Italian Cyber Security Report 2013

critical infrastructures and other sensitive sectors readiness

Roberto Baldoni (baldoni@dis.uniroma1.it)

www.cis.uniroma1.it

Roma 9 Dicembre 2013

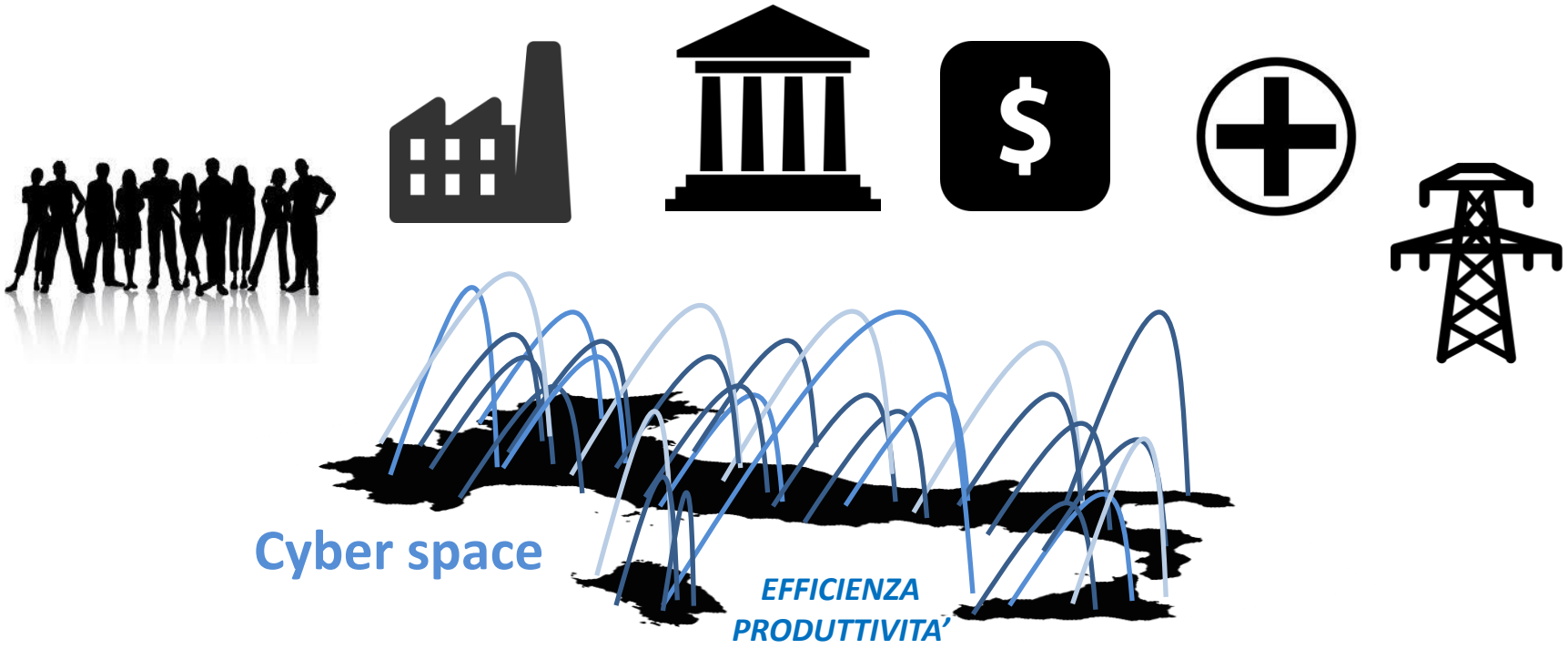
Joint work with Marco Angelini, Maria Cristina Arcuri, Claudio Ciccotelli, Giuseppe Antonio Di Luna, Luca Montanari, Ida Claudia Panetta, Leonardo Querzoni, Nino Vincenzo Verde

Work partially supported by TENACE PRIN Project and Microsoft

CIS SAPIENZA

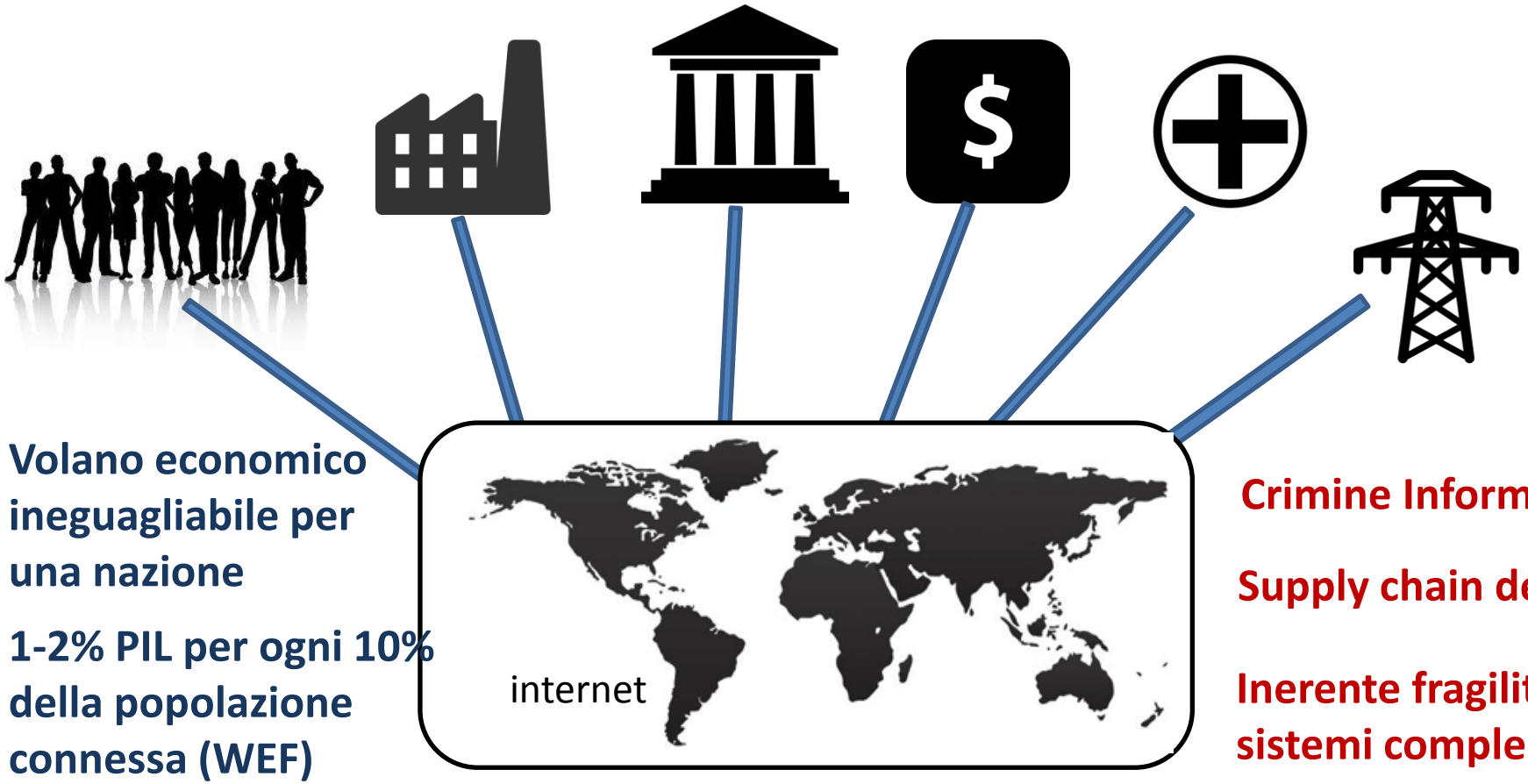
RESEARCH CENTER FOR CYBER INTELLIGENCE AND INFORMATION SECURITY

Cyber space e settori sensibili ad attacchi cibernetici



La prosperità economica di un sistema paese si misurerà anche in base al grado di sicurezza che si saprà dare al proprio spazio cibernetico

Cyber space e crescita economica



Volano economico ineguagliabile per una nazione

1-2% PIL per ogni 10% della popolazione connessa (WEF)

