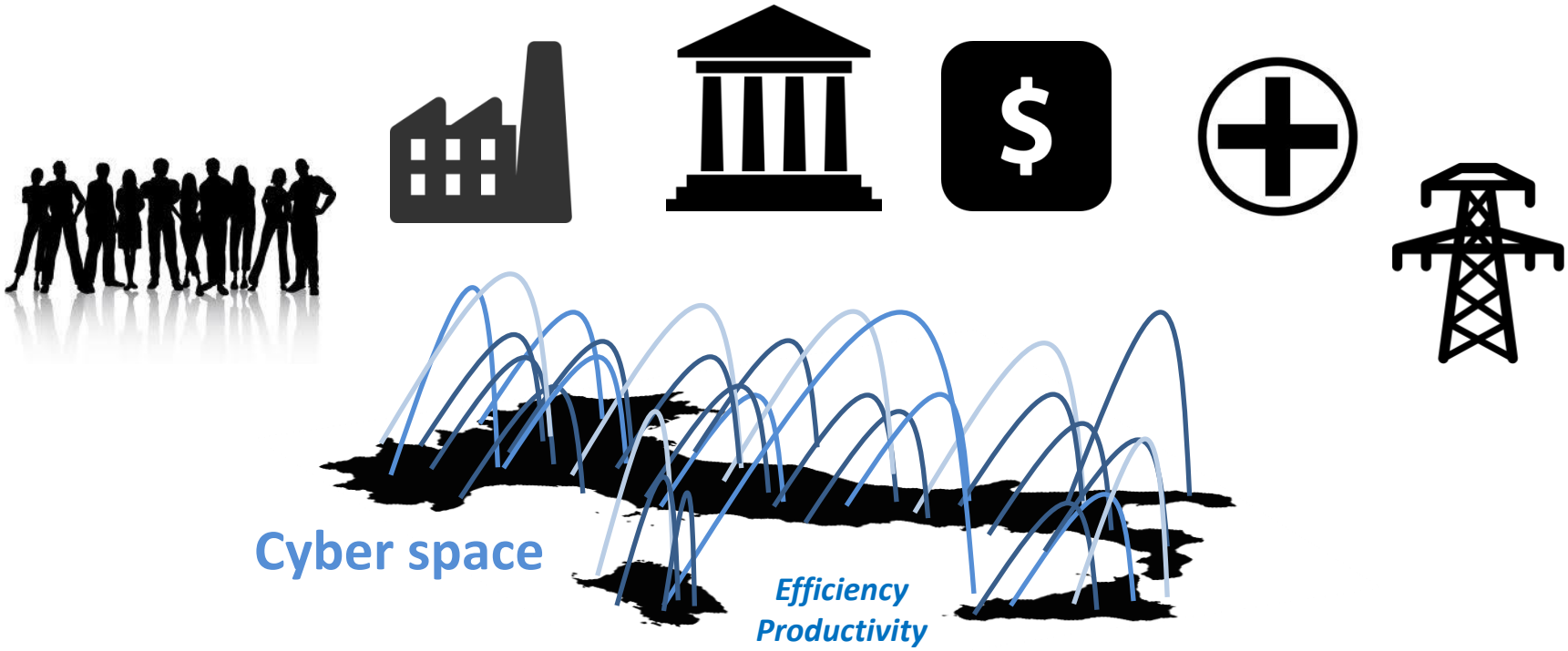
Laboratorio Nazionale di Cyber Security

Roberto Baldoni
Direttore Laboratorio Nazionale Cyber Security
baldoni@dis.uniroma1.it, @robertobaldoni

cini
Cyber Security National Lab

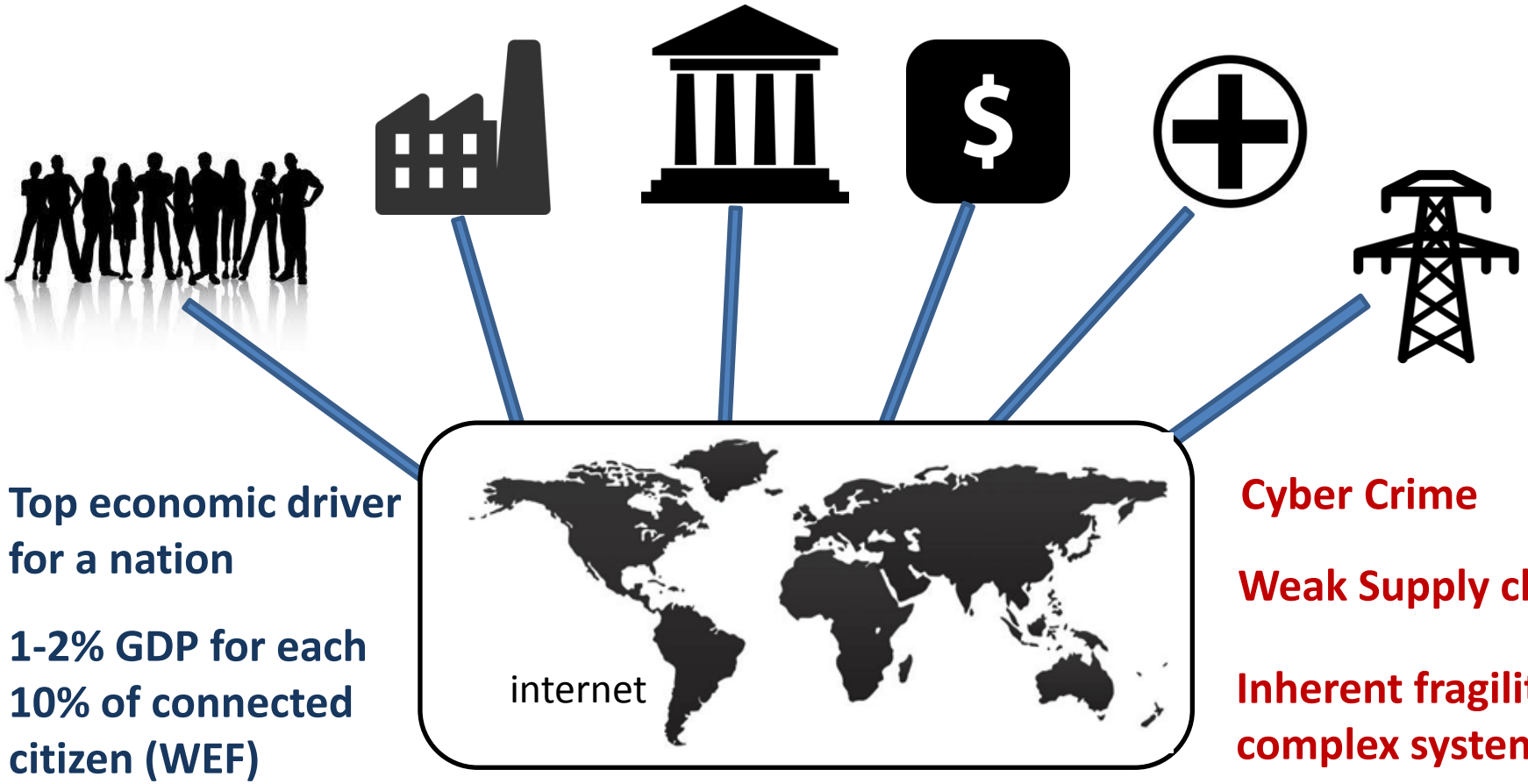
CIS SAPIENZA
RESEARCH CENTER FOR CYBER INTELLIGENCE AND INFORMATION SECURITY

Sensitive economic sectors to cyber threats



in the close future the economic prosperity of a country will be measured according to the degree of security of its cyberspace

Cyber space and economic growth



Top economic driver for a nation

1-2% GDP for each 10% of connected citizen (WEF)

