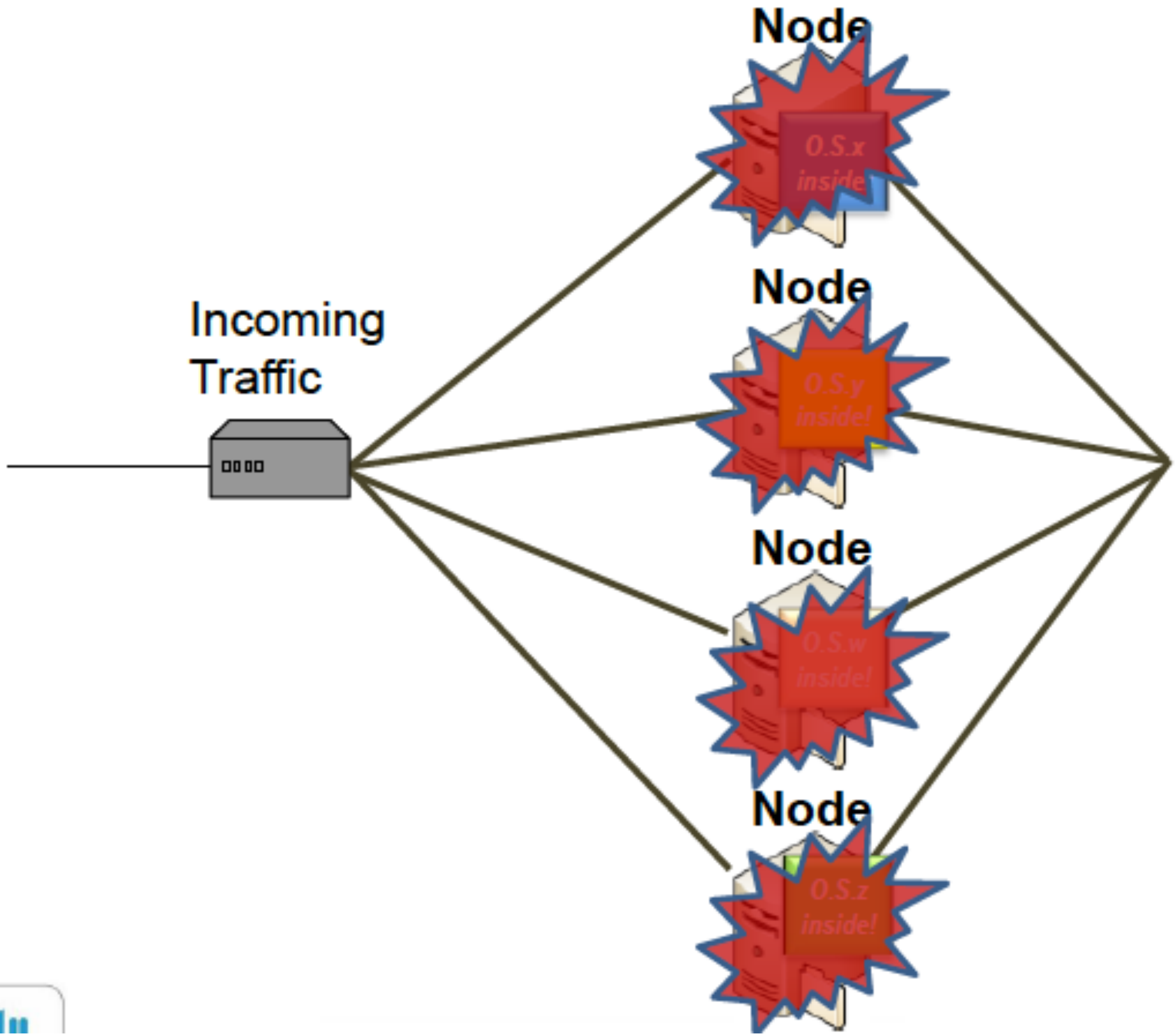
Fault and Intrusion Tolerance (FIT)

