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

DAL CYBER-CRIME ALLE ATTIVITÀ DI CYBER-WARFARE

Analisi dell'evoluzione della minaccia cibernetica e scenari futuri

Avv. Stefano Mele
Dott. Luigi Martino

Roma 16 luglio 2014

Chi siamo..

@MeleStefano

Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza ed Intelligence.

Dottore di ricerca presso l'Università degli Studi di Foggia.

Vive e lavora a Milano come "*of Counsel*" di Carnelutti Studio Legale Associato.

Collabora presso le cattedre di Informatica Giuridica e Informatica Giuridica avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano.

Esperto di *cyber-security*, *cyber-intelligence*, *cyber-terrorism* e *cyber-warfare*.

- Direttore di Ricerca su "*Cyber-security & Cyber-Intelligence*" del Ce.Mi.S.S. (Centro Militare di Studi Strategici);
- Coordinatore dell'Osservatorio "*InfoWarfare e Tecnologie emergenti*" dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli';
- Consulente per organizzazioni nazionali ed estere, sia militari che civili;
- Docente presso Istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO;
- Inserito dalla NATO nella lista dei «*Key Opinion Leaders for Cyberspace Security*»;
- Inserito da *Forbes* nella lista dei 20 migliori «*Cyber Policy Experts*» al mondo da seguire on-line.

Chi siamo..

@Mrtlgu

Laureato in Relazioni Internazionali, con una Tesi di Studi Strategici dal titolo:

La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica

Membro del CSSII -Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze-

Autore di vari studi e pubblicazioni scientifiche sul cyberspace.

Tra gli altri:

Guerra dal cyberspazio. La difesa delle reti infrastrutturali critiche dalla minaccia cibernetica *(SISP 2013)*

Collabora presso le cattedre di:

- Cyberspace e International Relation (PhD Course) Scuola Superiore Sant'Anna Pisa;
- ICT, Facoltà di Relazioni Internazionali e Studi Europei, Università degli Studi di Firenze.

CYBER CRIME: ALCUNE CIFRE

378 MILIONI *vittime per anno*

QUASI 2,8 volte il numero di bambini nati ogni anno

1 MILIONE +
di vittime al giorno

12 *vittime al secondo*

CYBER CRIME: ALCUNE CIFRE (2)

Fonte: 2013-Norton-Report-Global-Price-cybercrime

Cyber Wanted

Dal Cyber Crime al Cyber Warfare:

Alcune domande

1. La nuova era digitale: quali implicazioni per la pace e la sicurezza internazionale ?
2. Quali sono le dinamiche di potere che caratterizzano il Cyberspazio ?
3. Quali sono le differenze e le peculiarità rispetto al Sistema Internazionale "classico" ?
4. È ancora valida la distinzione tra civile e militare?

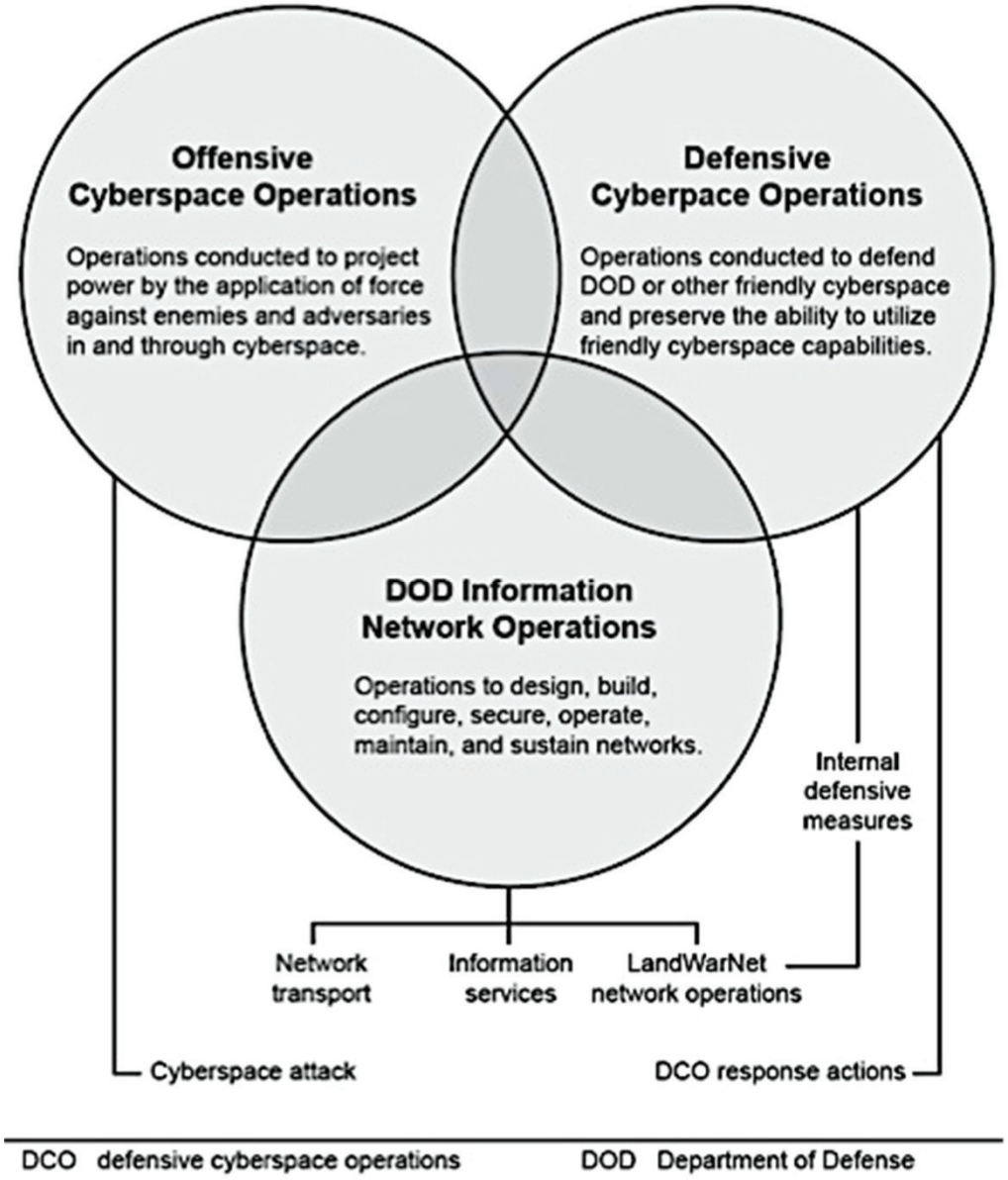
La militarizzazione del cyberspace

"La rivoluzione dell'informazione sta creando una Rivoluzione negli Affari Militari che cambierà profondamente il modo di combattere delle forze statunitensi. Dobbiamo sfruttare queste e altre tecnologie per dominare il campo di battaglia. Lo schema di riferimento in base al quale fare nostre queste nuove opportunità e garantirci così una posizione di supremazia è fissato dal documento ***Joint Vision 2010***, il piano predisposto dal presidente del Comitato dei Capi di Stato Maggiore per le operazioni militari del futuro"