Digitalizing primary services

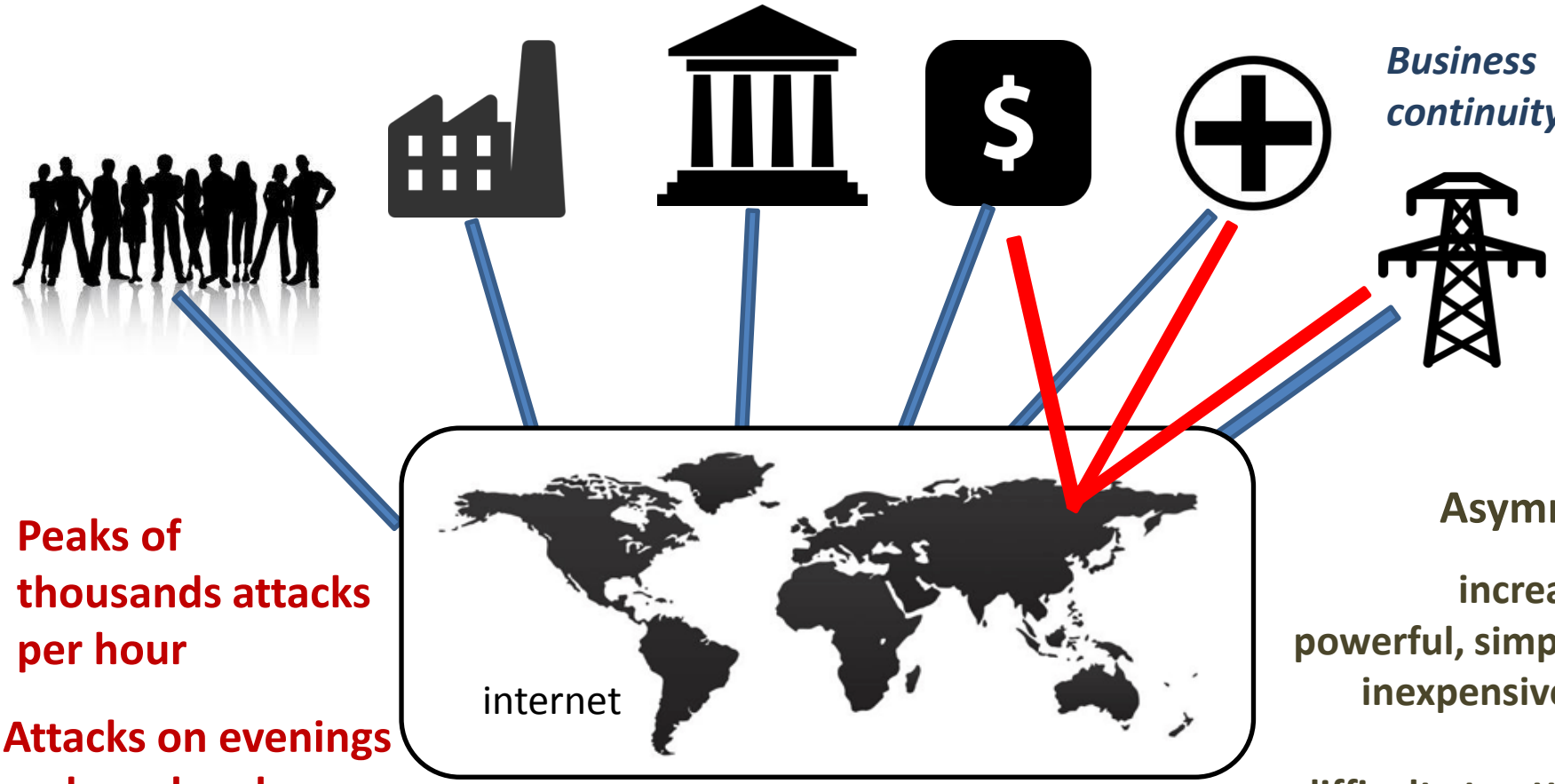
Cyber Crime

Weak Supply chain

Inherent fragility of complex systems

Denial of service

Cyber Attacks



Peaks of thousands attacks per hour

Attacks on evenings and weekends

Asymmetry

increasingly powerful, simple and inexpensive tools

difficulty to attribute

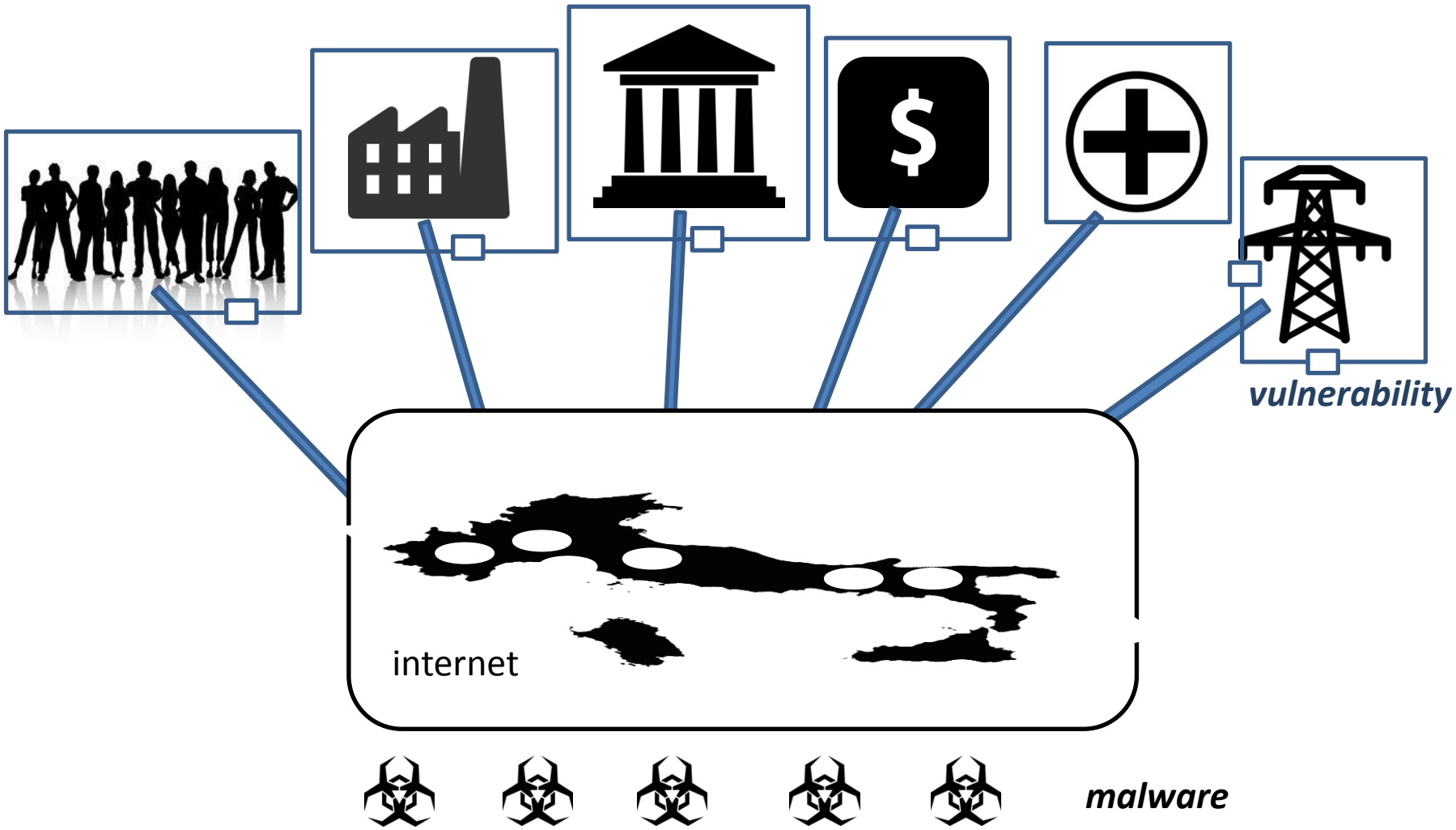
In cyber space is always emergency!

INTELLIGENCE AND ATTACKS IN CYBER SPACE

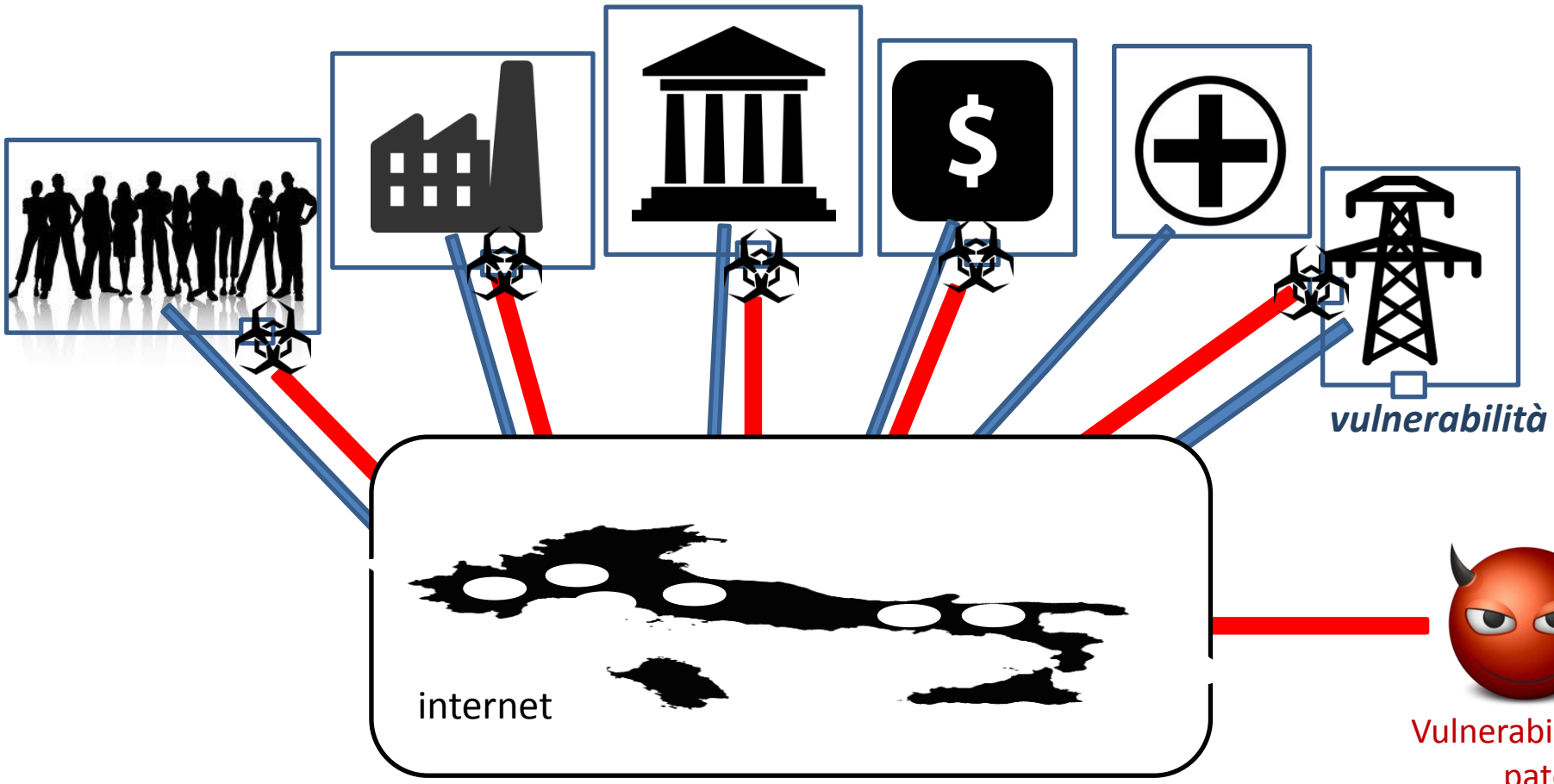
Attacks in cyber space

- «upstream monitoring» (agreement with Telco providers)
- «downstream monitoring» (agreement with ISP providers)
- Malware campaign and Advanced Persistent threats
- Denial of Service

