Thwarting Cyber Attacks: Scientific alignment and Italian landscape

Roberto Baldoni
baldoni@dis.uniroma1.it

Lucca, October 10th 2017

Views and opinions expressed in the following slides are those of the author and do not necessarily reflect the official policy or position of any Italian government organization. Plans and/or model of cybersecurity development made within the analysis are not reflective of the position of any Italian government entity

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cyber Security National Lab

TOP DOWN VIEW

Robots
AI

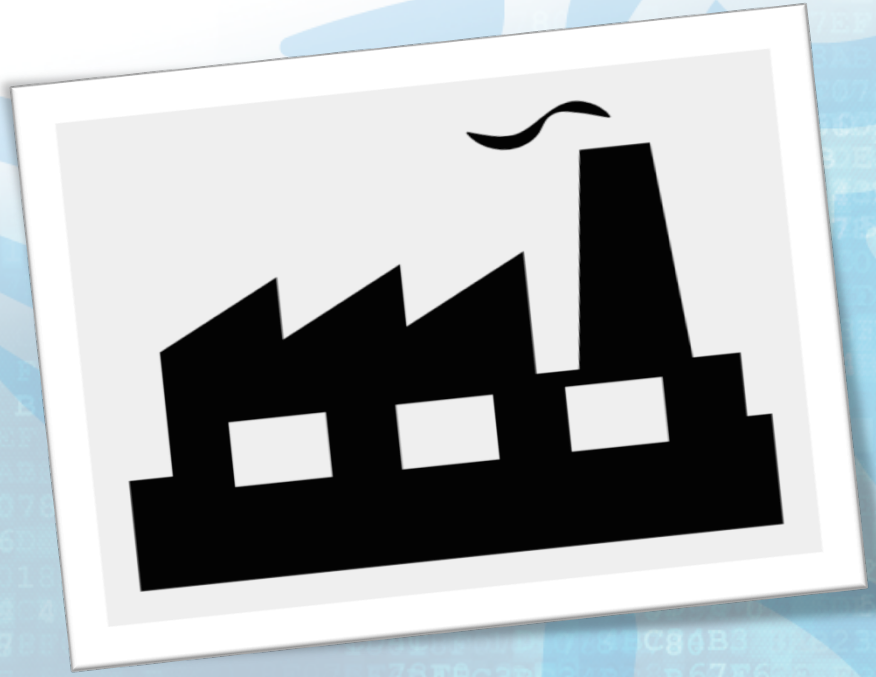
Economy
Humans
Conflicts

Physical World

Cyberspace

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cyber Security National Lab

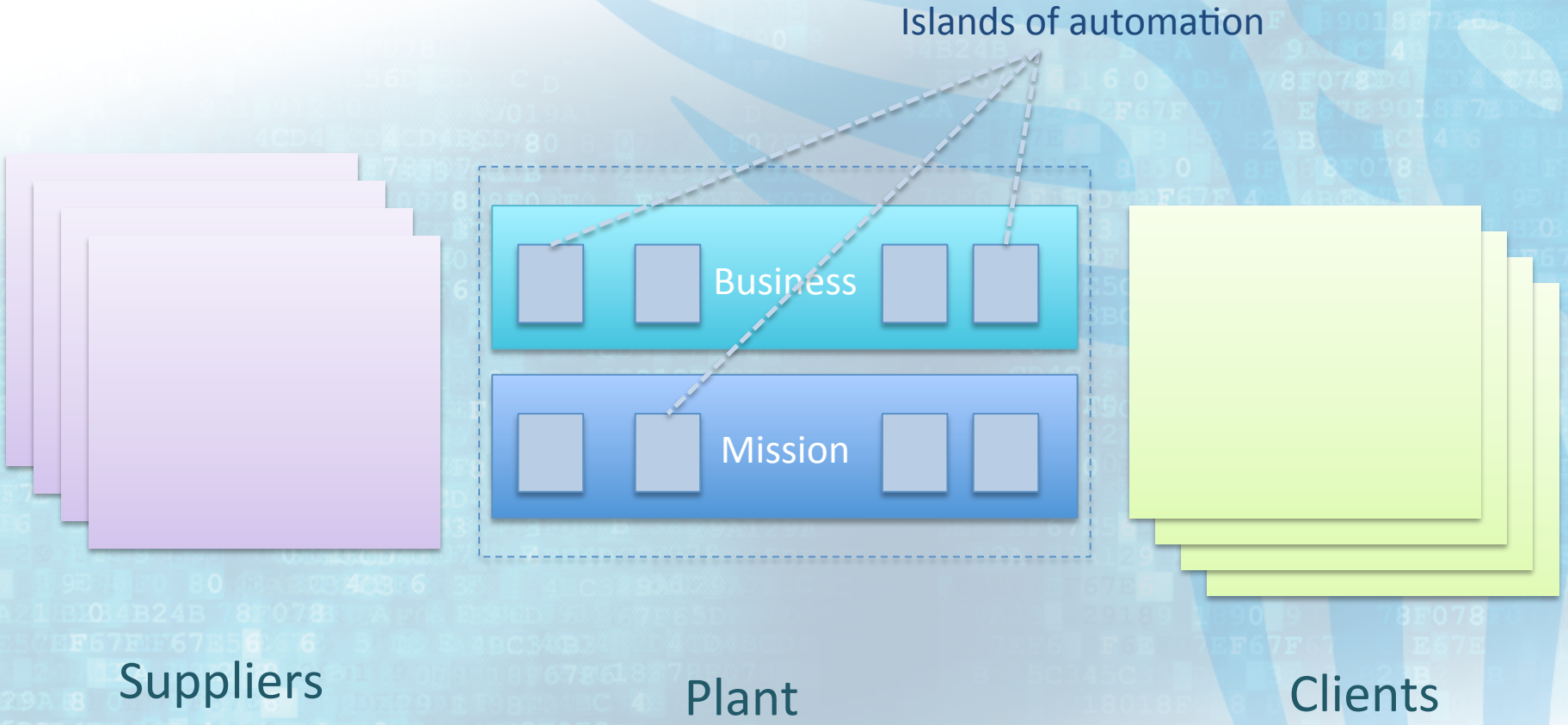
TOP DOWN VIEW



FACTORY TRANSFORMATION

(BOTTOM UP VIEW)

