ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Cybersecurity e le strategie nazionali

ing. Giuseppe G. Zorzino

Roma 21/05/2013

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Presentazione relatore

Giuseppe Giovanni Zorzino

Esperienze professionali

Sono consulente e docente di sicurezza delle informazioni. Attualmente mi occupo di sistemi di gestione della sicurezza, governance e sicurezza delle informazioni nelle organizzazioni, rapporti tra tecnologia e diritto (privacy, governance e compliance).

Sono responsabile del track di Cybersecurity nel Master di II°liv. "Sistemi avanzati di Comunicazione e Navigazione Satellitare“ dell'Univ. TorVergata.

Ho 32 anni di esperienza nell'IT di cui oltre 10 nella IT security nonché una consolidata esperienza pratica nell'analisi e sviluppo di basi di dati complesse e nell'amministrazione dei sistemi e applicazioni.

Ufficiale del Corpo del Genio dell'A.M., provengo dall'Accademia di Pozzuoli e sono membro del CTS di CESMA. Sono inoltre membro di ISACA, ISC2 Italian Chapter e C.T. presso il Trib. Civile di Roma.

Ho effettuato una vasta attività di divulgazione e formazione c/o enti pubblici e PMI. Ho conseguito e mantengo attive molte certificazioni tra cui ISO 27001 Lead Auditor, CISA, CGEIT, CRISC, Security+, MCSASec 2003. Certificatore etico, IBM_Cert_Specialist, …

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Cosa è successo?

Twitter Hacked; 250,000 User Accounts Potentially Compromised

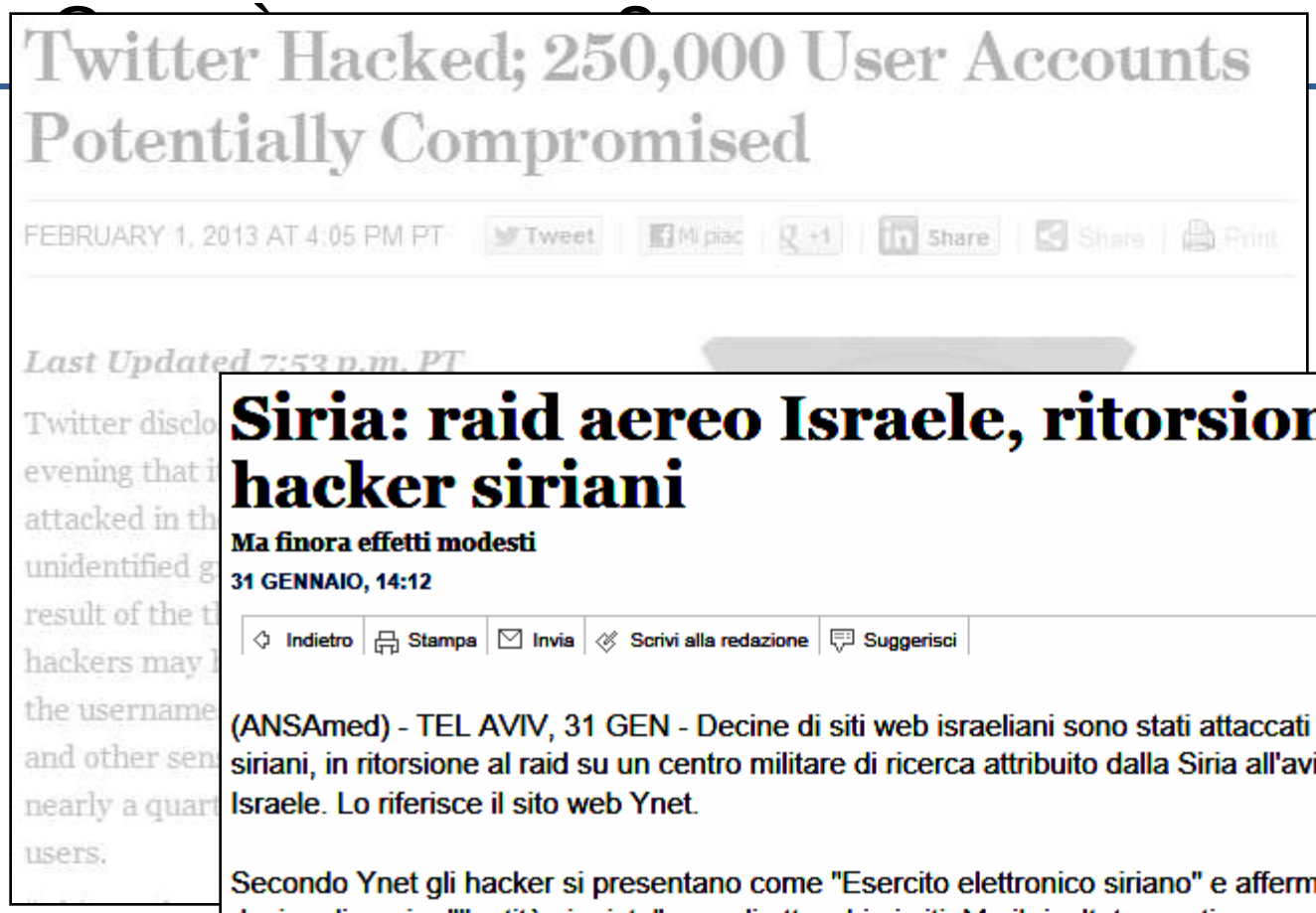
FEBRUARY 1, 2013 AT 4:05 PM PT

Tweet | Mi piac | +1 | Share | Share | Print

Last Updated 7:53 p.m. PT

Twitter disclosed on Friday evening that its systems had been attacked in the past week by an unidentified group of hackers. As a result of the the attack, the hackers may have had access to the usernames, email addresses and other sensitive information of nearly a quarter of a million twitter users.

http://allthingsd.com/20130201/twitter-hacked-250000-user-accounts-compromised/



Twitter Hacked; 250,000 User Accounts Potentially Compromised

FEBRUARY 1, 2013 AT 4:05 PM PT

Tweet | Mi piac | +1 | Share | Share | Print

Last Updated 7:53 p.m. PT

Twitter disclo
evening that i
attacked in th
unidentified g
result of the t
hackers may
the username
and other sen
nearly a quart
users.

Siria: raid aereo Israele, ritorsione da hacker siriani

Ma finora effetti modesti

31 GENNAIO, 14:12

Indietro | Stampa | Invia | Scrivi alla redazione | Suggerisci

(ANSAmed) - TEL AVIV, 31 GEN - Decine di siti web israeliani sono stati attaccati oggi da hacker siriani, in ritorsione al raid su un centro militare di ricerca attribuito dalla Siria all'aviazione di Israele. Lo riferisce il sito web Ynet.

Secondo Ynet gli hacker si presentano come "Esercito elettronico siriano" e affermano di aver deciso di punire "l'entità sionista" con gli attacchi ai siti. Ma il risultato, sostiene ancora Ynet, è modesto: i siti bersagliati "non sono importanti" e per lo più funzionano ancora.(ANSAmed).

http://ansamed.ansa.it/ansamed/it/notizie/stati/siria/2013/01/31/Siria-raid-aereo-Israele-ritorsione-hacker-siriani_8168160.html /

Twitter Hacked; 250,000 User Accounts

Siria: raid aereo Israele, ritorsione da hacker siriani

China admits cyber warfare unit in People's Liberation Army

Posted date: **January 29, 2013**

In: **Current Affairs**

The Chinese government for the first time admitted that it has highly skilled group of hackers in its army; supported, equipped and trained by the government officials.

Channel4 reports that an intelligence source inside the army shared the secret information which confirms the presence of hackers in Chinese army that are will be used at the time of cyber warfare.

The group of elite hackers in the China's People's Liberation Army is known as "cyber blue team" that will be working as a defensive wall against any kind of cyber attack against the country.

http://hackread.com/china-admits-cyber-warfare-unit-in-peoples-liberation-army/ /

Twitter Hacked; 250,000 User Accounts

Siria: raid aereo Israele, ritorsione da

China admits cyber warfare unit in People's Liberation Army

Posted date: January 29, 2013

Cyber attacchi al New York Times, sospetti su hacker cinesi

Violazioni dopo pubblicazione dossier su parenti del primo ministro cinese Wen Jiabao

Washington, 31 gen. (TMNews) - Un gruppo di hacker, che le autorità americane sospettano essere legati al governo cinese, ha ripetutamente attaccato il New York Times negli ultimi quattro mesi, violandone il sistema informatico e rubando numerose password. Questi attacchi, ha riferito lo stesso quotidiano, hanno avuto inizio nel periodo immediatamente successivo al 25 ottobre, giorno in cui il giornale ha pubblicato un articolo sulle indagini riguardanti il primo ministro Wen Jiabao e la fortuna fatta da alcuni suoi parenti.

http://www.tmnews.it/web/sezioni/top10/20130131_081256.shtml

Twitter Hacked; 250,000 User Accounts

US Government Warns of Hack Threat to Network Gear

Print Email

Reuters

TEXT SIZE

January 29, 2013

The U.S. Department of Homeland Security urged computer users on Tuesday to disable a common networking technology feature, after researchers warned that hackers could exploit flaws to gain access to tens of millions of vulnerable devices.

The U.S. government's Computer Emergency Readiness Team, on its website, advised consumers and businesses to disable a feature known as Universal Plug and Play or UPnP, and some other related features that make devices from computers to printers accessible over the open Internet.

http://www.voanews.com/content/network-vulnerability-computer-hack-reuters/1593376.html

Twitter Hacked; 250,000 User Accounts

Siria: raid aereo Israele, ritorsione da

China admits cyber warfare unit in People's Liberation Army

Cyber warfare between Koreas, a warning for any cyber power

by paganinip on January 18th, 2013

Earlier this month is has been spread the news that South Korea is investing to improve the cyber capabilities of the country recruiting and training hackers to involve in the cyber defense due the increasing number of attacks suffered.

http://securityaffairs.co/wordpress/11834/intelligence/cyber-warfare-koreas-warning-cyber-power.html

Twitter Hacked; 250,000 User Accounts

Red October, RBN and too many questions still unresolved

by paganinip on January 17th, 2013

The recently discovered cyber espionage campaign "Red October" has shocked world wide security community, the principal questions raised are:

Who is behind the attacks?

How is possible that for so long time the campaign went undetected?

✖ Which is the role of AV company in these operations?

To try to understand who is behind the attacks it is necessary to evaluate the way the hackers have operated, they used old Java exploits to infect system from various sectors, in particular government agencies and diplomatic offices.

http://securityaffairs.co/wordpress/11779/cyber-crime/red-october-rbn-and-too-many-questions-still-unresolved.html

Twitter Hacked; 250,000 User Accounts

1 feb 2013

Siria: raid aereo Israele, ritorsione da

31 gen 2013

29 gen 2013

China admits cyber warfare unit in People's Liberation Army

31 gen 2013

Cyber attacchi al New York Times, sospetti

29 gen 2013

US Governi

18 gen 2013

Cyber w
cyber po

by paganinip on

17 gen 2013

Red October, RBN and too many questions still unresolved

by pagarin p or January 17th, 2013

The recently discovered cyber espionage campaign "Red October" has shocked world wide security community, the principal questions raised are:

Who is behind the attacks?