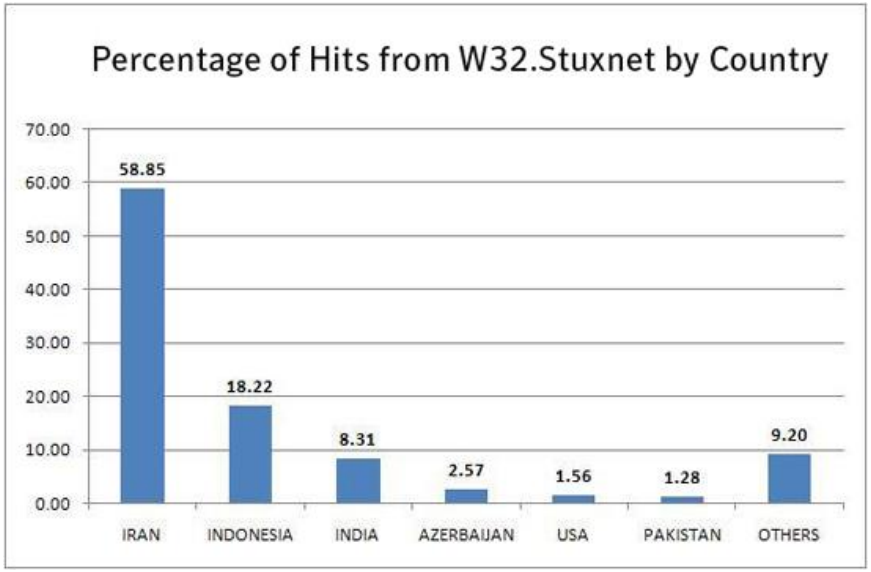
Cyber Espionage - Cyber Weapons



Cyber Espionage - Cyber Weapons



Vulnerabilities
patents
sensitive government information
sensitive industrial information etc.



Stuxnet Geography

Target: SIEMENS Scada Systems
slowing the infected centrifuges down to a few hundred hertz for a full 50 minutes to destroy the machine

Gauss Geography

Target: Lebanon Banks
surveillance tool used to monitor accounts and money flow.

Vocaboulary

- Vulnerability
- Software Bug
- Software bug vs vulnerability
- Exploit

THE ADVERSARY

Who is behind the cyber threat

Till 2004

I LOVE YOU

BLASTER

Virus

today

CONFIKER

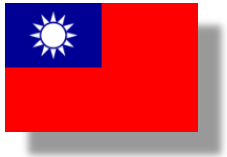
DUQU

STUXNET

Flame

ZEUS

GAUSS



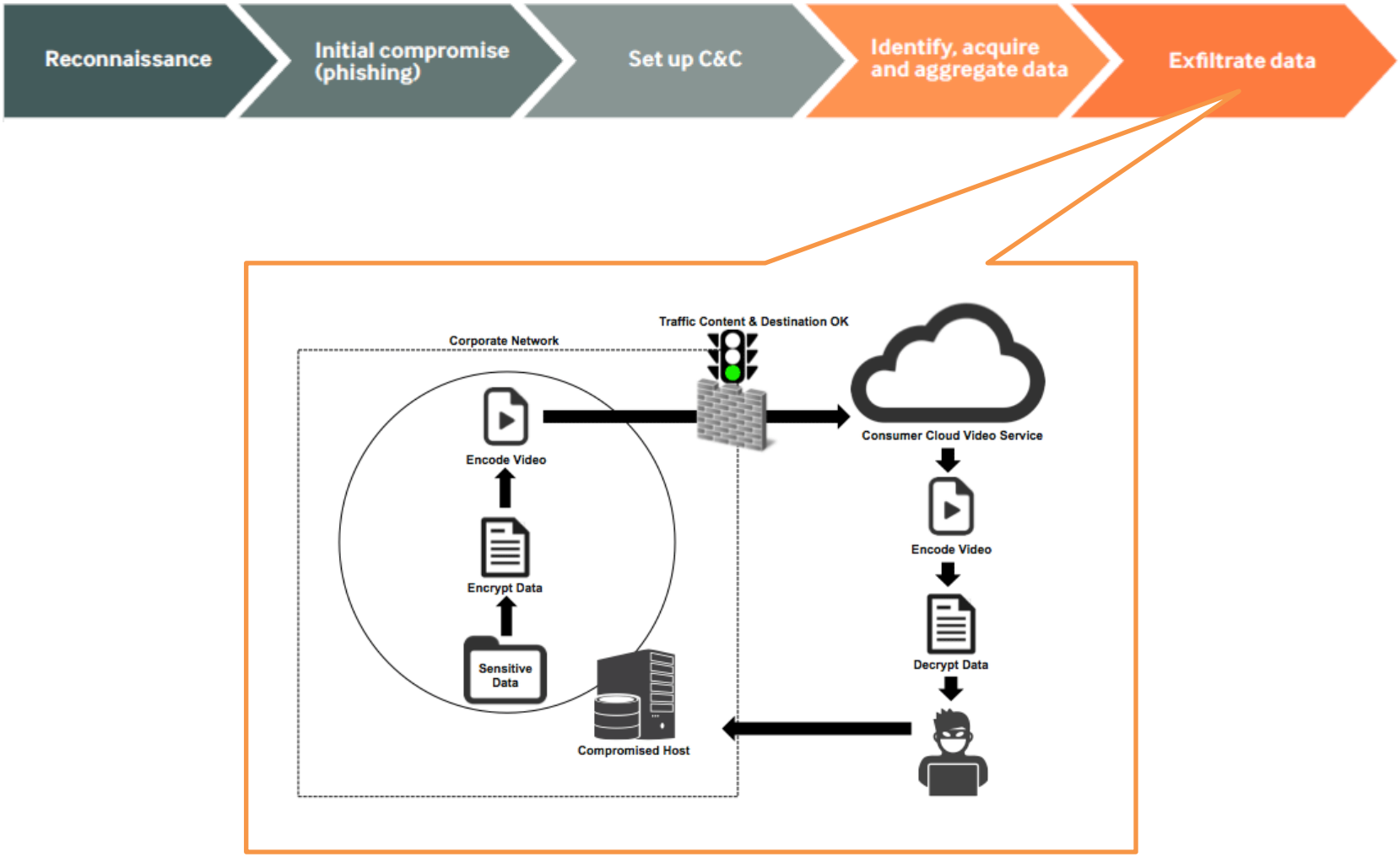
MIRAGE

APT, Malware

Adversary

- Levels of expertise
- Available resources
- Objectives
- Attack vectors
- Behaviour