before 1993

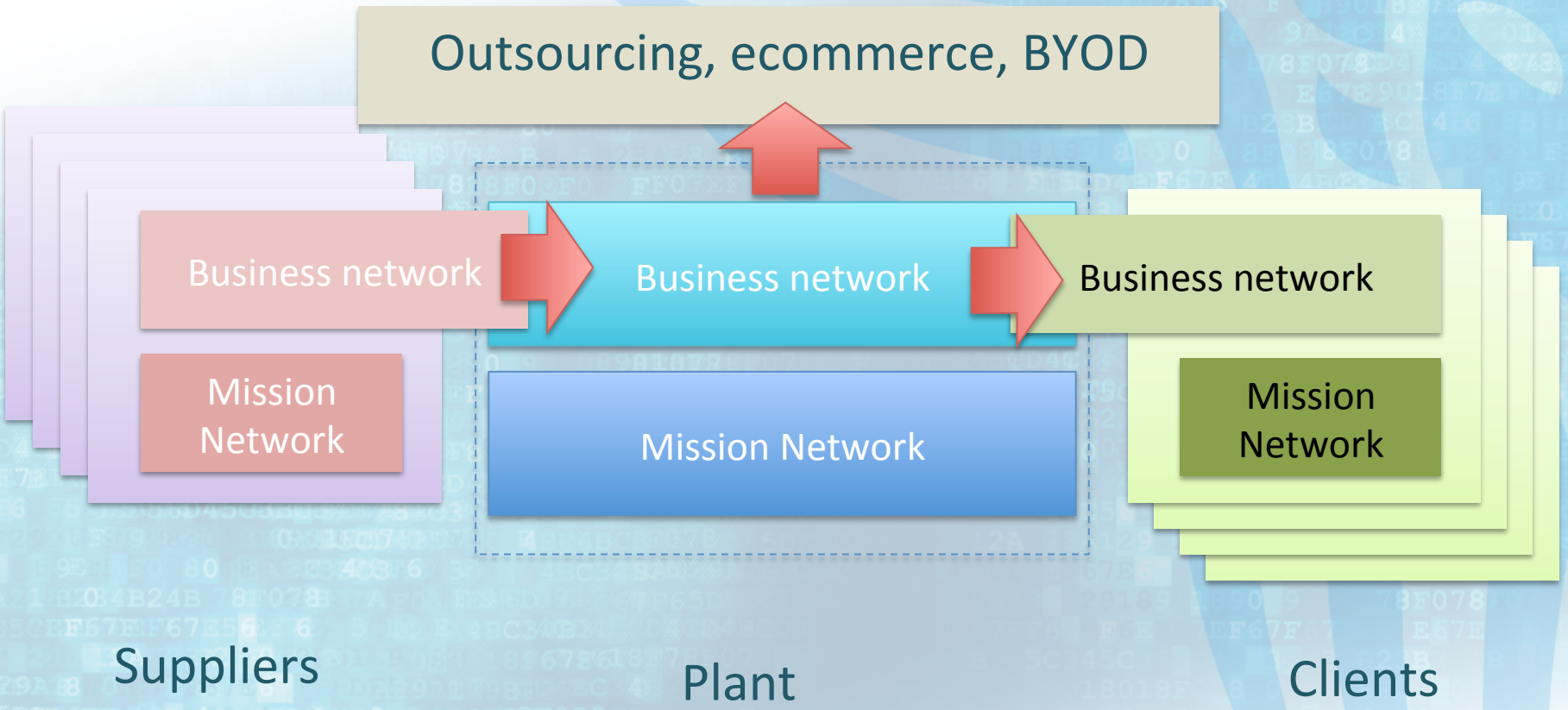

Islands of automation
Business
Mission
Suppliers
Plant
Clients

1993-2000: platform and network integration

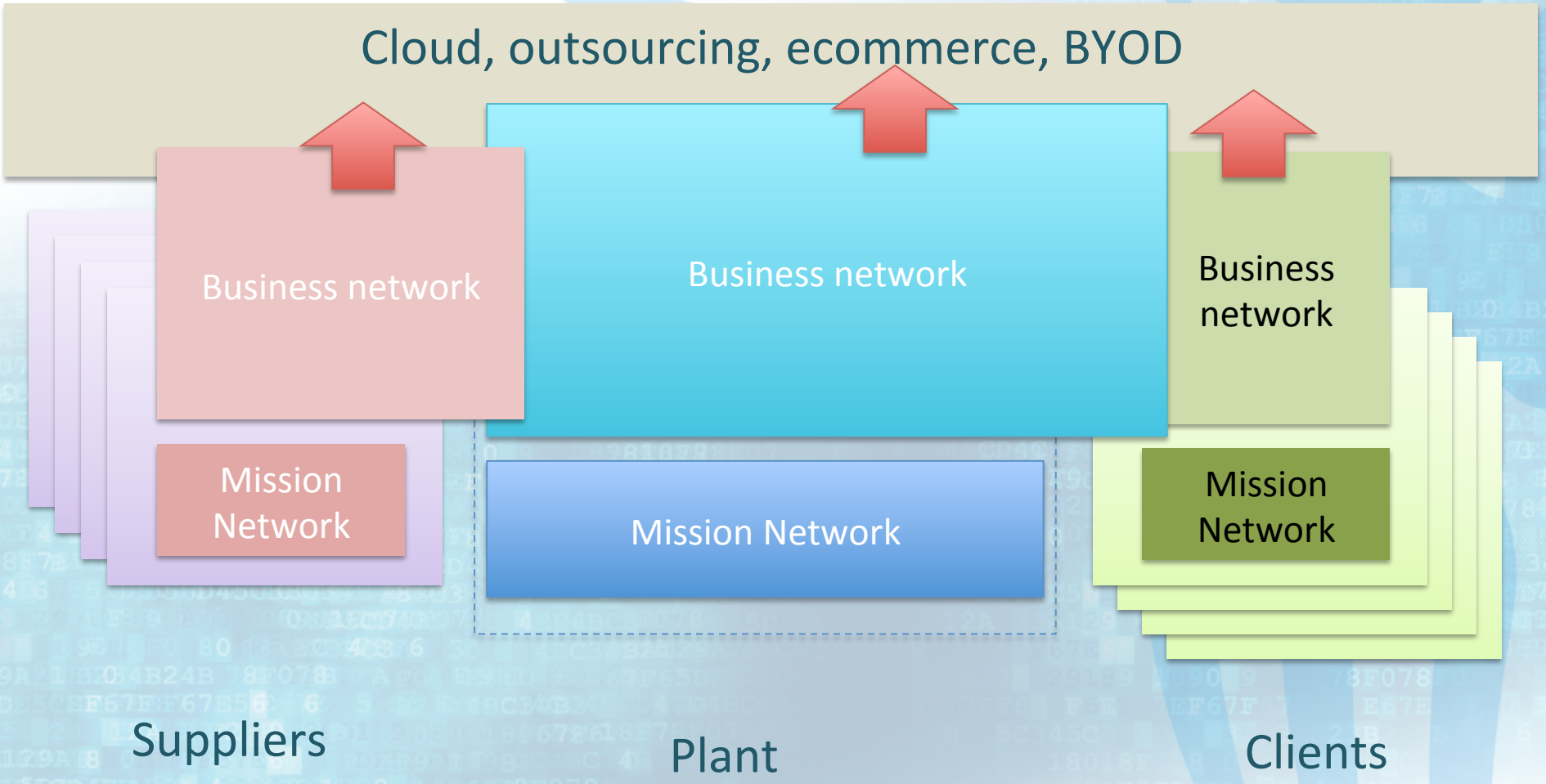
- ANSA
- CORBA
- Publish-Subscribe
- RPC

Middleware

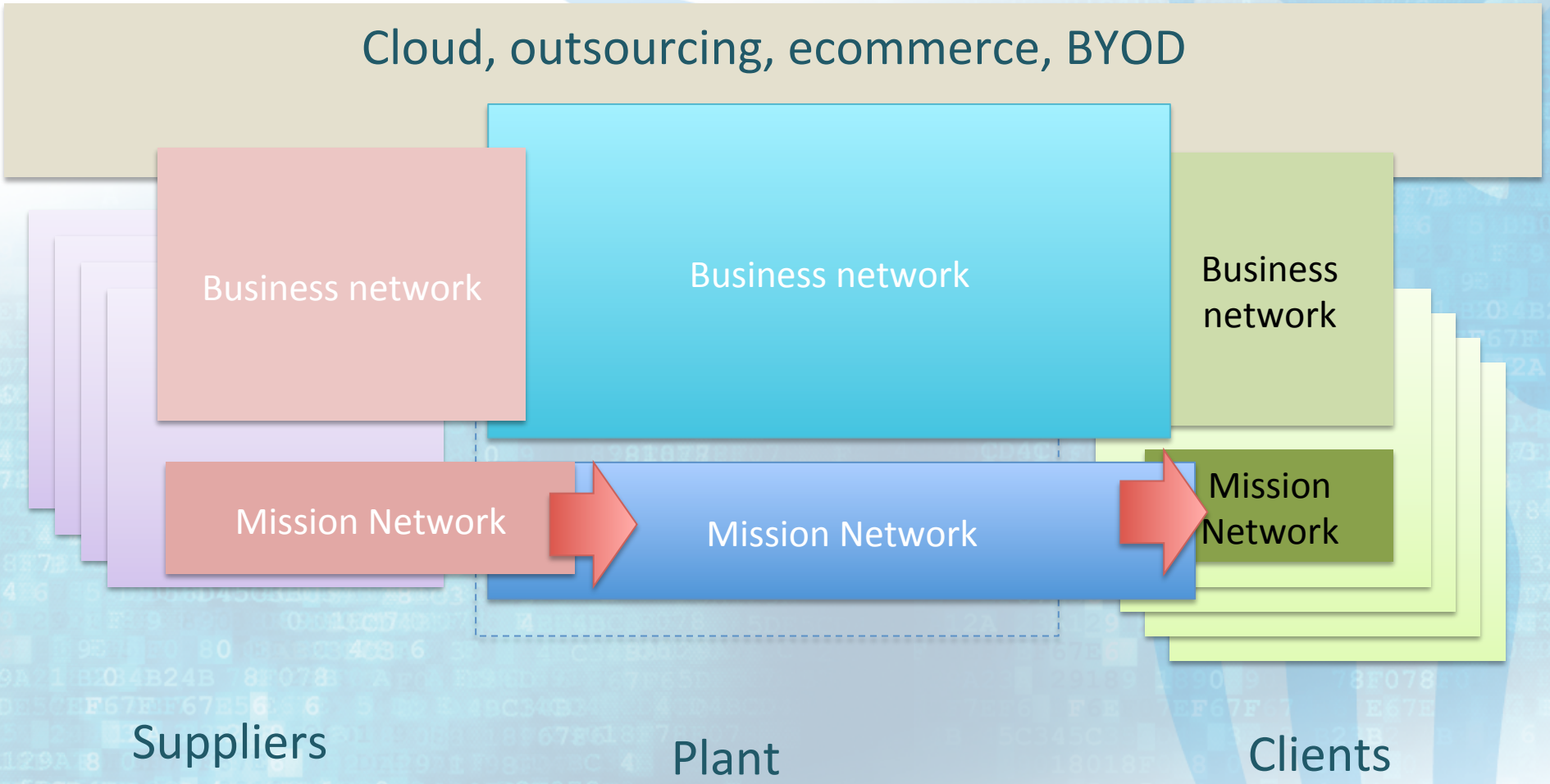
2000-now: web services, third parties, ecommerce, BYOD