How is possible that for so long time the campaign went undetected?

- Which is the role of AV company in these operations?

To try to understand who is behind the attacks it is necessary to evaluate the way the hackers have operated, they used old Java exploits to infect system from various sectors, in particular government agencies and diplomatic offices.

Cosa è successo?

China admits cyber warfare unit in PLA

Emblem of the People's Liberation Army

Posted date: **January 29, 2013**

In: **Current Affairs**

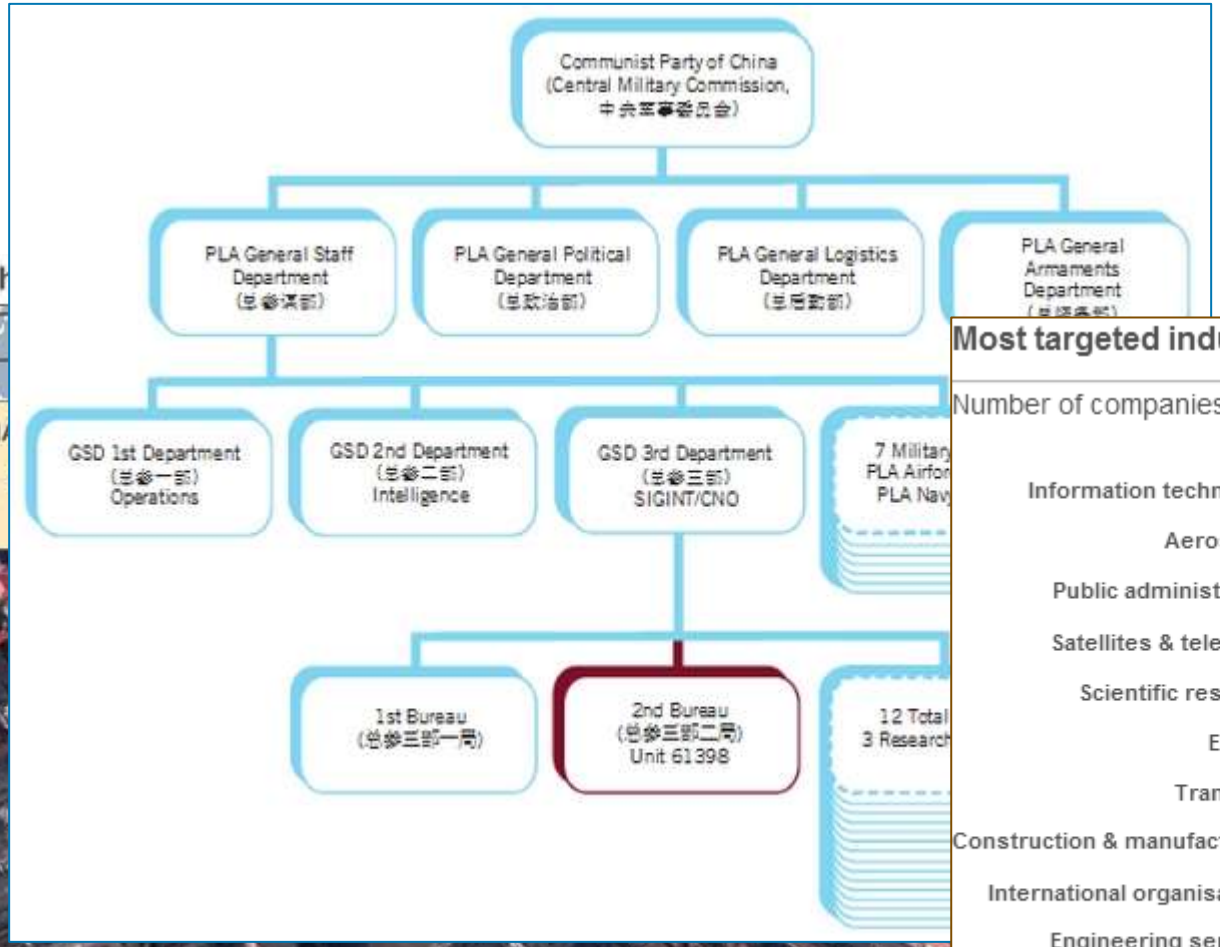
The Chinese government for the first time admitted that it has highly skilled group of hackers in its army; supported, equipped and trained by the government officials.

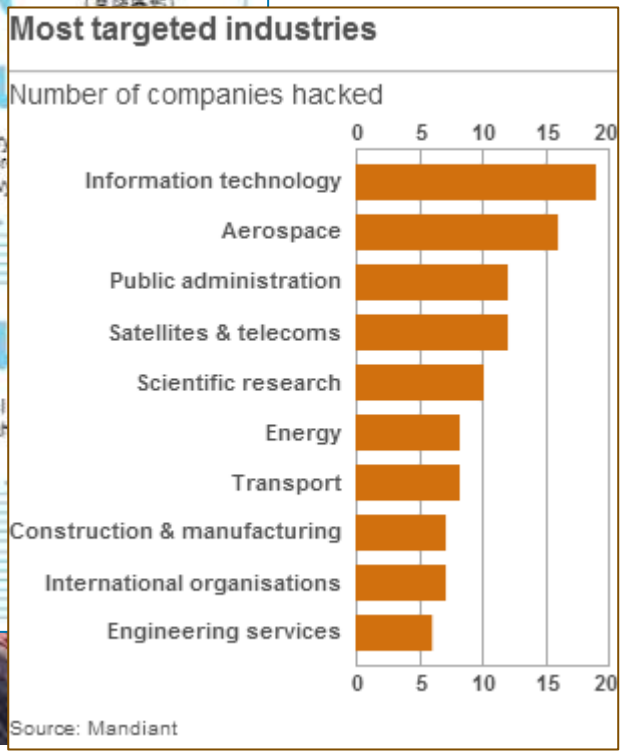
Channel4 reports that an intelligence source inside the army shared the secret information which confirms the presence of hackers in Chinese army that are will be used at the time of cyber warfare.

The group of elite hackers in the China's People's Liberation Army is known as "**cyber blue team**" that will be working as a defensive wall against any kind of cyber attack against the country.

Cosa è successo?

China military Unit 61398 **'behind prolific hacking'**





Cosa è successo?

"China defense ministry refutes cyber attack allegations"

China.org.cn

"China's laws ban any activities disrupting cyber security and the Chinese government always cracks down on cyber crimes", Geng Yansheng, spokesman with the Ministry of National Defense, said at a briefing.

The spokesman further said China actually is a major victim of cyber attacks.

http://www.china.org.cn/china/2013-02/20/content_28008680.htm

Chinese background

中華人民共和國 (People's Republic of China's)

"To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds."

毛泽东 Mao Tse-Tung

"China should enhance integrated combat capability based on extensive IT application … We should attach great importance to maritime, space and cyberspace security."

胡锦涛 Hu JinTao

http://news.xinhuanet.com/english/special/18cpcnc/2012-11/08/c_131959900.htm

Cosa è successo?

Eight Principles of Chinese Unrestricted Warfare

- Omnidirectionality
- Synchrony
- Limited objectives
- Unlimited measures
- Asymmetry
- Minimal consumption
- Multidimensional coordination
- Adjustment and control of the entire process

"Unrestricted Warfare", Senior Colonels Qiao Liang and Wang XiangSui , 1999

Chinese Cyber-attack Threat Vectors

4 attack vettors

- Communist Party of China (CPC)
- People's Liberation Army (PLA)
- State Owned Enterprises (SOE)
- Civilian Hackers (CH - Hacktivists)

… motivation of the People's Republic of Chinese to conduct cyber-warfare is comprised of fear, self-preservation and hegemony

"21st Century Chinese Cyber Warfare", Bill Hagestad II, ltCol marine (ret)

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

"cyberthreats … the 21st century nuclear weapons equivalent"

24 Jan 2013

Hilary Clinton e John Kerry:
cybersecurity - a word that is rarely mentioned in these [House] hearings

http://www.govinfosecurity.com/blogs/kerry-sees-cyber-as-21st-century-nuke-p-1411

- cyberdiplomacy
- cybernegotiations
- cyber-intrusions

Minacce e contromisure

Published January 12, 2013 Associated Press

WASHINGTON – The U.S. Department of Homeland Security is advising people to temporarily disable the **Java** software on their computers to avoid potential hacking attacks.

…

Oracle, which is based in Redwood Shores, Calif., had no immediate comment late Friday.

http://www.foxnews.com/tech/2013/01/12/us-government-advises-computer-users-to-disable-java-software/

Minacce e contromisure

Published January 12, 2013 Associated Press

WASHING ecurity is
advising p are on
their comp

http://www.foxnews.com/tech/2013/01/12/us-government-advises-computer-users-to-disable-java-software/

Minacce e contromisure

FOX NEWS .com
Fair & Balanced

Search

Listen to Fox News Radio Live ›

ON AIR NOW ›
FOX & friends FIRST 5a et
FOX & Friends First
WATCH LIVE

Home | Video | Politics | U.S. | Opinion | Entertainment | Tech | Science | Health | Travel

Technology Home | Gadgets | Social | Computers | Military Tech | Mobile | Internet | Slideshows

US government advises computer users to disable Java software

Published January 12, 2013 / Associated Press

Minacce e contromisure

Published January 12, 2013 Associated Press

WASHINGTON – The U.S. Department of Homeland Security is advising people to temporarily disable the **Java** software on their computers to avoid potential hacking attacks.

Tue Jan 29, 2013 3:16pm EST

(Reuters) - The U.S. Department of Homeland Security urged computer users on Tuesday to disable a feature known as Universal Plug and Play or **UPnP**, after researchers warned that hackers could exploit flaws to gain access to tens of millions of vulnerable devices.

http://www.reuters.com/article/2013/01/29/us-cybersecurity-bugs-idUSBRE90S06320130129

Minacce e contromisure

Publishe

WASHIN urity is
advising e on
their co

Tue Jan

(Reuter rged
comput as
Univers ed that
hackers ons of
vulnera

U.S. government warns of hack threat to network gear

Consiglia 605 persone lo consigliano.

Tweet 342

Share 62

Share this

+1 37

Email

Print

By Jim Finkle
Tue Jan 29, 2013 3:16pm EST

(Reuters) - The Department of Homeland Security urged computer users on Tuesday to disable a common networking technology feature, after researchers warned that hackers could exploit flaws to gain access to tens of millions of vulnerable devices.