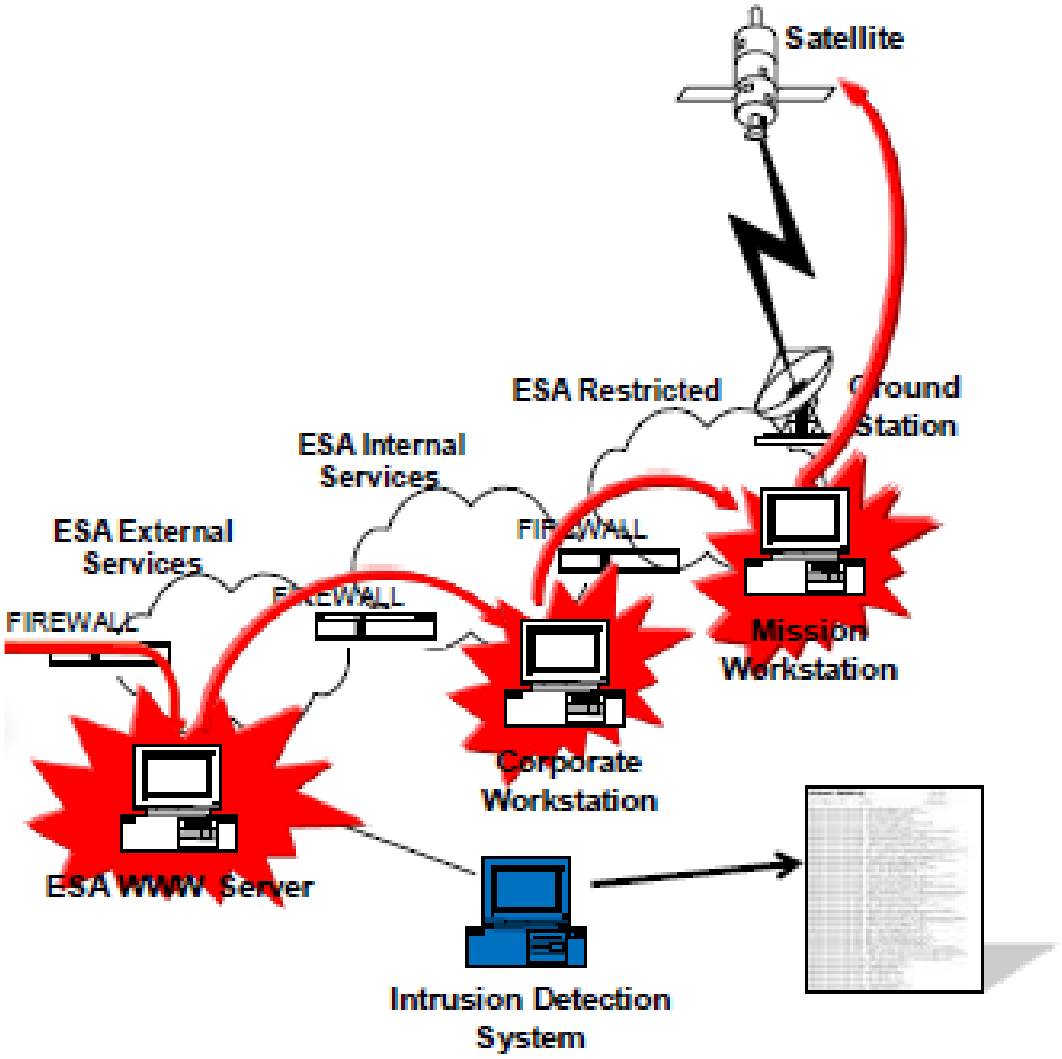
Data Exfiltration



Advanced Persistent Threats

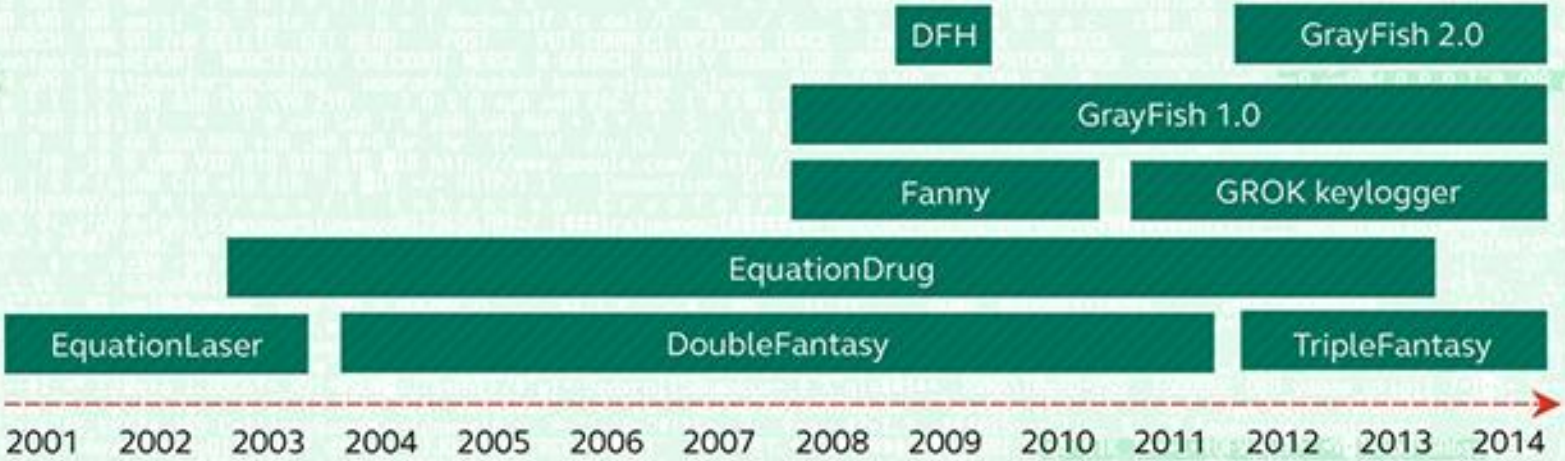
- sophisticated levels of expertise
- significant resources
- Objectives (footholds within the information technology infrastructure of the targeted organizations)
  - exfiltrating information
  - undermining or impeding critical aspects of a mission, program, or organization
  - positioning itself to carry out these objectives in the future

- multiple attack vectors
- behavior
  1. pursue its objectives repeatedly over an extended period of time;
  2. adapt to defenders' efforts to resist it
  3. determined to maintain the level of interaction needed to execute its objectives.


Satellite
ESA Restricted
Ground Station
ESA Internal Services
ESA External Services
FIREWALL
FIREWALL
FIREWALL
Mission Workstation
Corporate Workstation
ESA WWW Server
Intrusion Detection System

THE EQUATION GROUP

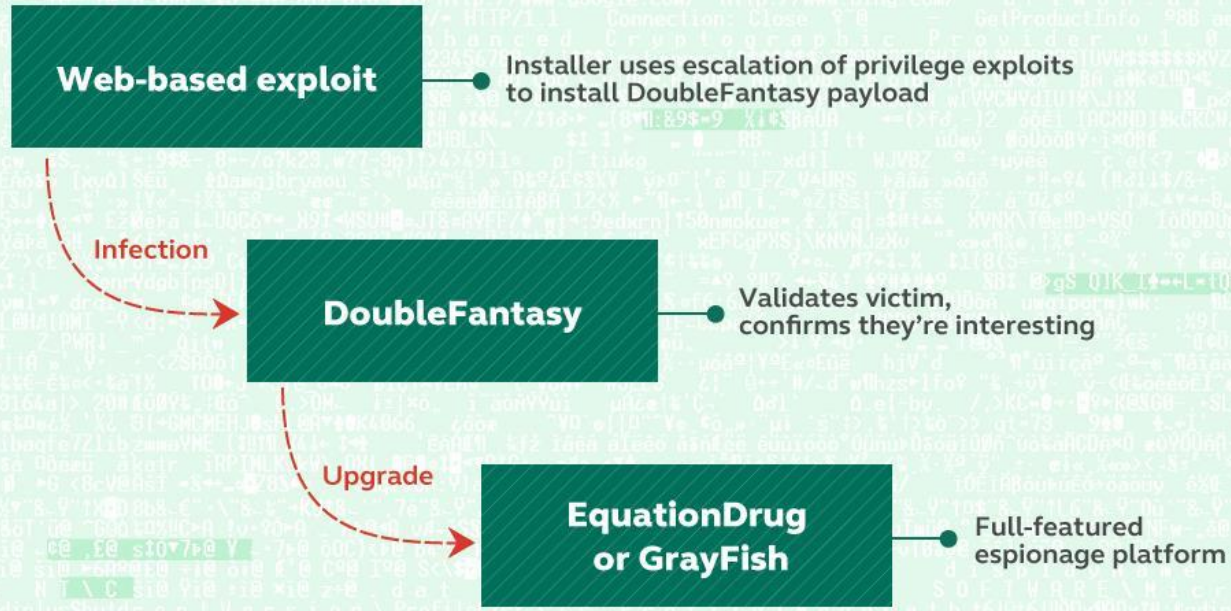
Equation group's malware timeline



- The Fanny timeline is based on C&C server IP activity
- TripleFantasy compilation timestamps seem to be fake, graph based on compiler versions and C&C registrations
- EquationDrug appears to have been replaced with Grayfish in somewhere in 2013; development started earlier
- DFH refers to "Disk from Houston"

GREAT KASPERSKY

Infection lifecycle of EquationDrug



GREAT KASPERSKY

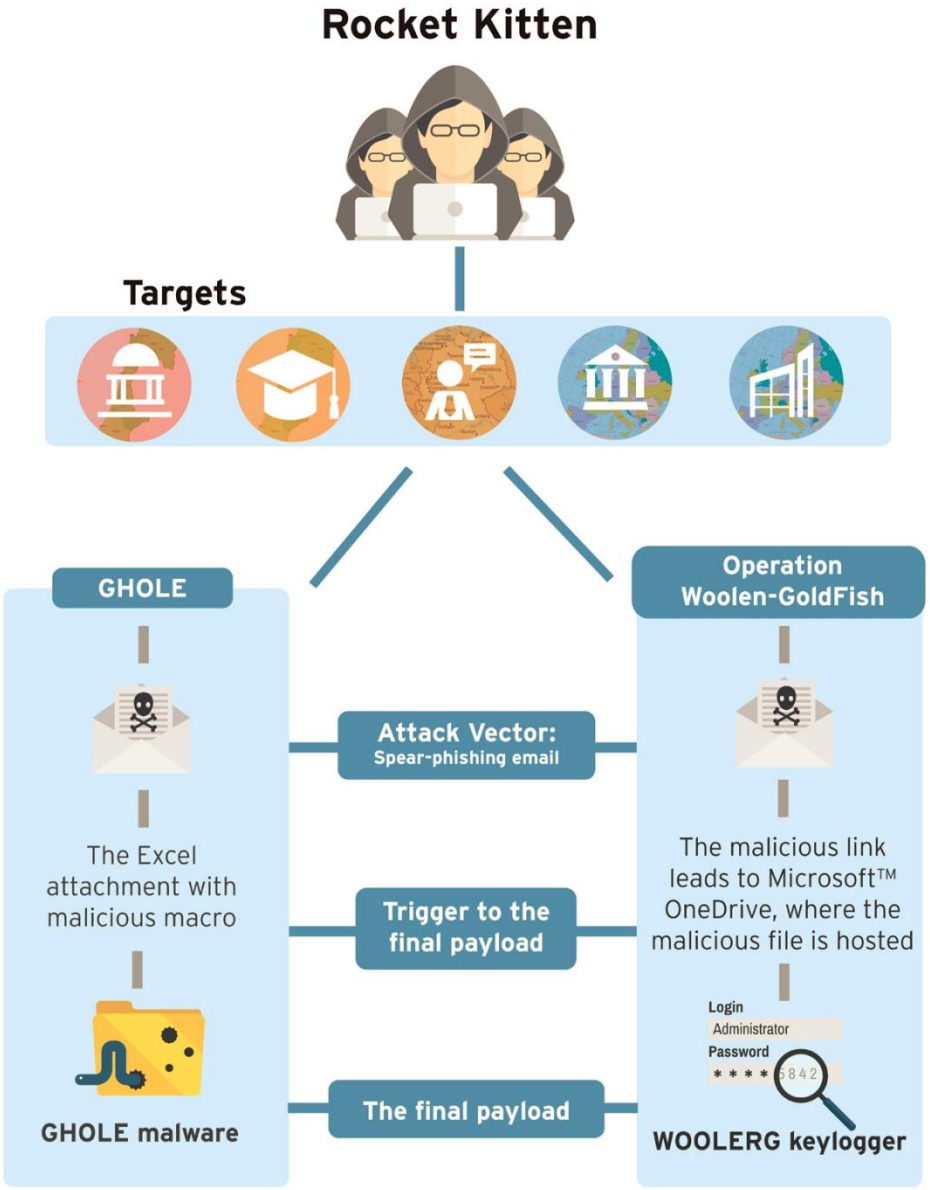
Implant the malware

- The equation group
  - Self-replicating (worm) code – Fanny
  - Physical media, CD-ROMs
  - USB sticks + exploits
  - Web-based exploits