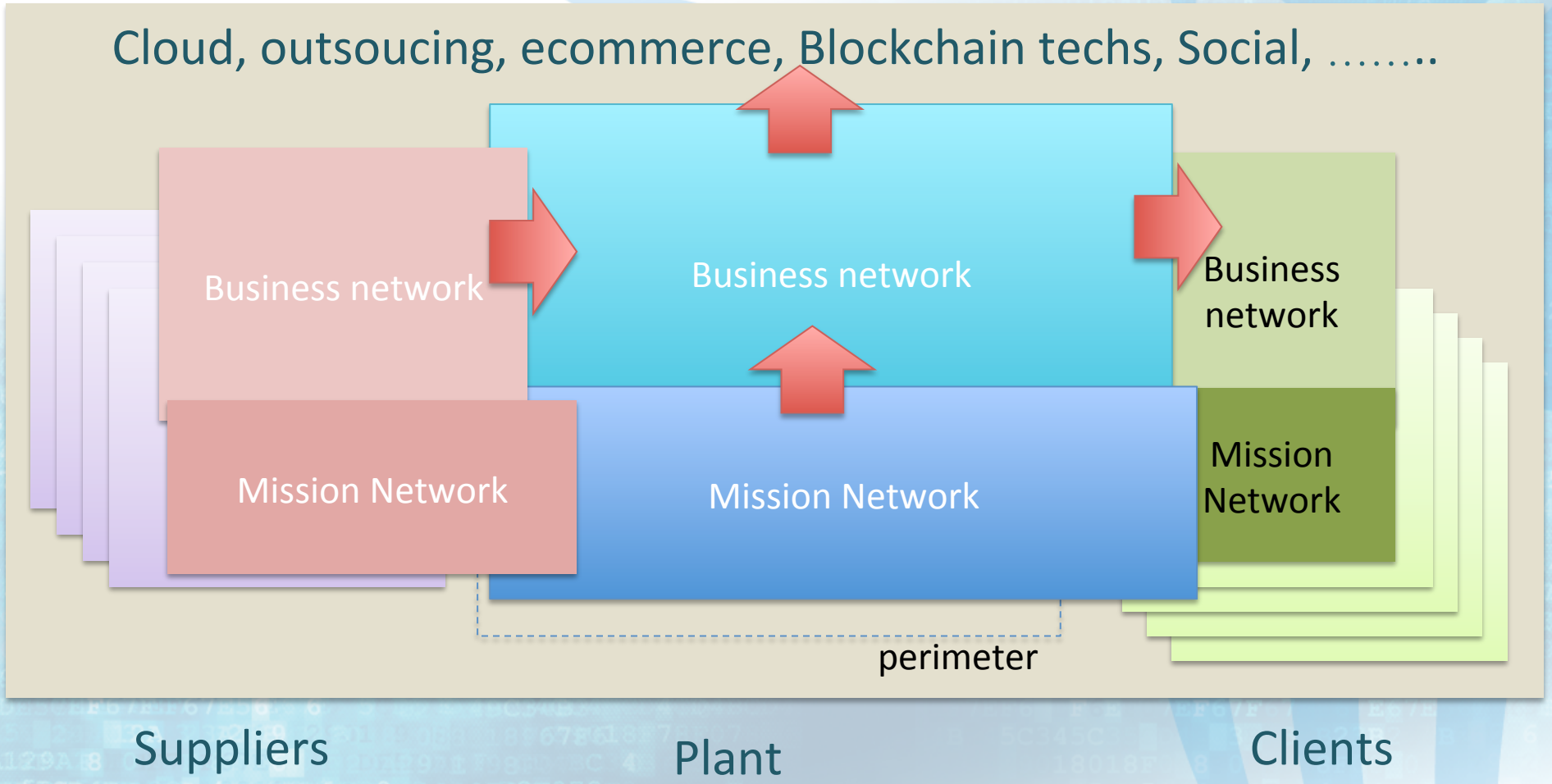
2010-now: cloud computing



2015-now: cyber-physical systems

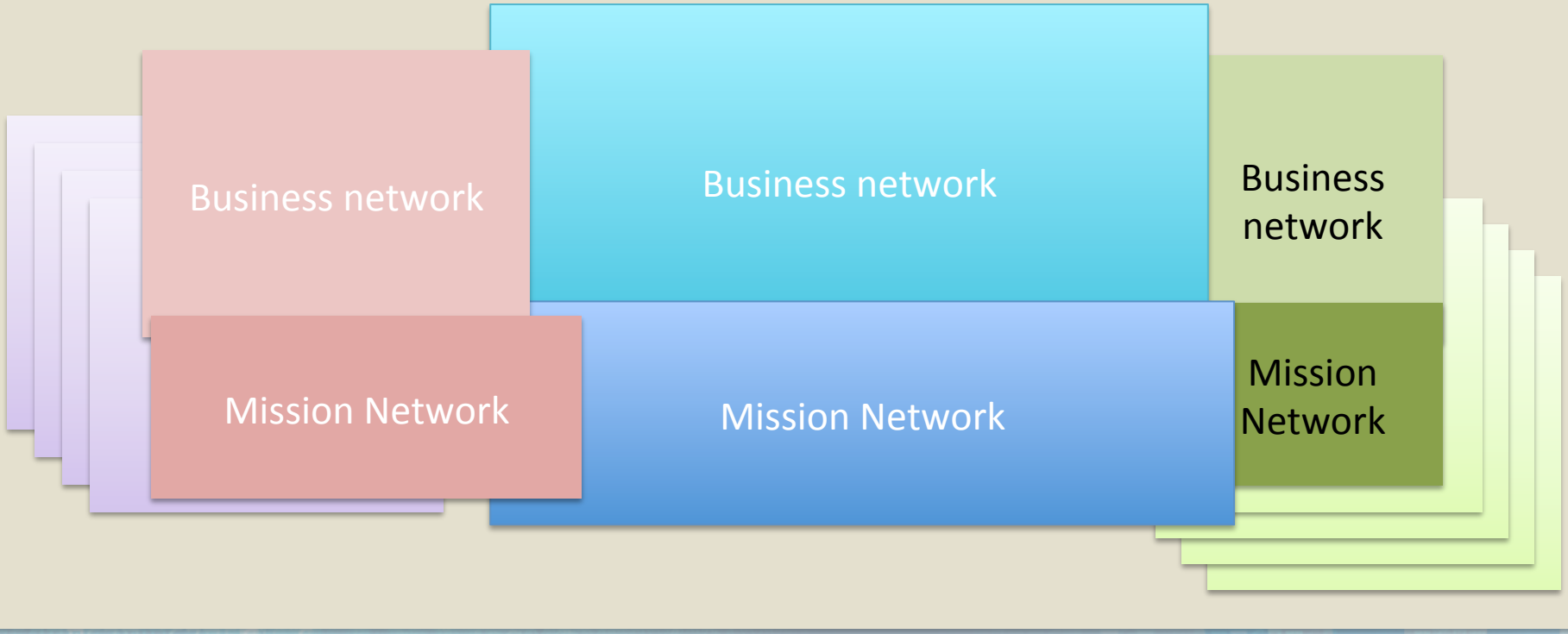


Future: AI, Pervasive Robotics, IoT, Bigdata, Blockchain



Where Cybersecurity is in this picture?

Cloud, outsoucing, ecommerce, BYOD, Blockchain techs, Social, ……..