Related News

REFILE-DEALTALK-Cisco eager to regain ground as network security leader
Mon, Jan 14 2013

U.S. warns on Java software as security concerns escalate
Fri, Jan 11 2013

Exclusive: U.S. nuclear lab removes Chinese tech over security fears
Mon, Jan 7 2013

E90S06320130129

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Glossario

→ INFORMATION SECURITY

→ COMPUTER SECURITY

→ INFORMATION ASSURANCE

USATI SPESSO COME SINONIMI

Facciamo luce sui termini

- Cyber space
- Cyber security
- Cyber attack
- Cyber warfare
- Cyber deterrence
- Cyber war
- Cyber warrior
- Cyber weapon
- Cyber threat
- Cyber defence
- Cyber intelligence
- Cyber incident
- Cyber crisis
- Cyber terrorism
- Cyber criminal
- Cyber …

Cyberspace

"L'insieme delle infrastrutture informatiche interconnesse, comprensivo di *hardware, software, dati ed utenti nonché* delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete."

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyberspace

- Spettro elettromagnetico
- Richiede tecnologia
- È persistente basato sulla fantasia e tortuosità
- Basso costo d'ingresso
  - COTS S/W
  - budget ridotto
  - accesso ad Internet
  - motivazione

Cyberspace

"In cyberspace, the low cost of entry and easy access creates an asymmetric environment in which public and private sector organizations incur a disproportionate cost to defend compared to the consequence of attack."

https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf

What exactly is cyberspace?

- **Ubiquitous** – l'impatto strategico è significativo
- **Complementary** – gli attacchi Cyber russi a Estonia e Georgia – effetto combinato
- **Stealth method of attacking a foe** – senza alcuna attribuzione di responsabilità – impianto di Trojans da attivare in futuro

Quale è il valore?

- Un vantaggio può essere quello di controllare/ manipolare ambienti strategici

Cyber-security

"Condizione in cui il *cyber-space risulti protetto rispetto ad* eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittime ovvero nel blocco dei sistemi informativi, grazie ad idonee misure di sicurezza fisica, logica e procedurale."

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyber security è

"a shared responsibility, and each of us has a role to play."

Janet Napolitano, Blueprint for a Secure Cyber Future, DHS

"the ability to protect or defend the use of cyberspace from cyber attacks"

http://itlaw.wikia.com/wiki/Cybersecurity

4.20 "… preservation of confidentiality, integrity and availability of information in the Cyberspace. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved."

ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity

Cyber security

Garantire la sicurezza informatica richiede sforzi coordinati in tutto il sistema informativo

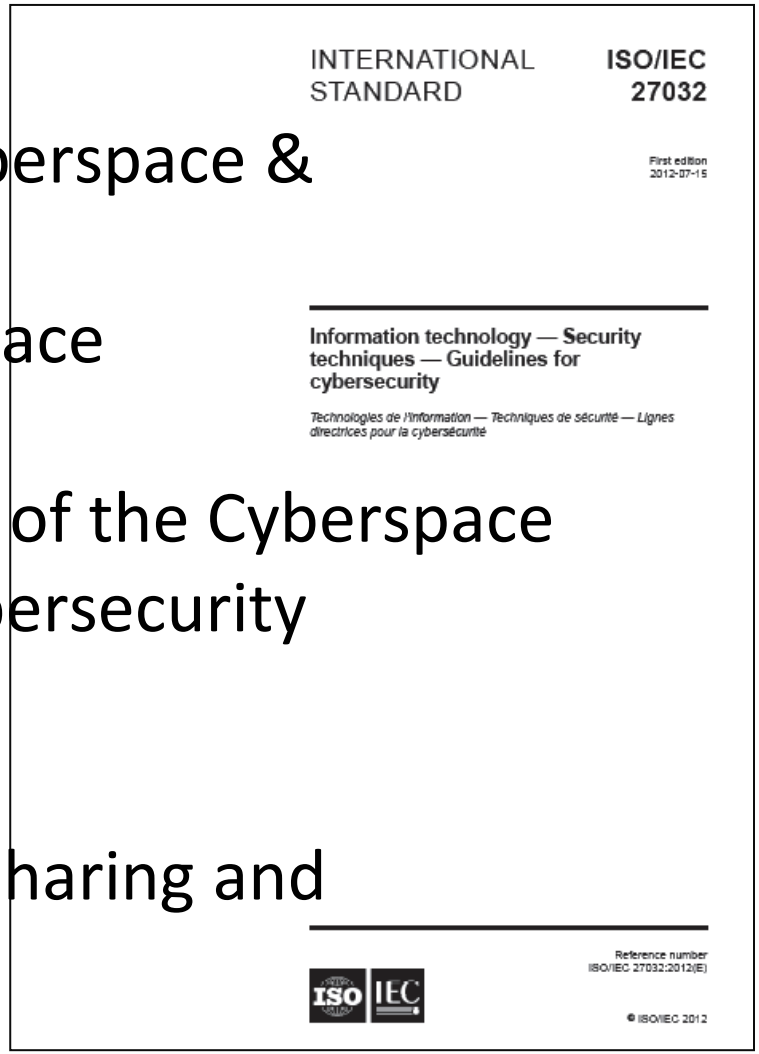
Elementi della cybersecurity sono:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- End-user education

ISO/IEC 27032:2012

Guidelines for cybersecurity

6 Overview (nature of the Cyberspace & Cybersecurity)
7 Stakeholders in the Cyberspace
8 Assets in the Cyberspace
9 Threats against the security of the Cyberspace
10 Roles of stakeholders in Cybersecurity
11 Guidelines for stakeholders
12 Cybersecurity controls
13 Framework of information sharing and coordination


INTERNATIONAL STANDARD

ISO/IEC 27032

First edition
2012-07-15

Information technology — Security techniques — Guidelines for cybersecurity

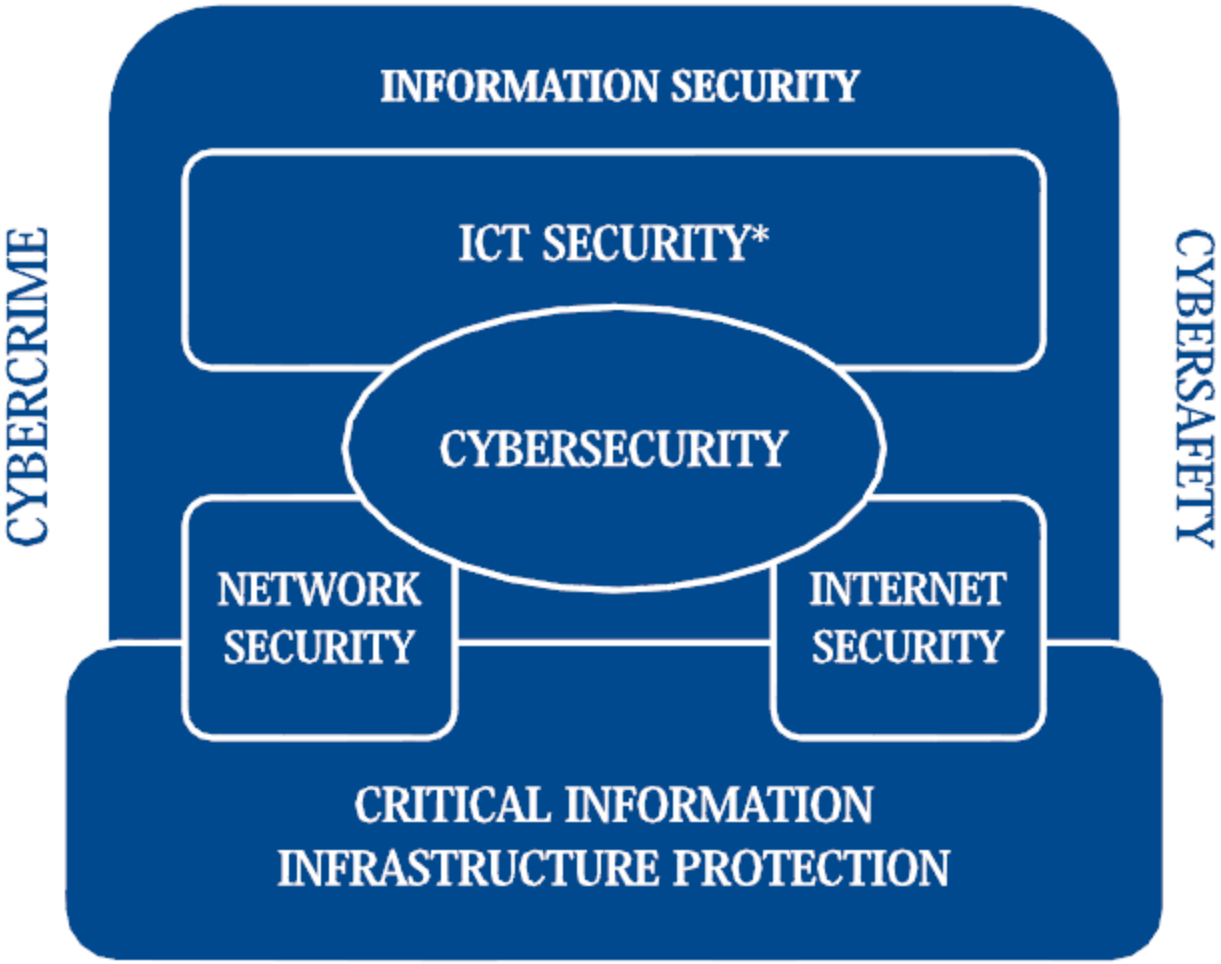
Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

Reference number
ISO/IEC 27032:2012(E)

© ISO/IEC 2012

http://www.iso.org/iso/catalogue_detail?csnumber=44375

ISO/IEC 27032:2012



ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity'

Glossario

- **Cybercrime** has been defined as the ‘criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime’
- **Cybersafety** has been defined as the ‘condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable’

ISO/IEC 27032:2012, ‘Information technology – Security techniques – Guidelines for cybersecurity’

Cosa è il Cyber Warfare (CW)?

- uso calcolato di attacchi informatici offensivi e difensivi di rete - computer network attacks (CAN),
- sfruttamento di reti di computer - computer network exploits (CNE),
- approfittare delle vulnerabilità della rete informatica - computer network vulnerabilities (CNV) – a livello geopolitico,
- combattere nel cyberspazio.

Cyber defence

L’insieme della dottrina, dell’organizzazione e delle attività volte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti nel e tramite il *cyber-space ovvero* in danno di uno o più dei suoi elementi costitutivi.

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyber deterrence

- basata su capacità di risposta cross domain
- la rappresaglia ha molte forme: economiche, diplomatiche, …
- defence-by-deterrence vs comprehensive hardening
- probabilmente è efficace verso gli attacchi più dannosi, equivalenti ad attacchi militari tradizionali

NO MAD DOCTRINE

MUTUALLY ASSURED DESTRUCTION

Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012

Cyberwar

L'insieme delle operazioni condotte nel e tramite il *cyberspace* al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del *cyber-space). …* Può rappresentare l'unica forma di confronto ovvero costituire uno degli aspetti di un conflitto che coinvolga altri domini (terra, mare, cielo e spazio); in entrambi i casi, i suoi effetti possono essere limitati al *cyber-space* ovvero tradursi in *danni concreti*, inclusa la perdita di vite umane.