Segretario alla Difesa William Cohen, 1997

La militarizzazione del cyberspace

Fonte: *United States Army, Department of the Army Headquarters*


Offensive
Cyberspace Operations
Operations conducted to project power by the application of force against enemies and adversaries in and through cyberspace.
Defensive
Cyberpace Operations
Operations conducted to defend DOD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.
DOD Information
Network Operations
Operations to design, build, configure, secure, operate, maintain, and sustain networks.
Internal defensive measures
Network transport
Information services
LandWarNet network operations
Cyberspace attack
DCO response actions
DCO defensive cyberspace operations
DOD Department of Defense

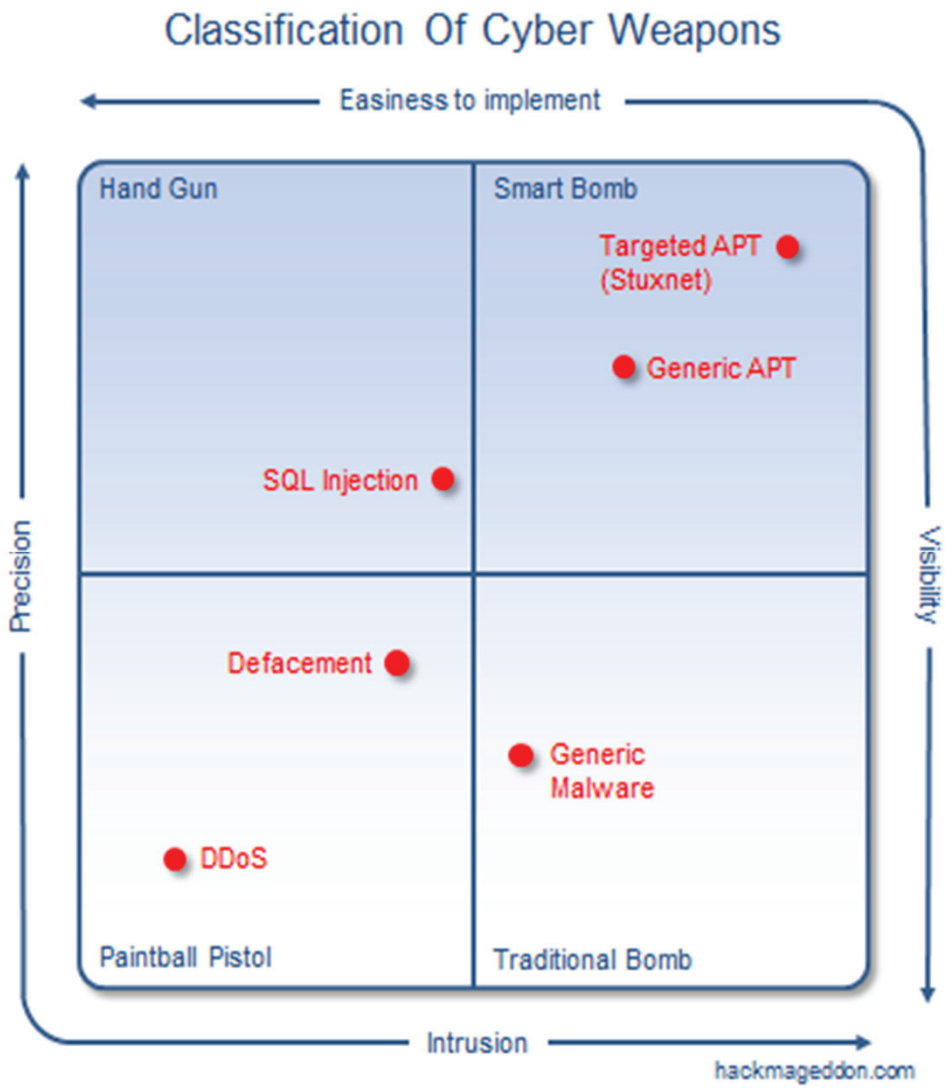
Indicatori per le cyber capabilities

Table 1 **Possible Indicators of Cyber Capability**

Political	Political system
	Social stability
	National ambitions
	International standing
	Relationship of hackers with state sponsors and political aims
	Regulatory action
	Parliamentary discussions National security documentation National technical strategies
Military	Military cyber strategy and doctrine
	Organisational structure/units
	Education, training, exercises
	Known/suspected operations
	Intelligence and fusion
	Materiel, logistics, infrastructure
Economic	Defence budget/service budgets
	Programme budgets
	GDP
	Raw materials/indigenous production
	Export/import restrictions
	Acquisitions, procurements
	Patents
	R&D funding
	High-tech public companies
	Products with high R&D loads
	Manufacturing capability
Social	Maturity of information society
	Top technical universities
	Post-graduate students
	Graduation in science, engineering, manufacturing and construction
	Known hackers
	R&D intensity
	Researcher concentration
Information/ Technology	Domain control
	High-tech density
	Know-how, experience
	Innovation
	State-of-the-art technology
	Retail electronics
	Advanced technologies (unmanned systems, robotics)
Infrastructure	Military networks
	SIGINT + Platforms
	Communications
	High-speed access
	Advanced services
	Numbers of ISPs
	Space exploration capabilities
	Industrial base
Other	Manufacturers' advertisements
	Strategic purchases and sales
	Unusual policy/security attention

Fonte: Military Balance 2014, International Institute for Strategic Studies (IISS)

Cyber Weapons: classificazione base



Cyber Weapons: minacce, sfide e rischi

"Gli effetti catastrofici, [delle Armi di Distruzione di Massa] sono possibili anche nel cyberspazio a causa del legame esistente tra lo spazio cibernetico e le infrastrutture critiche sistemi SCADA. Attacchi ben pianificati a nodi chiave delle infrastrutture del cyberspazio hanno il potenziale di causare il collasso della rete e effetti a cascata che possono danneggiare seriamente infrastrutture a livello locale, nazionale o finanche globale".