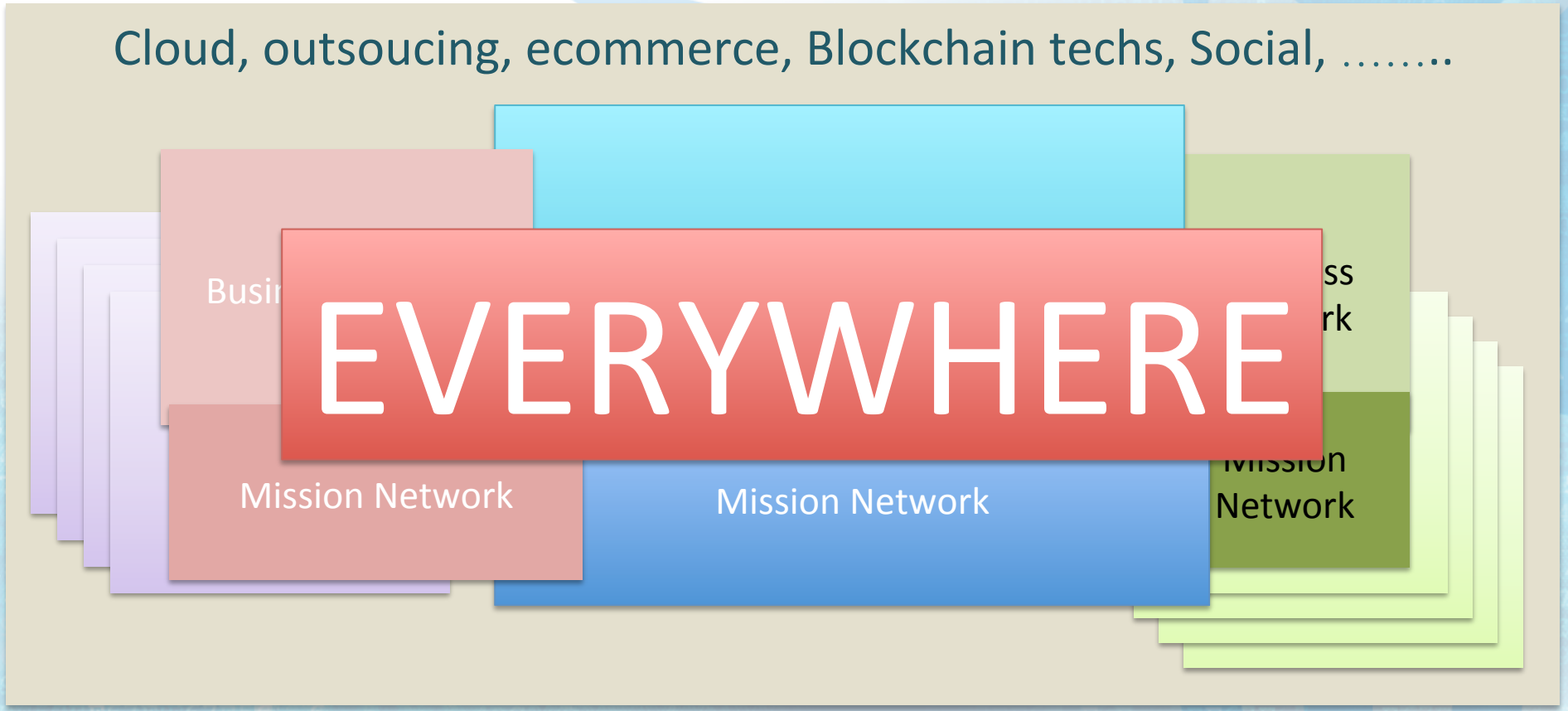


Suppliers

Plant

Clients

Where Cybersecurity is in this picture?



Every piece/layer is concerned by cybersecurity

- CPUs
- Software
- Smart devices
- Computers
- Humans

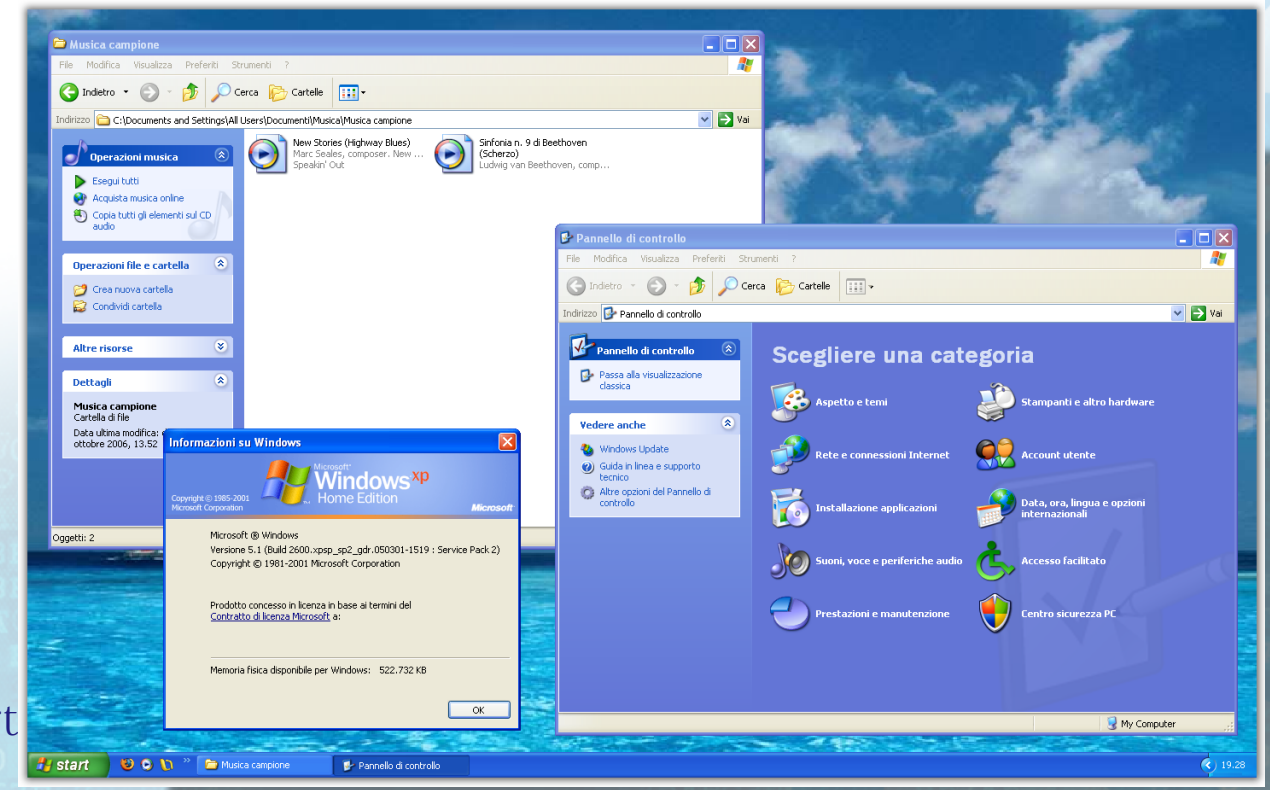
- Enterprises
- Processes:
  - Design
  - Organization
- Supply Chain
- Contracts

WANNACRY ATTACK (MAY 12 2017)

Wannacry components

- EternalBlue: allow to execute arbitrary code in a target machine employing SMBv1 – Server Message Block. EthernalBlue exploits (CVE-2017-0144) Microsoft Windows vulnerability

- DoublePulsar: backdoor uploaded through EthernalBlue that run in kernel mode and it allows to upload and run a third software component (the cryptolocker in wannacry)



End of Support
Windows XP
Feb 2014

Windows XP
including SMB
25 Oct 2001

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cyber Security National Lab

lash: SHA256

:rom:

)itmessage = BM-NBvAHfp5Y6wBykgbirVLndZtEFCYGht8

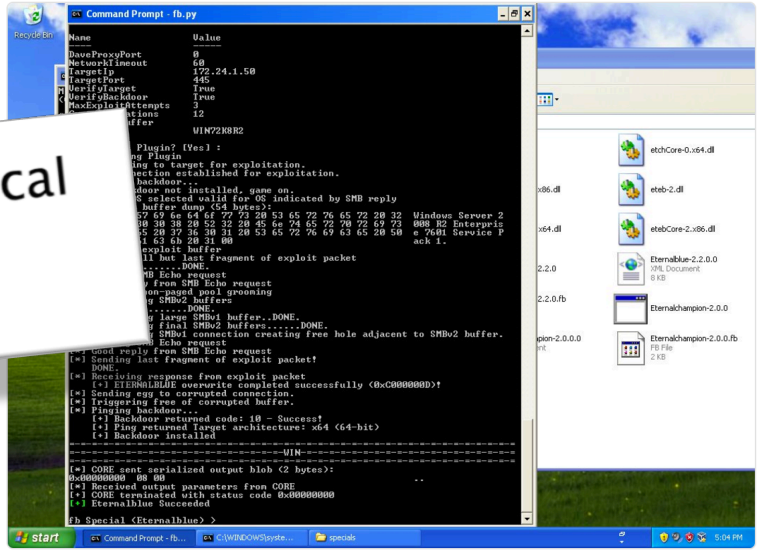
.2p-bote = o1uHOkOcMoFEa7O7dbEilzfMvWzo7bDu~td3x9gYz4b4t5OriJ7U6GUWr5GZoWxQ9f2TrIY5RzhpIMVP6hTLXZ

Microsoft Security Bulletin MS17-010 – Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