Crimine Informatico

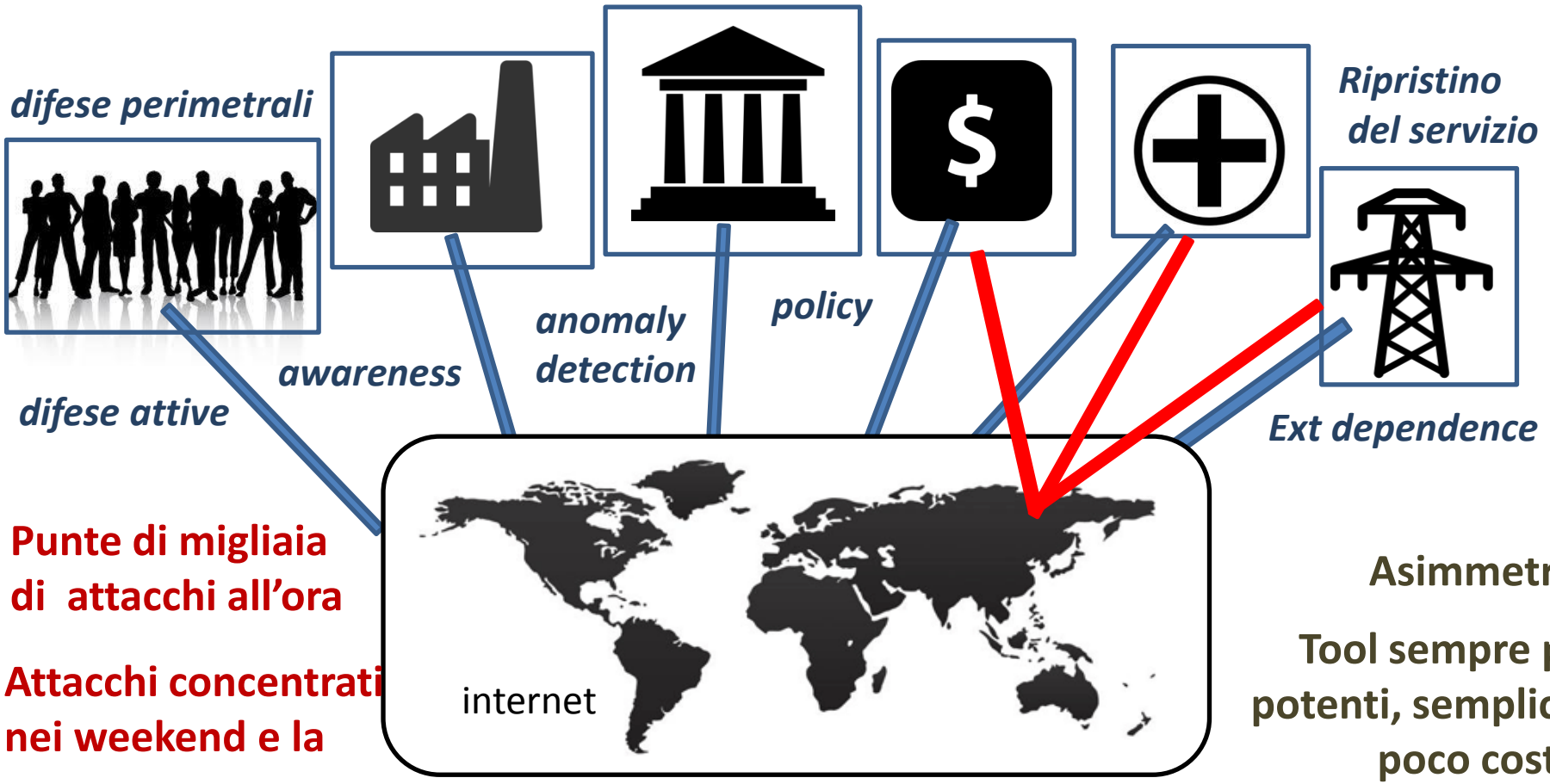
Supply chain debole

Inerente fragilità dei sistemi complessi

Rendere digitali servizi essenziali

Distruzione del servizio

Attacchi cibernetici



Punte di migliaia di attacchi all'ora

Attacchi concentrati nei weekend e la sera

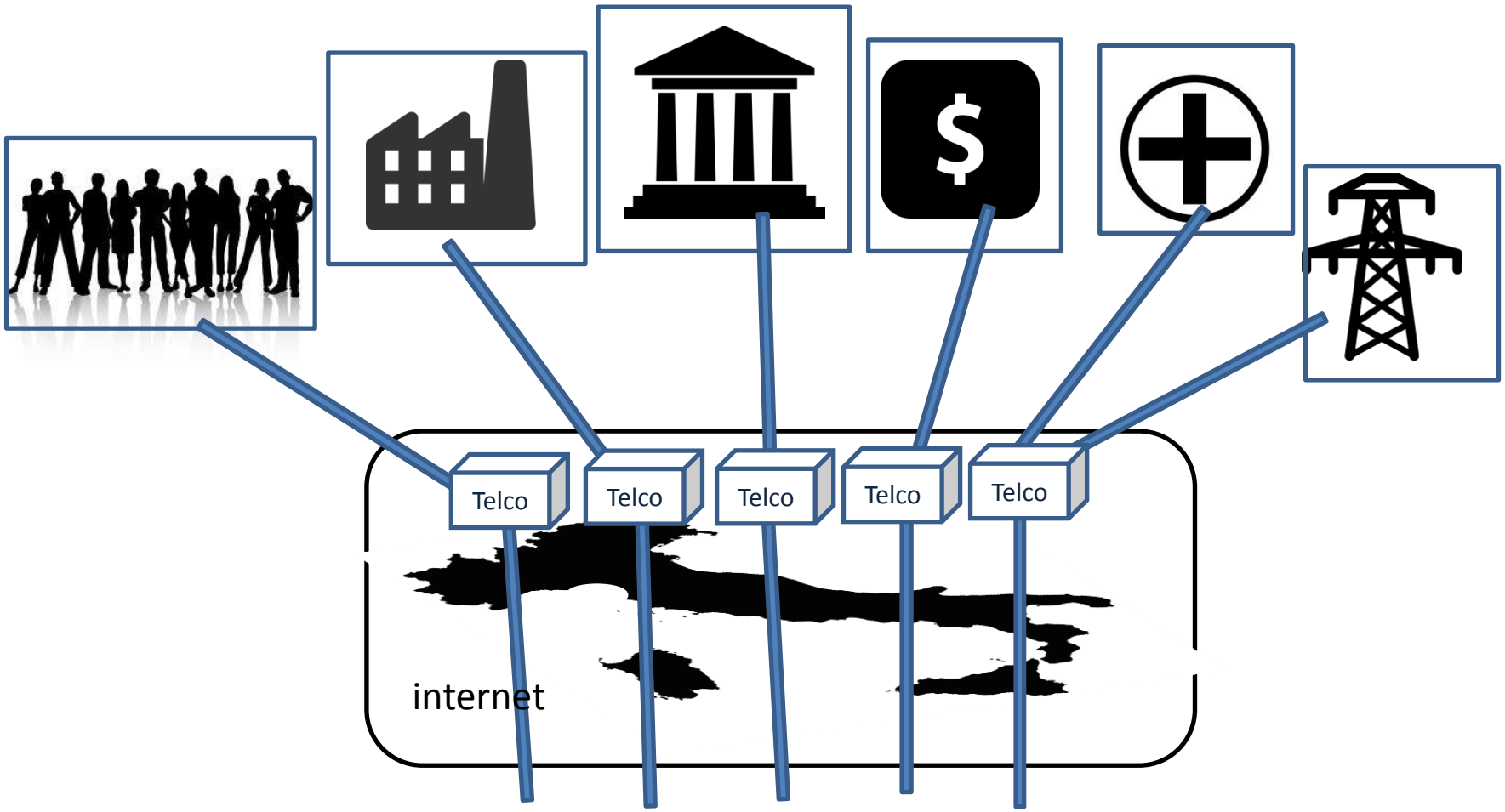
Asimmetria

Tool sempre più potenti, semplici e poco costosi

nel cyber space è sempre emergenza!

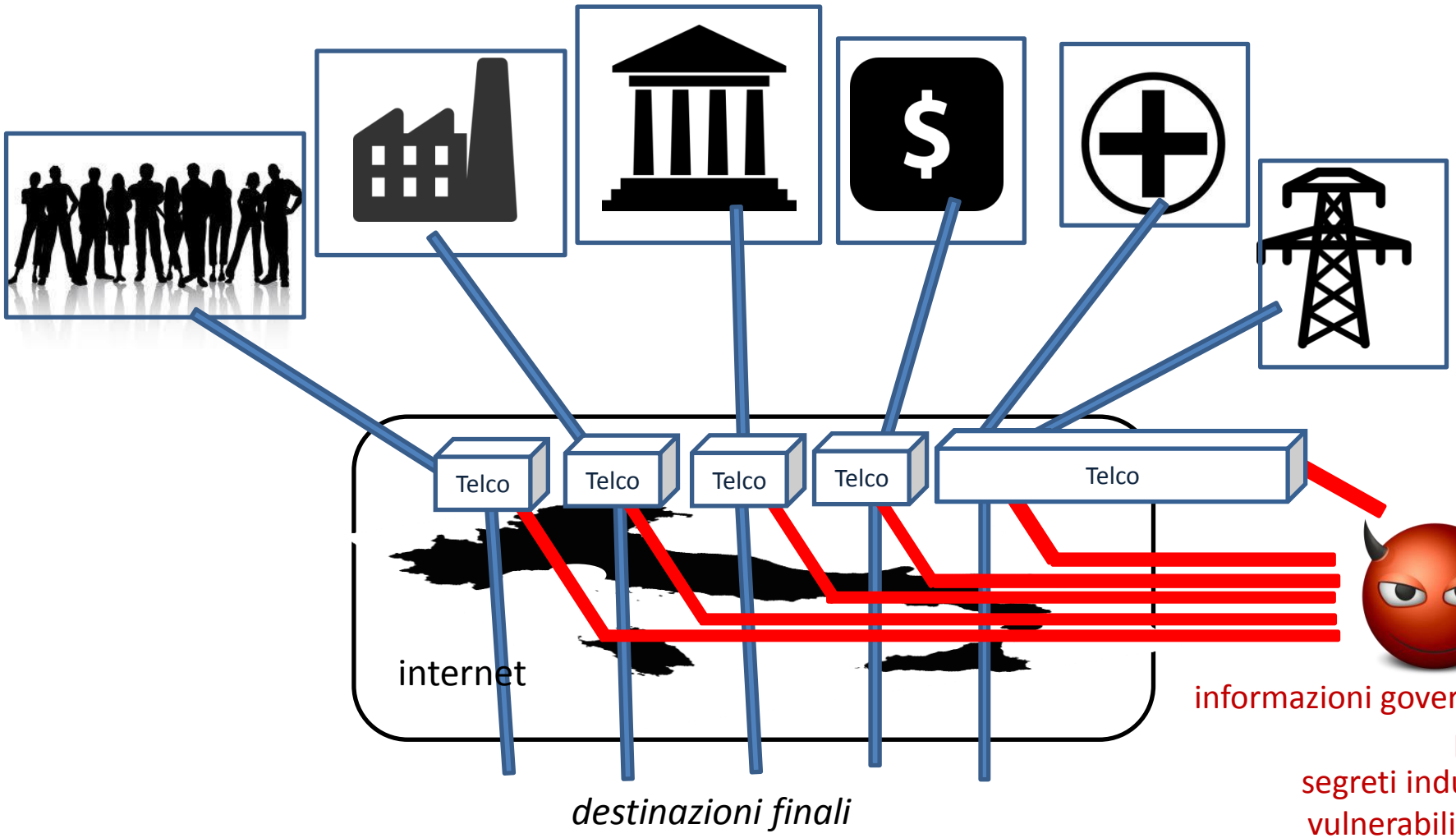
ATTACCHI E INTELLIGENCE NEL CYBER SPAZIO