The common-mode fault problem



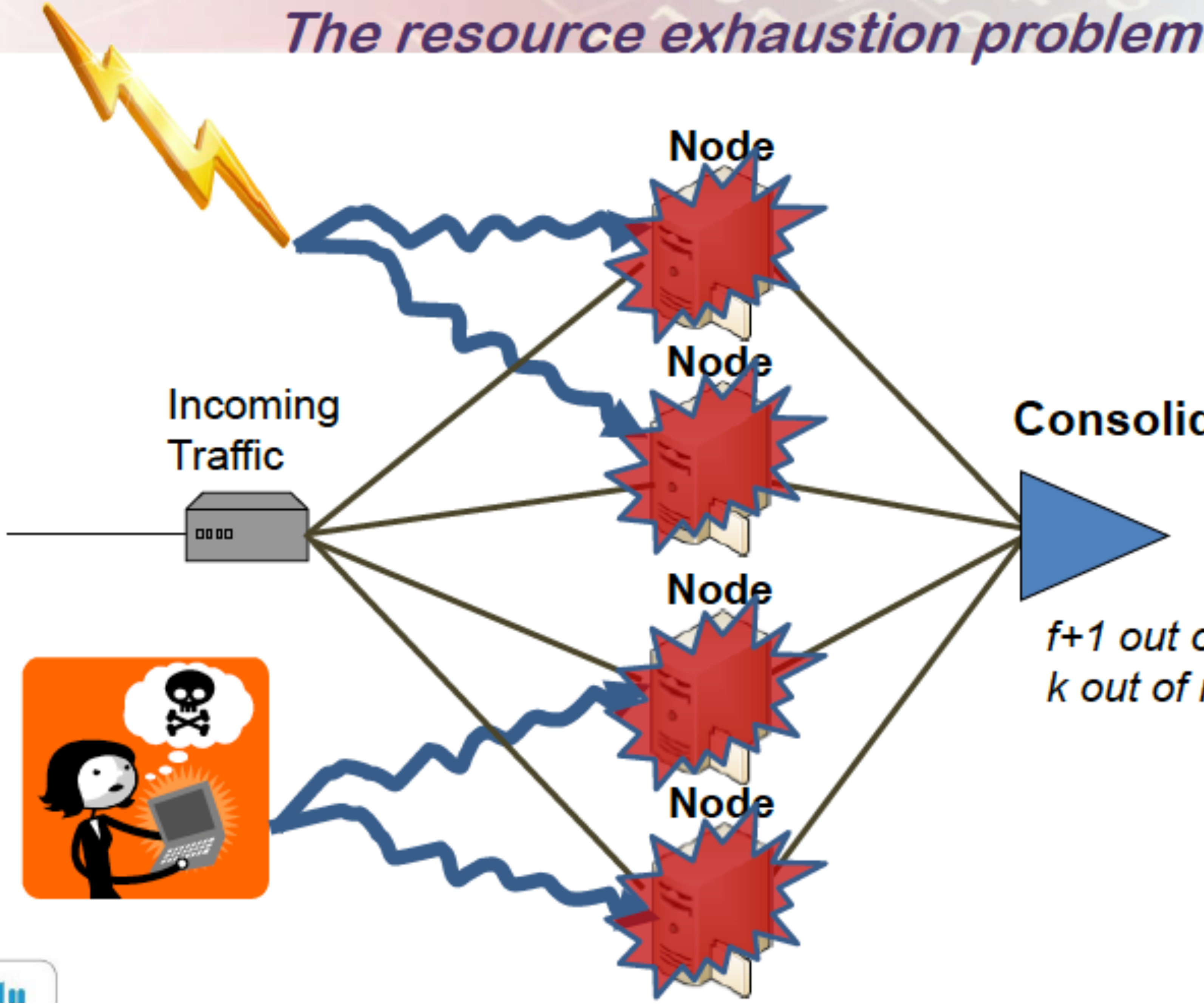
Fault and Intrusion Tolerance (FIT)

Mitigating common-mode faults



Fault and Intrusion Tolerance (FIT)

