

# Introduzione

*Francesco Palmieri*  
*fpalmieri@unisa.it*

# Panoramica del corso

- Scopo:
  - Costruire l'ecosistema delle competenze di cybersecurity adeguate a gestire strumenti ed architetture a supporto della sicurezza
  - Chiarire i principali concetti e problematiche in ambito cybersecurity, ed evidenziare le potenziali minacce e le tecnologie disponibili per fronteggiarle
- Articolazione
  - 9 CFU
    - 7 di lezione frontale (56 ore)
    - 2 di laboratorio (16 ore)
- Modalità di Esame
  - Colloquio individuale

# Informazioni di base

- Prerequisiti:
  - Fondamenti di Sicurezza
  - Reti di Calcolatori
  - Familiarità con i sistemi Unix/Linux
- Impegno
  - Nel seguire costantemente le lezioni
    - Nota: domande e richieste di chiarimento sono sempre benvenute!
  - Nel partecipare alle esercitazioni in laboratorio
- Chiarimenti ed integrazioni
  - Durante le ore di lezione o ricevimento
    - Su appuntamento via mail a *fpalmieri@unisa.it*

# Sbocchi professionali: la domanda

**R.it | Economia & Finanza** con Bloomberg

HOME LAVORO RICERCA AREA PERSONALE NOTIZIE E SERVIZI AREA AZIENDE

TROVA TUO **miojob** Dossier Interviste Calcolo Stipendio Contratti Calcolo pensione Modelli CV Busta paga | Canale neolaureati | Pubblica la tesi

Che lavoro Località Scegli area geografica Area funzionale Scegli area

 Lavora per una stagione all'Apple Store. Vivi un'esperienza che ricorderai per sempre. [More](#)

[f](#) [t](#) [g+](#) [in](#) [e](#)

**Offerte della settimana**

**RESPONSABILE ANALISI DEL VALORE**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCARESPONSABILE...

**ANALISTA FUNZIONALE SENIOR**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCANAALISTA...

**TECNOLOGO ESPERTO NEI PROCESSI DI ASSEMBLAGGIO E COLLAUDO**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCATECNOLOGO...

**PROGETTISTA FIRMWARE/SOFTWARE**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCAPROGETTISTA...

**INFORMATICO**  
[Tutte le offerte](#)

Entro tre anni 135mila posizioni nel settore Ict rimarranno scoperte. Secondo un'indagine di Modis dal sistema formativo italiano escono pochi laureati in ambito Itc, tant'è che il 40% delle aziende fatica a trovare i candidati ideali. Un problema per la futura competitività delle imprese. Il data analyst è il più richiesto oggi

di BARBARA ARDU'

Lo leggo dopo | 22 marzo 2018

[f](#) [t](#) [g+](#) [in](#) [p](#) [e](#)



**ROMA** - C'è uno squilibrio tutto italiano che peserà nei prossimi anni sul mercato del lavoro. Dal sistema formativo usciranno troppi diplomati e pochi laureati in ingegneria o comunque in facoltà che preparano i professionisti dell'Itc. Non è una novità, ma il dato viene sempre più certificato dalle agenzie che mettono in contatto le aziende con potenziali candidati. L'ultima ricerca inizia su un vero a priori

**R.it | Economia & Finanza** con Bloomberg

HOME LAVORO RICERCA AREA PERSONALE NOTIZIE E SERVIZI AREA AZIENDE

TROVA TUO **miojob** Dossier Interviste Calcolo Stipendio Contratti Calcolo pensione Modelli CV Busta paga | Canale neolaureati | Pubblica la tesi

Che lavoro Località Scegli area geografica Area funzionale Scegli area

 Lavora per una stagione all'Apple Store. Vivi un'esperienza che ricorderai per sempre. [More](#)

[f](#) [t](#) [g+](#) [in](#) [e](#)

**Offerte della settimana**

**RESPONSABILE ANALISI DEL VALORE**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCARESPONSABILE...

**ANALISTA FUNZIONALE SENIOR**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCANAALISTA...

**TECNOLOGO ESPERTO NEI PROCESSI DI ASSEMBLAGGIO E COLLAUDO**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCATECNOLOGO...

**PROGETTISTA FIRMWARE/SOFTWARE**  
AZIENDA LEADER NEL SETTORE AUTOMOTIVE PER IL BOLLENAMENTO DELLA PROPRIA STRUTTURA RICERCAPROGETTISTA...

**INFORMATICO**  
[Tutte le offerte](#)

Da un report del Digital Transformation Institute di Capgemini emerge come sia difficile trovare talenti specializzati in cibersecurity, una figura professionale che sta diventando sempre più indispensabile per le aziende che hanno puntato la loro crescita sull'innovazione digitale. Mettere al sicuro i dati è diventato il problema numero uno

di BARBARA ARDU'

Lo leggo dopo | 06 marzo 2018

[f](#) [t](#) [g+](#) [in](#) [p](#) [e](#)



**ROMA** - E' la sicurezza informatica il vero buco nero di questa stagione di incertezze. Un report del Digital Transformation Institute di Capgemini evidenzia un urgente e crescente divario legato ai talenti in ambito cybersecurity. Dalla ricerca *Cybersecurity talent: the big gap in cyber protection* emerge infatti come tra le varie competenze digitali necessarie a quella società

• laurea in discipline economico/finanziarie o comunque in discipline che abbiano un indirizzo economico-finanziario;

• precedente esperienza in ruoli di elevata responsabilità nell'ambito dell'amministrazione e del controllo aziendale e della gestione delle risorse umane, maturata in realtà finanziarie, bancarie o della Pubblica Amministrazione e di Società a partecipazione pubblica;

• laurea in discipline economico/finanziarie o comunque in discipline che abbiano un indirizzo economico-finanziario;

• precedente esperienza in ruoli di elevata responsabilità nell'ambito dell'amministrazione e del controllo aziendale e della gestione delle risorse umane,

# Sbocchi professionali: la domanda

L'Economia

TROVLAVORO

## Lavori che mancano: le 5 professioni più ricercate (e meno trovate) dalle aziende

di Irene Consigliere, Claudia Voltattorni, Federico De Rosa | 20 dicembre 2021



5/6



### Esperti della sicurezza informatica

Con l'aumento dello smart working in seguito alla pandemia i profili professionali della cyber security, ovvero della sicurezza informatica sono diventati **indispensabili**. Il cyber risk analyst che analizza i principali rischi aziendali e il security consulting engineering, l'ingegnere che si occupa dei software e il chief information security officer, che autorizza le misure di sicurezza informatica sono tra le figure principali. A ricercarli sono soprattutto le big della consulenza: in particolare Accenture ha da poco aperto 300 posizioni per la divisione Security e per raggiungere la parità di genere in azienda entro il 2025 ha organizzato la Pink Academy, per favorire l'ingresso delle donne in posizioni che richiedono una formazione scientifica. Altre realtà interessate a questi profili: Deloitte, Price Waterhouse Coopers, EY, Cisco, Microsoft. Per la formazione a Milano c'è il Master della Bocconi in collaborazione con il Politecnico e l'Hackademy della stessa Accenture.

Where is your team working from today?  
Our Secure Remote Work solution is all you need.

[Tell me more](#)



la Repubblica Martedì, 22 dicembre 2021

Cronaca

L'intervista al direttore dell'Agenzia nazionale

pagina 19

Fatto l'aggresso per la cybersecurity nazionale, ora bisogna fare gli agenti. Anche se non è facile: i posti sono chiamati a rimbombare la testa e le ossa e le loro cifre sono spesso esagerate. Agente o agente, ovvero le norme minacciose che proteggono i dati? Chi l'obiettivo è cambiato: ovvero le politiche che cominciano a lavorare per il proprio Paese, per la sua sicurezza. Per esempio Amazon, mettetevi a piedi una banca, non è un problema per il mercato mondiale. Ma non è così. Roberto Baldoni, direttore generale dell'Agenzia nazionale per la sicurezza, cresce fino a 300. Dalle 100, dall'interno e dall'estero. L'obiettivo è chiaro: 200 sono i posti per cui bisogna trovare persone.

**Che soggetti cercate?**

Ingegneri, matematici, fisici e informatici, ma anche esperti di diritto e di sicurezza. Se poi è tempo di trovare un esperto in cloud computing, dev'essere un professore universitario, ma non solo. Bisogna trovare un esperto in cybersecurity, anche di controllo della sicurezza.