Monitoraggio «upstream»: tapping the internet

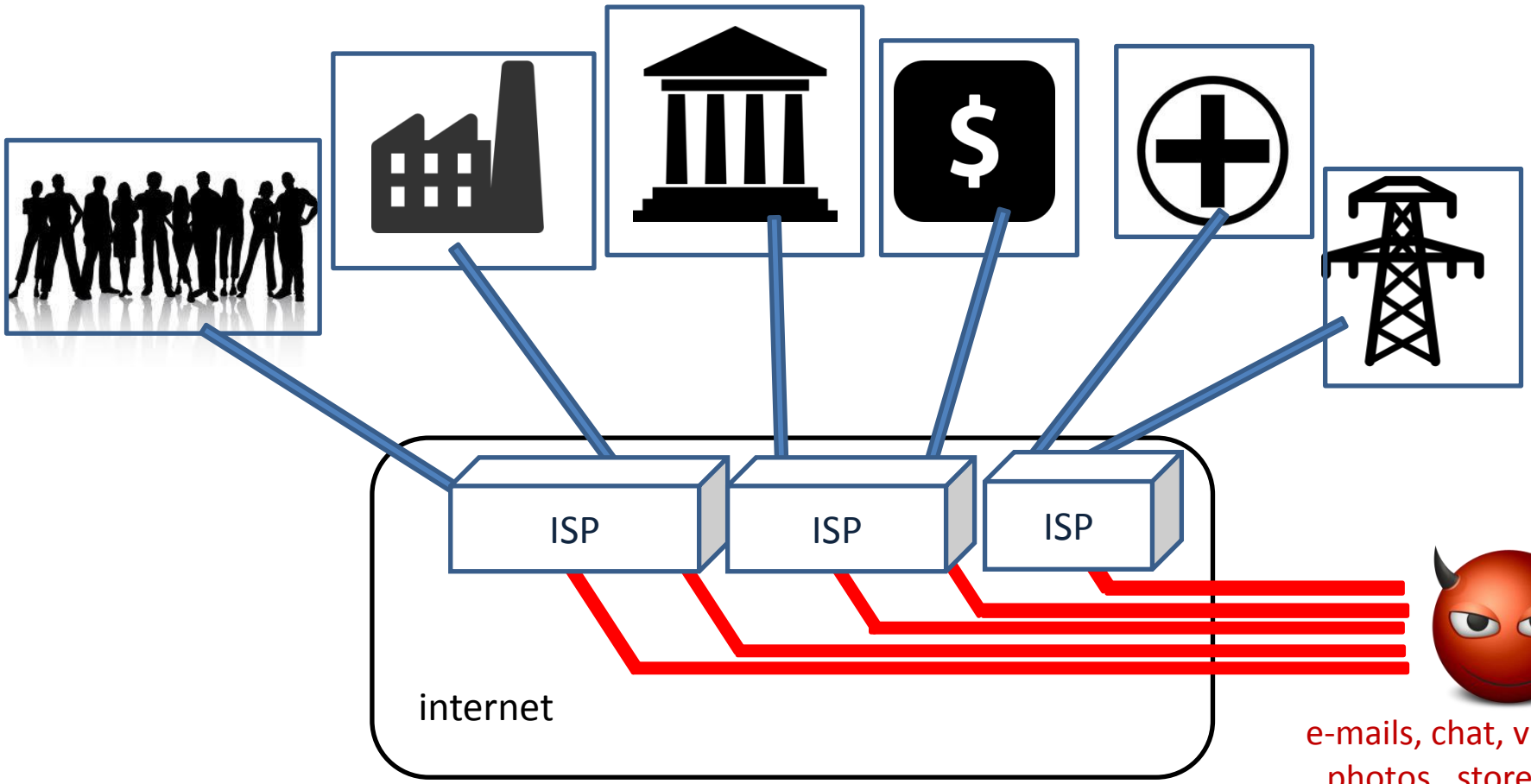


destinazioni finali

Monitoraggio «upstream»: tapping the internet

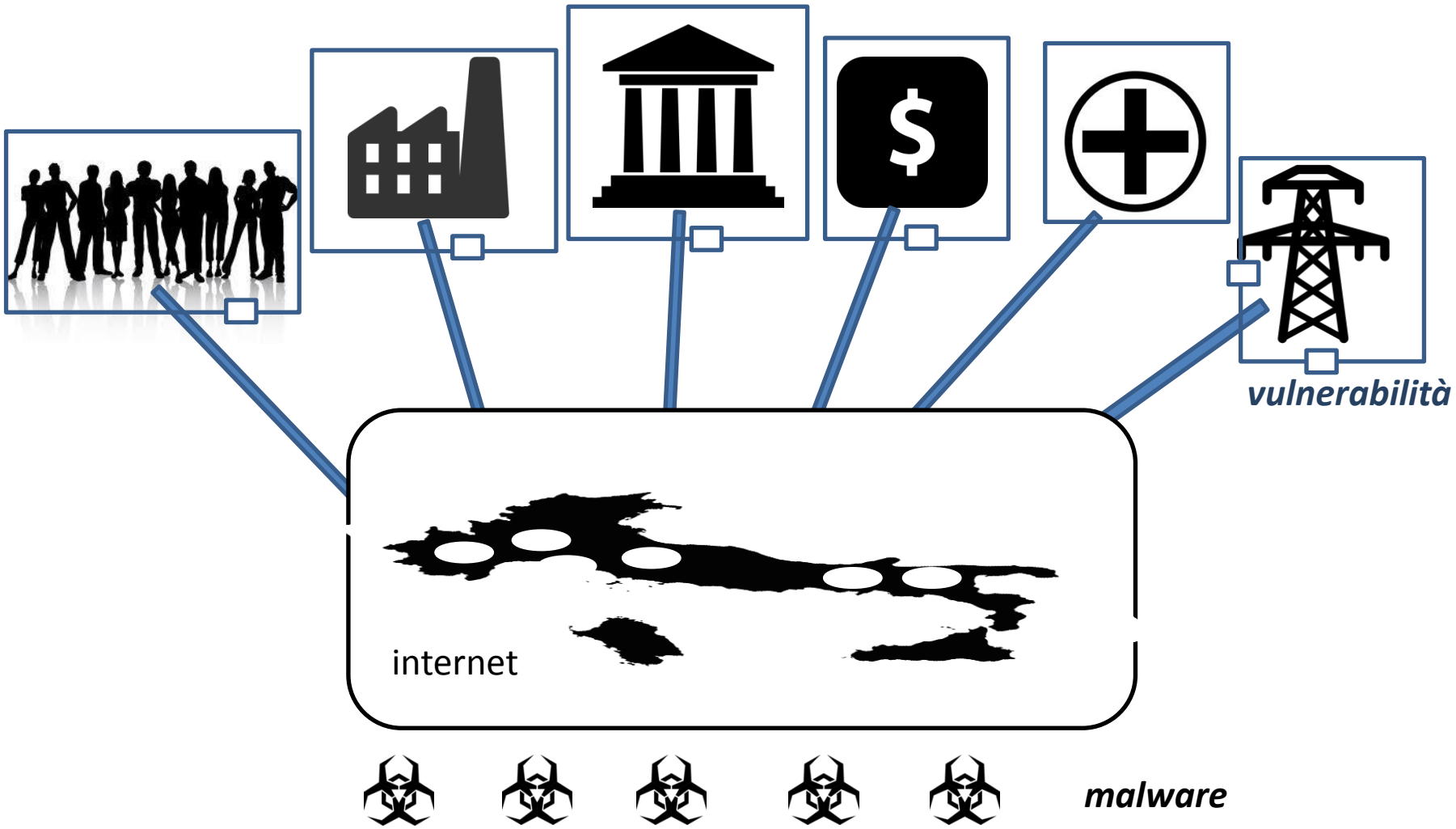


Monitoraggio «downstream»