Infecting the hard drive firmware

- Reprogramming and Flashing HDD firmware
- Modules in EQUATIONDRUG and GRAYFISH platforms (from 2010 to 2013)
- 12 Drives categories: “WDC WD”, “ST”, “Maxtor STM”, “SEAGATE ST”, “SAMSUNG”, “WDC WD”, “IC”, “IBM”, “Hitachi”, “HTS”, “HTE”, “HDS”, “HDT”, “ExcelStor” etc.
- reprogrammed by a series of ATA commands. The plugin uses a lot of undocumented, vendor-specific ATA commands
- Identified only a few victims. This indicates that it is probably only kept for the most valuable victims

ROCKET KITTEN: EXPERTS IN PHISHING



Victims

- Civilian organizations in Israel
- Academic organizations in Israel
- German-speaking government organizations
- European organizations
- European private company

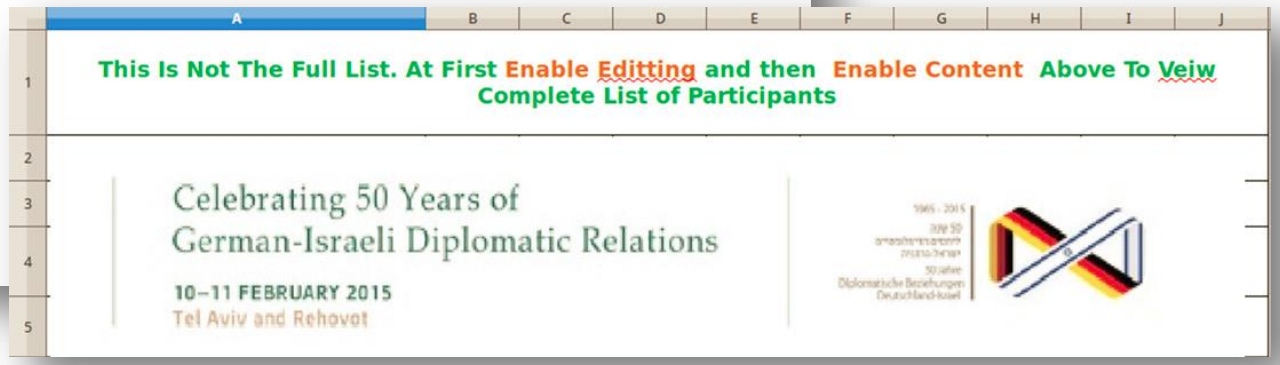
Rocket Kitten spear-phishing emails

From: [redacted]
Date: Apr 23, 2014 10:08 AM
Subject: Message
To: [redacted]

Dear all,
Enclosed is some information that I hope you will find it useful.
Hag Sameah.

--
[redacted]
CEO, [redacted]

[redacted]



From: FirstName [mailto: firstnamelastname1@gmail.com]
Subject: Possible Scenarios for Hezbollah's Retaliation? your comments are most welcome.

Dear experts,

As you know Israeli helicopter had conducted a strike against "terrorists" near Quneitra, on the Syrian side of the Golan Heights
that killed several of Hezbollah's members including one Iranian commander.
I wrote an article about possible scenarios about Hezbollah's reactions and
would like to know your ideas about it?

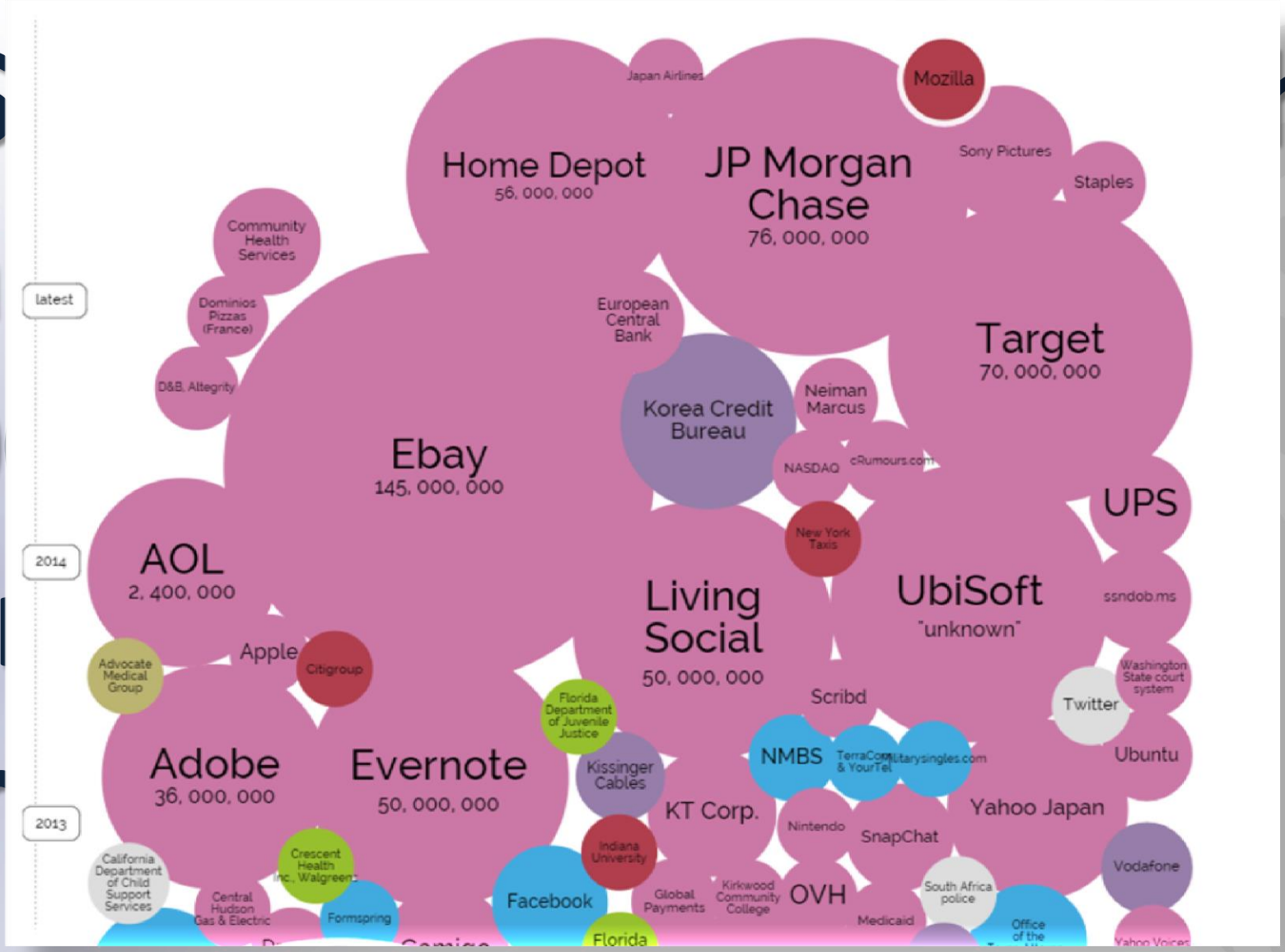
I answered some questions about possible reactions:

- Is it in the common interest between Hezbollah and Iran to retaliate?
- What can be the worst-case scenario?
- Time and place to hit back?
- Will the retaliation be restrained enough to provoke a war?
- ...

You can download and see the article in my Drive:
https://onedrive.live.com/redir?resid=xxxxxxxxxxxxxx
Best regards,
FirstName

--
(here followed an official signature)