ETERNALBLUE -here is a 0day exploit successfully getting RCE on Windows 2008 SP1 (x64) via SMBv2 #0day from FUZZBUNCH



RETWEET 301 MI PIACE 272

09:06 - 14 apr 2017

Windows XP including SMB 25 Oct 2001

End of Support Windows XP Feb 2014

Shadow Brokers 1st dump August 2016

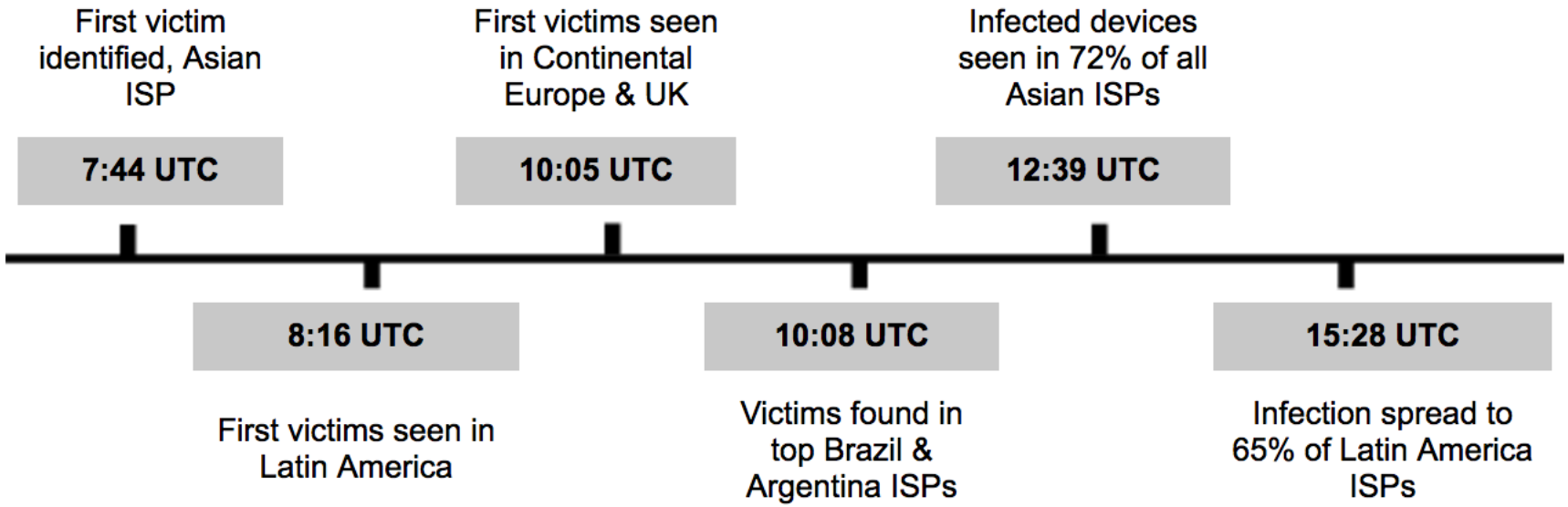
Microsoft patch for SMB 14 March 2017

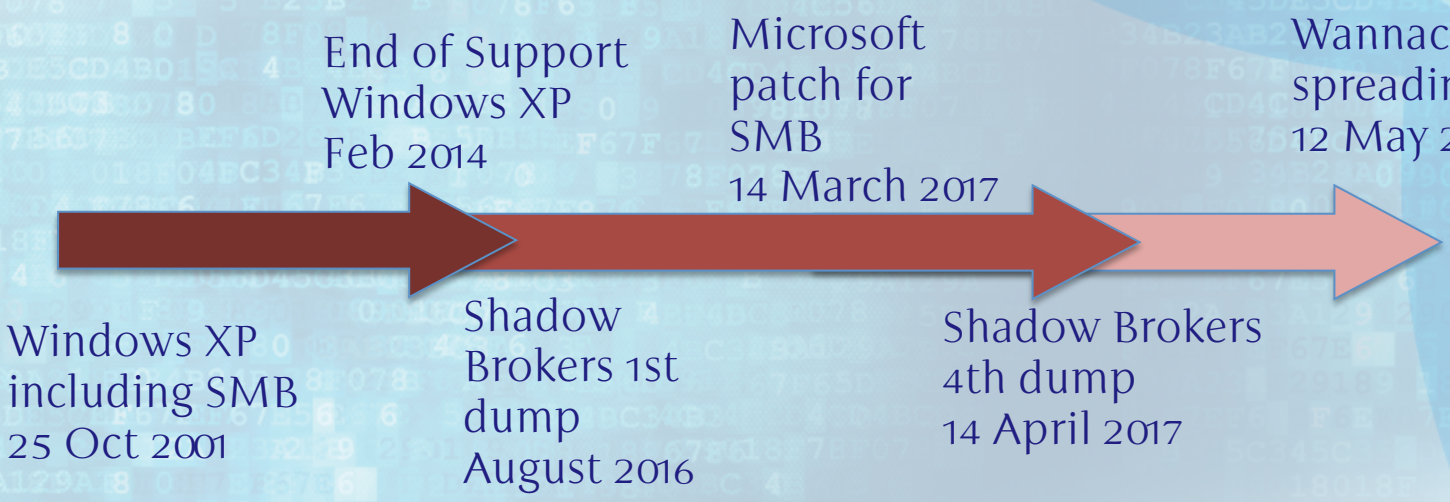
Shadow Brokers 4th dump 14 April 2017

CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER

SAPIENZA UNIVERSITÀ DI ROMA

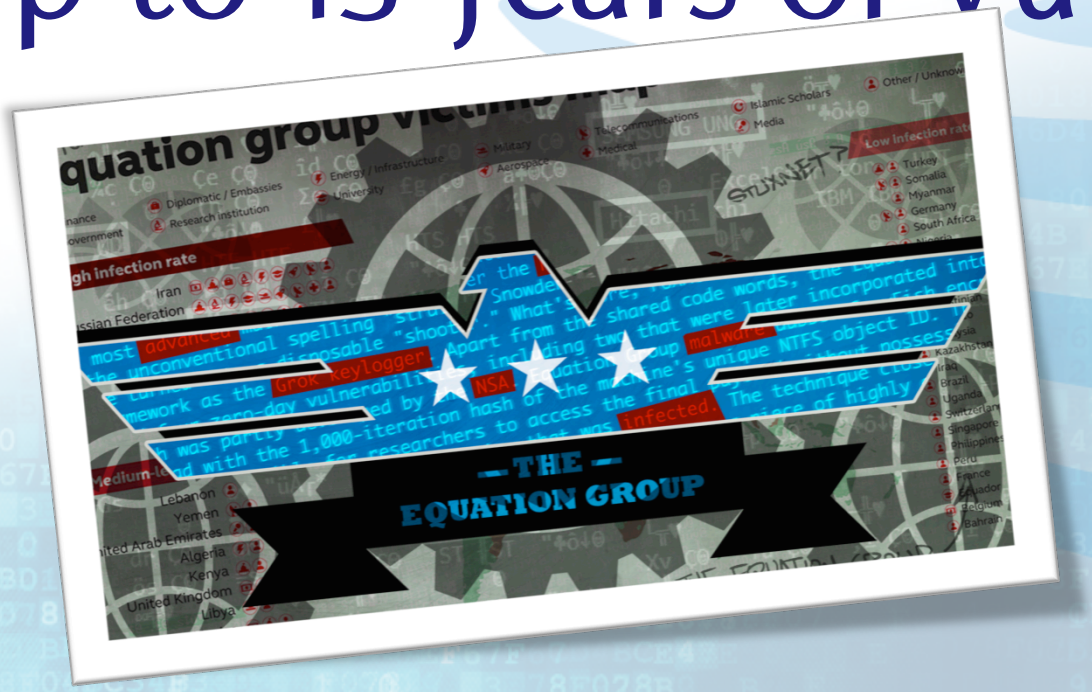
cini Cyber Security National Lab


First victim identified, Asian ISP
7:44 UTC
8:16 UTC
First victims seen in Latin America
First victims seen in Continental Europe & UK
10:05 UTC
10:08 UTC
Victims found in top Brazil & Argentina ISPs
Infected devices seen in 72% of all Asian ISPs
12:39 UTC
15:28 UTC
Infection spread to 65% of Latin America ISPs


Windows XP including SMB 25 Oct 2001
End of Support Windows XP Feb 2014
Shadow Brokers 1st dump August 2016
Microsoft patch for SMB 14 March 2017
Shadow Brokers 4th dump 14 April 2017
Wannacry spreading 12 May 2017