**Perché solo cittadini italiani?**

Perché le aziende italiane hanno sempre fatto molto per la sicurezza informatica, ma non solo.

**Dove pensate di dovervi?**

Un po' ovunque. In Italia, ma anche all'estero.

**È stata creata l'Agenzia nazionale per la sicurezza della cyberspace. Alla direzione c'è Baldoni. Alla**

menti un po' maglie da qualche anno sono andati via diversi esperti, soprattutto da Francia, Germania, Svizzera, Olanda, Gran Bretagna, dove il cloud computing, delфт intelligence e altri settori sono molto più avanzati. Infine, l'esperienza internazionale del leader del settore.

**Come si fa oggi?**

Attraverso la rete, attraverso i portali, e poi attraverso i portali.

**Cosa è cambiato?**

Il mondo ha cambiato. E' un mondo

che non ha più confini, dove i

movimenti nel terreno sono più circostanti della sicurezza che era nei primi anni Novanta, quando erano solo i militari.

**Il concorso pubblico è aperto anche a giornalisti neodiplomati?**

Non è vero. Non è vero che non ci sono posti per i giornalisti.

**Cosa è cambiato?**

Il mondo ha cambiato. E' un mondo

che non ha più confini, dove i

movimenti nel terreno sono più circostanti della sicurezza che era nei primi anni Novanta, quando erano solo i militari.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cavalcata"?**

È un termine che indica la

cooperazione tra le agenzie di sicurezza.

**Cosa significa "cav**

# Sbocchi professionali: l'offerta



HOME LAVORO RICERCA AREA PERSONALE NOTIZIE E SERVIZI AREA AZIENDALE

TROVA IL TUO JOB | Dati ISTAT | Notizie | Dossier | Interviste | Calcolo Stipendio | Contratti | Cognizioni

Busta paga | Canale neolaureati | Pubblica la tesi

Che lavoro

Località Scegli area geografica ▾ Area funzionale Scegli area



Lavora per una stagione all'Appartamento Vivi un'esperienza che ricorderai per sempre

## E' il Cyber security manager a guadagnare di più nel mondo Ict

Modis ha analizzato le sei competenze più richieste. Le differenze retributive si riscontrano soprattutto tra grandi e piccole aziende, tra chi sa solo leggere i linguaggi web e chi ha capacità superiori. Si guadagna più al Nord che al Sud. E anche in uno dei settori più innovativi permangono le differenze salariali tra uomini e donne. La laurea o i master servono per fare carriera

di BARBARA ARDU'



IMPRESE & MERCATI ▾ CARRIERE ▾ CULTURE ▾ INCENTIVI ▾ FUTURA ▾ CRONACHE ▾ RUBRICHE ▾

ALTRÉ SEZIONI ▾

Home ▸ Approfondimenti ▸ Ict, indagine Modis: stipendi al top per gli specialisti della Cyber Security

Approfondimenti

## Ict, indagine Modis: stipendi al top per gli specialisti della Cyber Security

Da ildenaro.it - 15 gennaio 2018

235

f Condividi su Facebook t Tweet su Twitter G+ p



Young hacker in data security concept

Quali sono le competenze da acquisire per guadagnare di più? Quali sono i professionisti meglio pagati nel settore ICT? Dove lavorano e con quali mansioni quelli

Guarda la Newsletter di oggi

il denaro.it



Guarda Confindustria News

il denaro.it



Infotraffic del 9 Luglio 2018

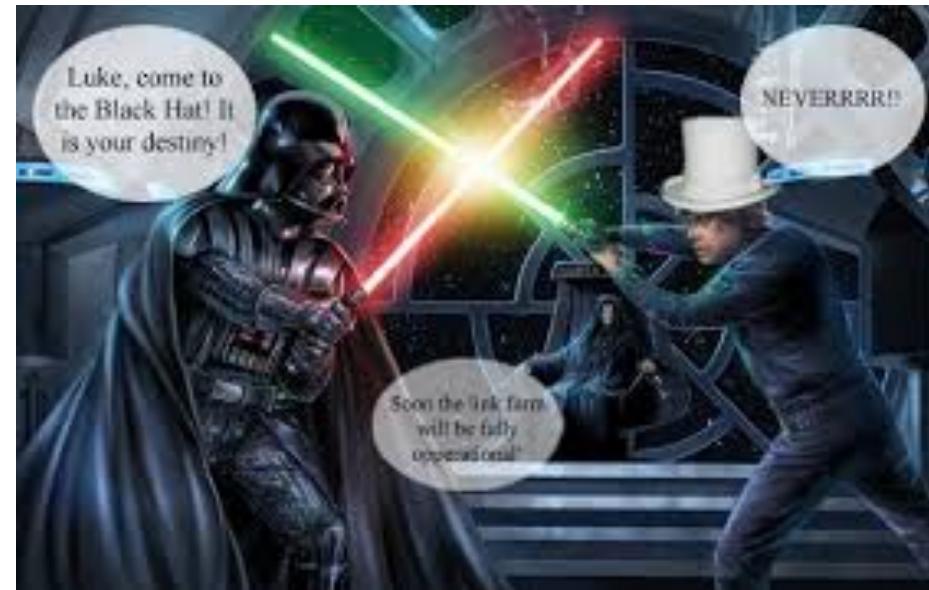


# Etica del corso e legalità

- Nel contesto del corso discuteremo (lanciandoli in ambiente simulato) diversi **attacchi**, alcuni alquanto pericolosi in termini di potenziale offensivo e faremo uso di tecnologie di **intervettazione telematica** e vulnerability scan
- Nessuna di tali tecniche o strumenti va usata su una rete reale ed in particolare senza il consenso informato di tutte le parti coinvolte
- L'esistenza di accessi non adeguatamente protetti o buchi di sicurezza non è una scusa valida
- Questo non riguarda solo concetti di etica in rete ma il rispetto **di leggi e normative nazionali ed internazionali**
- Le conseguenze di un mancato rispetto di queste norme possono essere anche **molto gravi**

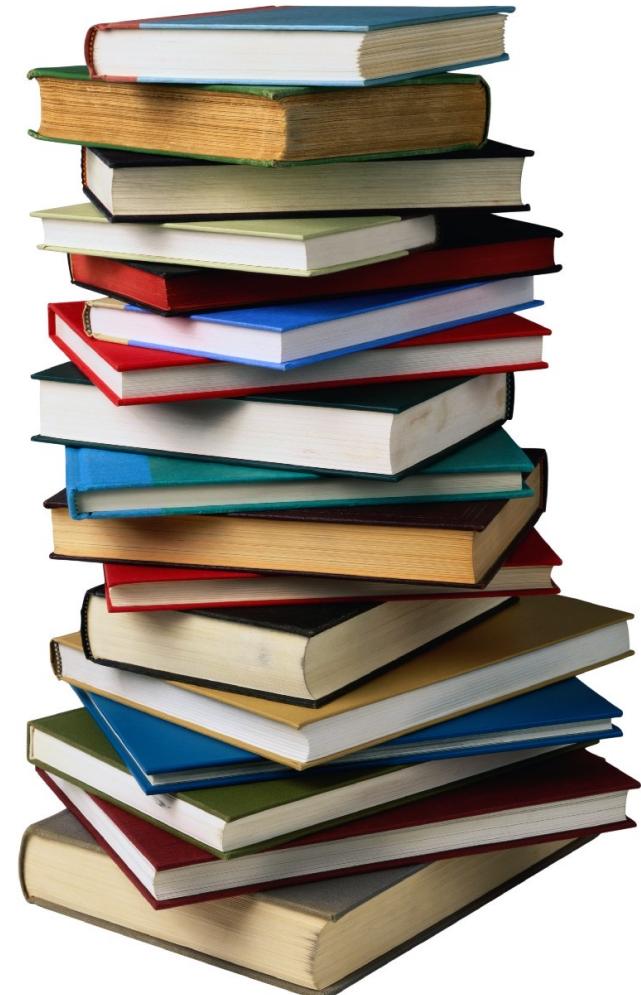
# Black Hat vs White Hat

- Lo scopo del corso è formare esperti in grado di fronteggiare gli attacchi e **proteggere** i sistemi informatici e le reti, non quello di attaccarli e violarne l'integrità e la sicurezza
- Esiste una grande **domanda** di **professionisti** in grado di difendere le infrastrutture e **combattere** il crimine informatico, rintracciando le origini e i colpevoli dei reati relativi
- E', come sempre, una **scelta di campo...**



# Testi di Riferimento

- “Security in Computing”, 4th ed., Charles P. Pfleeger, Shari Lawrence Pfleeger; Prentice Hall, 2007
- “Security Engineering”, 2nd ed., Ross Anderson; Wiley, 2008.
- “Network Security - Private Communication in a Public World”, Charlie Kaufman, Radia Perlman and Mike Speciner, 2nd Edition, Prentice Hall, 2002.
- “Cryptography and Network Security”, William Stallings, 5th Edition, Prentice Hall, 2011.
- “Firewalls and Internet Security: Repelling the Wily Hacker”, 2nd edition, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, Addison Wesley, 2003.