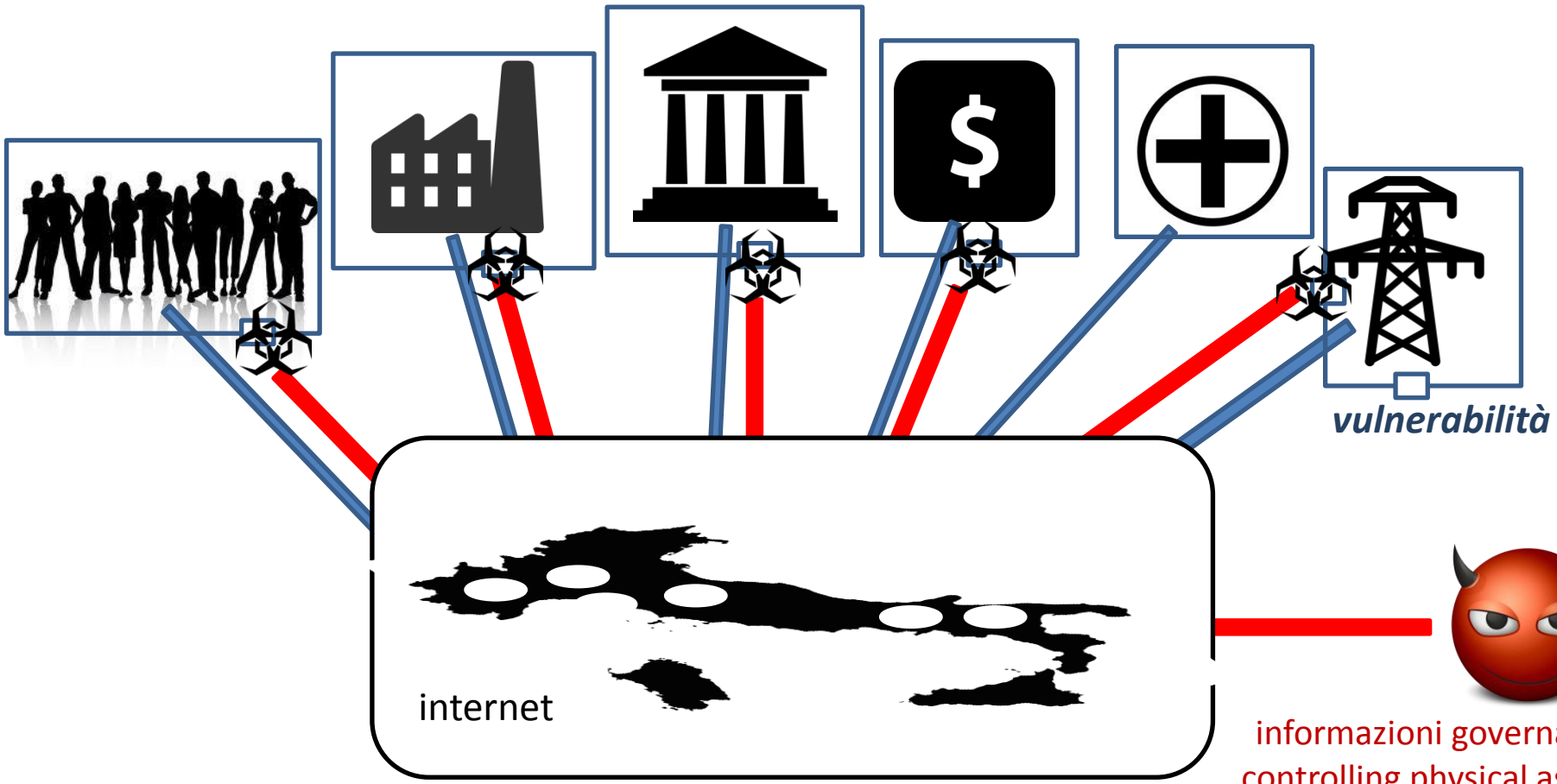


e-mails, chat, videos,
photos, stored data
VoIP, file transfers,
video conferencing

Attacchi di tipo Malware

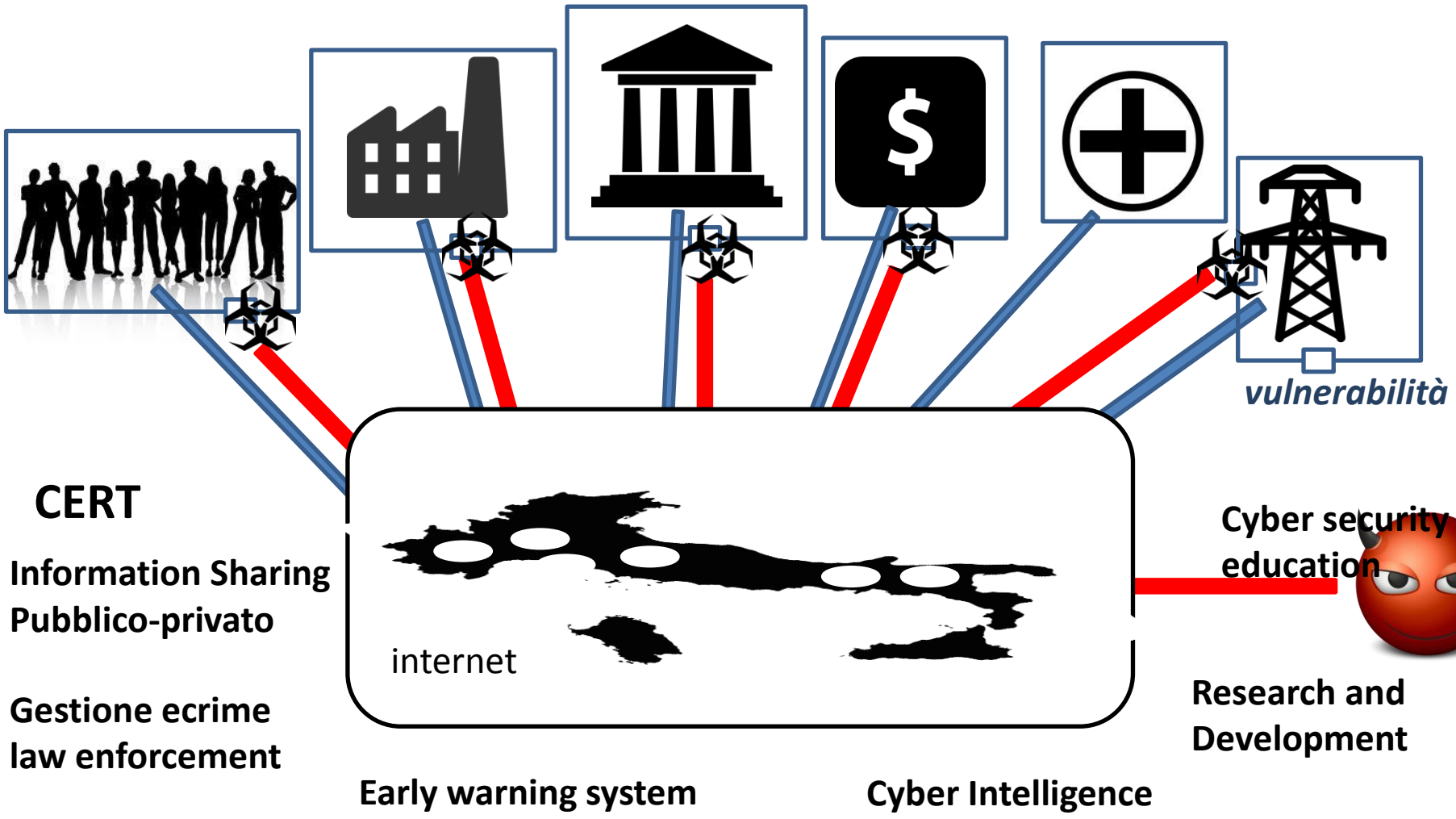


Attacchi di tipo Malware



informazioni governative
controlling physical assets
segreti industriali
vulnerabilità ecc.