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyber intelligence

Ricerca ed elaborazione di notizie di interesse nel e sul *cyber-space* al fine di *prevenire, rilevare, contenere* e *contrastare* le minacce alla sicurezza nazionale, con riguardo ad esempio alle infrastrutture critiche.

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyber threat

Espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il *cyber-space* ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici:

- azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare integrità e riservatezza di dati/informazioni.

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyber threat

A seconda degli attori e delle finalità, si parla di:

- criminalità cibernetica (*cyber-crime): complesso delle attività* con finalità criminali (quali, per esempio, la truffa o frode telematica, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali);
- spionaggio cibernetico (*cyber-espionage): acquisizione indebita* di dati/informazioni sensibili, proprietarie o classificate;
- terrorismo cibernetico (*cyber-terrorism): insieme delle* azioni ideologicamente motivate, volte a condizionare uno stato o un'organizzazione internazionale.

http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario/glossario-intelligence.pdf

Cyber threat

- **cybercriminal:** A hacker illegally stealing data from another computer for personal financial gain.
- **cyberwar:** Politically motivated hacking to conduct sabotage and/or espionage against a nation state.
- **cyberterrorism:** The use of Internet-based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks.

"Definitive Guide to Next-Generation Threat Protection", FireEye

Cyber Incident

A Significant Cyber Incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the **confidentiality**, **integrity**, or **availability** of electronic information, information systems, services, or networks; and/or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

The Cybersecurity Strategy for the Homeland Security Enterprise, nov 2011

Altri termini

- **cyber counterintelligence** — Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.
- **cyberspace operations** — The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

DoD Dictionary of Military and Associated Terms - http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Altri termini

- **Counter cyber*:*** A mission that integrates offensive and defensive operations to attain and maintain a desired degree of cyber superiority.
- **Cyber interdiction*:*** An action to divert, disrupt, delay, or destroy the enemy's military cyber surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives.
- **Close cyber support*:*** Cyber action against hostile targets' information systems that are in close proximity to friendly forces and that require detailed integration of each cyber mission with the fire and movement of those forces.

Proceedings of a Workshop on Deterring Cyberattacks, National Academy of Sciences, 2010

Altri termini

- **Cyber reconnaissance in force*:*** An offensive cyber operation conducted by military (not intelligence) forces designed to discover and/or test the enemy's strength or to obtain other information.
- **Suppression of enemy cyber defenses*:*** Activity that neutralizes, destroys, or temporarily degrades enemy cyber defenses by destructive and/or disruptive means.
- **Strategic cyber mission*:*** A mission directed against one or more of a selected series of enemy cyber targets with the purpose of progressive destruction and disintegration of the enemy's war making capacity and will to make war.

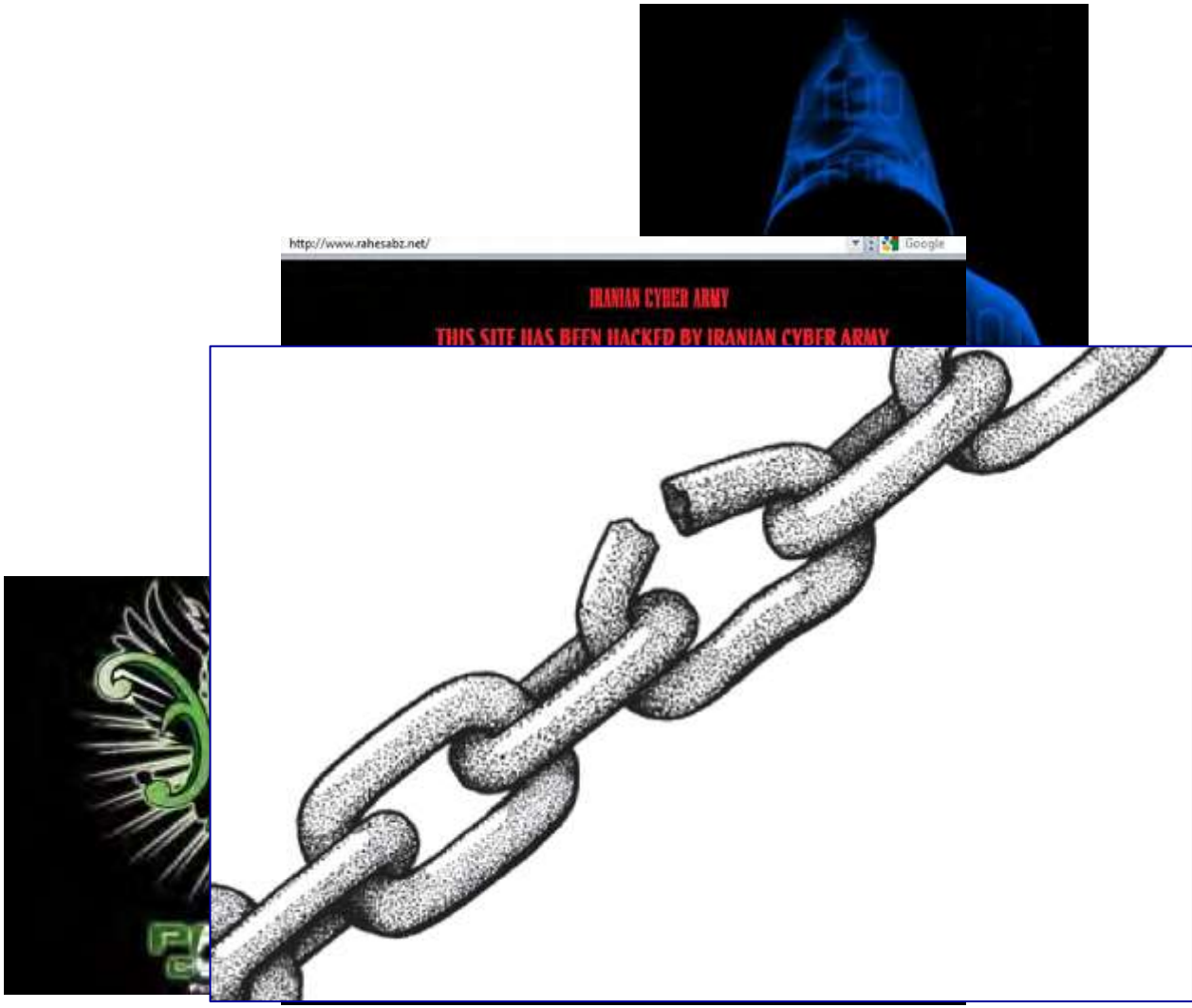
Proceedings of a Workshop on Deterring Cyberattacks, National Academy of Sciences, 2010

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Gli attori

- Entità statuali
- Gruppi criminali
- Gruppi terroristici
- Hacktivists
- Insiders



Tassonomia del Cyberthreat

Cyberthreat	Motivo	Obiettivi	Metodologie	Capacità
Stati (in tempo di pace)	Economico, politico, militare	Imprese, intelligence, Difesa, istituzioni, Infrastrutture	Dottrine informatiche specifiche militari e di intelligence, hacktivists	Uso asimmetrico del dominio informatico senza l'aspetto cinetico
Stati (in tempo di guerra)	Economico, politico, militare	Imprese, intelligence, Difesa, istituzioni, Infrastrutture	Dottrine informatiche specifiche militari e di intelligence, hacktivists	Uso asimmetrico del dominio informatico con l'aspetto cinetico
Cyber terroristi e movimenti insurrezionali	Politico	Infrastrutture, estorsioni, esposizione mediatica	Combinazione di advanced persistent threats (APT)	In continua evoluzione
Cyber criminali, Grey & Black Markets	Finanziario	Furto di proprietà intellettuali, frode, furto, truffa, sequestro di risorse di rete e computer, ciminalità cyber a noleggio	Exploits, Malware, Botnets, Worms, Trojans	Struttura di tipo cellulare
Organizzazioni criminali, RBN	Finanziario		Uso delle stesse tecniche con pianificazione distinta	Altamente professionali, pericolosi
Organizzazioni canaglia, Anonymous, LulzSec	Finanziario	Furto di informazioni e proprietà intellettuali, pressioni dirette/indirette su strutture governative	Capacità di hacking senza confronti	Organizzate e decentrate

Gli hacker individuali

- **black-hat**
  - Wannabe, spesso etichettato come “Lamer”
  - Script Kiddie
  - Cracker
  - Cyber-Warrior (mercenario)
- **grey-hat**
  - Ethical Hacker
  - QPS (Quite, Paranoid, Skilled hacker)
- **white-hat**

Relazione sulla politica dell'informazione per la sicurezza 2012

Hacktivism

È una combinazione di politica, Internet e altri elementi.

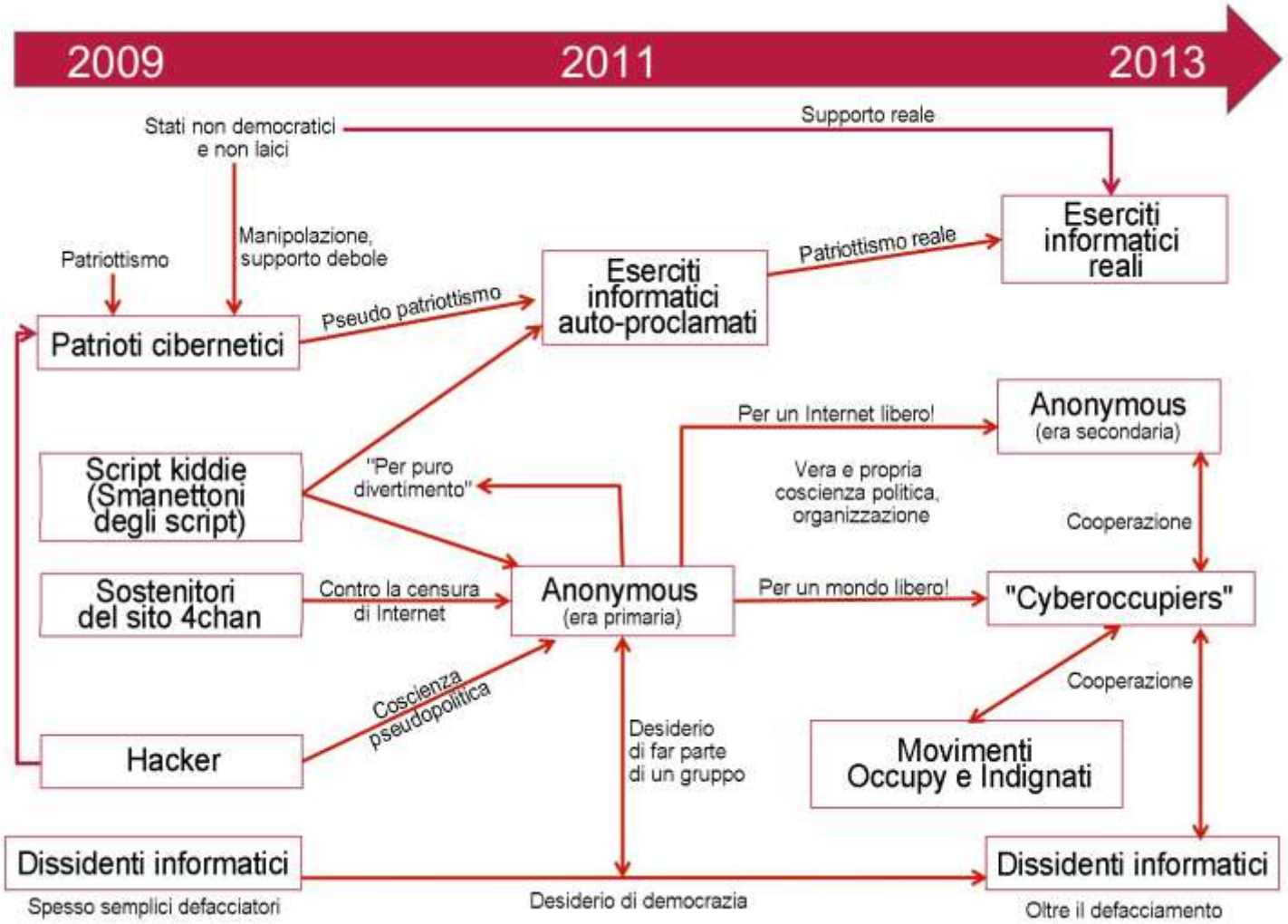
Oggi si compone di tre gruppi:

- ✓ Anonymous
- ✓ Cyberoccupiers o occupanti informatici
- ✓ Cyberwarriors o combattenti informatici

- Hacktivism 2012 - Mcafee -

Gli attori

Hacktivism



- Hacktivism 2012 - Mcafee -

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Gli obiettivi

asset

2.1 Anything that has value to the organization

NOTE There are many types of assets, including:

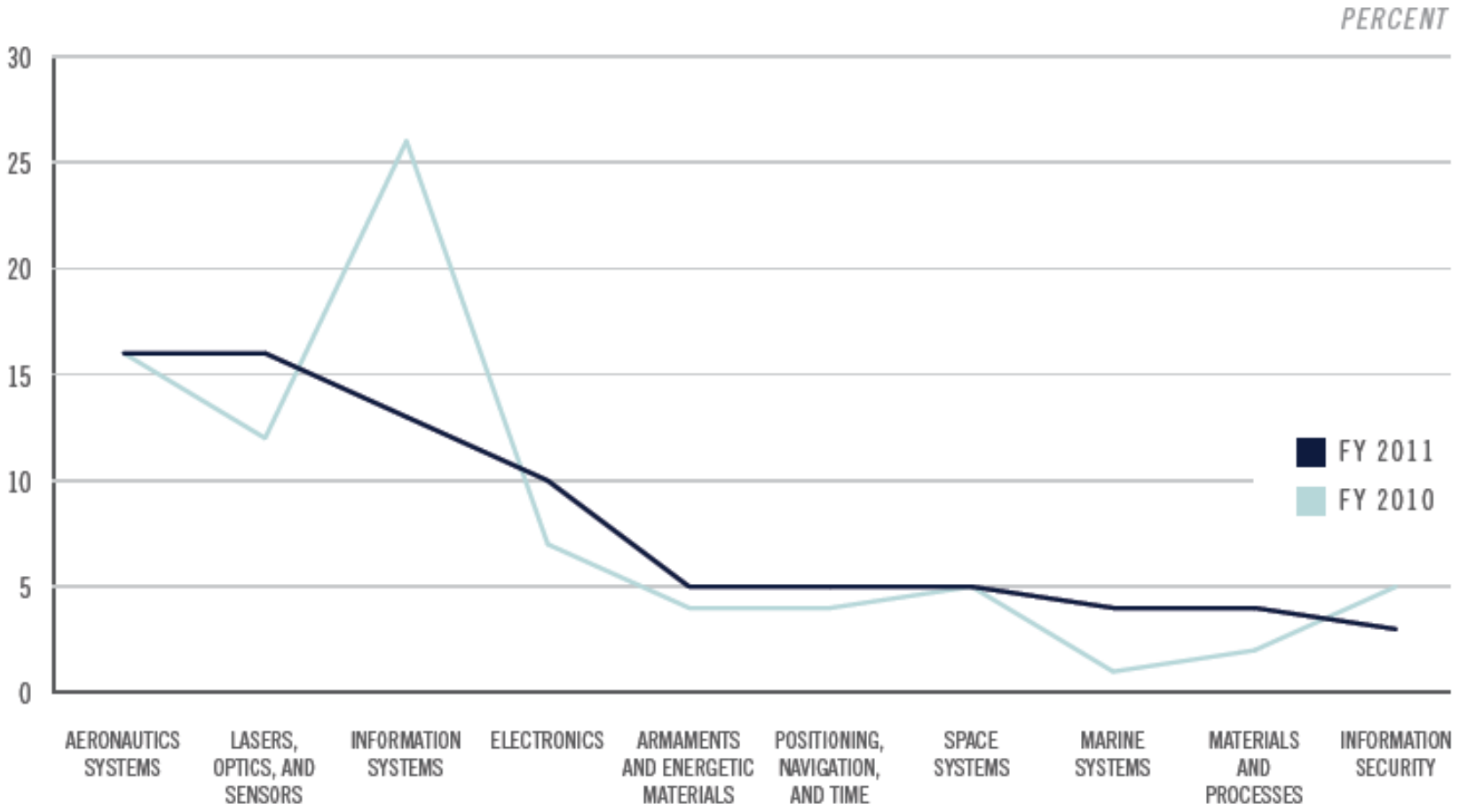
a) **information (2.18);**
b) software, such as a computer program;
c) physical, such as computer;
d) services;
e) people, and their qualifications, skills, and experience; and
f) intangibles, such as reputation and image.

[ISO/IEC 27000:2009 - Overview and vocabulary]

Minacce agli assets

- Threats to personal assets
- Threats to organisational assets
- Threats to virtual assets
- Threats to infrastructure

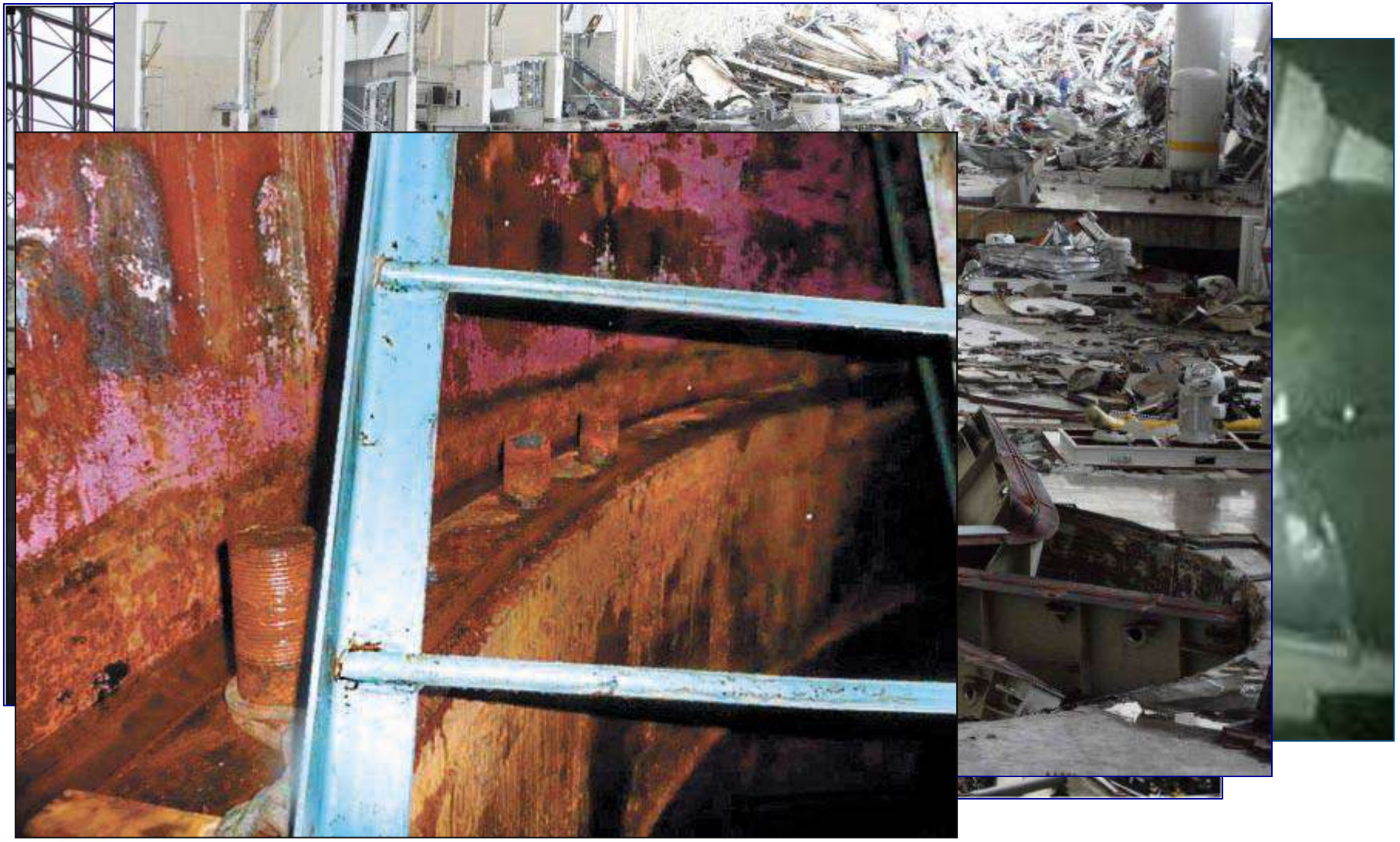
Europe and Eurasia



Defense Security Service U.S. http://www.dss.mil/documents/ci/2012-unclass-trends.pdf

Minacce alle infrastrutture

Accident at Russia's Biggest Hydroelectric Plant Sayano-Shushenskaya – August 17, 2009