# Di cosa parliamo?

**cybersecurity** = Sicurezza del cyberspazio



# Di cosa parliamo?

**cybersecurity** = Sicurezza del cyberspazio

Insieme dei sistemi informatici  
e delle reti di interconnessione



# Cyberspazio?

- Alessandro Baricco lo ha definito l'*oltremondo*
- L'opera più *complessa* che l'uomo abbia mai realizzato:
  - unione di milioni di reti
  - stratificazioni di programmi e protocolli software
  - eterogeneità di dispositivi e terminali
- La complessità *genera vulnerabilità*
- Come nel mondo reale, nel cyberspazio tali vulnerabilità possono essere sfruttate per lanciare *attacchi*
- Questi attacchi possono coinvolgere il cyberspazio, ma anche il *mondo reale*!!



# Di cosa parliamo?

**cybersecurity** = Sicurezza dei sistemi  
informatici e delle reti di interconnessione



# Di cosa parliamo?

**cybersecurity** = Sicurezza dei sistemi  
informatici e delle reti di interconnessione

+ con lo scopo di proteggerne  
operatività ed assets strategici



# Di cosa parliamo?

**cybersecurity** = Sicurezza dei sistemi informatici e delle reti di interconnessione con lo scopo di proteggerne operatività ed assets strategici



# Di cosa parliamo?

**cybersecurity** = Sicurezza dei sistemi  
informatici e delle reti di interconnessione  
con lo scopo di proteggerne operatività ed  
assets strategici



In caso di attacchi,  
incidenti o generici  
guasti/indisponibilità

# Di cosa parliamo?

**cybersecurity** = Sicurezza dei sistemi informatici e delle reti di interconnessione con lo scopo di proteggerne operatività ed assets strategici in caso di attacchi, incidenti o generici guasti/indisponibilità



# Di cosa parliamo?

**cybersecurity** = Sicurezza dei sistemi informatici e delle reti di interconnessione con lo scopo di proteggerne operatività ed assets strategici in caso di attacchi, incidenti o generici guasti/indisponibilità

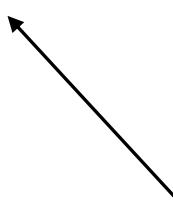
+ e garantire disponibilità, affidabilità, integrità e privatezza/secrezione delle trasmissioni e dei contenuti

# I tre pilastri della cybersecurity

- **Riservatezza/Confidenzialità**
  - Garantire che specifiche informazioni/risorse siano accessibili solo a soggetti autorizzati
- **Integrità**
  - Garantire che determinate informazioni/risorse non siano state modificate/manipolate o danneggiate/distrutte
- **Disponibilità**
  - Gli utenti legittimi hanno sempre accesso a determinate informazioni/risorse quando necessario

# I tre pilastri della cybersecurity

- **Riservatezza/Confidenzialità**
  - Garantire che specifiche informazioni/risorse siano accessibili solo a soggetti autorizzati
- **Integrità**
  - Garantire che determinate informazioni/risorse non siano state modificate/manipolate o danneggiate/distrutte
- **Disponibilità**
  - Gli utenti legittimi hanno sempre accesso a determinate informazioni/risorse quando necessario



Copre tre aree correlate:

- **Dati**
  - Protezione dei contenuti
- **Individui (Privacy)**
  - Garantisce il controllo degli individui su
    - quali informazioni ad essi relative possono essere raccolte e conservate
    - da chi e a chi possono essere divulgate
- **Organizzazioni (segretezza)**
  - Riguarda la riservatezza per le organizzazioni, come società commerciali o governi

# I tre pilastri della cybersecurity

- **Riservatezza/Confidenzialità**

- Garantire che specifiche informazioni/risorse siano accessibili solo a soggetti autorizzati

- **Integrità**

- Garantire che determinate informazioni/risorse non siano state modificate/manipolate o danneggiate/distrutte

- **Disponibilità**

- Gli utenti legittimi hanno sempre accesso a determinate informazioni/risorse quando necessario

Copre due aspetti correlati:

- **Integrità dei dati:**

- garantisce che le informazioni e i programmi vengano modificati solo in modo specifico e autorizzato

- **Integrità del sistema:**

- garantisce che un sistema esegua le sue operazioni in modo inalterato, libero da manipolazioni non autorizzate

# I tre pilastri della cybersecurity

- **Riservatezza/Confidenzialità**

- Garantire che specifiche informazioni/risorse siano accessibili solo a soggetti autorizzati

- **Integrità**

- Garantire che determinate informazioni/risorse non siano state modificate/manipolate o danneggiate/distrutte

- **Disponibilità**

- Gli utenti legittimi hanno sempre accesso a determinate informazioni/risorse quando necessario

- Assicura che i sistemi funzionino con continuità e il servizio non venga mai negato agli utenti autorizzati.
- La probabilità  $D(t)$  che il sistema funzioni correttamente in un dato istante  $t$  deve tendere a 1

# Riservatezza, autenticità, non ripudio

Legato al concetto di confidenzialità ci sono quelli di:

- **Autenticità o Genuinità**

- proprietà di determinati dati essere stati certamente prodotti da un soggetto e poter essere verificati in qualsiasi momento come tali

- **Fiducia**

- nella validità di una specifica azione, di una trasmissione, di un messaggio o del mittente del messaggio.

- **Non ripudiabilità**

- Protezione contro un individuo che nega falsamente di aver compiuto una specifica.

Implica la capacità di determinare in maniera certa se un determinato individuo ha intrapreso un'azione particolare come la creazione di informazioni, l'invio di un messaggio, l'approvazione di informazioni o la ricezione di un messaggio.

# Disponibilità e Resilienza

Legato al concetto di disponibilità c'è quello di resilienza, legato alla capacità di un sistema informativo di continuare a:

- operare in condizioni avverse o di stress, anche se in uno stato di operatività degradata o parziale, pur mantenendo le capacità operative essenziali;
- recuperare operatività efficace in un arco di tempo coerente con le esigenze della propria missione;

La resilienza aiuta un'organizzazione a proteggersi dai rischi, difendersi e limitare la gravità degli attacchi e garantire la sopravvivenza del proprio business nonostante un attacco.

La resilienza è una misura tangibile di quanto bene un'organizzazione può gestire (ovvero prepararsi, rispondere e recuperare) un attacco informatico o una violazione dei dati, pur continuando a svolgere la propria attività in modo efficace.

# Gli elementi da proteggere

- Le persone
- L'ambiente circostante
- Gli oggetti connessi in rete
- I Computers
- Le informazioni memorizzate
- L'intera infrastruttura

# Gli elementi da proteggere

- Le persone
- L'ambiente circostante

*SAFETY*

- Gli oggetti connessi in rete
- I Computers
- Le informazioni memorizzate
- L'intera infrastruttura

Proprietà che riflette la capacità di funzionare, normalmente o in modo anomalo, senza provocare danni alle persone o all'ambiente circostante

# Gli elementi da proteggere

- Le persone
- L'ambiente circostante

*SAFETY*

- Gli oggetti connessi in rete
- I Computers
- Le informazioni memorizzate
- L'intera infrastruttura

*SECURITY*

Proprietà legate alla garanzia disicurezza, in termini di riservatezza, integrità e disponibilità di tutte le risorse di un sistema informativo, inclusi hardware, software, elaborazione, memorizzazione e comunicazione in rete

# Gli elementi da proteggere

- Le persone
- L'ambiente circostante

*SAFETY*

- Gli oggetti connessi in rete
- I Computers
- Le informazioni memorizzate

*SECURITY*

- L'intera infrastruttura

*CYBERSECURITY*

Proprietà che garantisce a un'entità (organizzazione, individuo, nazione) la protezione di tutte le proprie risorse fisiche, le proprie informazioni e infrastrutture dalle minacce che vengono dall'esterno