Strategia Nazionale di Cyber Security



CERT

Information Sharing
Pubblico-privato

Gestione ecrime
law enforcement

Cyber security education

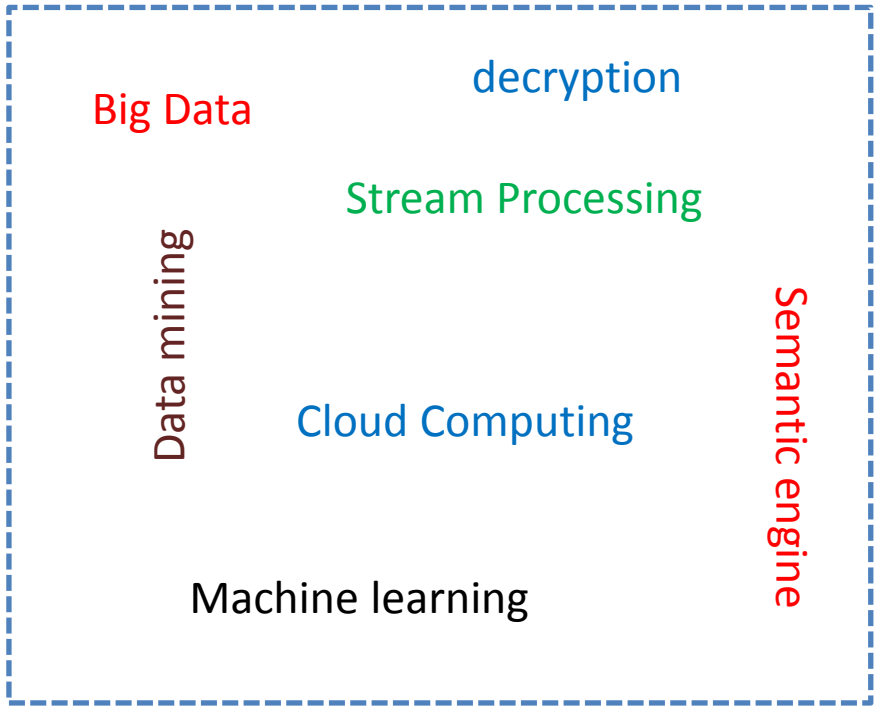
Research and Development

Early warning system

Cyber Intelligence

Surveillance program

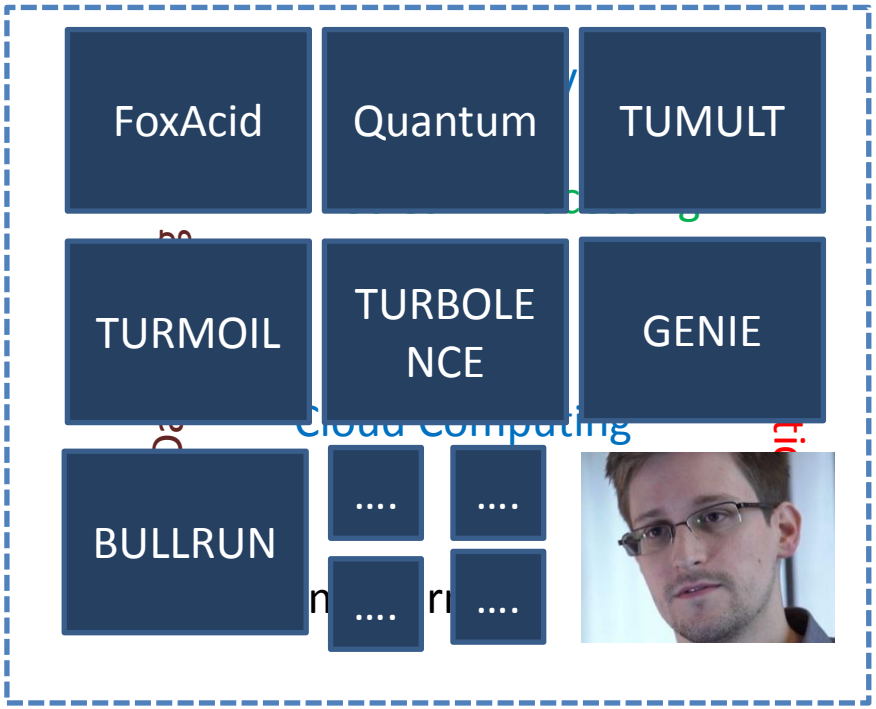
Systems and Algorithms for mass electronic surveillance



- Upstream monitoring
  - Accordi tra NSA e le maggiori US Telco
  - Internet routers, switches and firewalls hackings
- Downstream Monitoring (PRISM)
  - Accordi tra NSA e le maggiori US ISP
  - Più di 2,000 PRISM-based reports al mese
- Decrypto program
  - Investimenti in “groundbreaking cryptanalytic capabilities” per rompere sistemi crittografici adottati da avversari and decriptare internet traffic online e traffico 3G
- Malware
  - Identificare utenti TOR attraverso le vulnerabilità del software utilizzato dagli utenti stessi

Surveillance program

Systems and Algorithms for mass electronic surveillance



- Upstream monitoring
  - Accordi tra NSA e le maggiori US Telco
  - Internet routers, switches and firewalls hackings
- Downstream Monitoring (PRISM)
  - Accordi tra NSA e le maggiori US ISP
  - Più di 2,000 PRISM-based reports al mese
- Decrypto program
  - Investimenti in “groundbreaking cryptanalytic capabilities” per rompere sistemi crittografici adottati da avversari and decriptare internet traffic online e traffico 3G
- Malware
  - Identificare utenti TOR attraverso le vulnerabilità del software utilizzato dagli utenti stessi

Surveillance program

Systems and Algorithms for mass electronic surveillance

- Upstream monitoring
  - Più di 2,
- Decrypto programs
  - Investimenti in “groundbreaking cryptanalytic capabilities” per rompere sistemi crittografici adottati da avversari and decriptare internet traffic online e traffico 3G
- Malware
  - Identificare utenti TOR attraverso le vulnerabilità del software utilizzato dagli utenti stessi

Rischio balcanizzazione di internet

- Labile confine tra spiare per sicurezza della nazione e interessi economici nazionali, casi:
  - Petronas, Qatar's Ras Gas, Saudi Aramco
- Strategie nazionali di cyber security

constructing submarine cables that do not route through the US, building internet exchange points in Brazil, creating an encrypted email service through the state postal service and having Facebook, Google and other companies store data by Brazilians on servers in Brazil. Dilma Roussef

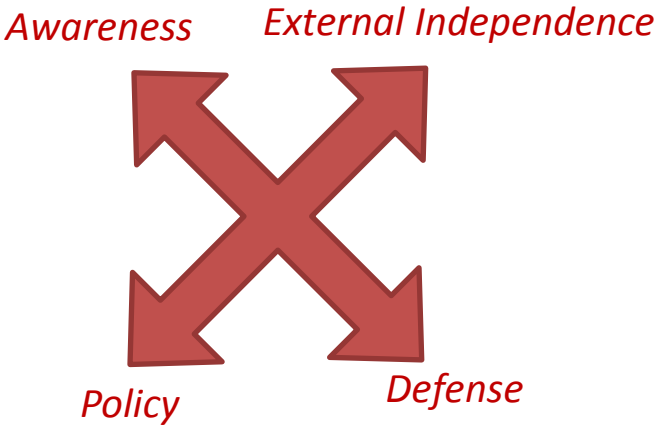
2013 Cyber Security Report

Italy policy standpoint

Analisi dello scenario di cyber security in Italia

Target groups	Questionnaires sent	Questionnaires returned	Number of organizations	% of returned questionnaires
PA	31	13	26	41.9%
Utilities	8	4	7	50%
Financial	17	6	17	35.3%
Industrial	12	5	12	41.7%
Total	68	28	62	Avg. 42.23%

- **60 domande**
- **Luglio 2013- Settembre 2013**
- **50% delle organizzazione consultate operano nel territorio nazionale**
- **75% dei questionari è stato riempito da persone centrali alla cyber sicurity dell'organizzazione**



External Dependency

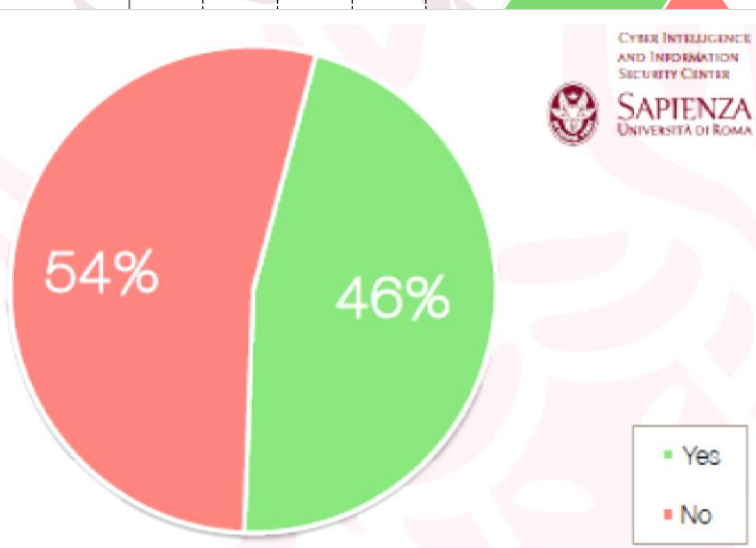
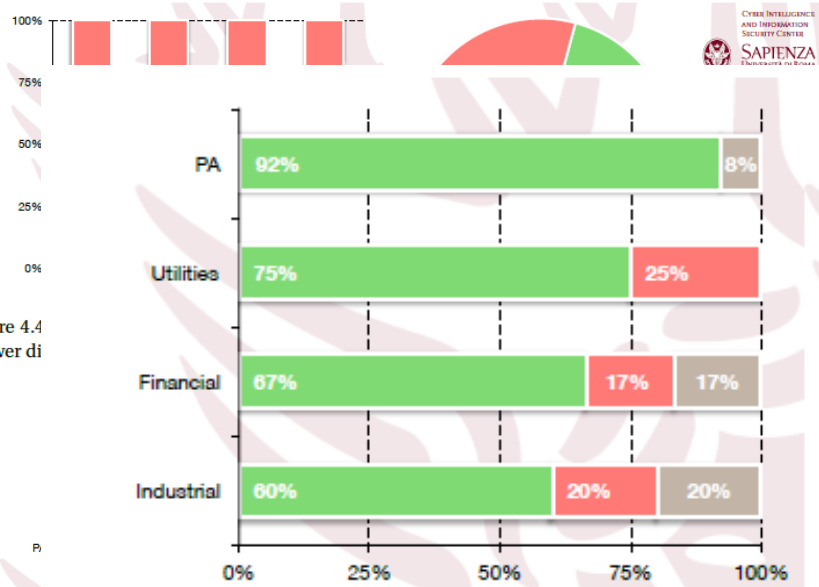


Figure 4.4: Question #1.2.1 - "Is your company using (or planning to use) cloud services?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Figure 4.5: Question #1.2.2 - "Do cloud services support core business processes that are necessary to deliver critical services?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Figure 4.7: Question #1.2.6 - "Do you know if your software providers are following a strategic approach to address application risks in each phase of the application development process?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