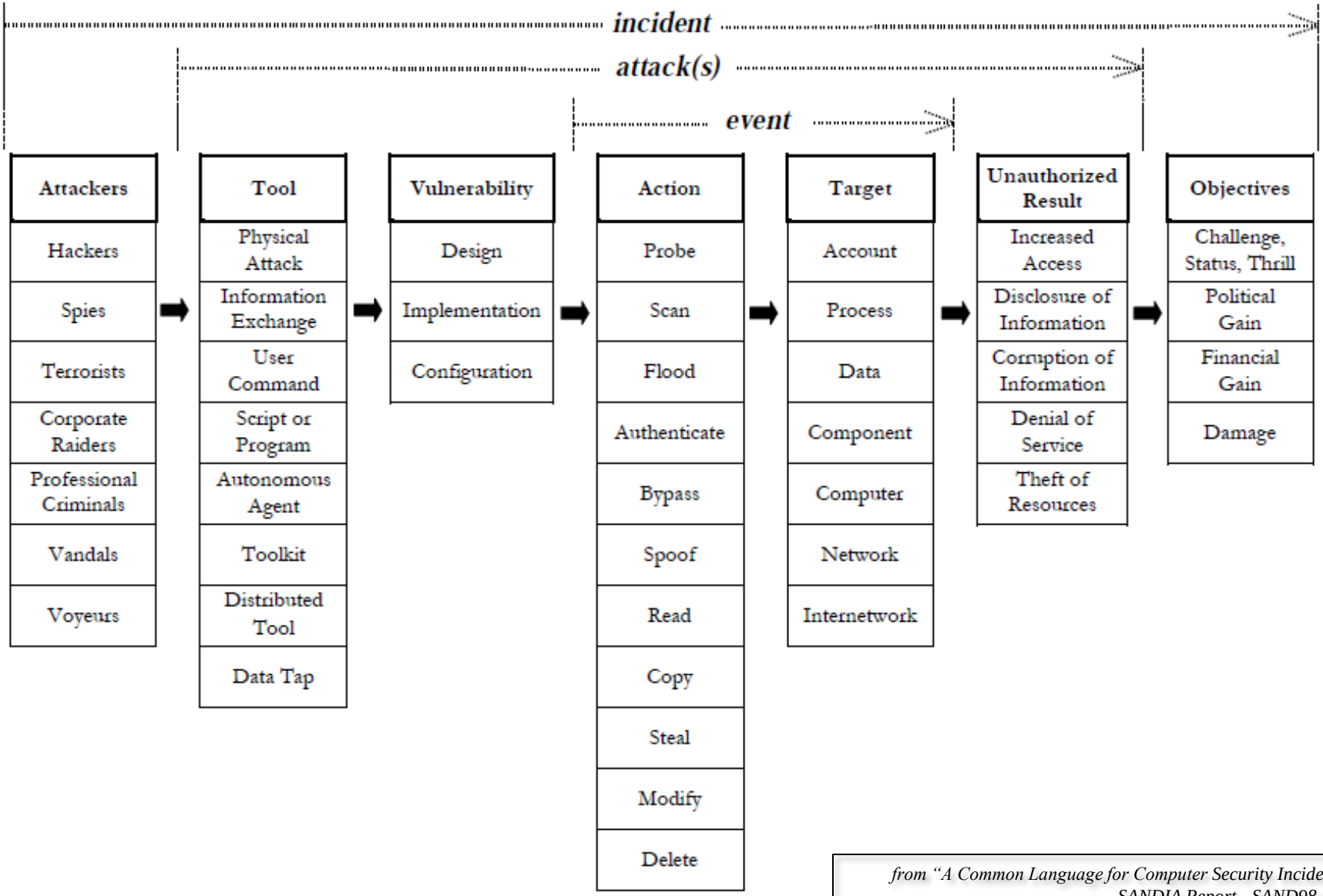


http://www.hss.doe.gov/sesa/analysis/oec/docs/LL_from_Accident_at_Russia's_Hydroelectric_Plant.pdf

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Un linguaggio comune



from "A Common Language for Computer Security Incidents", SANDIA Report - SAND98-8667

Tipi di Minacce

- ✓ WEB
- ✓ Mobile
- ✓ Mail
- ✓ APT e ATT
- ✓ Governative
- ✓ …

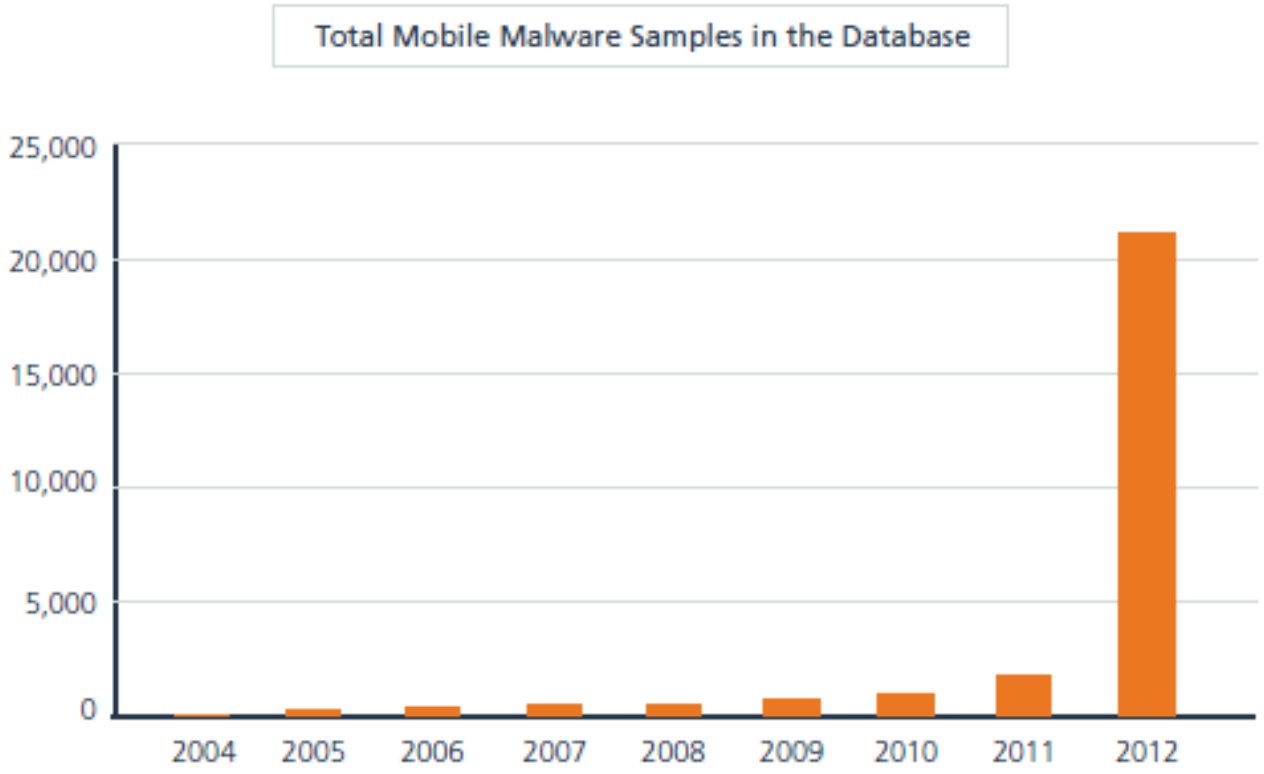
Attacchi al WEB

"The typical Web application experiences attack incidents 274 times per year, with one target experiencing as many as 2,766 attack incidents. While under attack, the average Web application attack incident lasts 7 minutes and 42 seconds with the longest attack incident reaching one hour and 19 minutes."

Imperva Web Application Attack Report, 2012

Attacchi al Mobile

- BYOD
- Android



Attacchi al Mobile

- BYOD
- Android
- Javascript e mobile Java
- malware in App Stores
- HTML 5
- Operation High Roller, SpyEye, Eurograbber
  - ZITMO Trojan

Attacchi tramite Mail

- Allegati con malware
- Phishing
  - Spear-phising – persone specifiche
  - Whaling – senior executives e altri high-profile targets
  - Baiting
- Diffuse da botnet
- Attacchi mirati: lunedì e venerdì

Advanced Persistent Threat

APT as “a sophisticated network attack in which an unauthorized person gains access to a network and stays undetected for a long period of time.”

Although this is quite true, it’s only part of the story. APTs are unlike any cyber attack seen before.

Definitive Guide to Next-Generation Threat Protection - FireEye

APT

- NON è un singolo malware o una collezione
- È costruito per un obiettivo o un target specifico
- Si struttura in una serie di attività ben coordinate e motivate da interessi politici, militari o finanziari
- Si compone di tecniche di attacco multiplo e si sviluppa in più passi per formare un singolo attacco coordinato

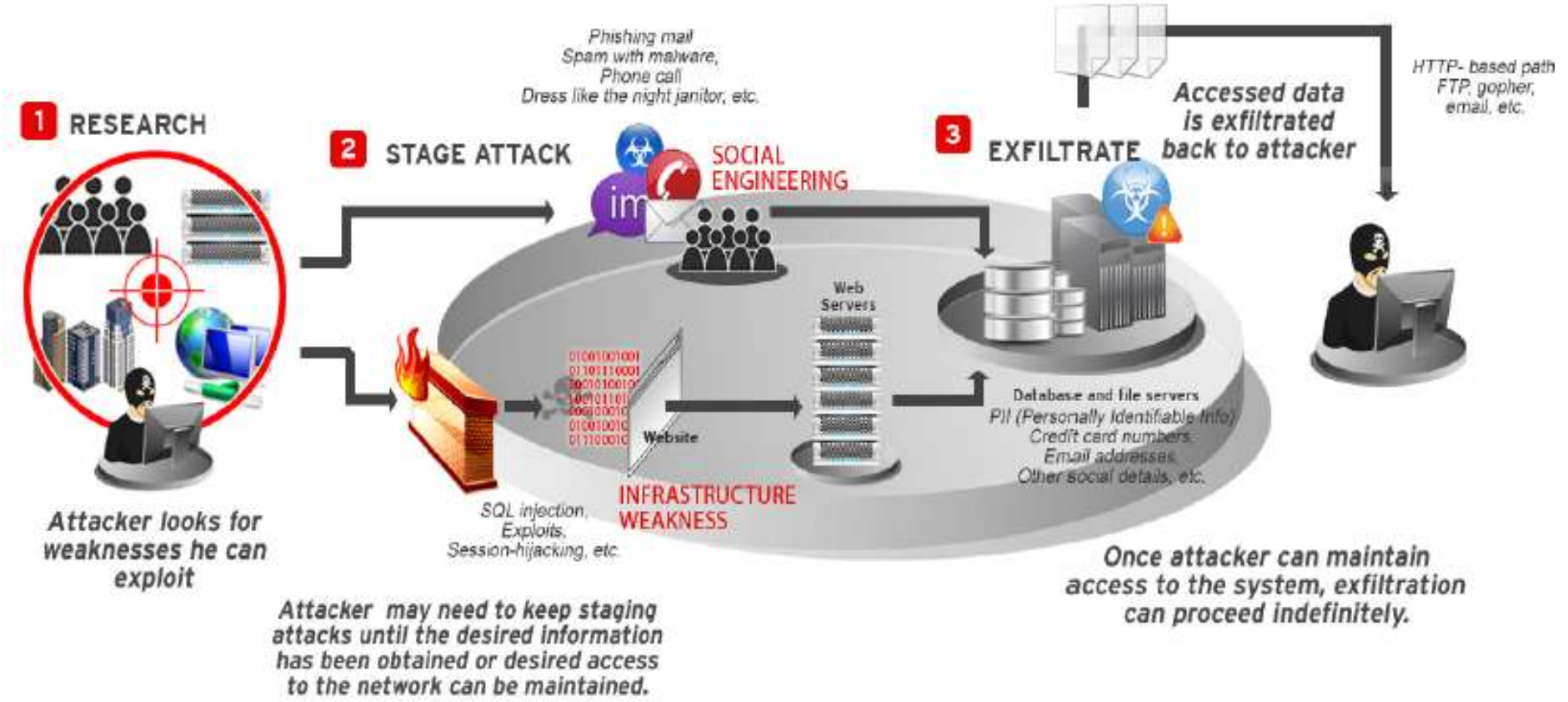
Definitive Guide to Next-Generation Threat Protection - FireEye

Attacchi APT e ATT

(Advanced Persistent Threat)
(Advanced Targeted Threat)

1. Intelligence gathering
2. Point of entry
3. Compromise
4. Command-and-control (C&C) communication
5. Lateral movement
6. Asset/Data discovery
7. Data exfiltration

Attacco APT



Fonte: Trend Micro

Malware governativo ?