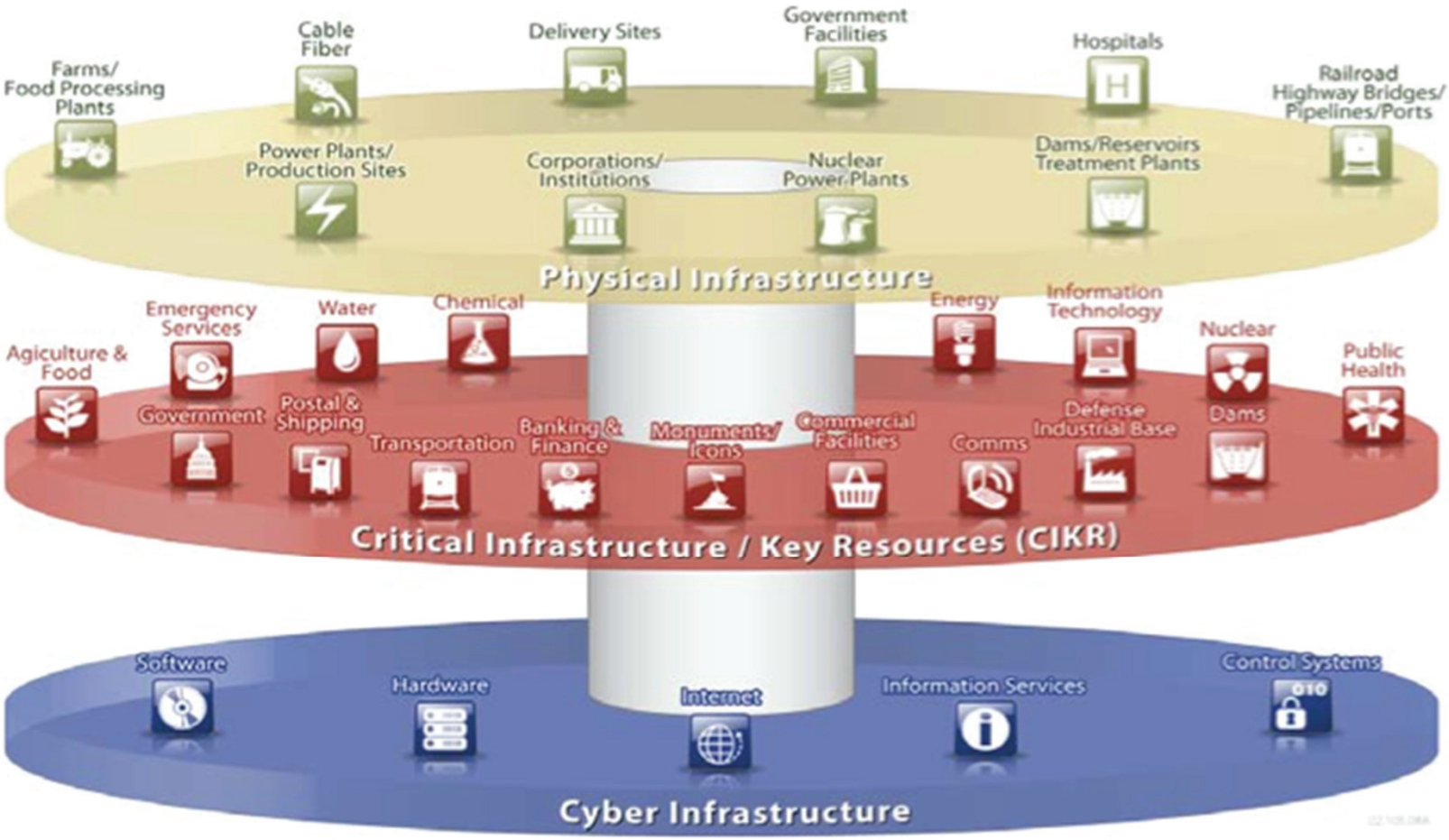
Generale Peter Pace

Chairman of the Joint Chiefs of Staff

Cyber weapons: gli obiettivi

- Incidere sulle azioni politiche del nemico al fine di mutarne le decisioni;
- Prevenire i rischi sulla sicurezza come ad esempio la produzione di armi non convenzionali;
- Costruire una capacità di attacco come parte integrante di una dottrina di deterrenza;
- Mezzo per costruire una contromisura adeguata per rispondere agli attacchi provenienti dallo spazio cibernetico

Cyber Weapons: gli obiettivi (2)



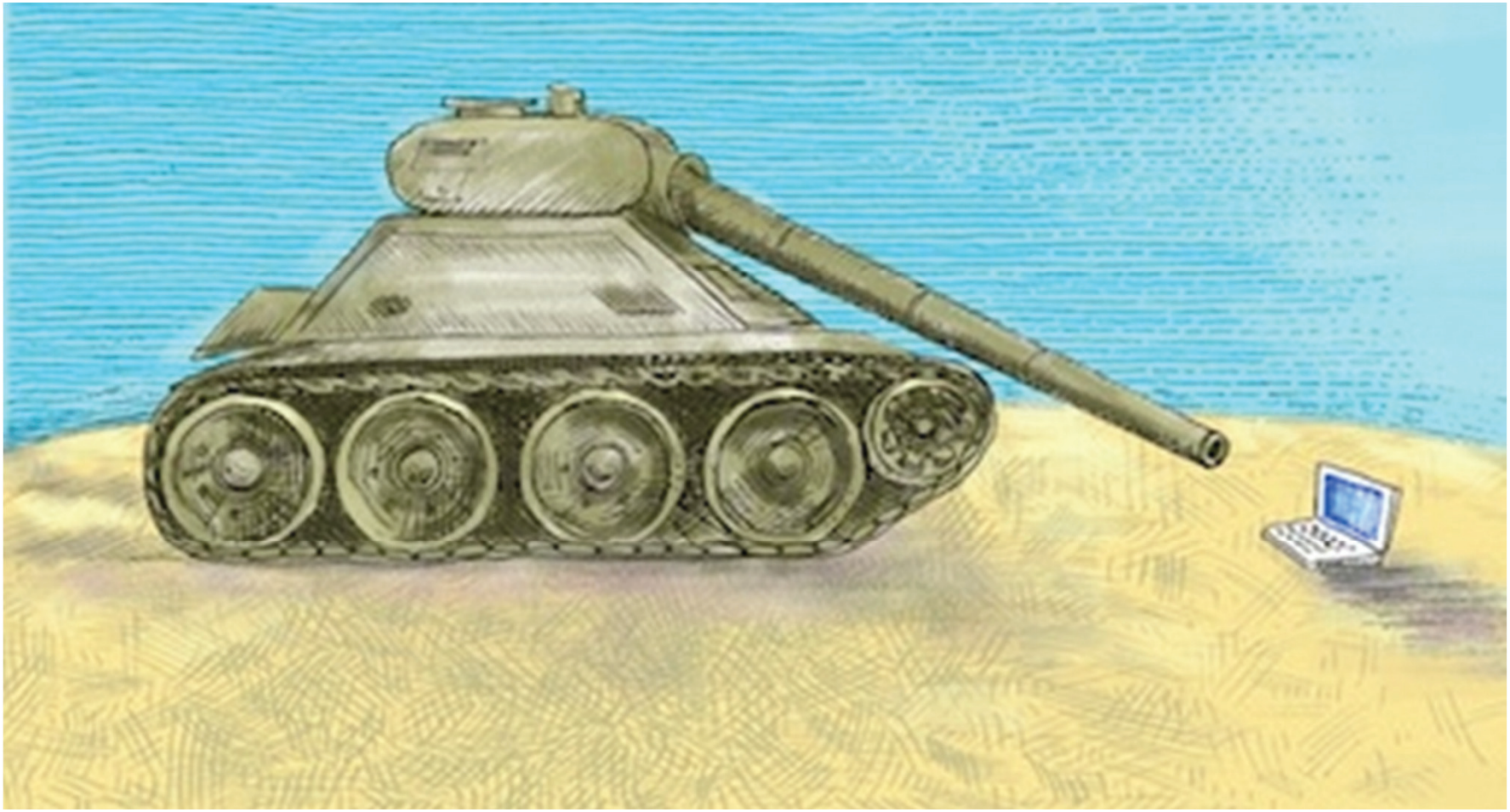
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Dalla deterrenza nucleare alla resilienza cibernetica