The resource exhaustion problem



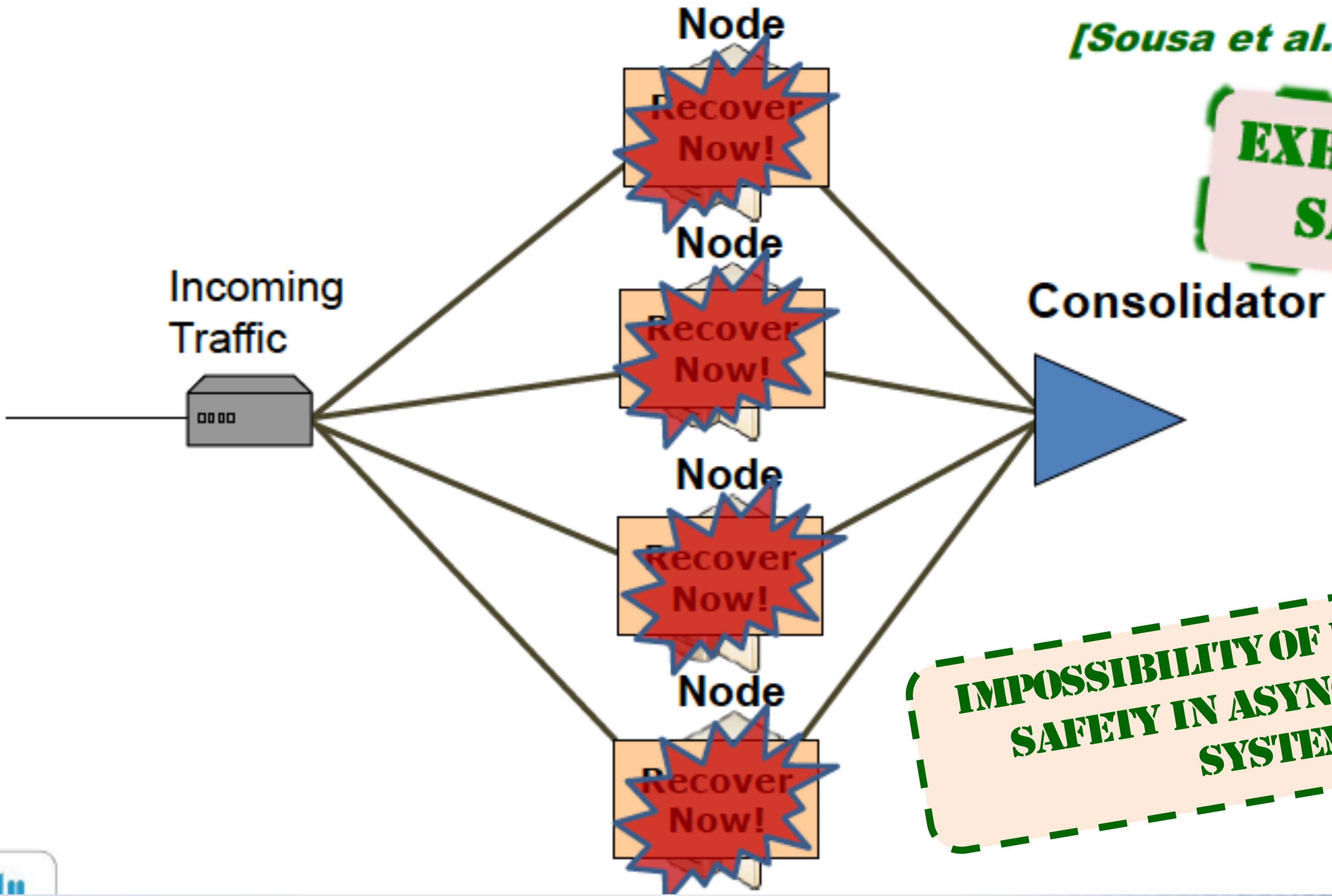
f+1 out of 3f+1
k out of n

Fault and Intrusion Tolerance (FIT)

Resisting Continued Threats

Seeking (unattended) perpetual execution

[Sousa et al., DSN 05]



EXHAUSTION SAFETY!

IMPOSSIBILITY OF EXHAUSTION SAFETY IN ASYNCHRONOUS SYSTEMS

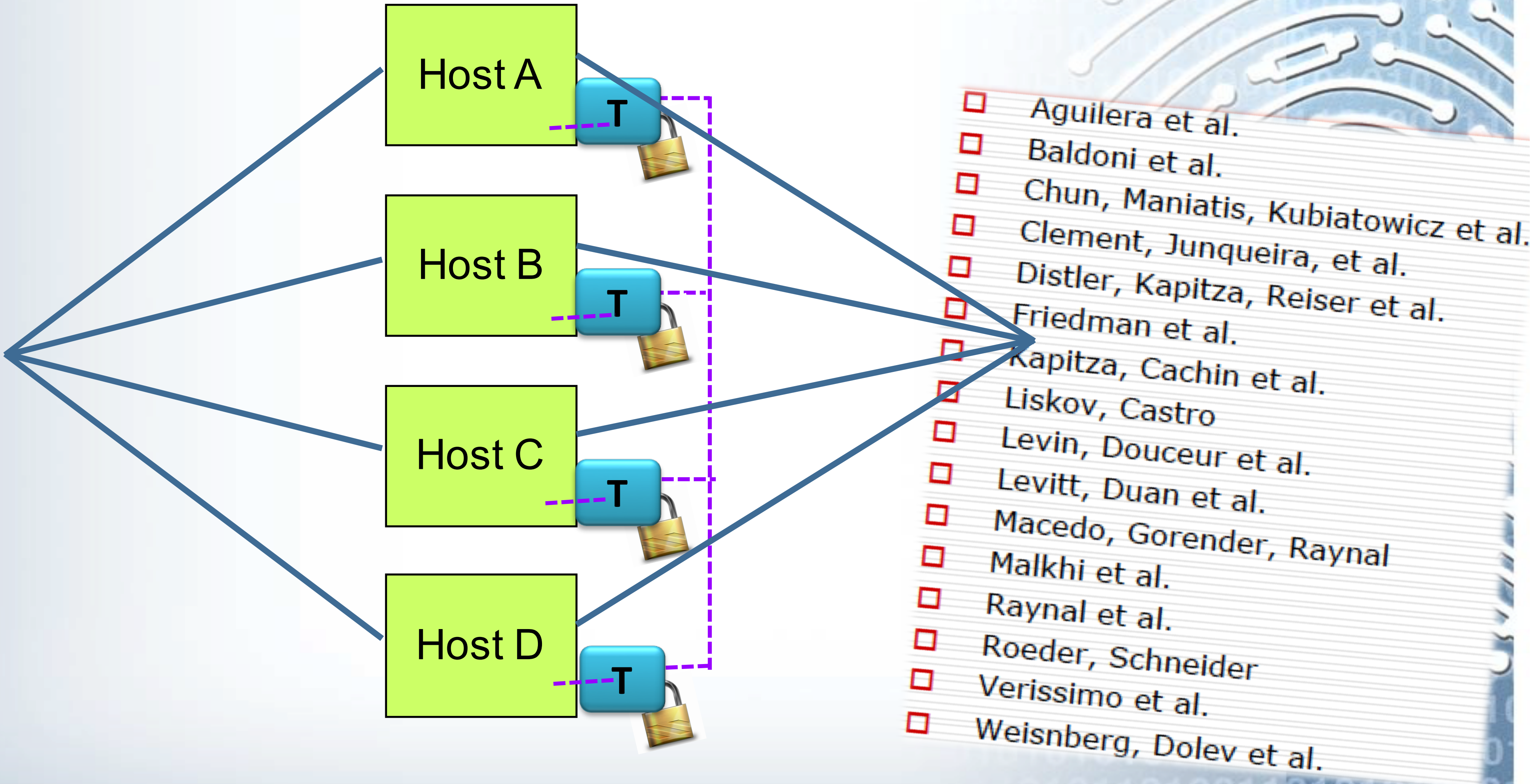
A methodic approach to modular and distributed resilient computing