US
pa
20
co
str



GOVERNMENTS AND CYBER THREATS

Towards a Cyber Security National Strategy

CERT

vulnerability

Public Private Information Sharing

Law enforcement

Adequate response measures

Improve preparadeness

internet

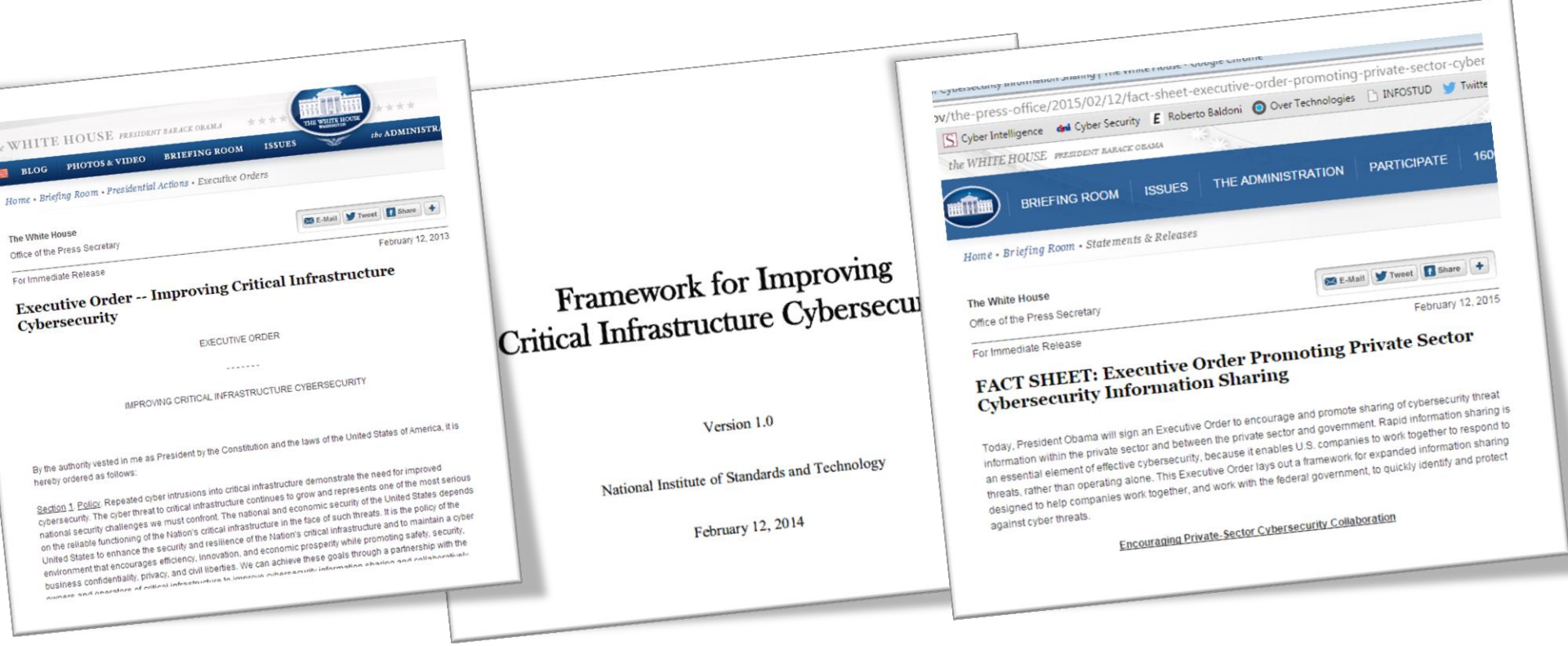
Cyber security education

Research and Development

Early warning system

Cyber Intelligence

Grow of security experts



12/2/2013

12/2/2014

15/2/2015

Complex Implementation

Forbes.com

"Problematic voluntary adoption plan"

14 Feb 2013

"Google, Apple and Microsoft may be exempt from Obama's cybersecurity order"

"Obama's Cybersecurity Order Exempts Software" 5 March 2013

Complex Implementation

The Federal Government's Track Record
on Cybersecurity and Critical Infrastructure

A report prepared by

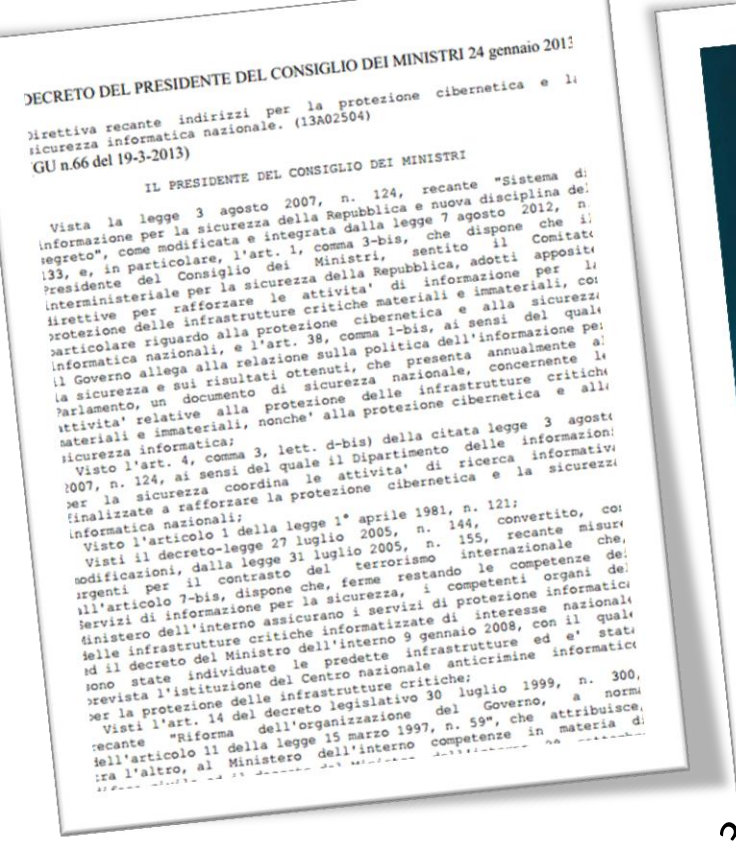
the Minority Staff of the Homeland Security and Governmental Affairs Committee

Sen. Tom Coburn, MD, Ranking Member

February 4, 2014

The report draws on previous work by agency inspectors general and the Government Accountability Office to paint a broader picture of chronic dysfunction, citing repeated failures by federal officials to perform the unglamorous work of information security. That includes installing security patches, updating anti-virus software, communicating on secure networks and requiring strong passwords. A common password on federal systems, the report found, is "password."

In March 2013, GAO [Government Accountability Office] reported that IRS allowed its employees to use passwords that "could be easily guessed." Examples of easily-guessed passwords are a person's username or real name, the word "password," the agency's name, or simple keyboard patterns (e.g., "qwerty"), according to the National Institute of Standards and Technology.



DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 201

Direttiva recante indirizzi per la protezione cibernetica e l
sicurezza informatica nazionale. (13A02504)
(GU n.66 del 19-3-2013)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 3 agosto 2007, n. 124, recante "Sistema d
informazione per la sicurezza della Repubblica e nuova disciplina de
segreto", come modificata e integrata dalla legge 7 agosto 2012, n.
133, e, in particolare, l'art. 1, comma 3-bis, che dispone che il
Presidente del Consiglio dei Ministri, sentito il Comitato
interministeriale per la sicurezza della Repubblica, adotti apposite
direttive per rafforzare le attivita' di informazione per la
protezione delle infrastrutture critiche materiali e immateriali, con
particolare riguardo alla protezione cibernetica e alla sicurezza
informatica nazionali, e l'art. 38, comma 1-bis, ai sensi del quale
il Governo allega alla relazione sulla politica dell'informazione per
la sicurezza e sui risultati ottenuti, che presenta annualmente al
Parlamento, un documento di sicurezza nazionale, concernente le
attivita' relative alla protezione delle infrastrutture critiche e
materiali e immateriali, nonche' alla protezione cibernetica e alla
sicurezza informatica;
Visto l'art. 4, comma 3, lett. d-bis) della citata legge 3 agosto
2007, n. 124, ai sensi del quale il Dipartimento delle informazioni
per la sicurezza coordina le attivita' di ricerca informativa
finalizzate a rafforzare la protezione cibernetica e la sicurezza
informatica nazionali;
Visto l'articolo 1 della legge 1° aprile 1981, n. 121;
Visti il decreto-legge 27 luglio 2005, n. 144, convertito, co
modificazioni, dalla legge 31 luglio 2005, n. 155, recante misure
urgenti per il contrasto del terrorismo internazionale che,
all'articolo 7-bis, dispone che, ferme restando le competenze dei
Servizi di informazione per la sicurezza, i competenti organi del
Ministero dell'interno assicurano i servizi di protezione informatica
delle infrastrutture critiche informatizzate di interesse nazionale
ed il decreto del Ministro dell'interno 9 gennaio 2008, con il quale
sono state individuate le predette infrastrutture ed e' stata
prevista l'istituzione del Centro nazionale anticrimine informatico
per la protezione delle infrastrutture critiche;
Visti l'art. 14 del decreto legislativo 30 luglio 1999, n. 300,
recante "Riforma dell'organizzazione del Governo, a norma
dell'articolo 11 della legge 15 marzo 1997, n. 59", che attribuisce,
tra l'altro, al Ministero dell'interno competenze in materia di