È possibile una deterrenza nel cyberspace?

- Sistema Internazionale tendenzialmente "multipolare"
- Pervasività e anarchia del dominio cibernetico
- Abbattimento della soglia di accesso alla violenza
- Ambiente Operativo Dromologico (compressione dello spazio e del tempo)
- Asimmetria intrinseca e moltiplicazione della potenza/velocità
- Difficoltà di distinzione civile/militare
- Difficoltà fattuale di geolocalizzazione
- Difficoltà di rappresaglia

Dal confronto dal forte al forte alla logica dal forte al folle



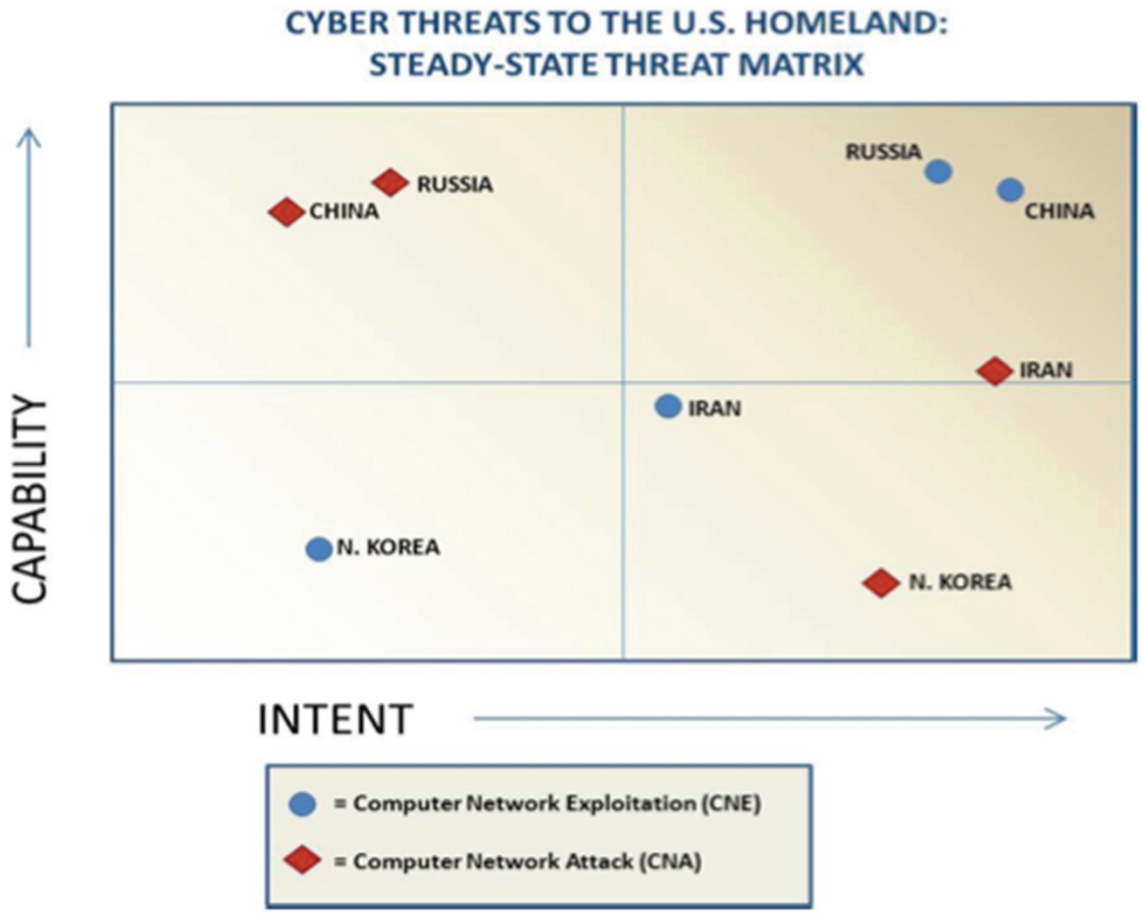
La necessità di un Sistema Paese "elastico"

La resilienza come fattore vitale:

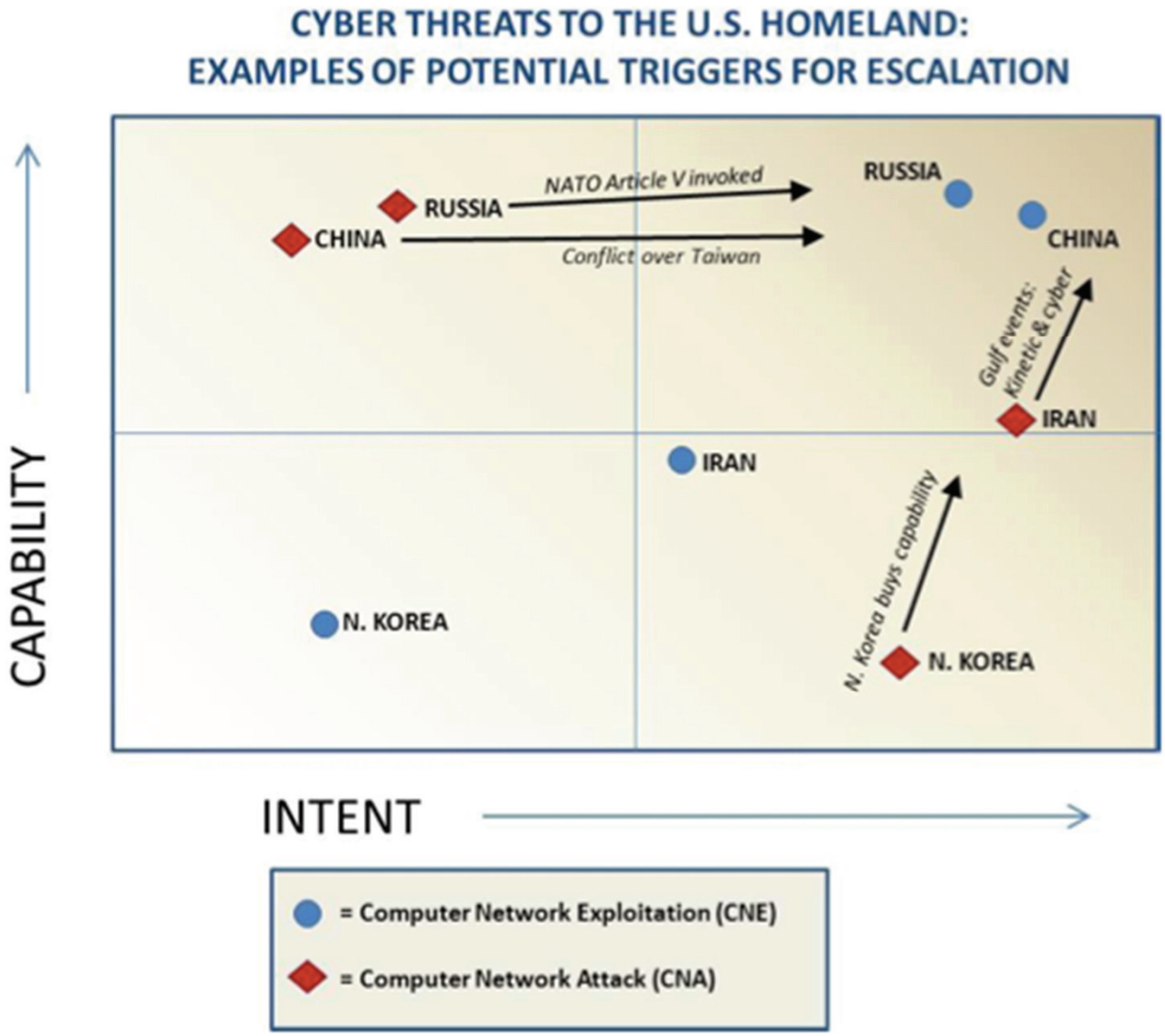
"capacità di un dato sistema di adattarsi alle condizioni d'uso, e di resistere agli eventi in modo tale da garantire la funzionalità e la continuità dei servizi erogati, nonché la capacità di recupero e una rapida ricostruzione di fronte agli attacchi cibernetici".

Anche le strutture politico-decisionali devono essere "elastiche" per rispondere in modo adeguato alla minaccia "istantanea".

Uno scenario possibile in caso di cyber war



Il rischio escalation militare



ISACA
Sistemi informativi: averne fiducia e trarne va...
Rome Chapter

#Spionaggio

#Spionaggio

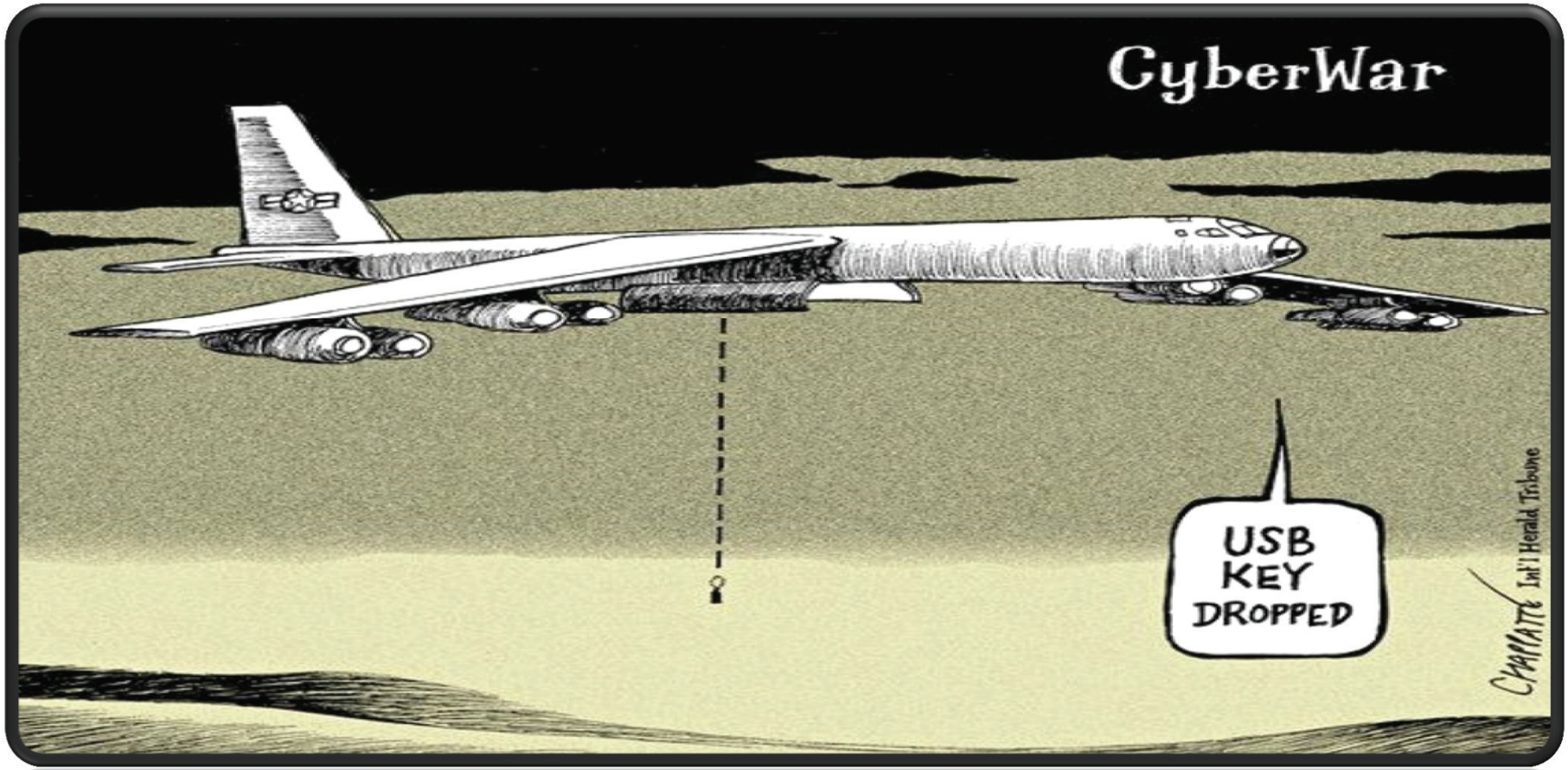
- ✓ Lo spionaggio costituisce uno degli strumenti migliori e più efficaci per ottenere – sia in tempo di pace che di guerra – vantaggi politici, militari ed economici nei confronti di nemici e alleati.
- ✓ Ciò è vero, ovviamente, anche nel caso in cui si tratti di **spionaggio elettronico**.