- Fault and intrusion tolerance, or automatic security and dependability
- Handle increasing threat severity
- Resist continued threats

- Divide-and-conquer to beat extreme threats
- Hybrid models and architectures
- Ultra-reliable trusted components
- High-confidence vertical verification
- Privacy- and integrity-preserving data processing

Hybrid models and architectures

Leveraging power at right place right time



- □ Aguilera et al.
- □ Baldoni et al.
- □ Chun, Maniatis, Kubiatowicz et al.
- □ Clement, Junqueira, et al.
- □ Distler, Kapitza, Reiser et al.
- □ Friedman et al.
- □ Kapitza, Cachin et al.
- □ Liskov, Castro
- □ Levin, Douceur et al.
- □ Levitt, Duan et al.
- □ Macedo, Gorender, Raynal
- □ Malkhi et al.
- □ Raynal et al.
- □ Roeder, Schneider
- □ Verissimo et al.
- □ Weisnberg, Dolev et al.

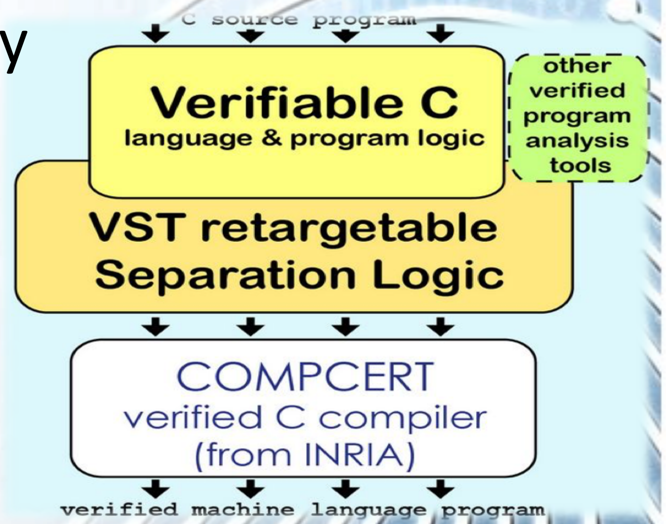
Ultra-reliable trusted components

Dependable Hypervisor and Manycore Architectures

- Extremely dependable computing architecture to withstand advanced and persistent threads
- Microhypervisor-based security and isolation is much better than legacy operating-systems, but still we see microhypervisor-level faults and attacks
- Verifying microhypervisor possible but at extreme costs / no protection against hardware faults
- Leverage properties of manycore systems to build dependable and secure microhypervisor-based systems

High-confidence vertical formal verification of critical components

- Verification of MinBFT's core trusted-trustworthy component (USIG):
- C implementation of USIG
- Coq specification/implementation for verification
- Verify that C code satisfies Coq, through VST (Verified Software Toolchain)
- Verify Coq spec satisfies desired safety properties through Coq
- generate target code from C with CompCert (formally verified C compiler)