External Dependency



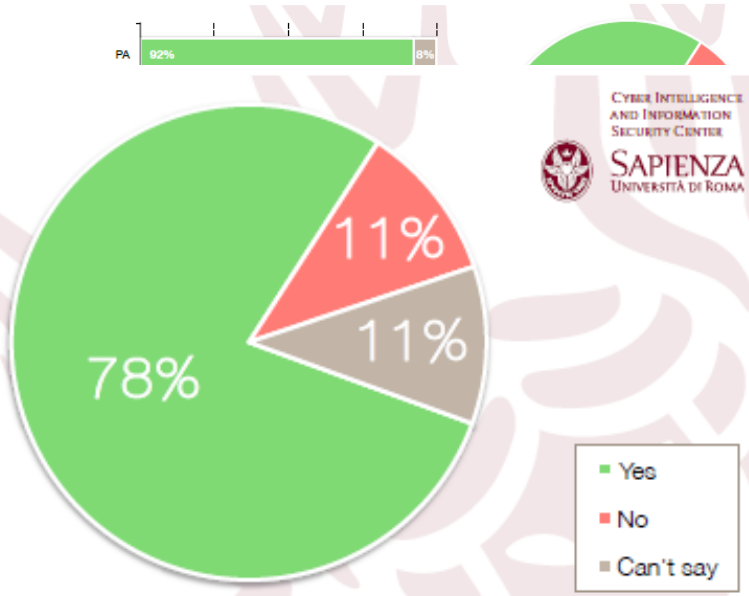


Figure 4.6: Question #1.2.5 - "Is it possible that an ICT service failure in one (or more) third-party company, will have a significant impact on your company?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Figure 4.5: Question #1.2.2 - "Do cloud services support core business processes that are necessary to deliver critical services?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Figure 4.7: Question #1.2.6 - "Do you know if your software providers are following a strategic approach to address application risks in each phase of the application development process?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

Defense: Attacchi esterni

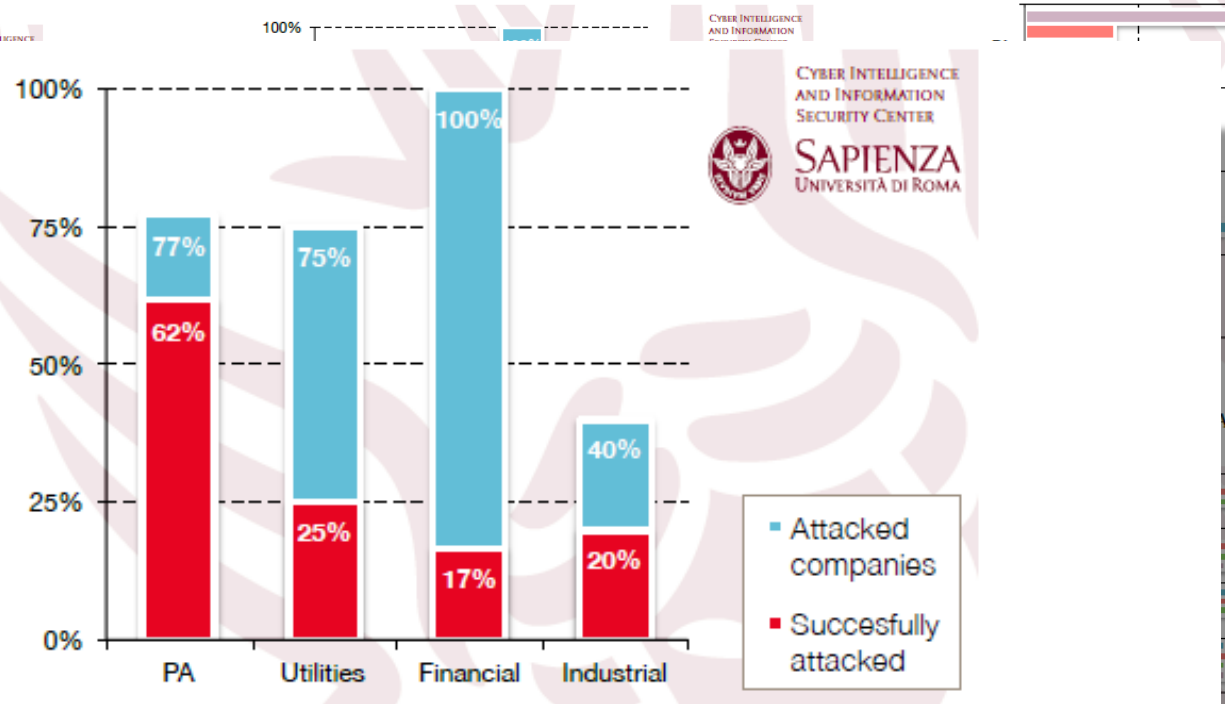


Figure 4.10: Question #1.3.5 - Companies experiencing external cyber attacks (per group).

Defense: misure di protezione

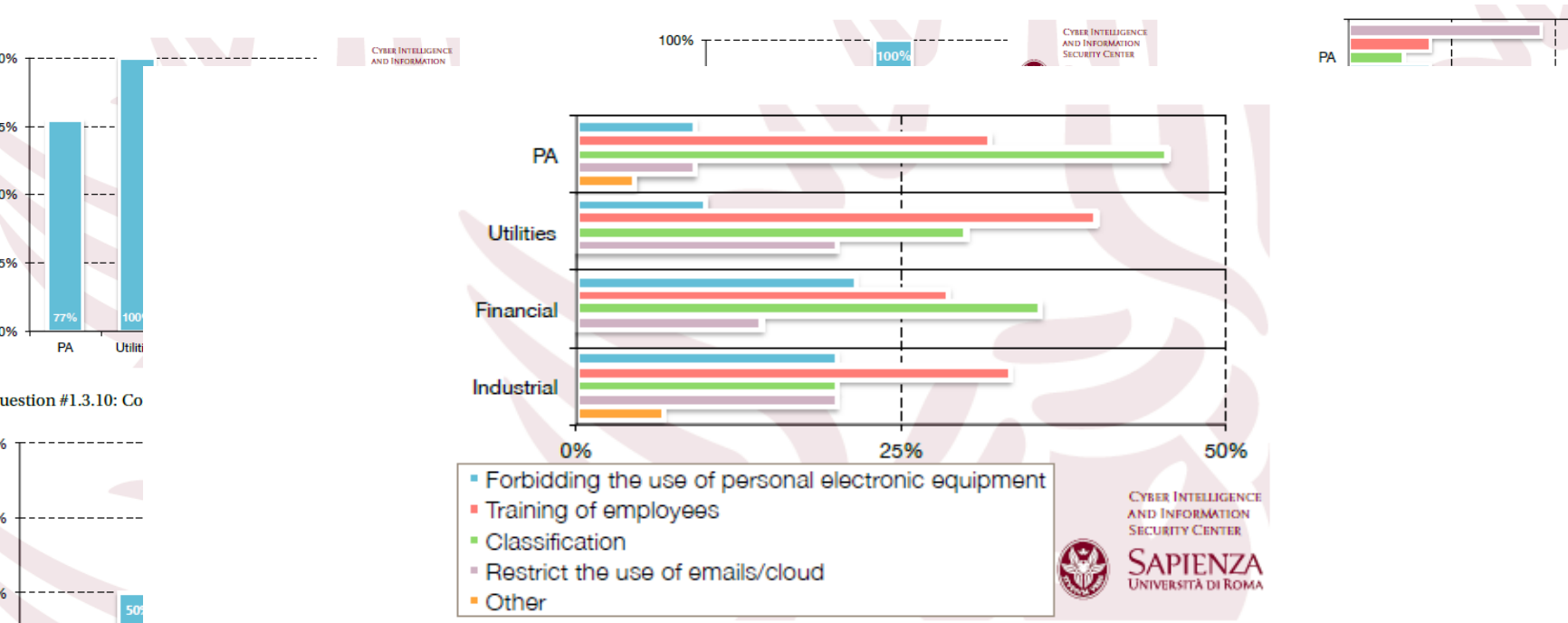


Figure 4.13: Question #1.4.8 - "Which of the following measures to protect data and critical systems from misuse by employees does your company implement?" Adoption rate for each of the countermeasures per group.