- ➢ Digitalizzazione delle informazioni
- ➢ Accentramento
- ➢ Scarsa percezione dei pericoli

Da dieci anni a questa parte, lo spionaggio elettronico è una delle principali e più importanti minacce alla sicurezza nazionale e alla competitività dei sistemi Paese

- ✓ Lo spionaggio non ha mai rappresentato la causa scatenante di alcun conflitto (Strategia aggressiva -> **Sanzioni mirate**)

#Stati Uniti



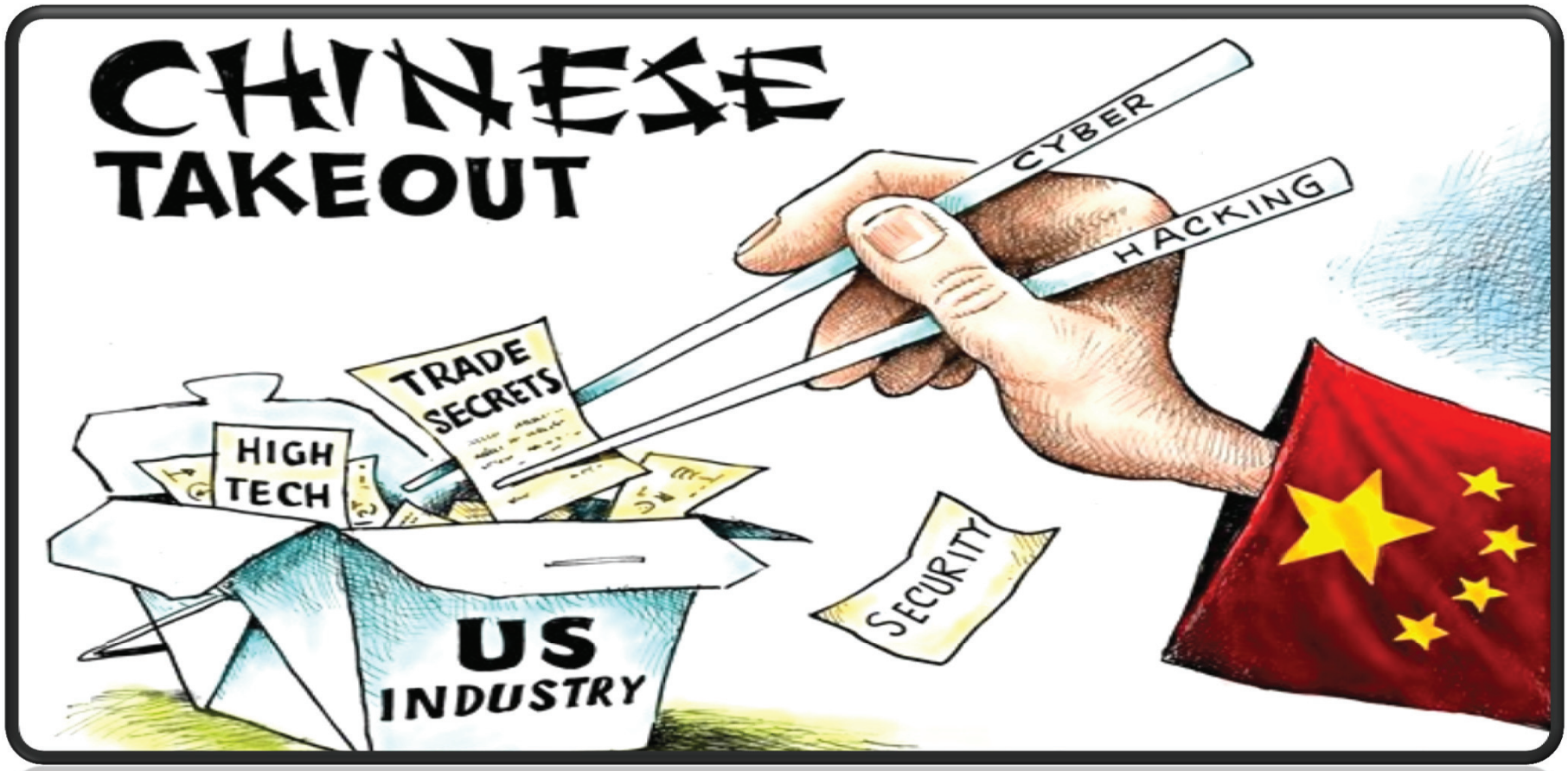
#Stati Uniti

- ✓ I 10 documenti strategici americani in materia di cyber-security e i loro limiti.

- ✓ Il ***Presidential Executive Order on Improving Critical Infrastructure Cybersecurity*** e la ***Presidential Policy Directive on critical infrastructures security and resilience****:*

  1. Rafforzare il livello di sicurezza delle infrastrutture critiche nazionali e la loro resilienza agli attacchi informatici;
  2. Rendere effettivo ed efficace lo scambio d'informazioni sulle minacce derivanti dal cyber-spazio, soprattutto attraverso il coinvolgimento attivo delle agenzie di Intelligence e del settore privato;
  3. Implementare le migliori e più appropriate funzioni di aggregazione e analisi dei dati relativi agli incidenti informatici avvenuti, alle minacce in atto e ai rischi emergenti.

#Cina


CHINESE
TAKEOUT
CYBER
HACKING
TRADE
SECRETS
HIGH
TECH
SECURITY
US
INDUSTRY

#Cina

- ✓ Benché non tutte le operazioni di spionaggio elettronico effettuate possano essere addebitabili al Governo cinese, appare indiscutibile come la maggior parte di esse venga portata a segno attraverso sistemi informatici residenti proprio sul territorio cinese (**nell'ultimo trimestre 2013 U.S. stimano oltre 1 su 3**).