OBSERVATIONS

Up to 15 years of vulnerability



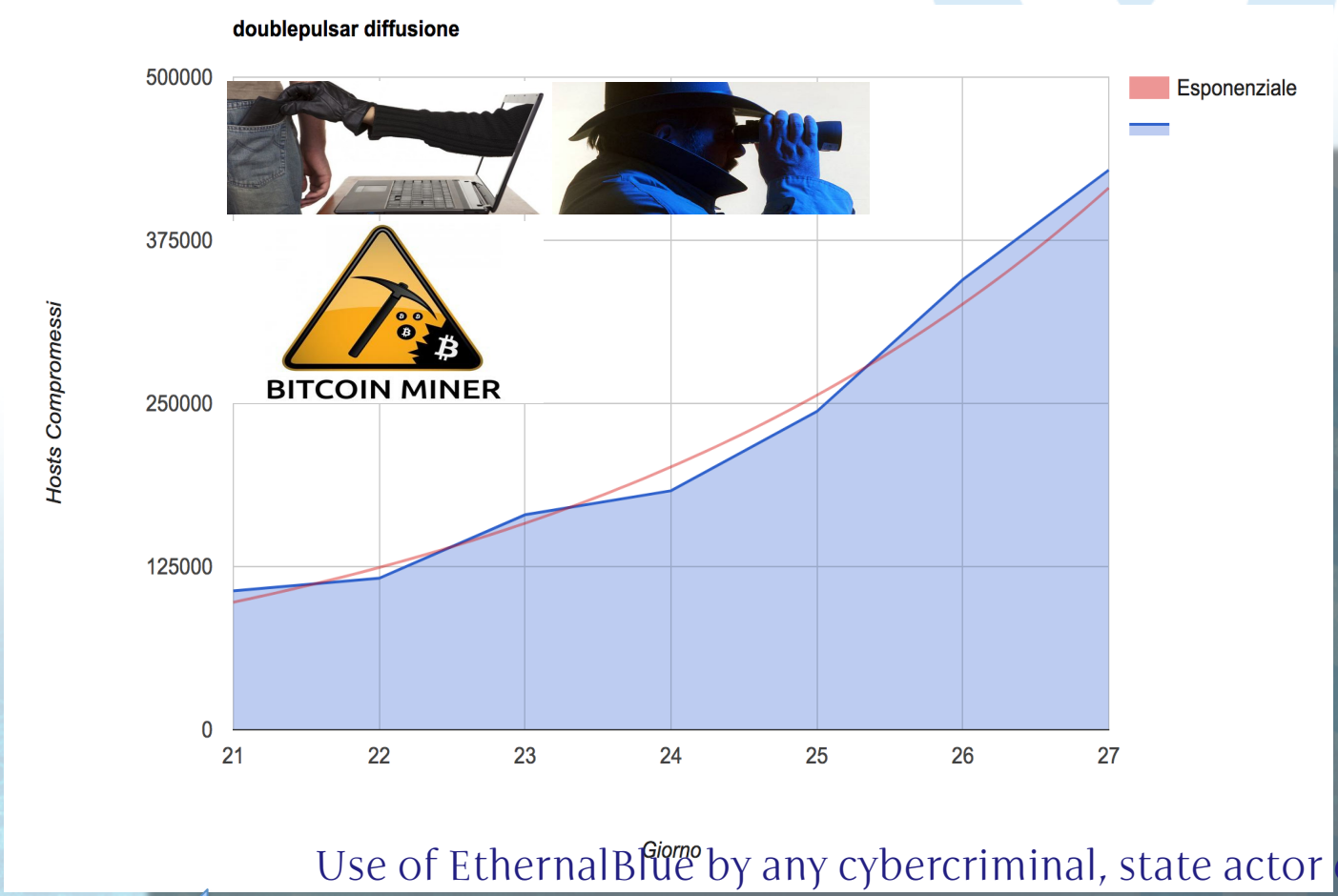
Potential use of EthernalBlue by Equation Group

Windows XP including SMB
25 Oct 2001

Shadow Brokers Leak Oct 2013

End of Support Windows XP
Feb 2014

Microsoft patch for SMB
14 March 2017



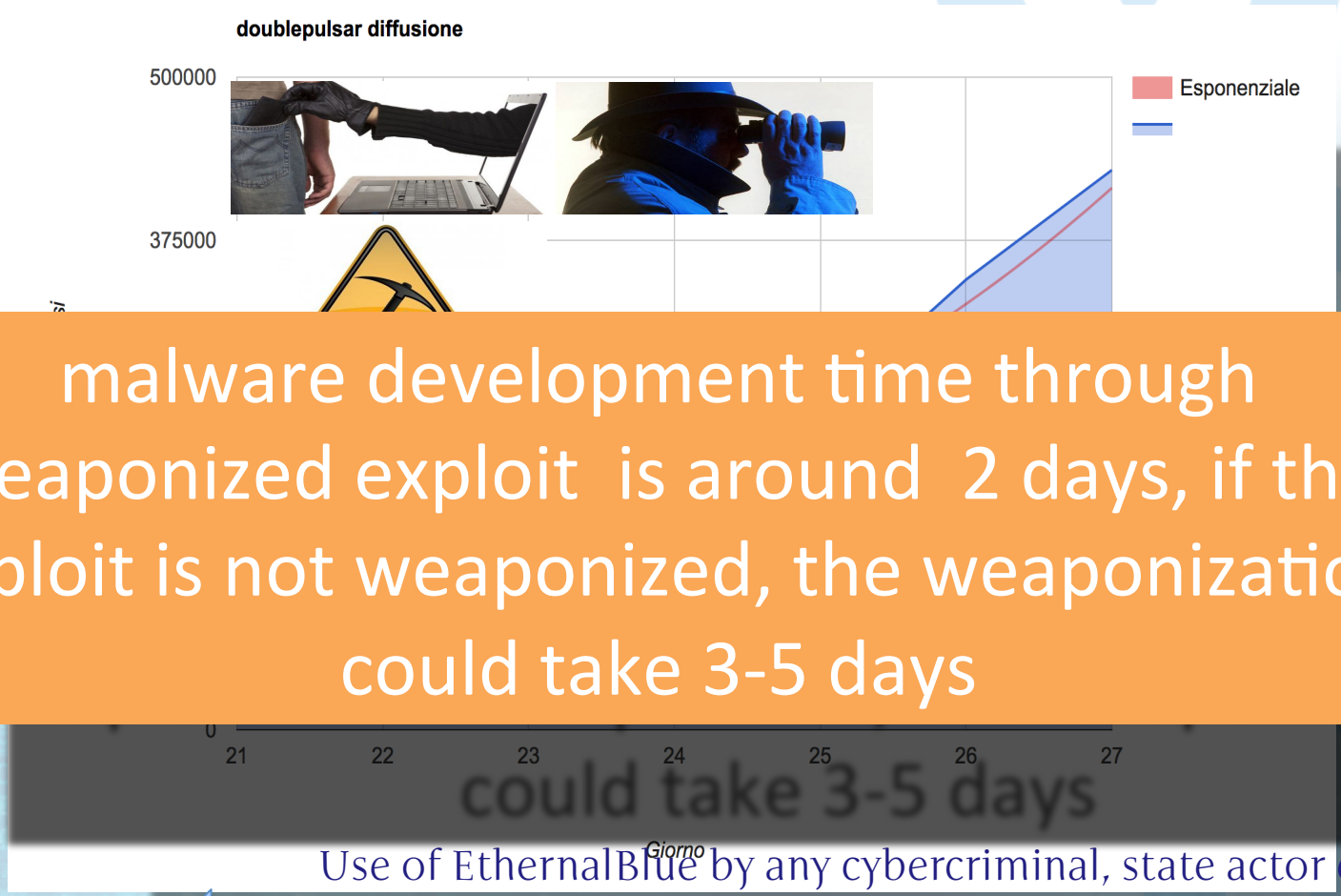
Use of EthernalBlue by any cybercriminal, state actor etc

Shadow Brokers Leak 14 April 2017

21 April-27 April

Wannacry spreading 12 May 2017

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cyber Security National Lab



malware development time through weaponized exploit is around 2 days, if the exploit is not weaponized, the weaponization could take 3-5 days