# Gli elementi da proteggere

- Le persone
- L'ambiente circostante

*SAFETY*

- Gli oggetti connessi in rete
- I Computers
- Le informazioni memorizzate

*SECURITY*

- L'intera infrastruttura

*CYBERSECURITY*



*DEPENDABILITY*

Proprietà di un sistema che consente di fare assoluto affidamento sul servizio fornito. Fa riferimento alla disponibilità, all'affidabilità, alla manutenibilità ed alle prestazioni

# Dependability: concetti di base

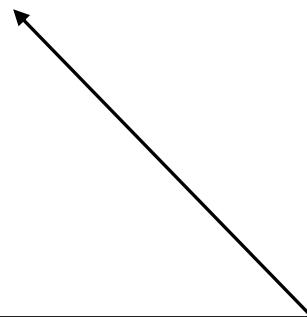
Una visione sistematica del concetto di dependability consta di tre componenti:

- le minacce
- gli attributi
- Gli strumenti attraverso cui si ottiene

# Dependability: concetti di base

Una visione sistematica del concetto di dependability consta di tre componenti:

- le minacce
- gli attributi
- Gli strumenti attraverso cui si ottiene



Circostanze indesiderate che portano alla perdita di affidabilità (non è possibile o non sarà più possibile fare affidamento sul servizio)

# Dependability: concetti di base

Una visione sistematica del concetto di dependability consta di tre componenti:

- le minacce
- gli attributi
- Gli strumenti attraverso cui si ottiene

Proprietà attese del sistema in base alle quali viene valutata la qualità del servizio offerto in base alle minacce potenziali e alle modalità di contrastarle

# Dependability: concetti di base

Una visione sistematica del concetto di dependability consta di tre componenti:

- le minacce
- gli attributi
- Gli strumenti attraverso cui si ottiene

Metodi e tecniche che consentono di fornire un servizio su cui fare affidamento ed avere adeguata fiducia nelle sue capacità

# Requisiti di dependability contrastanti

## Requisito di Safety

- Apertura delle porte in caso di capovolgimento vettura

## Soluzione

- Sensori di pressione sul tetto dell'auto

## Conseguenze in termini di Security

- Basta saltare sul tetto per causare l'apertura delle porte



# I contesti di interesse

**A livello utente** = cybersecurity nel contesto dei singoli soggetti connessi alla rete

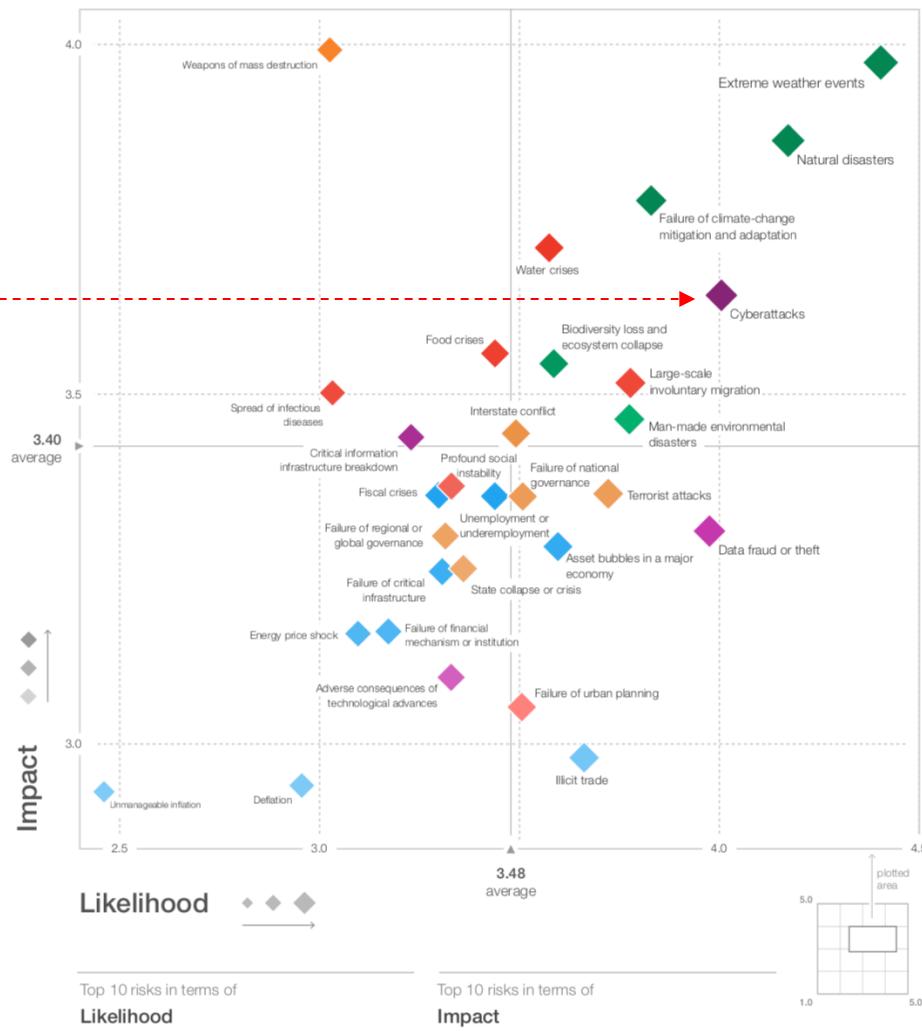
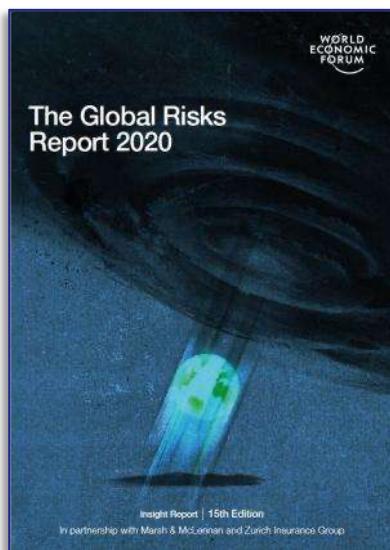
**A livello Corporate/Enterprise** = cybersecurity nel contesto delle singole organizzazioni/strutture (aziende, enti statali, associazioni, etc.)

**A livello nazionale** = cybersecurity come asset strategico a livello di intere nazioni o aggregati di nazioni o stati (es. EU, USA, etc.)

# Cybersecurity: un rischio globale

Figure I: The Global Risks Landscape 2018

Rischio di  
Attacchi cyber



- Fonte: world Economic Forum: The Global Risks Report 2020 15th Edition

# Il primo oggetto da proteggere: la rete

- Negli ultimi anni la rete è diventata elemento **strategico** per il **business** e strumento **essenziale** in tutte le attività lavorative e sociali
- In poche parole, la connettività in rete ha acquisito un valore **irrinunciabile** per tutte le istituzioni pubbliche o private nonché per le imprese

- **e-commerce**
- **e-banking**
- **e-procurement**
- **e-health**



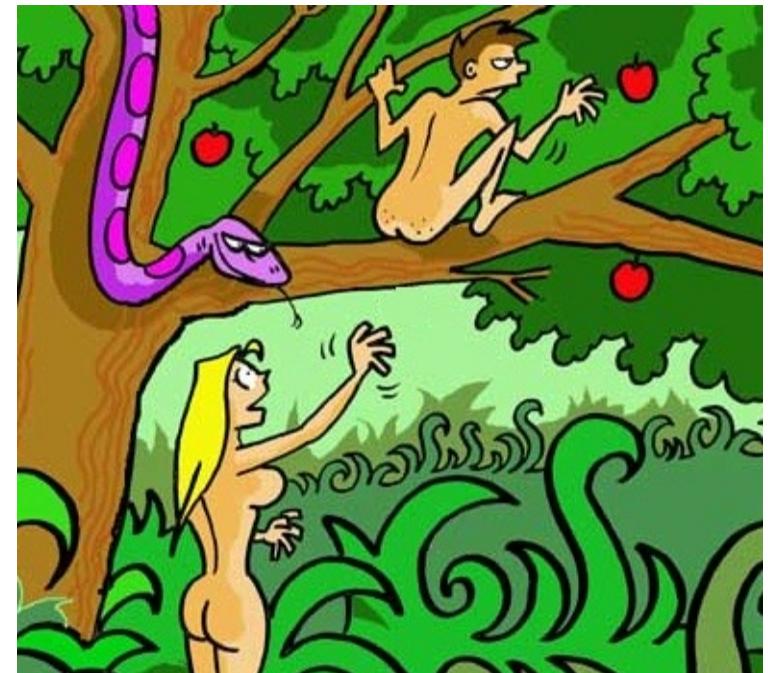
# Che succederebbe...