- ✓ **Metodo**: strategia aggressiva.
- ✓ **Obiettivo**: furto d'informazioni riservate/classificate dei Governi, ma anche furto di proprietà intellettuale, soprattutto nel settore ricerca e sviluppo, da cedere alle società presenti sul territorio cinese, affinché rivendano prodotti simili a prezzi fortemente concorrenziali sui mercati occidentali.

#Cina

- ✓ Esempi di operazioni di spionaggio attribuite alla Cina effettuate sfruttando il *cyber-spazio*:

- ➢ Operazioni ad **ampio spettro**: *Titan Rain* (2003), *GhostNet* (2009), *Shady RAT* (2011), *ecc.*
- ➢ Operazioni pianificate per colpire uno o più **determinati obiettivi** sensibili: *Operation Aurora* (2009), *RSA* (2011), *British Aerospace (BAE)* (2012), *New York Times/Wall Street Journal* (gennaio 2013), *U.S. Army Corps of Engineers' National Inventory of Dams* (01 maggio 2013), Lockheed Martin (12 maggio 2013), *ecc.*

#Cina

✓ **Reazione alla minaccia (U.S.)**:

- Marzo 2013, entra in vigore una legge che obbliga la NASA, il Dipartimento della Giustizia e il Dipartimento del Commercio americano a richiedere l'autorizzazione preventiva dell'FBI prima di compare materiale informatico di aziende "*appartenenti, direttamente o indirettamente, alla Repubblica Popolare Cinese*".
- White House, "*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*", 2013.

...

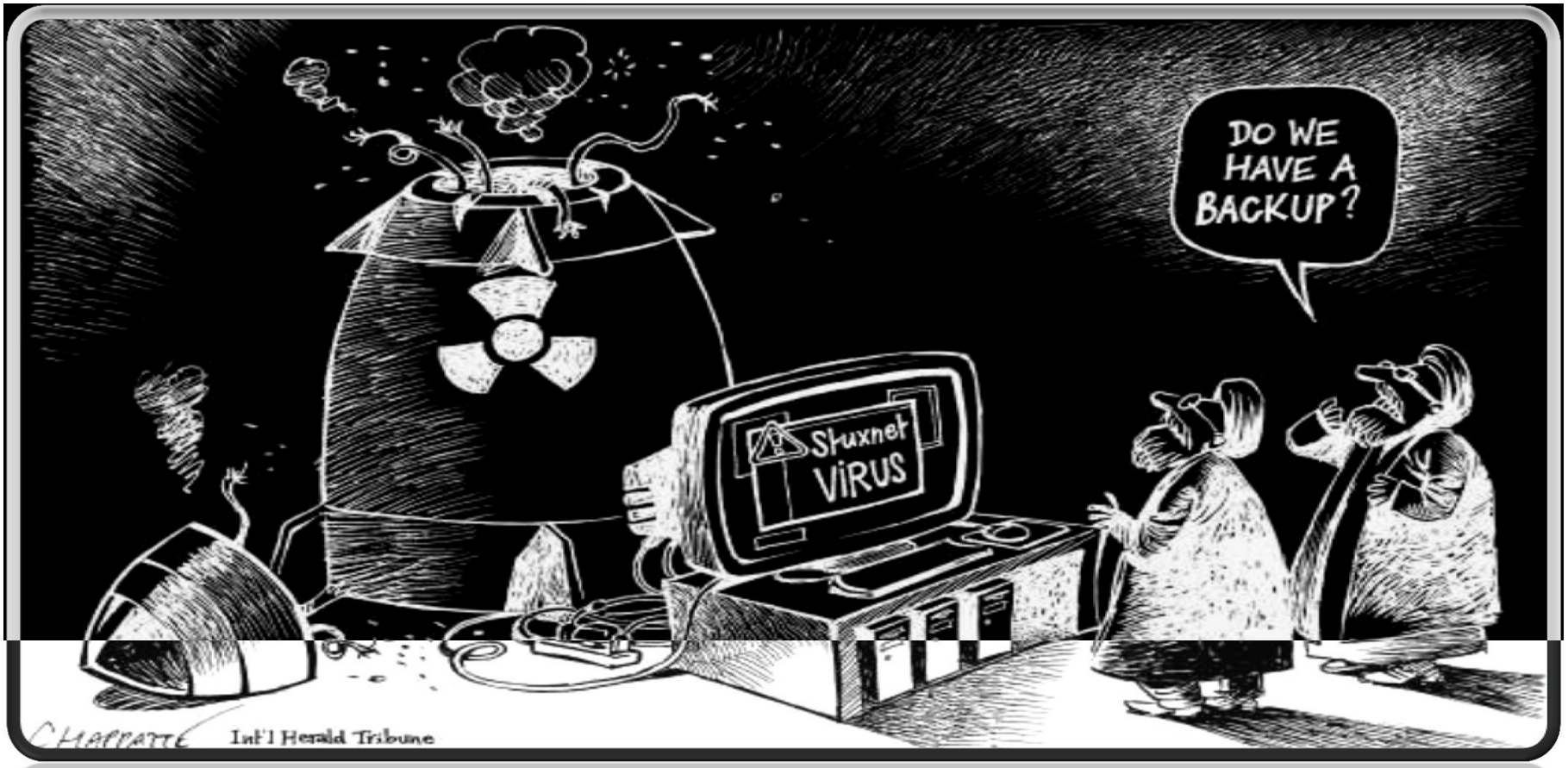
- Mandiant, "*APT1: Exposing One of China's Cyber Espionage Units*", 2013. [.. come lo classifichiamo?..]

#Cina

- ✓ **Reazione alla minaccia (altri)**:

- ➢ Australia ha impedito a Huawei di partecipare all'appalto per il cablaggio in fibra del paese (2012).
- ➢ Canada ha escluso Huawei dal bando di costruzione di una rete governativa per le comunicazioni (2012).
- ➢ India ha vietato la vendita di prodotti a marchio o collegati a Huawei e ZTE in tutta la nazione (2010).
- ➢ ecc.

#Iran



#Iran

- ✓ L'approccio verso Internet ("*Hallal Internet*", "*Mehr*", VPN).
- ✓ Supreme Council on Cyberspace (2012).
- ✓ National Center of Cyberspace (2013).

- ✓ $ 1 billion per lo sviluppo delle *cyber-capabilities* nazionali (2011).
- ✓ Il malware Shamoon.
- ✓ Il ruolo degli *hacktivist*.

- ✓ I rapporti dell'Iran verso gli atri Paesi.

#Italia

#Italia

Sei sono i pilastri strategici del "***Quadro strategico nazionale per la sicurezza dello spazio cibernetico***" su cui il nostro Governo ha deciso di incentrare la sua strategia:

1. Il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati.
2. Il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese.
3. L´incentivazione della cooperazione tra istituzioni e imprese nazionali.
4. La promozione e diffusione della cultura della sicurezza.
5. Il rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali on-line.
6. Il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica.