C source program

Verifiable C
language & program logic

other verified program analysis tools

VST retargetable Separation Logic

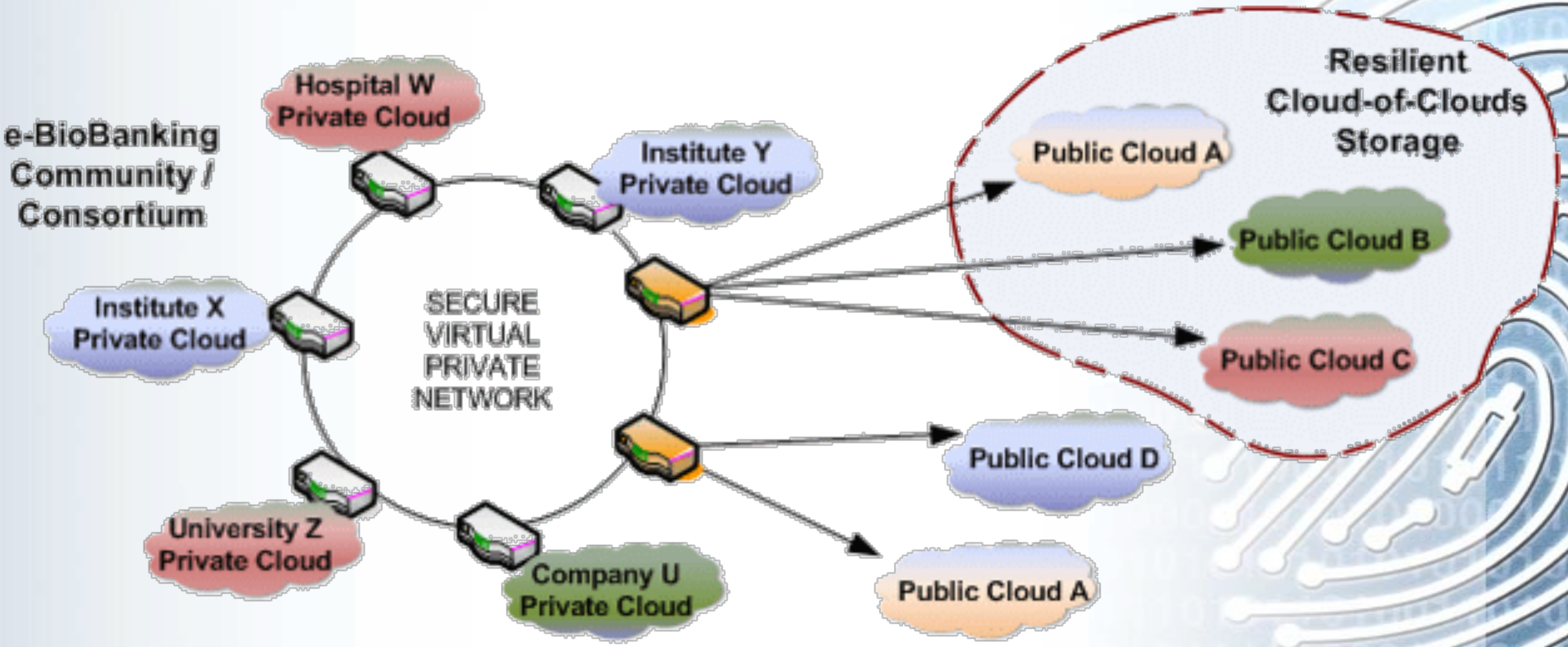
COMPCERT
verified C compiler
(from INRIA)

verified machine language program

- Re-design and partial verification of BFT-SMaRt
  - One of the few fully-implemented and efficient BFT-SMR protocols
  - We plan on building trustworthy leader change and reconfiguration components to plug into BFT-SMaRt
  - As mentioned above we will verify these components in Coq (theorem prover from INRIA)