- Operation Aurora
- Stuxnet
- Duqu
- Flame e la sua brutta copia Shamoon
- Bundestrojaner ('federal trojan')
- FinFisher (Gamma International)
- Mahdi
- Gauss
- Red October
- .....

1. Government
2. Diplomatic / embassies
3. Research institutions
4. Trade and commerce
5. Nuclear / energy research
6. Oil and gas companies
7. Aerospace
8. Military

Malware governativo ?

State-Sponsored Hacker Group Stealing 1TB of Data a Day

"Based on our research we estimate that up to 30,000 systems had data stolen over a period of a few years. This estimate is based on 500 servers each connected to about 20 victims at a time. Each server extracts about 2.4GB of data every day. That is a total of more than 1TB stolen, every day, ongoing.", 03/2013

http://www.team-cymru.com/Services/EIS/eis.pdf

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

La minaccia cibernetica

…

La natura complessa, impalpabile e pervasiva della *cyberthreat* rende le soluzioni al problema di non facile individuazione ed applicazione poiché gli attori, i mezzi, le tecniche di attacco ed i bersagli mutano più velocemente delle contromisure.

*www.**sicurezza**nazionale.gov.it/web.nsf/documenti/**Relazione-2012**.pdf*

Next-generation attacks

"Defending against next-generation threats requires a strategy that moves beyond signatures and behavioral heuristics. Over 95% of businesses unknowingly host compromised endpoints, despite their use of traditional and next-generation firewalls, intrusion prevention systems (IPS), antivirus and Web gateways. This situation—the new status quo—results from criminals leveraging multiple zero-day vulnerabilities, commercial-quality toolkits and social media to perpetrate next-generation attacks."

Protecting Against Advanced Malware and Targeted APT Attacks - FireEye

Cyber security vs national security

- Il termine ‘national security’ come ‘cyber security’ non ha una definizione univoca comunemente accettata
- Alcuni paesi OCSE hanno recentemente sviluppato delle ‘national security strategies’ (NSS) dedicate.
- La dottrina strategica è passata da focalizzarsi su poche minacce alla mitigazione di una miriade di rischi.
- La cyber security è un problema di sicurezza nazionale

Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012

5 aspetti della National Cybersecurity

- Military Cyber
- Counter Cyber Crime
- Intelligence and Counter-Intelligence
- Critical Infrastructure Protection and National Crisis Management
- ‘Cyber Diplomacy’ and Internet Governance

Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012

National Cyber Security Strategies

Estonia_Kuberjulgeoleku_strateegia_2008-2013_ENG	set-08
Cyber Security Strategy of the United Kingdom	giu-09
Canada's Cyber Security Strategy	ott-10
Dutch-cyber-security-strategy-2011	feb-11
Défense et sécurité des systèmes d'information - Stratégie de la France	feb-11
Cyber Security Strategy for Germany	mar-11
US International Strategy for Cyberspace	mag-11
Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019 - LITHUANIA	giu-11
NATO CCDCOE Strategic Cyber Security	giu-11
US DoD Strategy for Operating in Cyberspace	lug-11
Luxembourg_Stratégie nationale en matière de cyber sécurité	nov-11
The Cybersecurity Strategy for the Homeland Security Enterprise	nov-11
The UK Cyber Security Strategy	nov-11
US The Cybersecurity Act of 2012 final	feb-12

National Cyber Security Strategies

Security) for 2011-2019 - LITHUANIA	giu-11
NATO CCDCOE Strategic Cyber Security	giu-11
US DoD Strategy for Operating in Cyberspace	lug-11
Luxembourg_Stratégie nationale en matière de cyber sécurité	nov-11
The Cybersecurity Strategy for the Homeland Security Enterprise	nov-11
The UK Cyber Security Strategy	nov-11

Ti trovi in: **Home** : **Il Governo Informa** : **Comunicati stampa**

Nuove misure contro le minacce alla sicurezza informatica

23 Gennaio 2013

Il Presidente del Consiglio Mario Monti e i Ministri membri del Comitato interministeriale per la sicurezza della Repubblica hanno firmato il decreto per accrescere le capacità del Paese di confrontarsi con le minacce alla sicurezza informatica.

L'Italia si dota così della prima definizione di un'architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche. Il decreto pone le basi per un sistema organico, all'interno del quale, sotto la guida del Presidente del Consiglio, le varie istanze competenti possono esercitare in sinergia le loro competenze.

Nuove misure contro le minacce alla sicurezza informatica	gen-13

National Cyber Security Strategies

NATO CCDCOE Strategic Cyber Security	giu-11
US DoD Strategy for Operating in Cyberspace	lug-11
Luxembourg_Stratégie nationale en matière de cyber sécurité	nov-11
The Cybersecurity Strategy for the Homeland Security Enterprise	nov-11

Ti trovi in: **Home** : **Il Governo Informa** : **Comunicati stampa**

Nuove misure contro le minacce alla sicurezza informatica

23 Gennaio 2013

A luglio il Parlamento ha approvato la legge n. 133/2012, che pone in carico al sistema per la sicurezza nazionale e all'intelligence il ruolo di "catalizzatore" della protezione cibernetica del Paese.

Paese di confrontarsi con le minacce alla sicurezza informatica.

Il Decreto prevede inoltre la messa a punto, in raccordo con il settore privato, di un quadro strategico nazionale, che si tradurrà nella prossima adozione di un Piano nazionale per la sicurezza dello spazio cibernetico.

Nei prossimi giorni il decreto verrà pubblicato in Gazzetta Ufficiale.

Nuove misure contro le minacce alla sicurezza informatica	gen-13

DPCM 24 Gennaio 2013

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

Pubblicato il 19/03/2013

…

Ritenuto che … la definizione di un quadro strategico nazionale in materia di sicurezza cibernetica debba procedere secondo un percorso di graduale e progressiva razionalizzazione di ruoli, strumenti e procedure con l'obiettivo di accrescere la capacità del Paese di assicurare la sicurezza dello spazio cibernetico, ove necessario anche con interventi di carattere normativo