- ...senza Internet
  - Per un giorno intero
  - .. Oppure un mese
- No e-Mail
- No Internet Mobile
- No eCommerce – eBanking, etc.
- No social networks, chat etc.
- No telefonia, videoconferenza etc.!!



# Il peccato originale

- Internet è un'infrastruttura critica ma il suo modello di sicurezza di base **è cambiato molto poco** a partire dalle origini (anni 70).
- L'architettura di Internet è stata inizialmente concepita per garantire un alto livello di affidabilità ma ben **poco interesse** è stato dedicato alla sicurezza
- Stiamo utilizzando una tecnologia **vecchia** di **35-40** anni che non è nata per garantire la **sicurezza** di transazioni **mission-critical**.



# Le debolezze di Internet

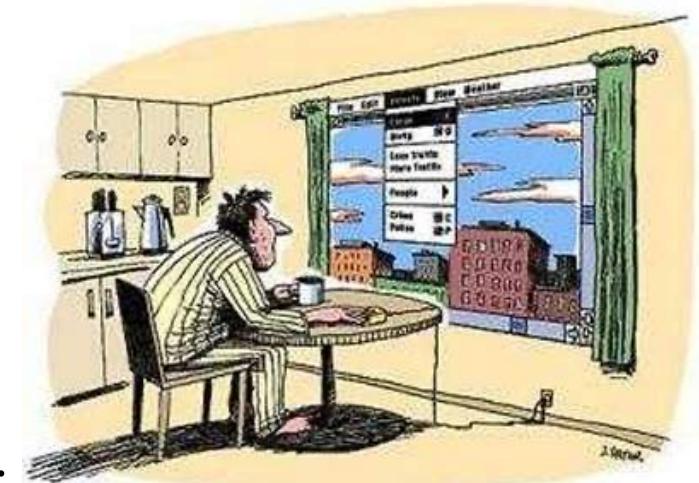
- **Non è strutturata**, essendo costituita da un mesh di interconnessioni ad hoc
- **Non esiste un' autorità centrale** di controllo né **un controllo centralizzato** o distribuito delle connessioni
- Non è fattibile **un tracciamento “sistematico”** delle stesse
- Perimetri di elevatissime dimensioni sono praticamente **impossibili da controllare e spesso rilassati**
- La rete è ormai **“porosa”** o meglio **“borderless”** grazie alla coesistenza di tecnologie di connettività wireless eterogenee



# ...e le bad practices degli utenti

"La sicurezza si misura nel suo anello più debole"

- utilizzo di post-it per ricordarsi le **password**
- **aggirare** le misure di sicurezza (es. Disattivazione antivirus)
- lasciare i sistemi/documenti "**unattended**"
- aprire **e-mail attachment**
- utilizzo di password **banali**
- **discorsi riservati** in aree/locali pubblici
- applicazione **poco rigorosa** delle policy
- sottovalutazione dello staff (**insider attacks**)
- **lentezza o inerzia** nell'update dei sistemi (patch)

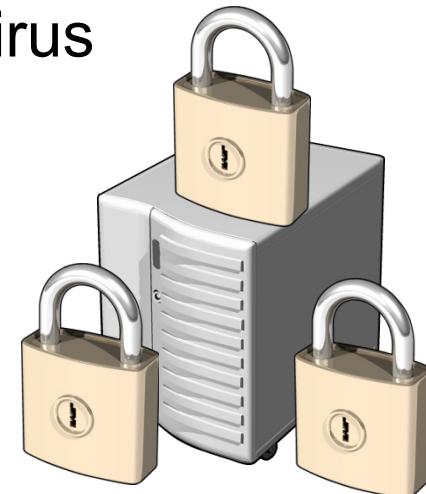


# L'illusione della “personal security”!

Con l'emergere della connettività personale ovunque si sta affermando un'approccio individualistico alla security:

- Devo evitare che la **mia** macchina venga compromessa
- Devo tutelare la privacy dei **miei** dati sensibili
- Devo evitare che il **mio** Hard Disk venga cancellato
- Devo proteggere la **mia** macchina dai virus

Tale approccio è **PERICOLOSISSIMO**  
perché spesso vanifica qualsiasi ottica  
di cooperazione!



# Ma è una contraddizione!

- Internet è nata come un'infrastruttura ad uso della collettività e deve il suo enorme successo al suo essere mezzo di **aggregazione globale** cresciuto in una logica **di collaborazione e interscambio** del transito
- In un modello di aggregazione così complesso, nessuna entità o insieme di entità può essere **completamente autosufficiente** e di conseguenza bastare del tutto a se stessa
- Di fronte a buona parte delle moderne minacce alla network security l'unica logica vincente è quella dell' **interscambio continuo di informazioni e della mutua cooperazione per tracciamento, filtraggio etc.**



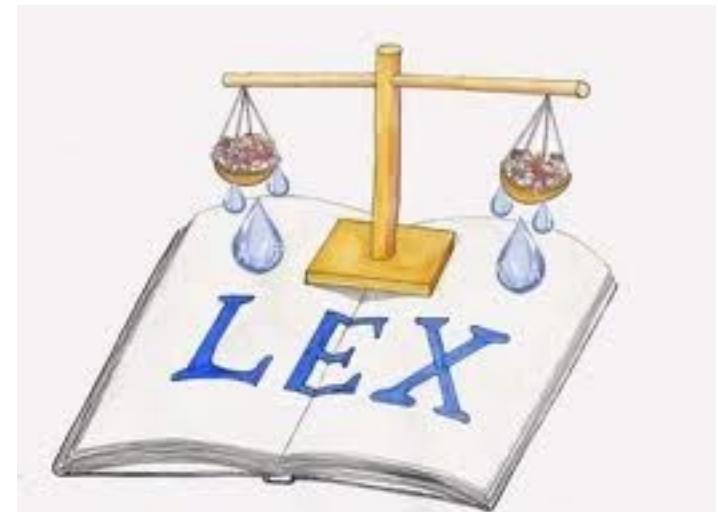
# Il problema della cooperazione

- Grande quantità di providers di fatto **disinteressati** al problema e a collaborare
- **Disattenzione** agli elementi legislativi locali e internazionali
- Complessa mediazione con **altri paesi** e **altre culture**
- Esistenza di **elementi non sorvegliati** nella catena internazionale
- Problemi **legislativi**: ciò che è illegale da noi potrebbe non esserlo altrove



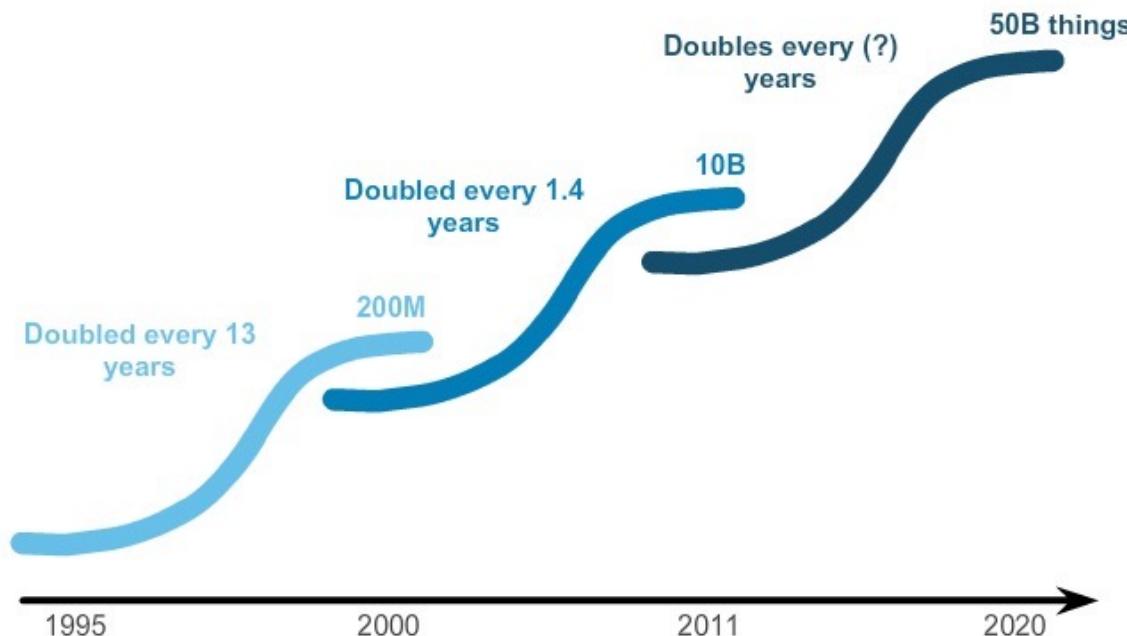
# Difficoltà normative...