Privacy- and integrity-preserving data processing

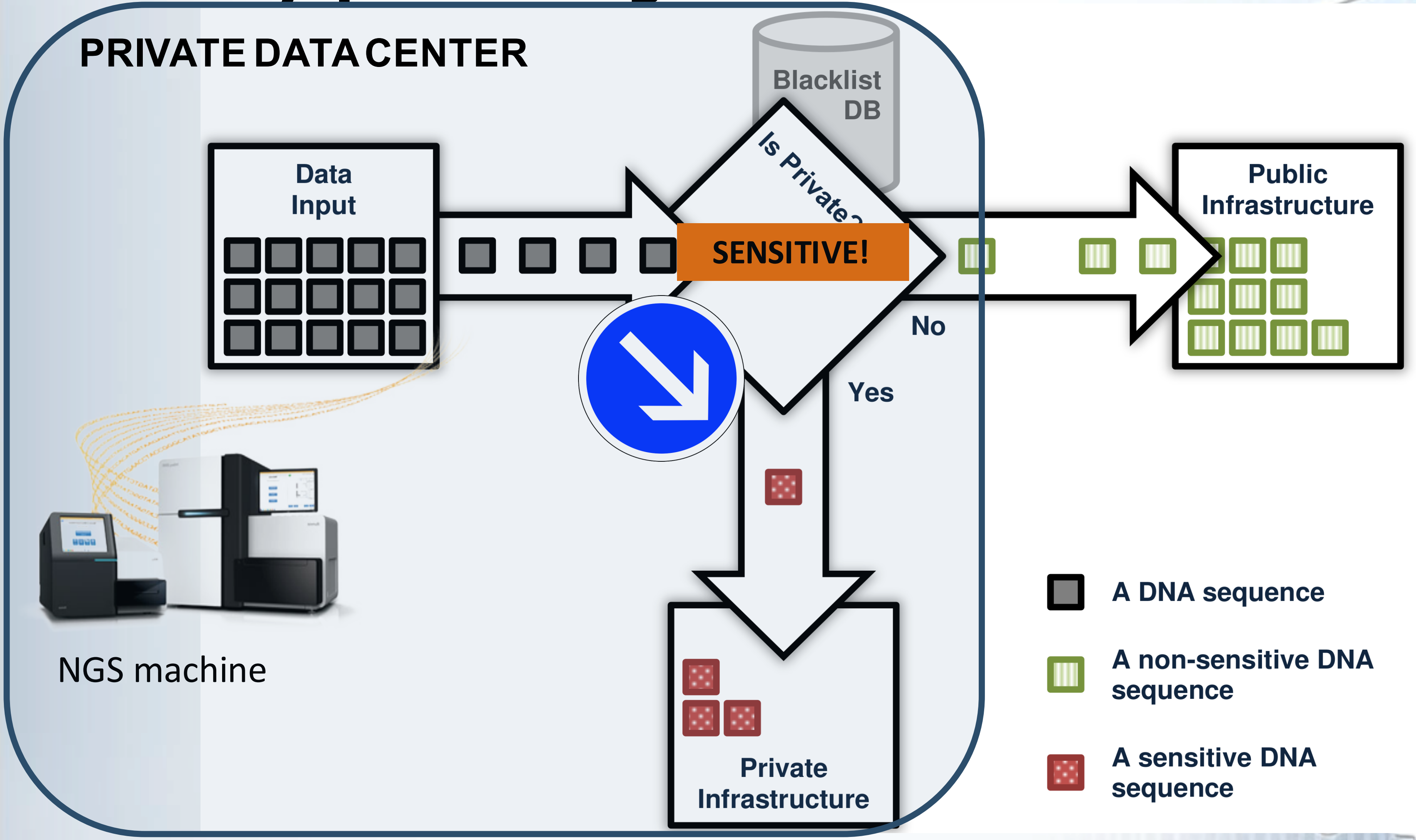
The e-biobanking vision



e-BioBanking Community / Consortium
Hospital W Private Cloud
Institute Y Private Cloud
Institute X Private Cloud
SECURE VIRTUAL PRIVATE NETWORK
University Z Private Cloud
Company U Private Cloud
Resilient Cloud-of-Clouds Storage
Public Cloud A
Public Cloud B
Public Cloud C
Public Cloud D
Public Cloud A

Alysson Bessani et al., BiobankCloud: a Platform for the Secure Storage, Sharing, and Processing of Large Biomedical Data Sets", in *Proc's of the 1st Int. Workshop on Data Mgt. and Analytics for Medicine and Healthcare (DMAH 2015)*, Hawaii, US, Sept. 2015.