Italian Framework for cyber security

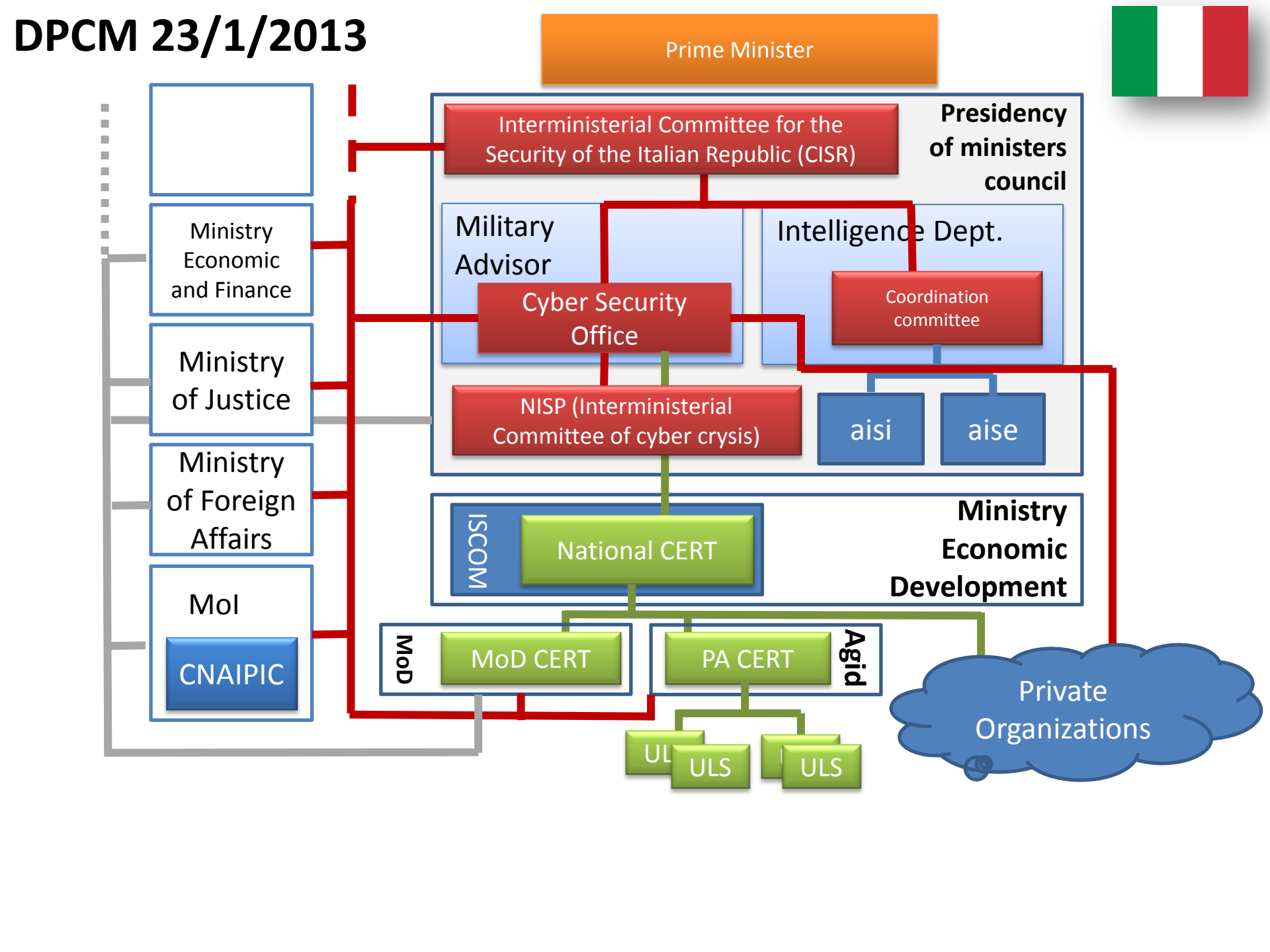
24/1/2013

27/12/2013

implementation

31/12/2015

DPCM 23/1/2013



IL LABORATORIO NAZIONALE DI CYBER SECURITY

Il Ruolo delle Università nel Quadro Strategico di Sicurezza Cibernetica Nazionale

«A livello Nazionale è imperativo sviluppare un approccio coordinato e multi-dimensionale con obiettivi condivisi e ampiamente partecipati tra le amministrazioni dello Stato, il mondo privato, accademico e della ricerca scientifica» **(pagina 6)**

cini Cyber Security National Lab

Ruolo dell'Università

- **Ricerca**
- **Formazione**
- **Innovazione**
- **Consapevolezza**

Problemi dell'Università

- **Eccessiva frammentazione delle competenze**
- **Competenze monotematiche**
- **Distacco dall'economia reale**
- **Autoreferenzialità**

Local vs Nationwide approach

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

Per affrontare la minaccia cyber c'e' bisogno di attori Nazionali che siano in grado di mettere in rete le eccellenze del paese nella ricerca e di assicurare una efficace azione di supporto all'implementazione di azioni governative, di formazione e di awareness

cini Cyber Security National Lab

Laboratorio Nazionale di Cyber Security

- Creato a Maggio 2014, operativo da Ottobre 2014
- Orchestrare ed organizzare l'eccellenza Accademica di Cyber-Security (e.g., cryptography, dependability, information security, hardware security, malware analysis, CIP, risk management, intelligence etc.)
- Mappatura fine della ricerca e formazione in Italia
- Mettere a sistema l'esistenza di gruppi di eccellenze su specifici argomenti sparsi sul territorio Nazionale
- Supportare azioni governative a carattere locale e Nazionale
- Innovazione in ambito Cyber Security

cini Cyber Security National Lab

Laboratori Locali e Coordinatori

• IMT Lucca	Rocco De Nicola
• Politecnico di Milano	Stefano Zanero
• Politecnico di Torino	Antonio Lioy
• Seconda Univ. di Napoli	Beniamino Di Martino
• Univ. di Venezia	Riccardo Focardi
• Univ. del Sannio	Corrado Visaggio
• Univ. dell'Insubria	Elena Ferrari
• Univ. di Bari	Donato Malerba
• Univ. di Bologna	Gabriele D'Angelo
• Univ. di Cagliari	Massimo Bartoletti
• Univ. di Catania	Dario Catalano
• Univ. di Firenze	Andrea Bondavalli
• Univ. di Genova	Alessandro Armando
• Univ. di Milano	Pierangela Samarati
• Univ. di Milano-Bicocca	Claudio Ferretti
• Univ. di Modena e Reggio Emilia	Michele Colajanni
• Univ. di Napoli "Federico II"	Antonino Mazzeo
• Univ. di Napoli "Parthenope"	Luigi Romano
• Univ. di Padova	Mauro Conti
• Univ. di Palermo	Giuseppe Lo Re
• Univ. di Parma	Michele Tomaiuolo
• Univ. di Pavia	Antonio Barili
• Univ. di Perugia	Stefano Bistarelli
• Univ. di Pisa	Gianluca Dini
• Univ. Politecnica delle Marche	Marco Baldi
• Univ. di Roma "La Sapienza"	Luigi Mancini
• Univ. di Roma "Tor Vergata"	Maurizio Talamo
• Univ. di Salerno	Carlo Blundo
• Univ. di Torino	Francesco Bergadano
• Univ. di Trento	Fabio Massacci
• Univ. di Udine	Marino Miculan
• Univ. della Calabria	Domenico Sacca'
• Univ. di Reggio Calabria	Francesco Buccafurri

240 Faculties

- **68 Full Prof**
- **57 Ass. Prof**
- **100 Researchers**

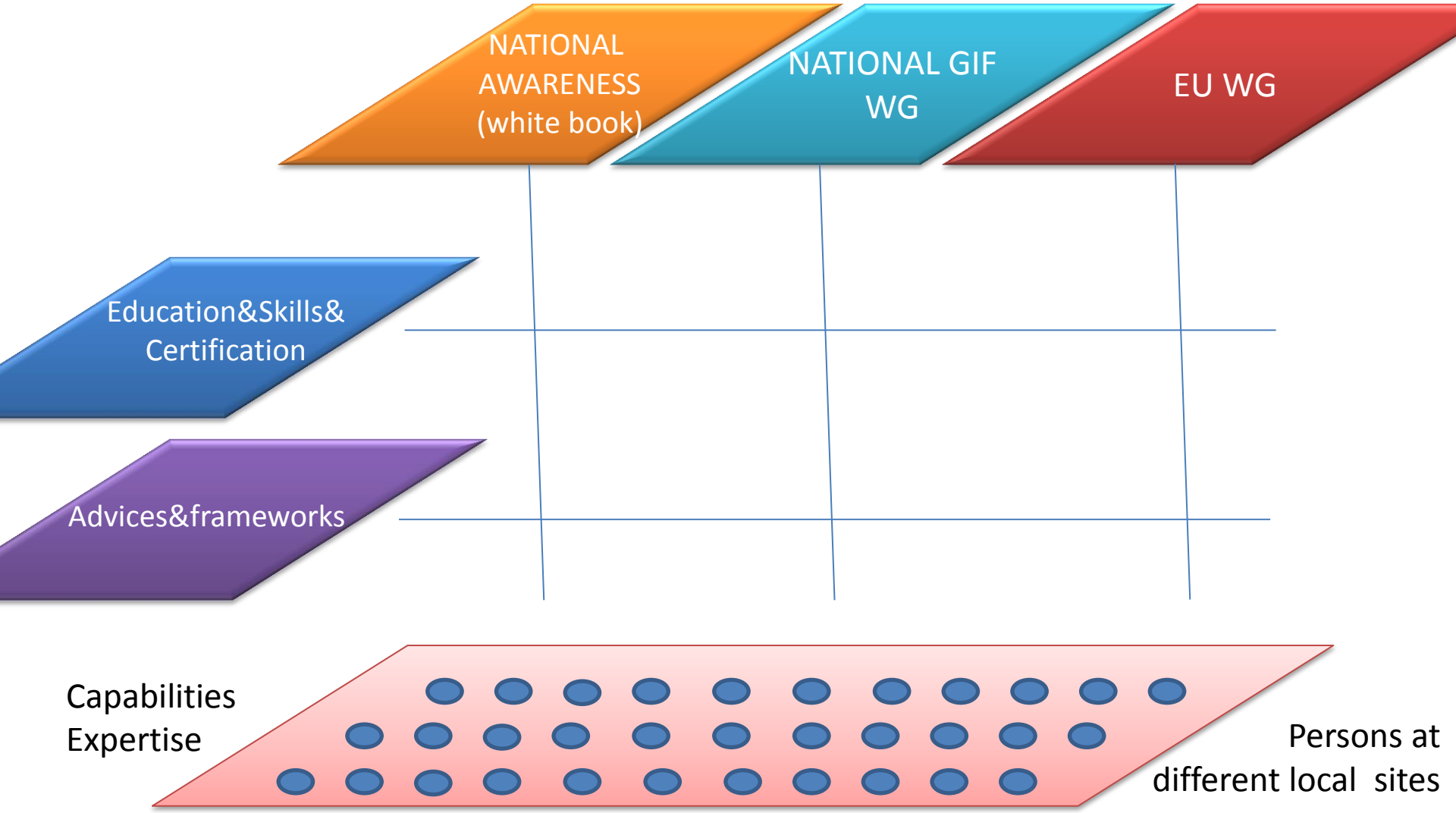
178 PhD students

76 postdocs

51 Experts

Laboratorio Nazionale di Cyber Security: Inclusività

- Allargare il Laboratorio Nazionale
  - ad altri enti di ricerca:
    - CNR
    - ENEA
    - FBK
  - ad altre Univ. Italiane rilevanti
  - ad altri consorzi rilevanti sul modello CINI
- Aumentare il grado di multidisciplinarietà come misura del successo del Laboratorio


NATIONAL AWARENESS (white book)
NATIONAL GIF WG
EU WG
Education&Skills& Certification
Advices&frameworks
Capabilities Expertise
Persons at different local sites