#Italia

Undici sono i punti operativi predisposti all'interno del "***Piano nazionale per la protezione cibernetica e la sicurezza informatica***":

1. Potenziamento delle capacità di intelligence, di Polizia e di difesa civile e militare.
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati.
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento.
4. Cooperazione internazionale ed esercitazioni.
5. Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteri.
6. Interventi legislativi e *compliance* con obblighi internazionali.
7. *Compliance* a standard e protocolli di sicurezza.
8. Supporto allo sviluppo industriale e tecnologico.
9. Comunicazione strategica.
10. Ottimizzazione della spesa nei settori della *cyber-security* e *cyber-defence*.
11. Implementazione di un sistema di *information risk management* nazionale.

#Italia

Il **Quadro Strategico** italiano mira «*ad accrescere la capacità di risposta del Paese alle presenti e future sfide riguardanti il cyber-space, indirizzando gli sforzi nazionali verso obiettivi comuni e soluzioni condivise, nella consapevolezza che* ***la protezione dello spazio cibernetico è un processo più che un fine****, che la continua innovazione tecnologica introduce inevitabilmente nuove vulnerabilità, e che* ***le caratteristiche stesse della minaccia cibernetica rendono la difesa, per ora, di tipo prevalentemente – anche se non esclusivamente – reattivo***».

- ✓ La sicurezza come processo
- ✓ Approccio difensivo evidente e di *active defence* 'latente'

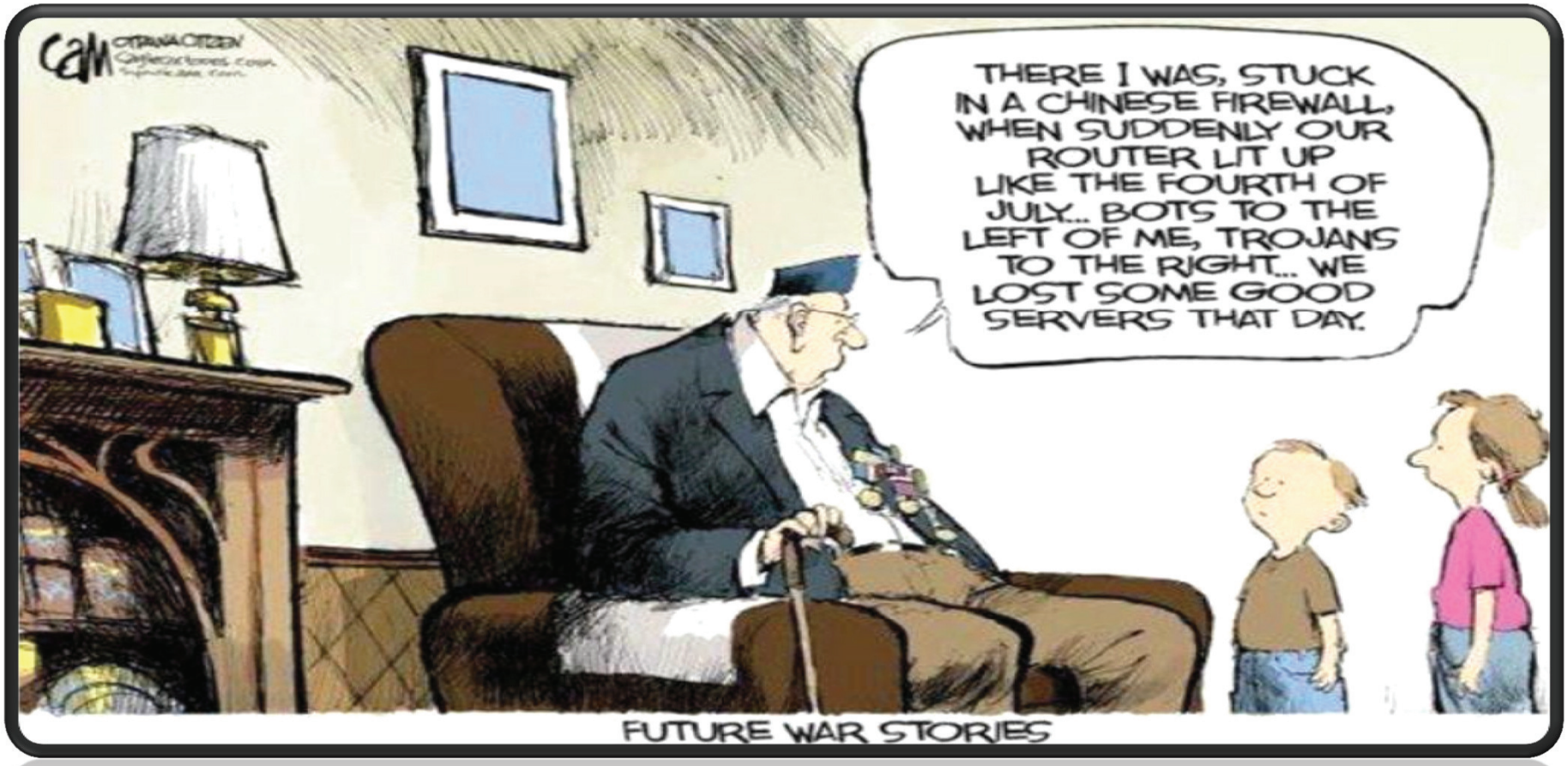
#Italia

Con il **Piano Nazionale** italiano «*l'Italia si dota di una strategia organica, alla cui attuazione sono chiamati a concorrere non solo gli attori, pubblici e privati, richiamati nel Quadro Strategico Nazionale ma anche* ***tutti coloro che, su base quotidiana, fanno uso delle moderne tecnologie informatiche, a partire dal singolo cittadino****.*

Tale strategia associa alla sua valenza organica un tratto di flessibilità, indispensabile a fronte delle rapide evoluzioni tecnologiche dello spazio cibernetico e delle relative sfide di sicurezza. La necessità, in sostanza, ***non è solo quella di essere "al passo con i tempi" ma anche di coglierne le "anticipazioni"****, così da prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare del nostro Paese*».

- ✓ Colma una lacuna presente nella maggior parte delle cyber-strategy degli altri Paesi
- ✓ Rilevanza della nascita di una cultura della sicurezza
- ✓ Rilevanza della cooperazione tra pubblico e privato
- ✓ Rilevanza dello sviluppo di capacità di analisi strategica e previsionale

#Riflessioni conclusive



Contatti

- http://www.stefanomele.it
- avv.stefanomele@gmail.com
- luigimartino@aol.com

Grazie per l'attenzione...