Data privacy and integrity: Privacy-preserving Disclosure Filter



⬛ A DNA sequence

🟩 A non-sensitive DNA sequence

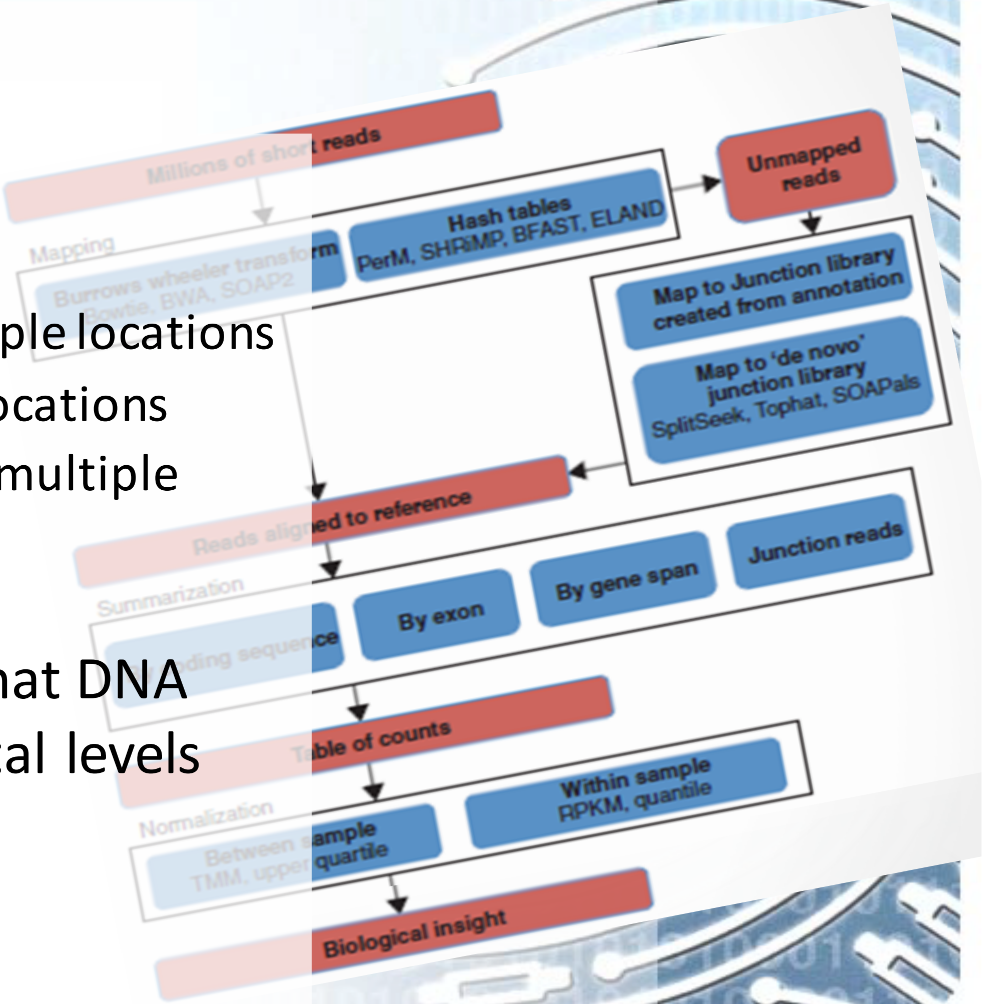
🟥 A sensitive DNA sequence

V. Cogo, A. Bessani, F. Couto, P. Verissimo, High-Throughput Method to Detect Privacy-Sensitive Human Genomic Data, in *Proc's of the Workshop on Privacy in the Electronic Society (WPES 2015)*, Denver, CO, US, Oct. 2015.

DNA workflows in an e-biobanking ecosystem

- Classical DNA workflow does not fit the e-biobanking vision, where:
  - data can be generated and stored in multiple locations
  - data should be accessible from different locations
  - data may be processed simultaneously at multiple locations, and/or remotely

- (any) DNA workflows must guarantee that DNA data must be protected, with incremental levels according to need:
  - when it is stored,
  - when computations are executed on it,
  - and when the results of algorithms are published.



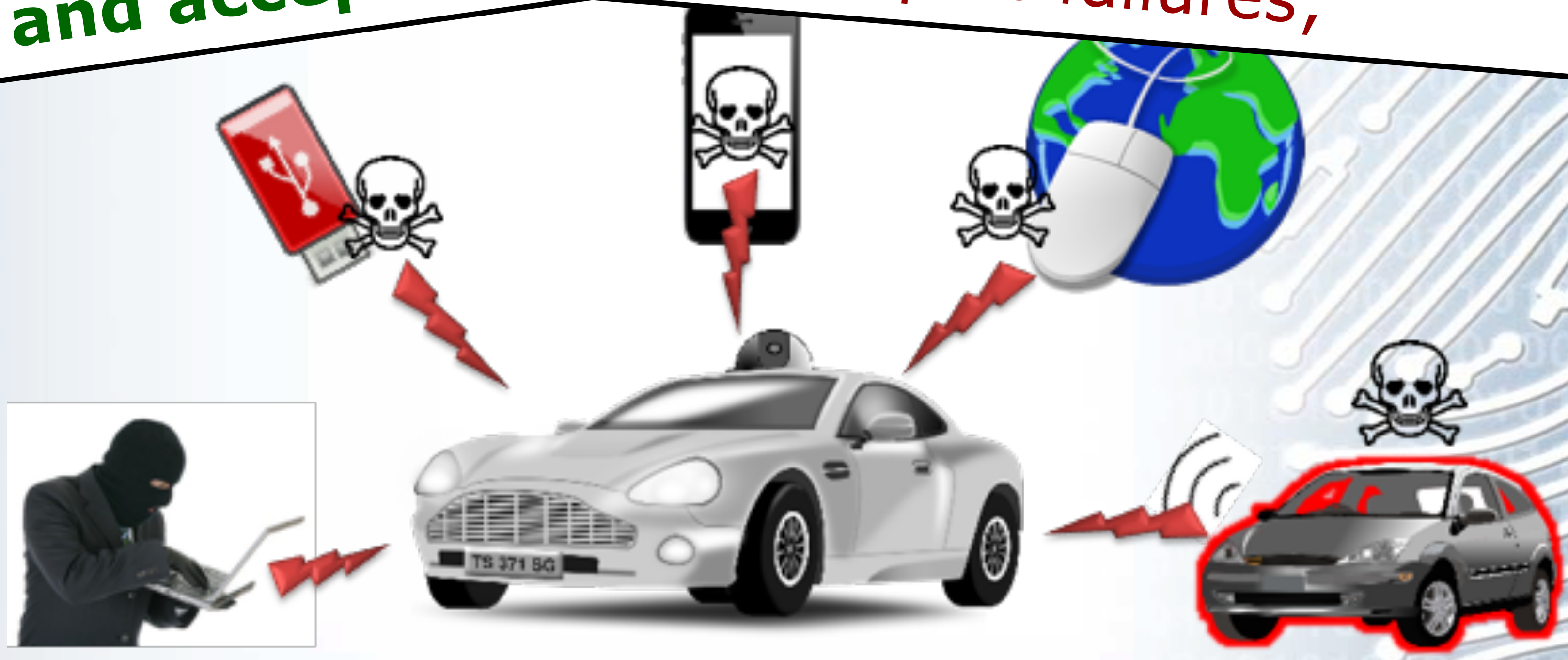
Privacy-preserving (really) distributed DNA alignment!