- La legislazione Italiana, dal 1993, ha introdotto tutta una serie di dispositivi che contemplano il crimine cosiddetto informatico.
- L'approccio iniziale è stato di tipo evolutivo, ovvero si è basato sulla modifica di leggi esistenti ricollegando reati "tradizionali" ai nuovi possibili basati su strumenti informatici
- Non è facile in uno scenario così complesso e in continua evoluzione contemplare tutte le possibili situazioni



# Le dimensioni del problema

"Fixed" Computing (You go to the device)	Mobility/BYOD (The device goes with you)	Internet of Things (Age of Devices)	Internet of Everything (People, Process, Data, Things)
---	--	--	---



- Dispositivi attualmente in rete: **19 Miliardi**
- Entro 5 anni: **50 Miliardi**
  - Di cui meno della metà legati direttamente ad attività umane
  - I rimanenti legati alla “Internet delle cose”

# Nuovi oggetti da proteggere

- Consumer electronics: TV, Microwaves, GPS
- Office electronics: Copier, Printer
- Finance: ATM
- Phone, PBX, IP Phone
- Surveillance Cameras
- Automobile
- Medical
- Software Programmable Radios



# ... con il loro valore

- Furti tradizionali e di identità via Copia e Spoofing di RFID, TAG e oggetti “passivi”



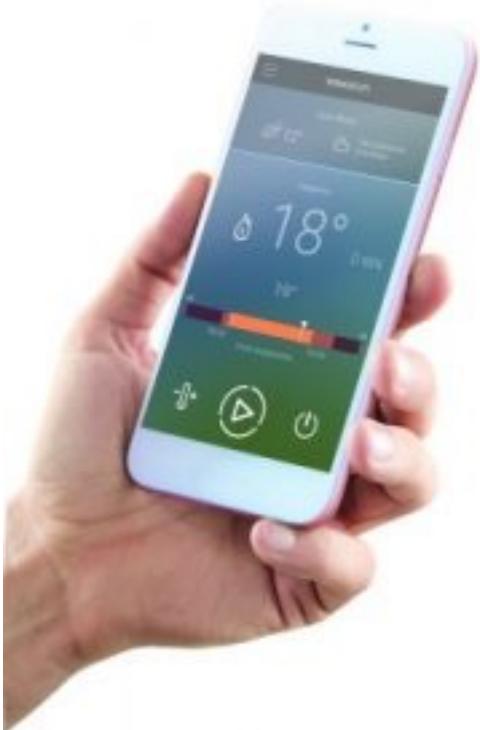
)) NFC ))



Apple Pay



# Oggetti che portiamo addosso...

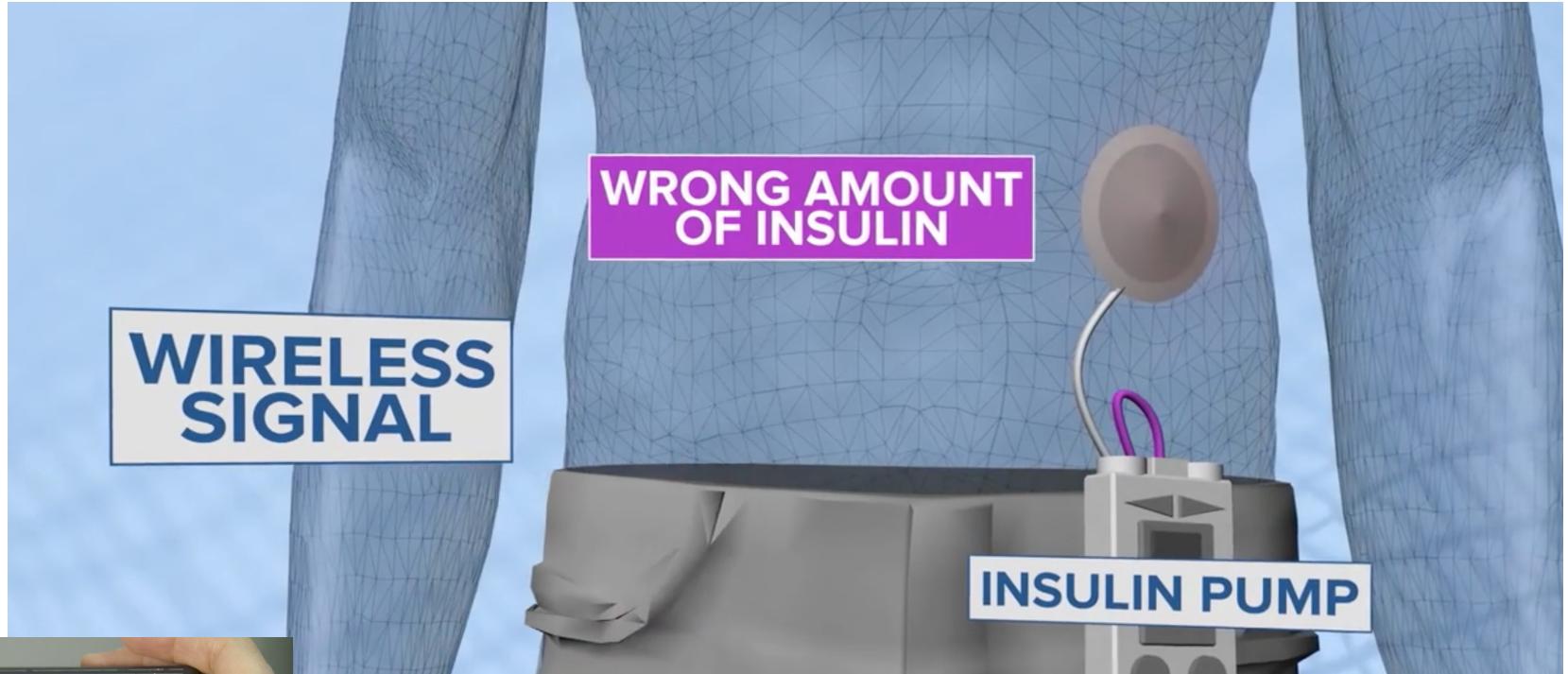


# O anche in sala operatoria...

- Google glasses per supportare gli interventi attraverso la realtà aumentata
- Da Vinci, pilotato da remoto attraverso la rete



# Che spesso diventano vitali...

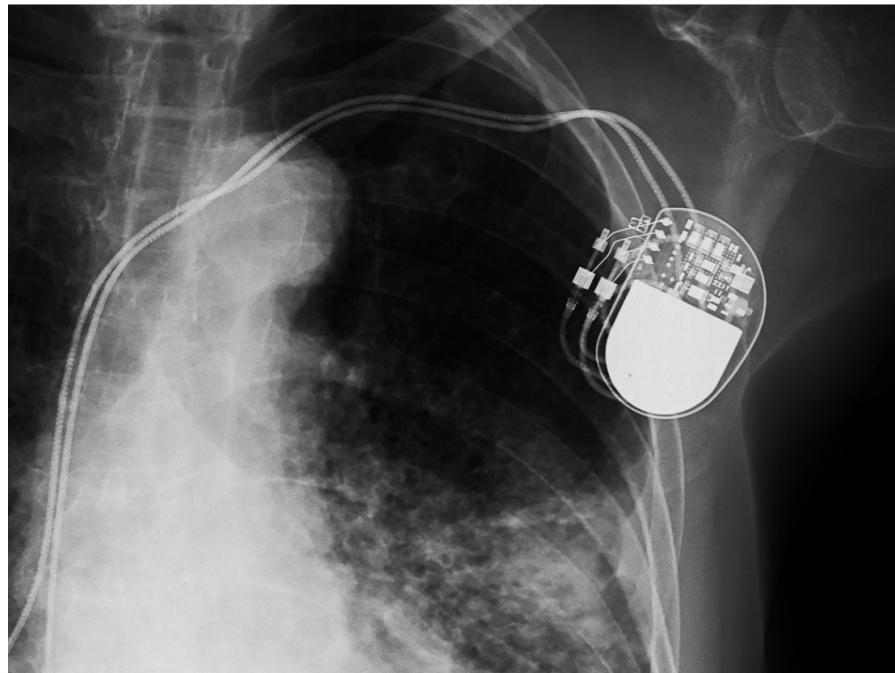


# E attaccabili...

LILY HAY NEWMAN SECURITY 08.09.18 12:30 PM

## A NEW PACEMAKER HACK PUTS MALWARE DIRECTLY ON THE DEVICE

WIRED



AUGUST 4-9, 2018  
MANDALAY BAY / LAS VEGAS

### Understanding and Exploiting Implanted Medical Devices

Billy Rios | Founder, Whitescope

Jonathan Butts | CEO, QED

**Location:** South Seas ABE

**Date:** Thursday, August 9 | 3:50pm-4:40pm

**Format:** 50-Minute Briefings

**Tracks:** Hardware/Embedded, Internet of Things

# Nuovi obiettivi: la minaccia cyber-fisica



## Important Cybersecurity Advisory

Information About Cybersecurity Firmware Update for Acurit™/Acuris™, Awest 2002™, Awest 3000™, Awest 5000™, and Awest 7000™ devices.