Come le organizzazioni vorrebbero migliorare la loro sicurezza cibernetica

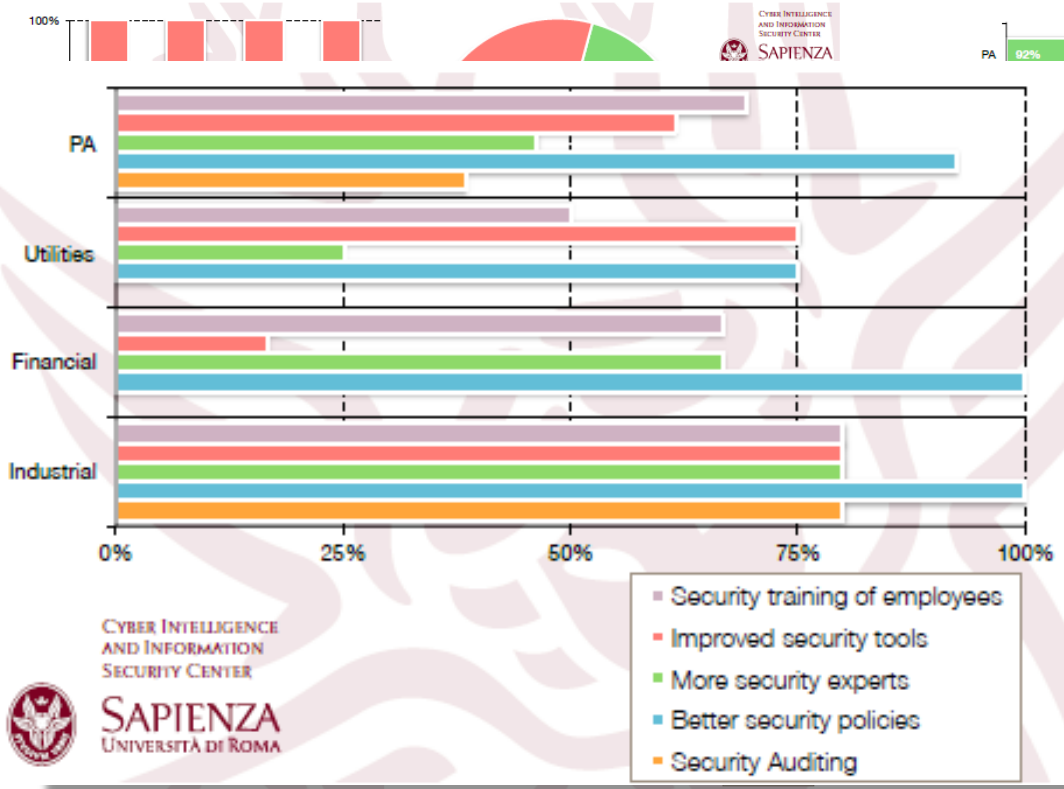


Figure 4.5: Question #1.2.2 - "Do cloud services support core business processes that are necessary to deliver critical services?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

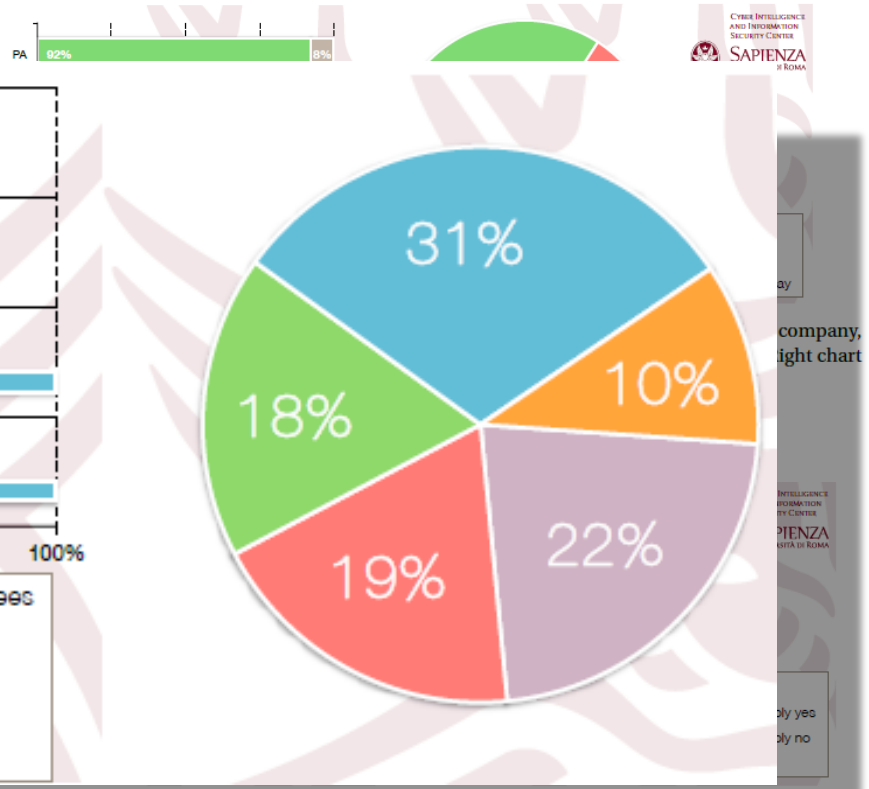
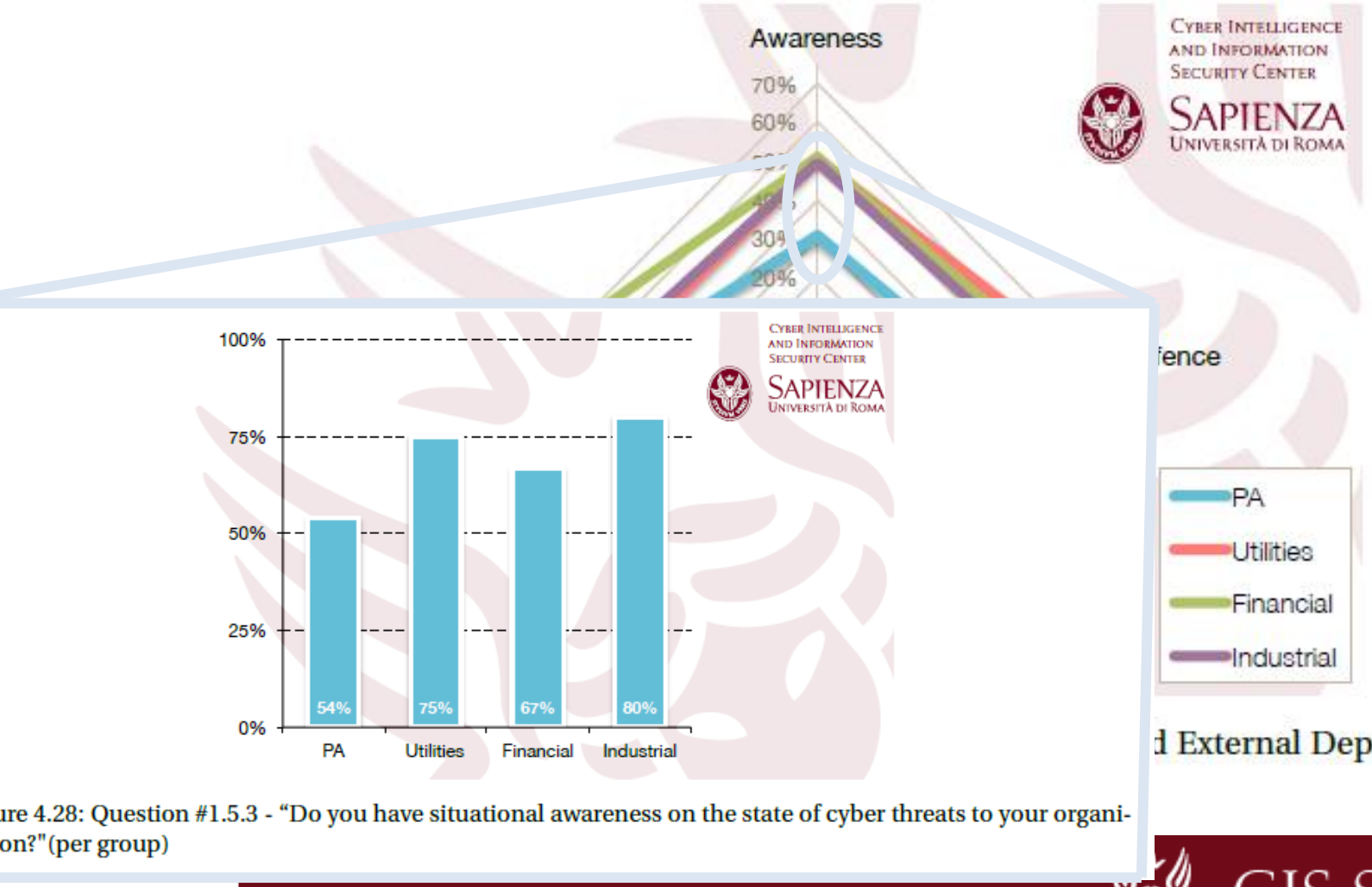


Figure 4.7: Question #1.2.6 - "Do you know if your software providers are following a strategic approach to address application risks in each phase of the application development process?" Left chart shows answer distribution by group. Right chart depicts the overall picture.

A cyber security readiness index



ure 4.28: Question #1.5.3 - "Do you have situational awareness on the state of cyber threats to your organi-on?"(per group)