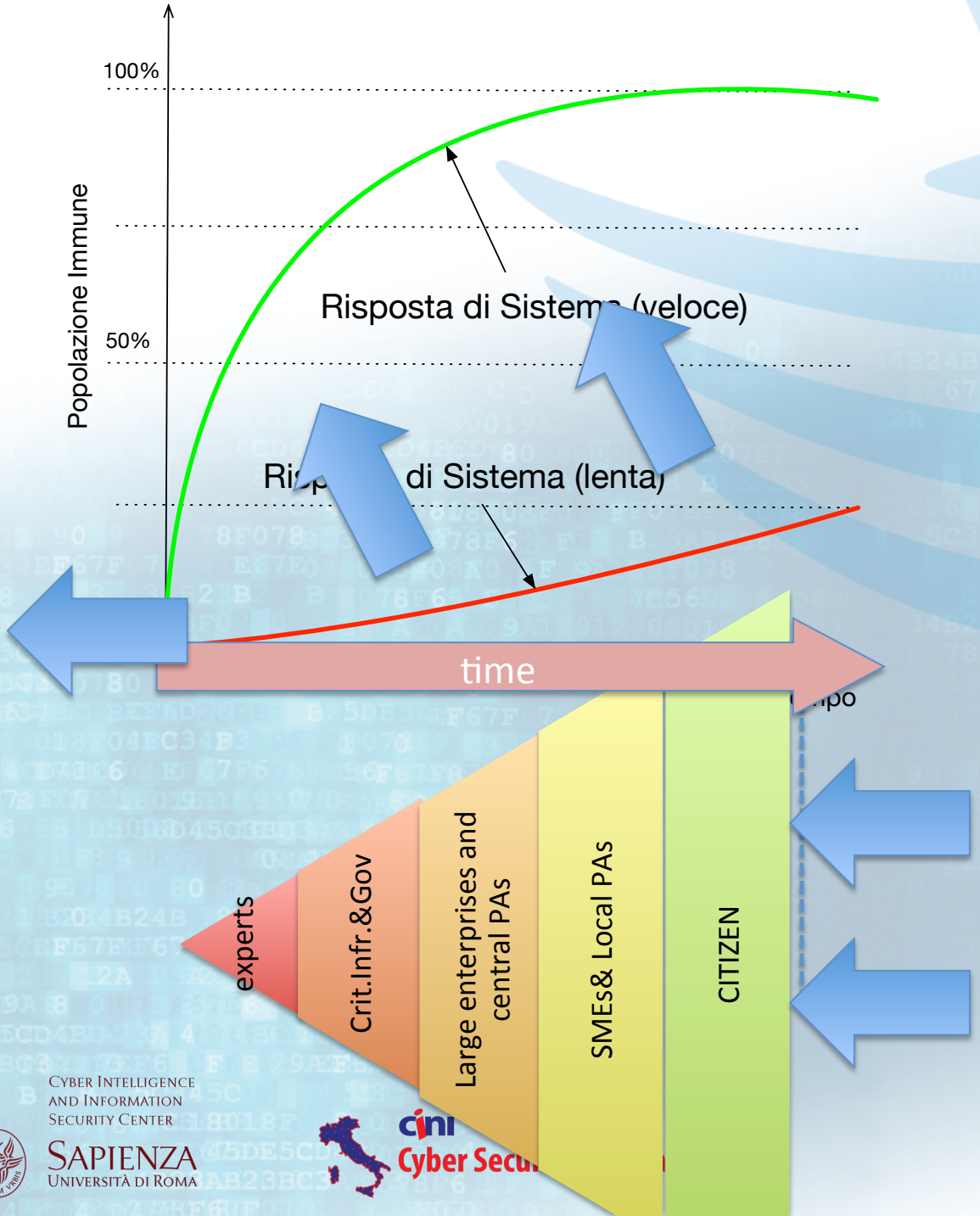
Use of EthernalBlue by any cybercriminal, state actor etc

Shadow Brokers Leak 14 April 2017

21 April-27 April

Wannacry spreading 12 May 2017

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cyber Security National Lab



Revised 31/5/2017

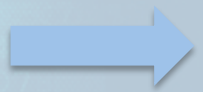
CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER
SAPIENZA UNIVERSITÀ DI ROMA

cini Cyber Secu


IL CASO
Attacco hacker alla Maschio Gaspardo
a casa per tre giorni 650 dipendenti
Padova, tre stabilimenti chiusi fino a lunedì: chiesta la cassa integrazione
PADOVA La Maschio Gaspardo è finita sotto attacco hacker.
Da martedì i sistemi operativi sono bloccati, tre stabilimenti
29 Giugno 2017
MASCHIO

Global Market vs Domestic Protection

- Economic interests are domestic interests and as such protected by each country
- Cyber Security National Strategies



Cyberspace Protection is a necessary condition for the independence and the economic prosperity of a nation

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini
Cyber Security National Lab

Major Risks in 10 Years

- New systems and infrastructures are created with the same weak development processes
- Cyberspace continue to grow in value, complexity, diversity, and scale
- Traditional companies are becoming IT-intensive (industry 4.0)
- Human resources are constrained by a growing gap in cybersecurity workforce size, diversity, capabilities, and agility

Reverse the Asymmetry Advantages of the Attacker

- identifying vulnerabilities and developing ways to exploit them is faster than the

These asymmetries must be reversed and this is a call to the research community

the Internet can provide is much ahead of current attribution capability

Increasing the cost to adversaries

- increasing risks and uncertainty for potential adversaries
- components, systems, users, and critical infrastructure resisting efficiently to malicious cyber activities
- efficiently detect, and even anticipate adversary decisions and activities
- dynamically adapt by efficiently reacting to disruption, recovering from damage, maintaining operations under attack
- thwarting similar future malicious activity

From "FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN ENSURING PROSPERITY AND NATIONAL SECURITY", NITRD, US 2016

Critical Dependencies for efficient cybersecurity

- Scientific foundation
- Effective Risk management
- Human aspects
- Technology transfer
- Cybersecurity workforce
- Research infrastructure

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cyber Security National Lab

A closer look at: Scientific foundation

- formal comprehensive theories including quantifiable defense, systems and adversaries
- innovative and principled design methodologies that are measurable and efficiency provable
- Are we eliminating old vulnerabilities faster than we are creating new ones?
- reasoning frameworks to anticipate threats in disruptive technologies
- metrics for evaluating success or failure

Examples of multidisciplinary challenges

- Forensic techniques robust enough to preserve evidence suitable for use in legal proceedings
- High-confidence attribution in real-time (from technical attribution to legal sanctions)
- Intelligence operations over internet to anticipate attacks

Use of computer science to thwarting attacks at the domestic system in the physical and logical domain

CIS SAPIENZA

CYBER INTELLIGENCE AND INFORMATION SECURITY

cini

Cybersecurity National Lab

FILIERA SICURA

Use of computer science to thwarting attacks at the domestic system in the physical and logical domain

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cybersecurity National Lab

COMITATO NAZIONALE RICERCA IN CYBERSECURITY

- Laboratorio Nazionale di Cybersecurity
- CNR

FILIERA SICURA

Cybersecurity National Laboratory aims to establish a research and academic asset for Italy spread through the territory. The Lab works towards a cybersecurity technical workforce creation, selection and training of cybersecurity talents, establishing national and international cooperations for information sharing, and the consolidation of a multidisciplinary domestic cybersecurity community. Cybersecurity National Laboratory is actively engaged in a number of scientific on-the-edge large projects on different aspects of the cybersecurity domain.

COMITATO NAZIONALE RICERCA IN CYBERSECURITY

ITASEC
ITALIAN CONFERENCE ON CYBERSECURITY

CyberChallenge.it

FILIERASICURA

- **Libro Bianco: Il futuro della Cybersecurity in Italia**
- **Framework Nazionale per la Cybersecurity**
- **Italian Cybersecurity Report Controlli essenziali di Cybersecurity**

- **MALWARE ANALYSIS**
- **MALWARE DETECTION**
- **PENETRATION TESTING**
- **VULNERABILITY ASSESSMENT**
- **DEPENDABILITY**
- **STREAM PROCESSING**
- **MACHINE LEARNING FOR SECURITY**
- **BIG DATA ANALYSIS**
- **BIG DATA FOR SECURITY**
- **SECURITY ORGANIZATION AND STRATEGY**
- **SECURE CLOUD COMPUTING**
- **SUPPLY CHAIN SECURITY**
- **HARDWARE SECURITY**

WHAT A COUNTRY SHOULD DO

Building a Cybersecurity capability

Supporting private sector

Digital Trasformation Project

Supporting citizen

Supporting PA

Implementing a national capability means creating critical mass national R&D organizations

Cyber Intelligence

Cyber crime

Structuring a long lasting national plan with precise objectives and adequate resources