28 August, 2017

Dear Doctor:

We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency (RF) communications (i.e., Awest™/Acuris™, Awest 3000™, Awest 5000™, Awest 7000™, and Awest 2002™). This firmware update provides an additional layer of security against unauthorized access to these devices that further reduces the potential for a successful cybersecurity attack.

This release is part of planned system updates that began with the January 2017 Merlin@Home™ v8.2.2 software. The update contains a software release for Merlin™ programmers (version 23.1.1) including data encryption, operating system patches, and disabling network connectivity features in addition to the firmware update.

Each pacemaker manufactured beginning August 28, 2017 will have this update pre-loaded in the device and these devices will not need to be updated.

The information provided below is intended to assist doctors and patients in understanding the cybersecurity vulnerability, the firmware update, and associated benefits and risks.

### Reputation of Cybersecurity Vulnerability and Associated Risks

We have received no reports of deliberate compromise related to the cybersecurity vulnerabilities in the implanted devices impacted by this communication. According to the Department of Homeland Security, compromising the security of these devices would require a highly complex attack. If there were a successful attack, an unauthorized individual (i.e., a 'scripter' attacker) could gain access and issue commands to the implanted medical device through radio frequency (RF) transmission capability, and these unauthorized commands could modify device settings (e.g., stop pacing) or impact device functionality.<sup>(1)</sup>

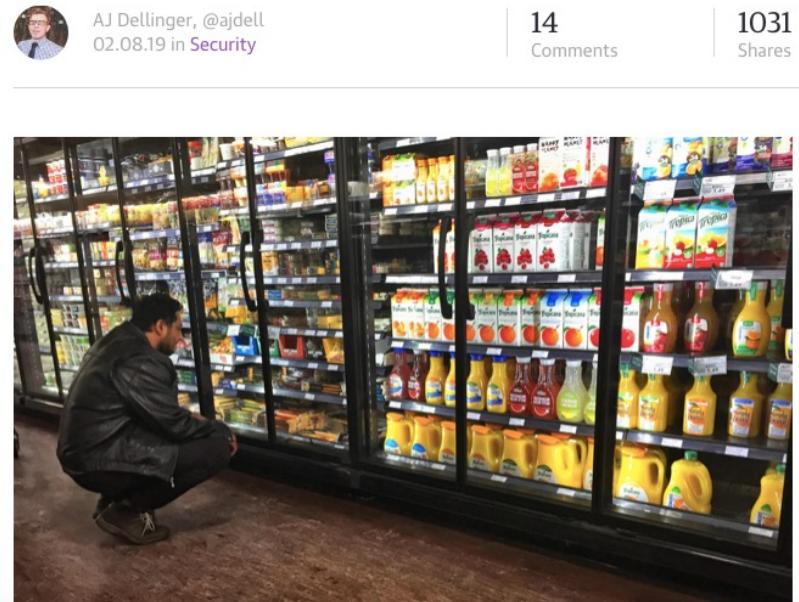
<sup>(1)</sup> Refer to the ICSI-CERT Communication XDRM-17-243-01 Abbott Laboratories Awest/Acuris Awest 2002/Awest 3000/Awest 5000/Awest 7000 Pacemaker Vulnerabilities.

- Nell'agosto 2017 Abbott ha lanciato una campagna di richiamo per 450.000 defibrillatori impiantati
- A seguito della scoperta di una vulnerabilità è stato necessario aggiornare il firmware di tutti i dispositivi installati nei pazienti
- Sfruttando questa vulnerabilità un attaccante avrebbe potuto prendere il controllo remoto del defibrillatore e riprogrammarlo...

# Obiettivi che non ci si aspetterebbe...

## Networked freezers at grocery stores are vulnerable to hacking

Default passwords make it easy to hijack the appliances.



Cookies on Forbes

- Milano: hacking logica di controllo via RF di una gru industriale
- Termostati di freezers con default password su Shodan

Forbes

Billionaires   Innovation   Leadership   Money   Consumer   Industry

36,208 views | Jan 15, 2019, 08:00am

## Exclusive: Hackers Take Control Of Giant Construction Cranes



Thomas Brewster Forbes Staff

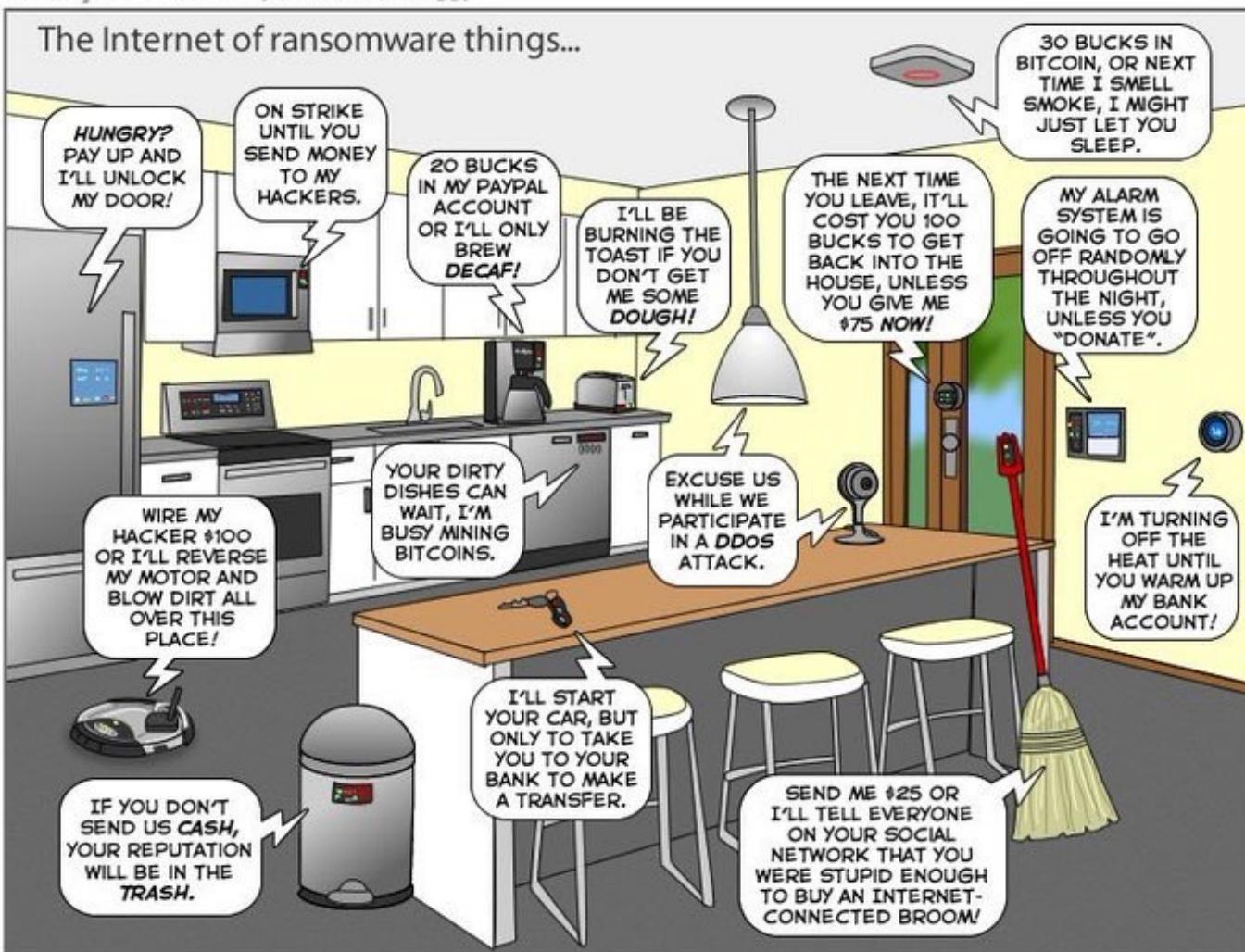
Cybersecurity

I cover crime, privacy and security in digital and physical forms.