The safety-security gap in vehicle ecosystems

r lead to an **infinitesimal**
trophic failure;

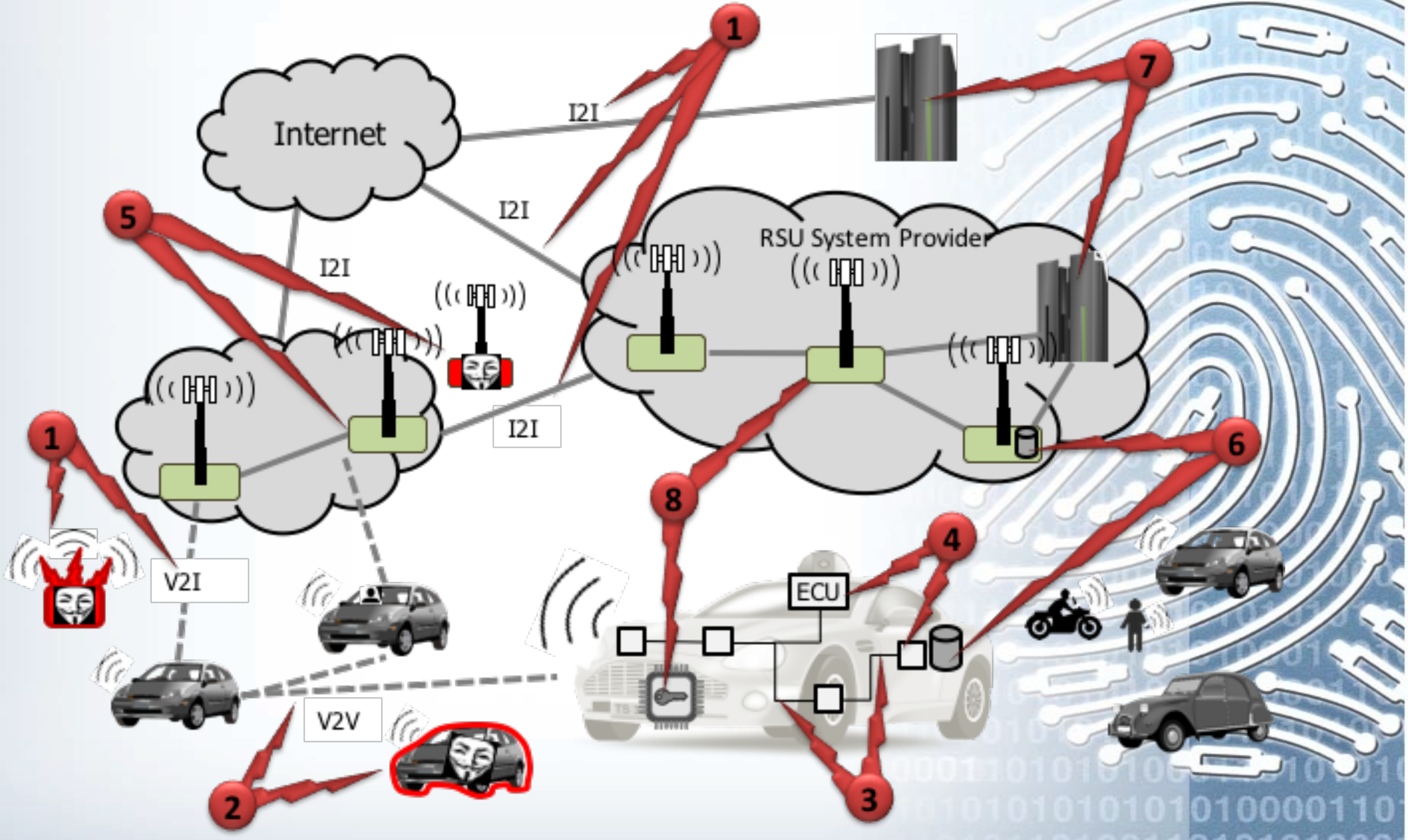
and accep

Vulnerabilities in a car **will** lead, rather sooner than later, to catastrophic failures;



Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems. Lima, A; Rocha, F; Volp, M; Verissimo, P. in Proc's 2nd ACM Workshop on Cyber-Physical Systems Security and PrivaCy (2016, October) @CCS, Vienna-Austria

Autonomous vehicle ecosystem threat plane



Paulo Esteves-Veríssimo

University of Luxembourg Faculty of Science, Technology and Communication

and SnT, the Interdisciplinary Centre for Security, Reliability and Trust

paulo.verissimo@uni.lu

http://wwwen.uni.lu/snt/people/paulo_esteves_verissimo

CRITIX @SnT

Critical and Extreme Security and Dependability

We’re hiring bright PhD students and willing to address these challenges!

Thank you!