National Government Industry Financy (GIF) Working Group

Questo Working Group si propone di stat… …li locali e nazionali, industrie e altre organizzazioni economiche e finanziarie s… …ostare le istituzioni Italiane nel rapporto con enti terzi su que… delle capacità nazionali di ricerca. Infine il… aiutarli a definire e raggiungere gli obietti…

Coordinatore del gruppo di lavoro:

	Università degli Studi di…

Membri Core del gruppo di lavoro - Sez…

IMT Institute for Advanced Studies Lucc…
Politecnico di Torino
Politecnico di Torino
Università degli Studi di Genova
Università degli Studi di Milano
Università degli Studi di Modena e Regg…
Università degli Studi di Napoli "Federic…
Università degli Studi di Roma "La Sapie…
Università degli Studi "Mediterranea" di …
Università della Calabria

Membri Core del gruppo di lavoro - Sez…

Politecnico di Milano			
Politecnico di Torino			
Università degli Studi del Sannio			
Università degli Studi di Napoli "Federico II"			
Università degli Studi di Napoli "Federico II"	Giorgio	…	
Università degli Studi di Napoli "Partenophe"	Luigi	Romano	link
Università degli Studi di Roma "La Sapienza"	Luigi Vincenzo	Mancini	link
Università degli Studi di Trento	Fabio	Massacci	link

Laboratorio Nazionale di Cyber Security

- Home
- MISSIONE
- AREE DI RICERCA
- PROGETTI DI RICERCA
- WORKING GROUPS
  - NATIONAL GIF
  - EUROPE AND INTERNATIONAL LAISON
  - AWARENESS
  - EDUCATION AND CERTIFICATION
- DIREZIONE
- NODI LOCALI E AFFERENTI
- FORMAZIONE IN CYBER SECURITY IN ITALIA
- RICERCA IN CYBER SECURITY IN ITALIA
- NEWS
- BANDI
- CONTATTI

Menu utente

Profilo
Crea articolo
Guida all uso del portale

Europe and International Laison

Questo Working Group si propone di fare da interfaccia con le istituzioni di ricerca Europee ed internazionali creando opportunità per i nodi locali attraverso partecipazione coordinata ad eventi o comitati internazionali sia a livello scientifico che tecnologico. Il gruppo ha anche come obiettivo quello di rappresentare e di promuovere in Europa ed a livello internazionale l'eccellenza delle attività scientifiche e tecnologiche realizzate in seno al laboratorio. Il lavoro in questo working group ha come obiettivo anche la sollecitazione di proposte di progetti internazionali in particolare creando unità cini intermodo. Un ultimo obiettivo è quello di migliorare il flusso informativo tra i laboratori locali. Il gruppo lavorerà a stretto contatto con il working group national GIF.

Coordinatore del gruppo di lavoro

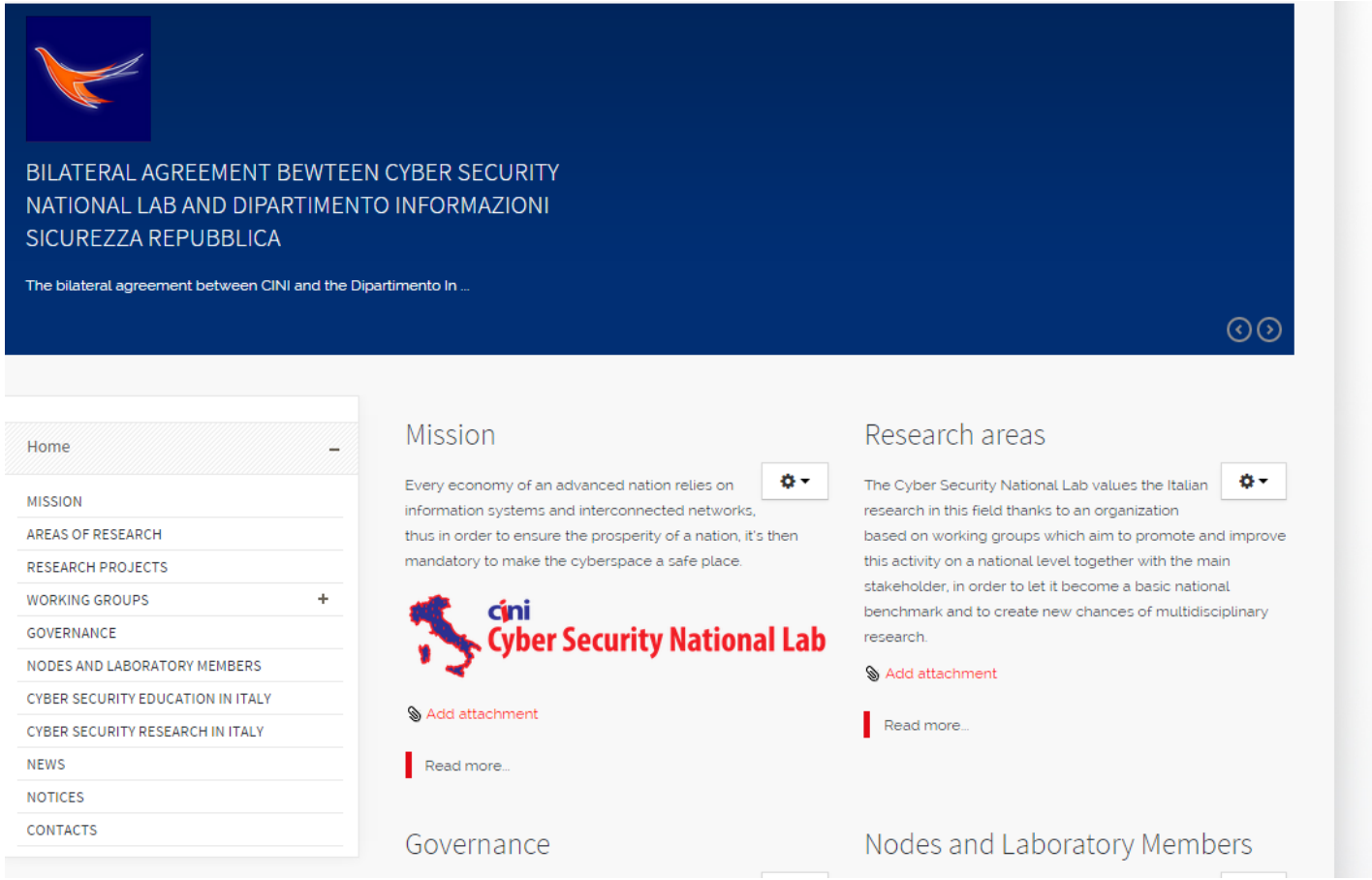
	Università degli Studi di Milano	Pierangela	Samarati	link

Membri Core del gruppo di lavoro

Politecnico di Milano	Federico	Maggi	link
Politecnico di Torino	Paolo	Prinetto	link
Seconda Università degli Studi di Napoli	Beniamino	Di Martino	link
Università degli Studi di Firenze	Andrea	Bondavalli	link
Università degli Studi di Genova	Giorgio	Delzanno	link
Università degli Studi di Napoli "Partenophe"	Luigi	Romano	link
Università degli Studi di Roma "La Sapienza"	Roberto	Baldoni	link
Università degli Studi di Roma "La Sapienza"	Chiara	Petrioli	link
Università degli Studi di Salerno	Giuseppe	Persiano	link
Università degli Studi di Trento	Fabio	Massacci	link

http://www.consorzio-cini.it/lab-cyber-security

Accordo con DIS



cini Cyber Security National Lab

Presidenza del Consiglio dei Ministri
Sistema di informazione per la sicurezza della Repubblica

RELAZIONE

SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA

2014

le i referenti di quei CERT acquisiscono la documentazione di sicurezza.

Tra le altre iniziative assunte dal DIS per il tramite del TTC – la maggior parte delle quali finalizzate a supportare, con prospettive diverse, la **PROMOZIONE E DIFFUSIONE DELLA CULTURA DELLA SICUREZZA CIBERNETICA** – vanno richiamate quelle con il mondo accademico e con i centri di ricerca, anche attraverso la messa a punto di progetti tesi a valorizzare, nel corso del semestre di presidenza italiana del Consiglio dell'Unione Europea, l'attenzione del nostro Paese verso la *cyber security*.

I contatti con il mondo accademico hanno conosciuto un ulteriore consolidamento con la firma, nel mese di ottobre, di un **ACCORDO DI COLLABORAZIONE** tra il DIS ed il Consorzio Interuniversitario Nazionale per l'Informatica (CINI), volto alla creazione di un rapporto di cooperazione nel settore della sicurezza cibernetica, finalizzato allo svolgimento di attività di ricerca e sviluppo ed alla realizzazione di iniziative formative.

A valle del citato accordo, il DIS ha supportato attivamente la creazione, nell'ambito del citato Consorzio, del **LABORATORIO NAZIONALE DI *CYBER SECURITY***.

Tale struttura, che federa oltre 250 tra professori e ricercatori provenienti da 32 Università italiane, ha, quale duplice obiettivo, quello di mettere a sistema le capacità di ricerca nazionali di settore attraverso un'azione di coordinamento delle eccellenze esistenti e di dare vita ad un flusso informativo tra i membri del Laboratorio e tra questi ed il mondo esterno. Ciò, a fronte della crescente consapevolezza che l'economia reale del Paese, sempre più legata all'uso del *cyber space*, è destinata a prosperare nell'ambito di un dominio cibernetico resiliente e sicuro. Il Laboratorio, quale motore di innovazione, mira in particolare a supportare il sistema Paese di fronte alla minaccia cibernetica, attraverso:

- il miglioramento della continuità di servizio dei sistemi critici;
- l'accrescimento della consapevolezza della minaccia presso la società;
- il potenziamento delle misure di protezione da attacchi cibernetici nella PA e nelle imprese;
- il supporto ai processi di definizione di *standard* e *framework* metodologici a livello nazionale.