d External Dependencies indexes

A cyber security readiness index

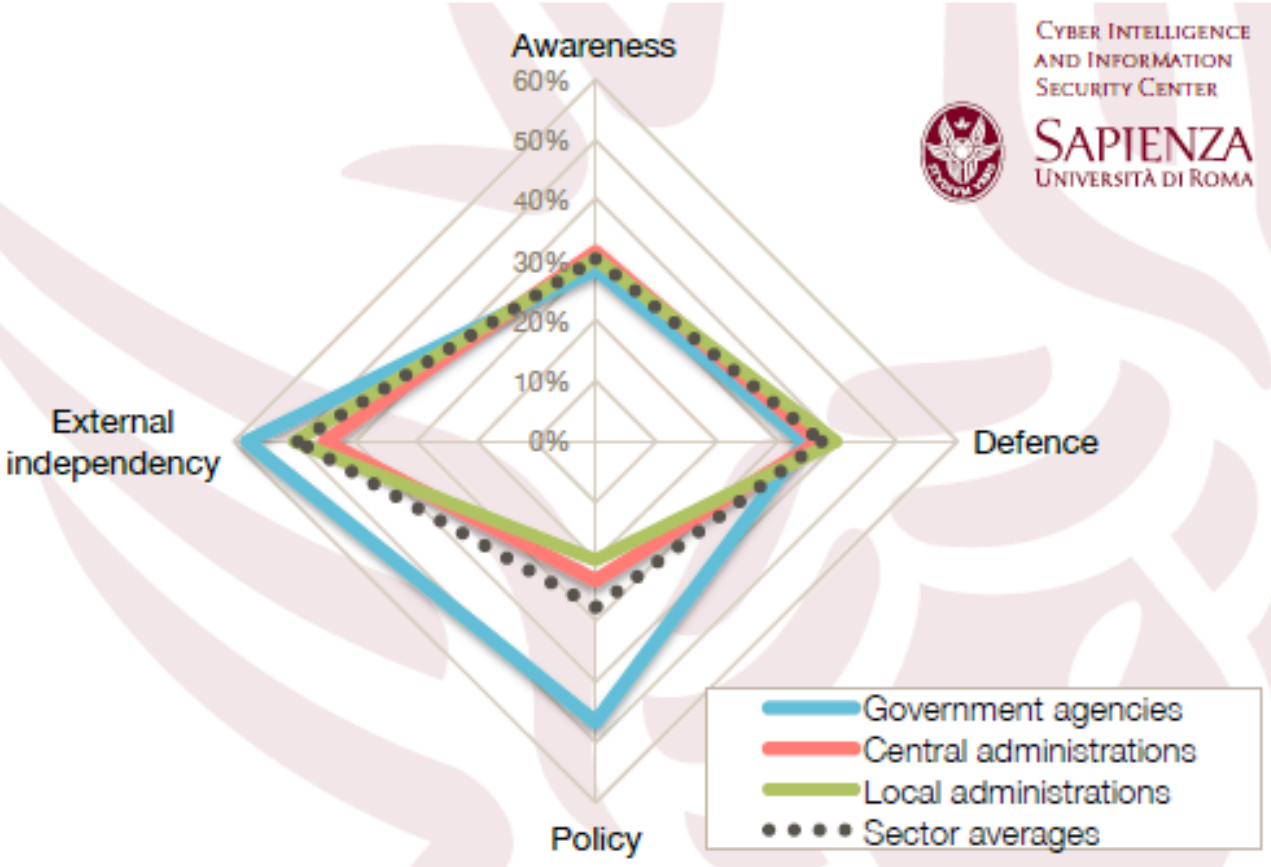


Figure 4.29: Cyber security readiness index for PA group.

Cyber Security Report 2014

- Abbiamo imparato molto
  - Migliorare il questionario
  - Renderlo specifico anche sul settore
- Servizi dedicati a coloro che parteciperanno al questionario
- Sperare che questa esperienza possa aumentare il trust e avere un maggior numero di risposte

Lista di Raccomandazioni per la definizione di una strategia nazionale

- Understanding the dimension of cyber threats
- Identify priorities within critical economic sectors
- Understanding attackers' habits
- Taking critical economic sector infrastructure inter-dependencies into account
- Cooperative assessment of threats and vulnerabilities
- Nationwide methodology for threat classification
- Clear guidelines governing how risks are accepted and documented
- Clear role and mission for the national CERT
- Set clear definitions and procedures for incident response
- Cooperative early threat and vulnerability warning dissemination
- Promote dissemination activities and enhance education skills
- Research, development and technology investments
- International engagements
- Critical economic sector organizations should adopt solid risk management processes
- Reducing the supply chain risk
- A national agency for cyber security

Raccomandazione #1:
Realizzazione del CERT nazionale

- Mattone base dell'incident-response
  - primo step dell'implementazione di una strategia di sicurezza cibernetica nazionale
- Relazioni internazionali
- Comprovata cyber security expertise
- Coinvolgimento del settore privato e accademia

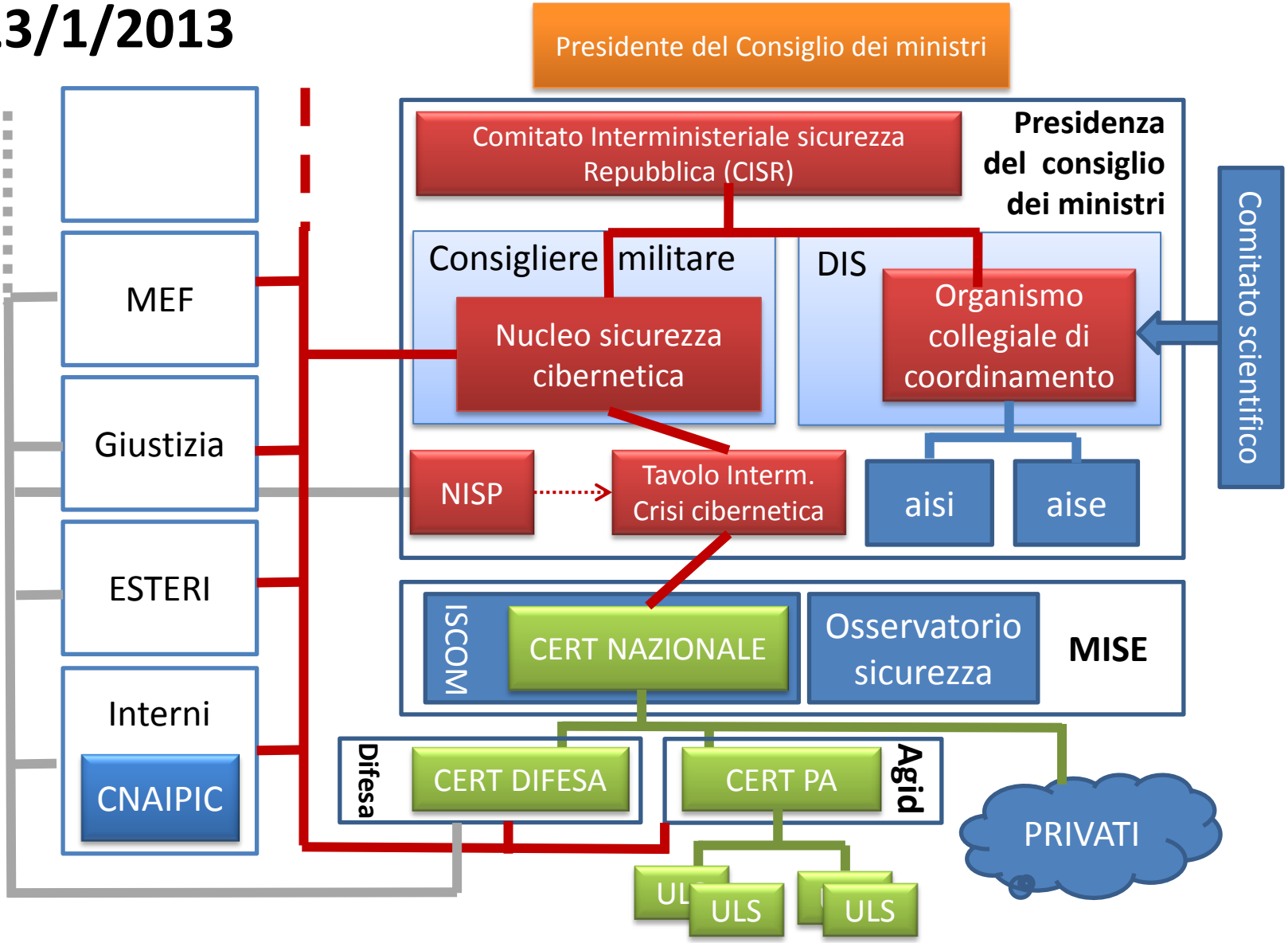
Raccomandazione #2:
Government-Business-Academia partnership

- La strategia nazionale non deve diventare un esercizio PA centrico
- Privato deve organizzarsi attraverso opportuni Information Sharing group (modello ISAC americani) e collaborare con il pubblico
- L'accademia e l'istruzione, in generale, devono attaccare il problema della sicurezza cibernetica su più fronti: dal creare una cultura della sicurezza cibernetica fino a sfornare esperti un materia

Raccomandazione #3:
Research, development and technology investments

- Non possiamo dare in outsourcing competenze di sicurezza cibernetica ad altri paese. E' imperativo consolidare e incrementare competenze nazionali nel creare/dominare tecnologie ICT.
- Iniziative di cyber security possono diventare una fonte di impiego per questa e le prossime generazioni di giovani.
- Agenda di ricerca e sviluppo per promuovere punte di eccellenza in ricerca e sviluppo high-tech (start-up in cyber security)
- Mantenere/portare in Italia I migliori ricercatori nel settore contribuendo ad assicurare l'indipendenza nazionale dai rischi tecnologici

DPCM 23/1/2013



Raccomandazione #3:
Agenzia Nazionale di Cyber Security

- La sicurezza è una missione che difficilmente si coniuga con altri obiettivi e dovrebbe essere confinata all'interno del minimo numero di organizzazioni possibili (possibilmente una)
- Esempio di altri paesi: US, Israele, Francia, Germania, Olanda etc.
- Ridurre la catena di comando per risposta e monitoraggio
- Concentrazione di Cyber Security Expertise

Conclusioni

Proteggere lo spazio cibernetico nazionale da attacchi è un dovere perché:

- sicurezza e prosperità della nazione sono un binomio inscindibile *(Mario Monti Gennaio 2013)*
- non ci possiamo permettere di essere un libro aperto per altre nazioni, ne va della nostra ricchezza, libertà personale e sicurezza nazionale
- la cyber security è una grossa opportunità economica nazionale per la presenza di grandi attori industriali, piccole medie imprese e grandi expertise scientifiche