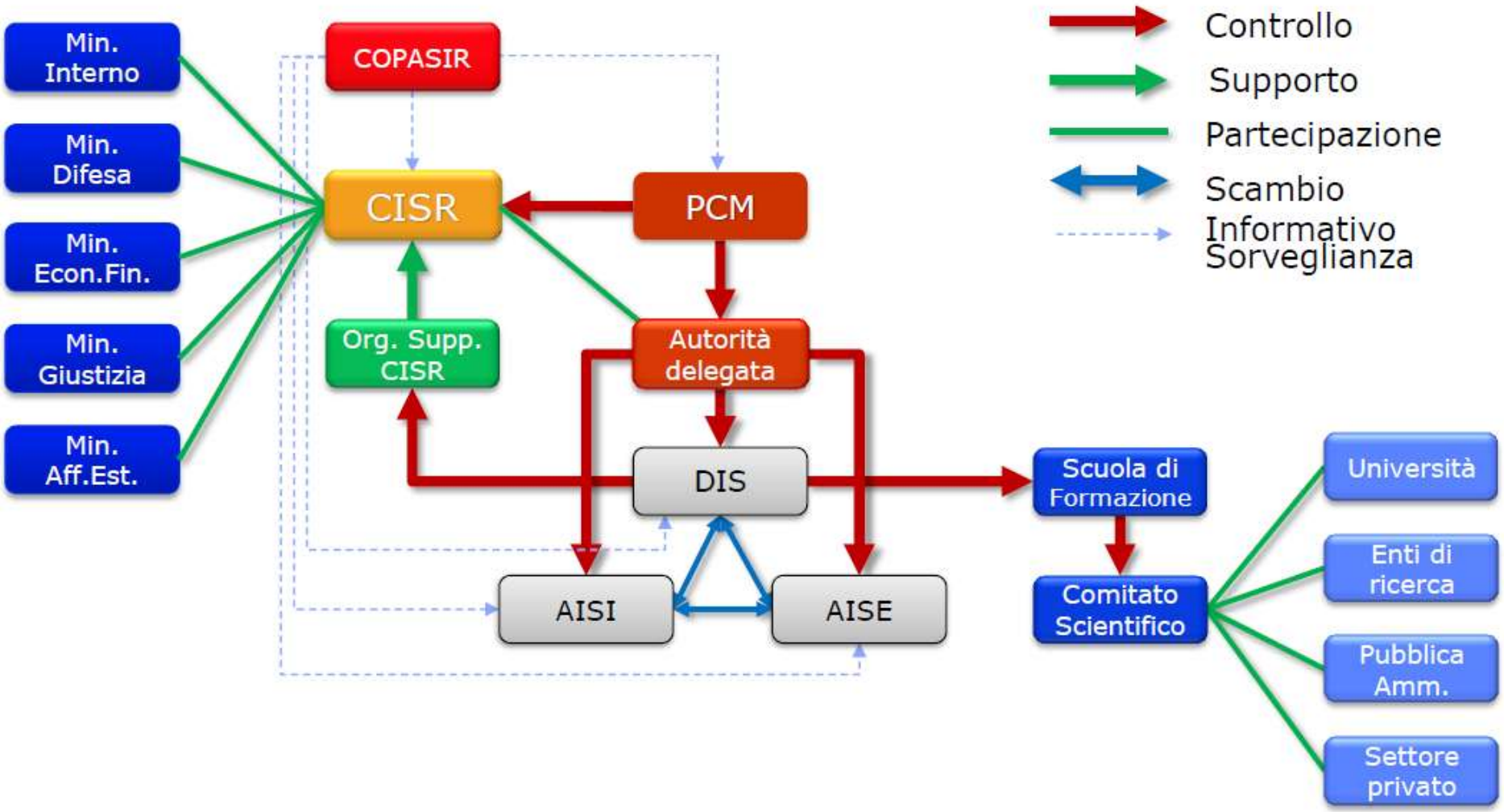
…

DPCM 24 Gennaio 2013

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

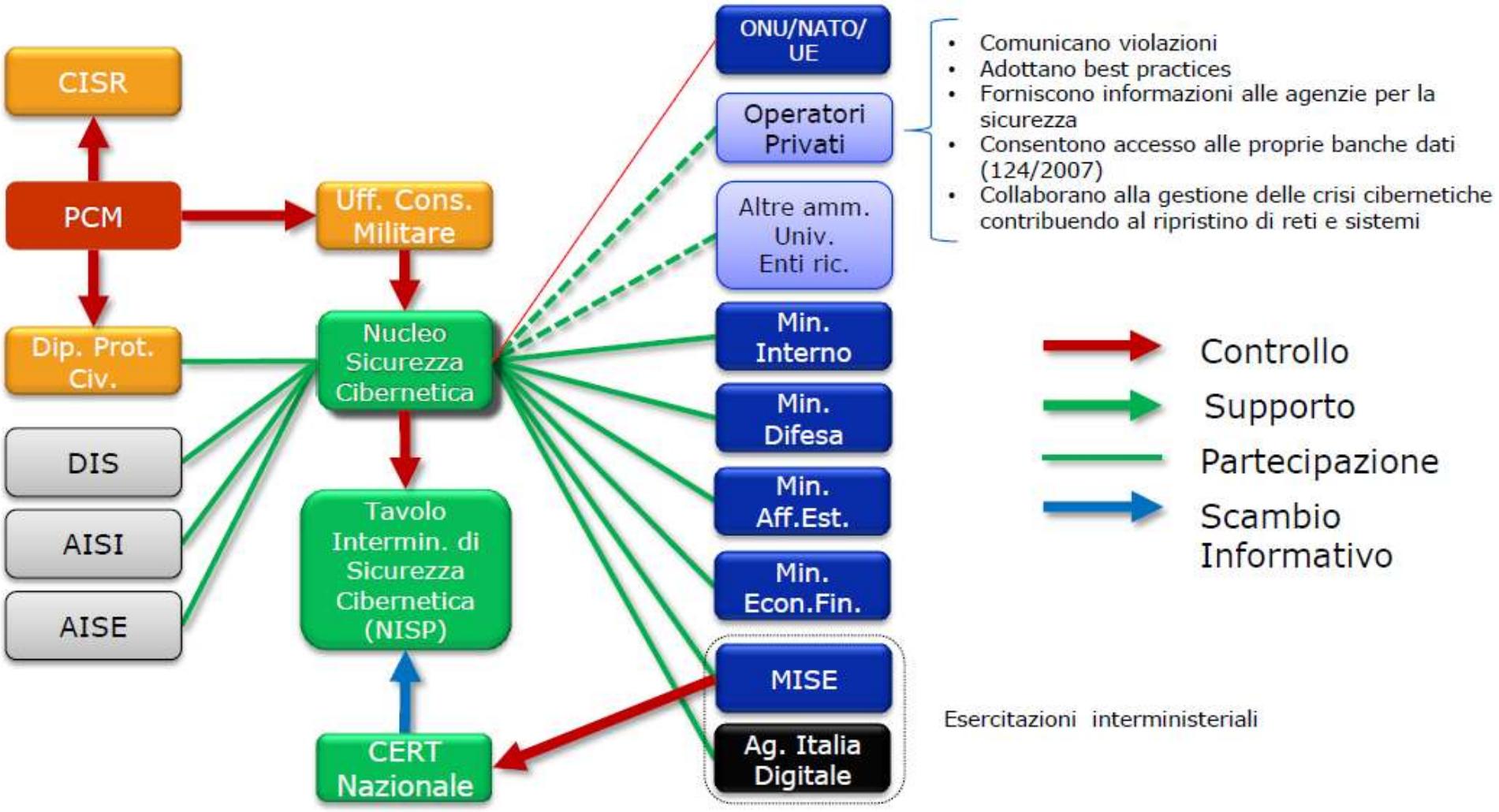
- Regola attività strategiche ed operative
- Definisce un contesto unitario ed integrato
- Prevenzione rischi
- Riduzione vulnerabilità
- Risposta tempestiva alle aggressioni
- Ripristino sistema in caso di crisi
- Integrazione pubblico-privato

DPCM 24 Gennaio 2013



Panzieri - UniRomaTre

DPCM 24 Gennaio 2013



Panzieri - UniRomaTre

‘‘Cybersecurity and American Cyber Competitiveness Act of 2013’’

A BILL

To secure the United States against cyber attack, to improve communication and collaboration between the private sector and the Federal Government, to enhance American competitiveness and create jobs in the information technology industry, and to protect the identities and sensitive information of American citizens and businesses.

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS

February 12, 2013

EXECUTIVE ORDER

- - - - - - -

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

Executive Order - Improving Critical Infrastructure Cybersecurity

- rafforzare il livello di sicurezza delle infrastrutture critiche nazionali e la loro resilienza agli attacchi informatici;
- rendere effettivo ed efficace lo scambio d'informazioni sulle minacce derivanti dal cyber-spazio;
- implementare sotto un'ottica sia strategica che operativa le migliori e più appropriate funzioni di aggregazione e analisi dei dati relativi agli incidenti informatici

http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Commissione Europea

2001 – Communication Network and Information Security: Proposal for a European Policy Approach

2004 – ENISA - Agenzia europea per la sicurezza delle reti e dell'informazione

2006 – Strategy for a Secure Information Society

2009 – Action Plan and a Communication on Critical Information Infrastructure protection (CIIP)

2009 – European Public-Private Partnership for Resilience

Agenda Digitale Europea:

- Computer Emergency Response Team per le istituzioni europee (CERT-EU) fine 2012
- strategia UE sulla sicurezza informatica presentata lo scorso 7 febbraio annuncia azioni in diverse aree e esplora le relative sinergie

Cybersecurity Strategy of the European Union

Principles for cybersecurity

- The EU's core values apply as much in the digital as in the physical world
- Protecting fundamental rights, freedom of expression, personal data and privacy
- Access for all
- Democratic and efficient multi-stakeholder governance
- A shared responsibility to ensure security

http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667

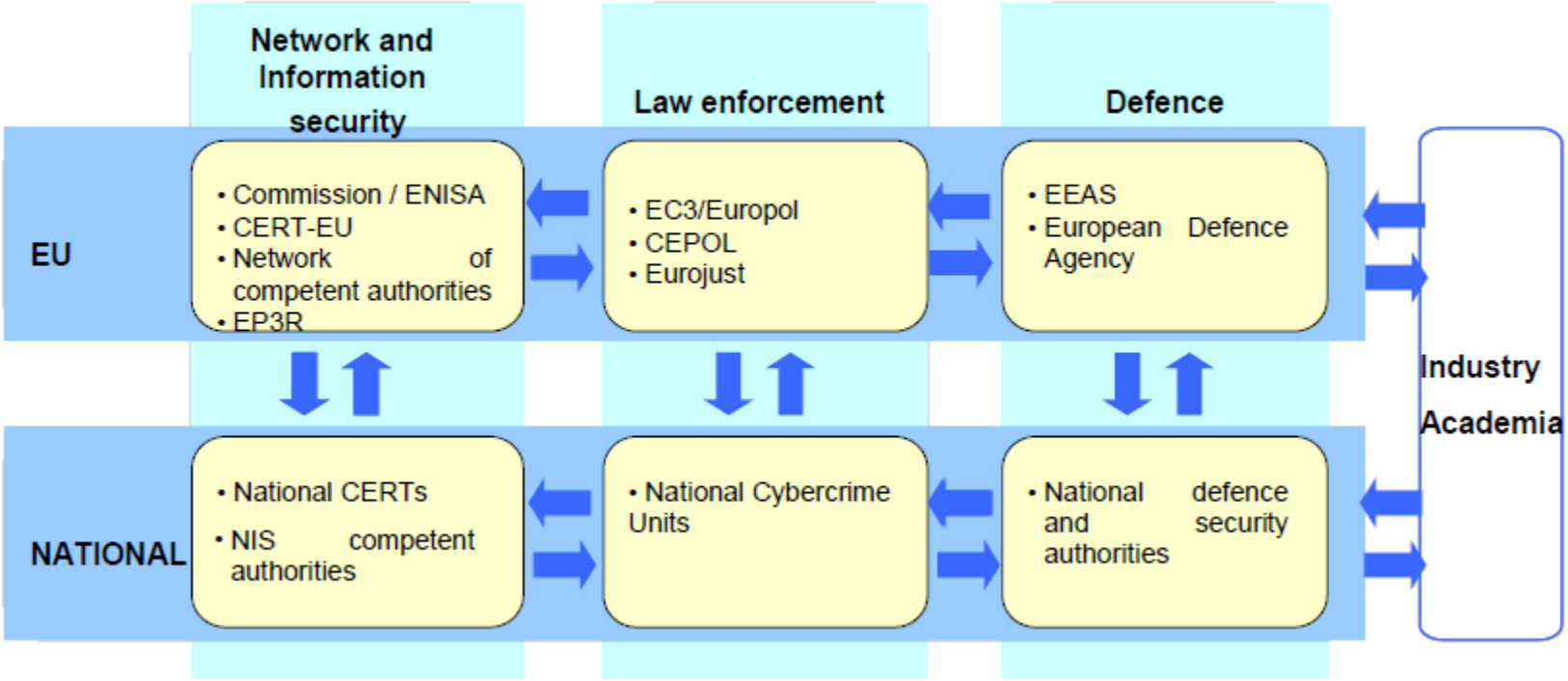
Cybersecurity Strategy of the European Union

STRATEGIC PRIORITIES AND ACTIONS

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

ROLES AND RESPONSIBILITIES



Coordination between NIS competent authorities/CERTs, law enforcement and defence

Cybersecurity Strategy of the European Union

- Ruoli e responsabilità
- Attività di contrasto nazionali alle minacce insieme al settore privato (infrastrutture critiche, ecc.).
- Ogni Stato membro deve provvedere alla scrittura di un proprio documento strategico nazionale in materia di cyber-security.
- La cyber-strategy include la possibilità per ciascun Stato membro di poter far ricorso alla clausola di solidarietà prevista dall'art. 222 del Trattato sul funzionamento dell'Unione Europea anche nel caso in cui lo Stato sia vittima di un rilevante cyber-incident ovvero di un attacco informatico.

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Conclusioni

- Minacce alle nazioni
- Cyber security ←→ enti governativi e industria
- Attacco alle infrastrutture critiche
- Active Defense - US Cyberwar Doctrine
- Iran – Israele – USA
- Analisti non vedono risvolti cyber
- DuQu, Flame, …
- ….

Agenda

- Presentazione relatore
- Cosa è successo?
- Minacce e contromisure
- Glossario
- Gli attori
- Gli obiettivi
- Gli attacchi
- Alcune risposte nazionali
- Conclusioni
- Q&A
- Bibliografia & sitografia

Domande?

Grazie per la vostra attenzione