- Protect
- Deter
- Building capacity

PUBLIC

RESEARCH

PRIVATE

National model of development

Enabling horizontal actions

Enabling technology transfer

Enabling international collaborations

Enabling industry support

Enabling horizontal actions

PUBLIC

RESEARCH

PRIVATE

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

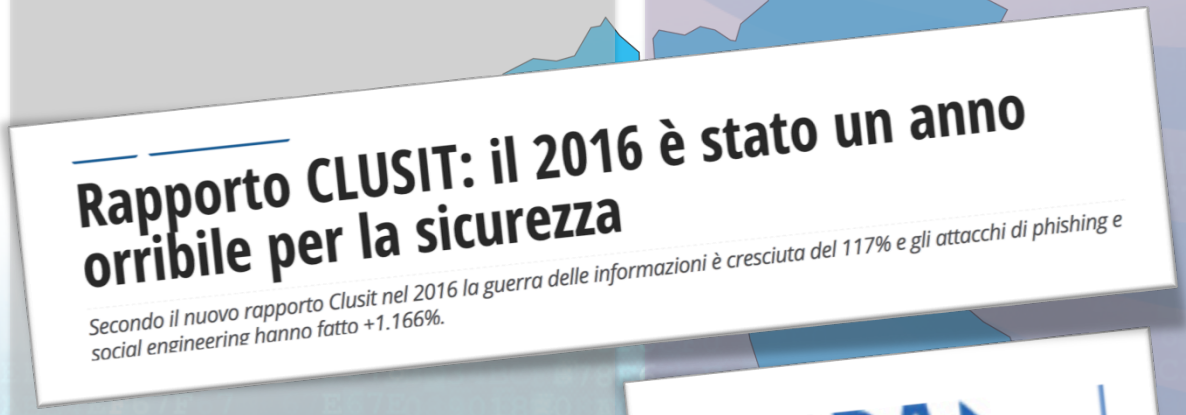
FILIERA SICURA

Enabling horizontal actions

PUBLIC

RESEARCH

PRIVATE



Awareness Campaigns

Enabling horizontal actions

Community Building

Awareness Campaigns

Enabling horizontal actions

PUBLIC | RESEARCH | PRIVATE

Common Language

Commu

Awarenes

Enabling horizontal actions

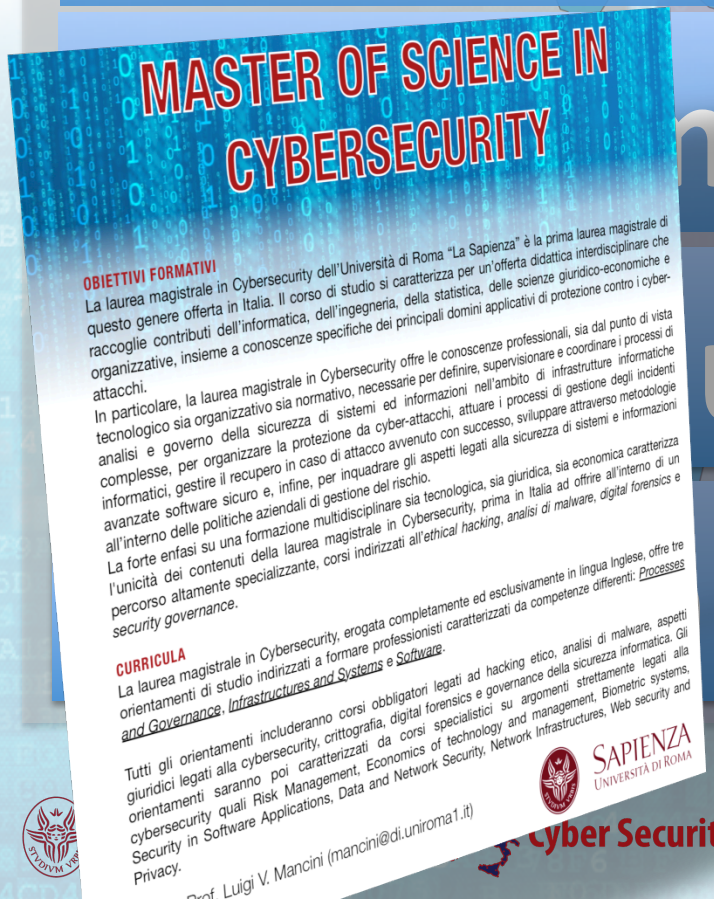
PUBLIC | RESEARCH | PRIVATE

Workforce

non La

unity

ess Ca



MASTER OF SCIENCE IN CYBERSECURITY

OBIETTIVI FORMATIVI

La laurea magistrale in Cybersecurity dell'Università di Roma "La Sapienza" è la prima laurea magistrale di questo genere offerta in Italia. Il corso di studio si caratterizza per un'offerta didattica interdisciplinare che raccoglie contributi dell'informatica, dell'ingegneria, della statistica, delle scienze giuridico-economiche e organizzative, insieme a conoscenze specifiche dei principali domini applicativi di protezione contro i cyber-attacchi.

In particolare, la laurea magistrale in Cybersecurity offre le conoscenze professionali, sia dal punto di vista tecnologico sia organizzativo sia normativo, necessarie per definire, supervisionare e coordinare i processi di analisi e governo della sicurezza di sistemi ed informazioni nell'ambito di infrastrutture informatiche complesse, per organizzare la protezione da cyber-attacchi, attuare i processi di gestione degli incidenti informatici, gestire il recupero in caso di attacco avvenuto con successo, sviluppare attraverso metodologie avanzate software sicuro e, infine, per inquadrare gli aspetti legati alla sicurezza di sistemi e informazioni all'interno delle politiche aziendali di gestione del rischio.

La forte enfasi su una formazione multidisciplinare sia tecnologica, sia giuridica, sia economica caratterizza l'unicità dei contenuti della laurea magistrale in Cybersecurity, prima in Italia ad offrire all'interno di un percorso altamente specializzante, corsi indirizzati all'*ethical hacking*, *analisi di malware*, *digital forensics* e *security governance*.

CURRICULA

La laurea magistrale in Cybersecurity, erogata completamente ed esclusivamente in lingua Inglese, offre tre orientamenti di studio indirizzati a formare professionisti caratterizzati da competenze differenti: *Processes and Governance*, *Infrastructures and Systems* e *Software*.

Tutti gli orientamenti includeranno corsi obbligatori legati ad hacking etico, analisi di malware, aspetti giuridici legati alla cybersecurity, crittografia, digital forensics e governance della sicurezza informatica. Gli orientamenti saranno poi caratterizzati da corsi specialistici su argomenti strettamente legati alla cybersecurity quali Risk Management, Economics of technology and management, Biometric systems, Security in Software Applications, Data and Network Security, Network Infrastructures, Web security and Privacy.

SAPIENZA UNIVERSITÀ DI ROMA

Prof. Luigi V. Mancini (mancini@di.uniroma1.it)

Cyber Security National Lab

Enabling technology transfer

PUBLIC

RESEARCH

PRIVATE

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

Enabling technology transfer

PUBLIC

RESEARCH

PRIVATE

Public Private partnership

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CSRC
Cyber Security Research Center

MITRE

R&D organizations

Enabling Technology Transfer

PUBLIC

RESEARCH

PRIVATE

Data center consolidation

Industry 4.0

Digital Transformation projects

R&D organizations

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

Enabling Technology Transfer

PUBLIC

RESEARCH

PRIVATE

Data center consolidation

FILIERA SICURA

Industry 4.0

Digi ects

elettrico

idrico

bancario

governativo

manifatturiero

---

alimentare

FILIERASICURA

Framework Nazionale per la Cybersecurity

Enabling technology transfer

PUBLIC

RESEARCH

PRIVATE

Startup & Patents

Digital Transformation projects

R&D organizations

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

Enabling technology transfer

PUBLIC | RESEARCH | PRIVATE

Financial leverage

Startup &

Digital Transform ts

R&D organ

Revisionato 31/5/2017

Indirizzo operativo 1 – Potenziamento delle capacità di *intelligence*, di polizia e di difesa civile e militare.....

Indirizzo operativo 2 – Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati .....

Indirizzo operativo 3 – Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento .....

Indirizzo operativo 4 – Cooperazione internazionale ed esercitazioni.....

Indirizzo operativo 5 – Operatività delle strutture nazionali, di *incident prevention*, *response* e *remediation*.....

Indirizzo operativo 6 – Interventi legislativi e *compliance* con obblighi internazionali .....

Indirizzo operativo 7 – *Compliance* a *standard* e protocolli di sicurezza .....

Indirizzo operativo 8 – Supporto allo sviluppo industriale e tecnologico .....

Indirizzo operativo 9 – Comunicazione strategica e operativa ....

Indirizzo operativo 10 – Risorse .....

Indirizzo operativo 11 – Implementazione di un sistema di *cyber risk management* nazionale .....

National committee for cybersecurity research and the National Lab of Cybersecurity will support the creation or the enpowering of the following "entities" and "operations" declared within the Italian Operational Plan:

- Centro di ricerca Nazionale in Cybersecurity
- Laboratorio di crittografia Nazionale
- Centro di Valutazione e Certificazione
- CERT
- CIOC
- Cyber Range
- Startup creation and venture capital
- Formazione
- National distributed ledger