# The Internet of Ransomware Things

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!  
[www.patreon/joyoftech](http://www.patreon/joyoftech)

[joyoftech.com](http://joyoftech.com)

# Reperire le risorse: Motori di Ricerca IoT

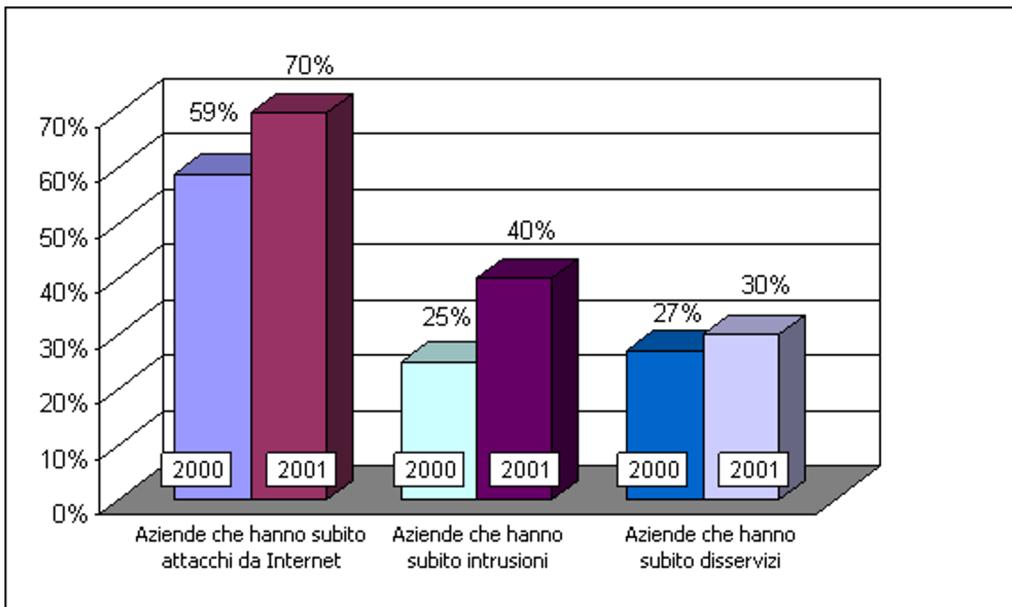
## Shodan

The screenshot shows the Shodan search engine homepage. At the top, there's a navigation bar with links like Google Scholar, Library Genesis, Google, Scopus - Author search, Google Maps, YouTube, Wikipedia, UniCredit Ban...Credit Banca, Notizie, I più conosciuti, Research, IXP, Traduci, Login / Sign Up, and Menu. Below the navigation is a search bar with fields for 'What?' and 'Where?'. The main content area features a large globe with numerous red dots representing discovered devices, with some coordinates labeled (e.g., 67.20, 69.165, 50.67, 75.184). To the left of the globe, there's a section titled 'The search engine for Security' with a sub-section 'Explore the Internet of Things' and a 'Monitor Network Security' section. To the right of the globe, there's a section titled 'See the Big Picture' and another titled 'Get a Competitive Advantage'. At the bottom, there are two blue boxes: one for '56% of Fortune 100' featuring a building icon, and another for '1,000+ Universities' featuring a graduation cap icon. A footer note at the very bottom states: 'Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.'

The screenshot shows the Thingful search engine homepage. At the top, there's a navigation bar with links like Google Scholar, Library Genesis, Google, Scopus - Author search, Google Maps, YouTube, Wikipedia, UniCredit Ban...Credit Banca, Notizie, I più conosciuti, Research, IXP, Traduci, Login / Sign Up, and Menu. Below the navigation is a search bar with fields for 'What?' and 'Where?'. The main content area features a large globe with various icons representing different IoT objects: a car, a person, a camera, a weather station, and a power plant. The text 'A Search Engine for the Internet of Things' and 'Interoperability for connected objects around the world' is displayed above the globe. To the right of the globe, there's a section titled 'Thingful makes the promise of IoT a reality' with a sub-section 'Thingful is built for real-world problems that exist today. Legacy systems need to interoperate with modern deployments but connected objects like smart meters, cars, mobile phones, weather stations, smart homes & building management systems are spread across thousands of different networks'. At the bottom, there's a large 'Thingful' logo.

# Altri numeri

## (Fonte CSI/FBI)



Gli attacchi hanno successo anche se le aziende sono dotate di sistemi di sicurezza:

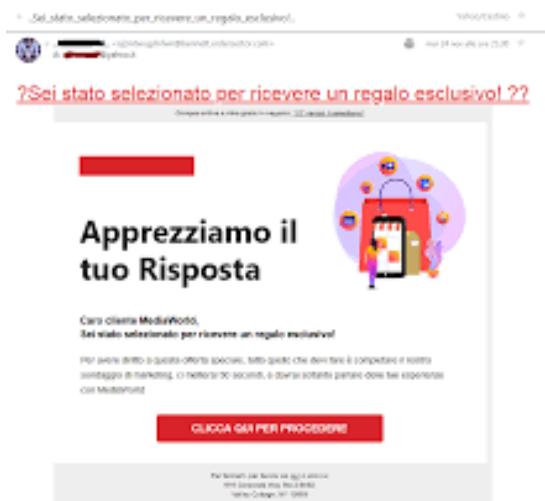
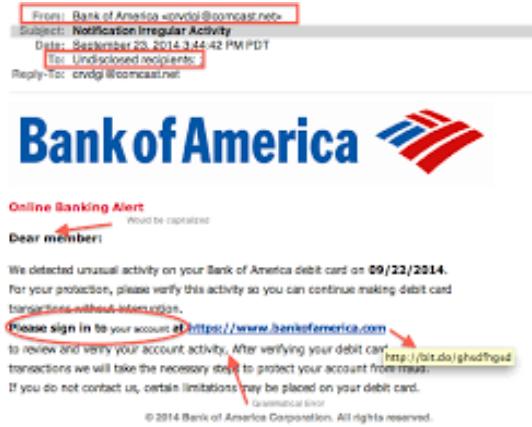
- il 95% possiede un Firewall,
- il 61% un IDS,
- il 90% un sistema di AAA
- il 42% certificati digitali

Fonte: CSI/FBI Computer Crime and Security Survey

Un nuovo server collegato ad Internet senza tutte le patch di sicurezza disponibili **ha meno del 20% di probabilità di superare le tre settimane di vita** senza essere stato attaccato e violato in qualche modo.

# Gli attacchi

Attività ostili nei confronti di una componente nel cyberspazio, spesso compiute sfruttando le debolezze della componente umana.



# Attacchi: strumenti, obiettivi e motivazioni



Malware  
phishing

Web attack  
Vulnerabilità

DDoS  
botnet



**Monetizzare**



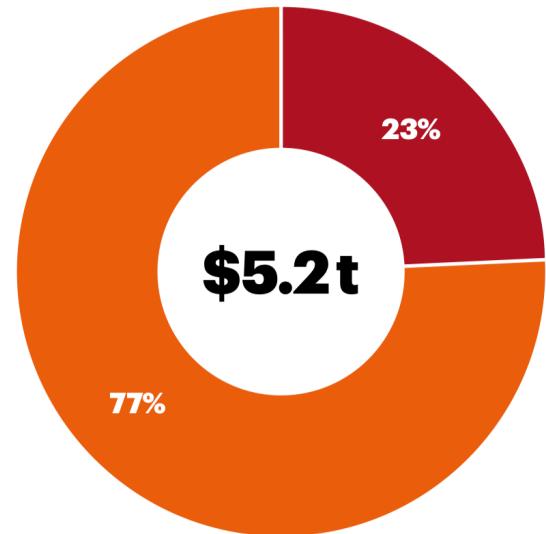
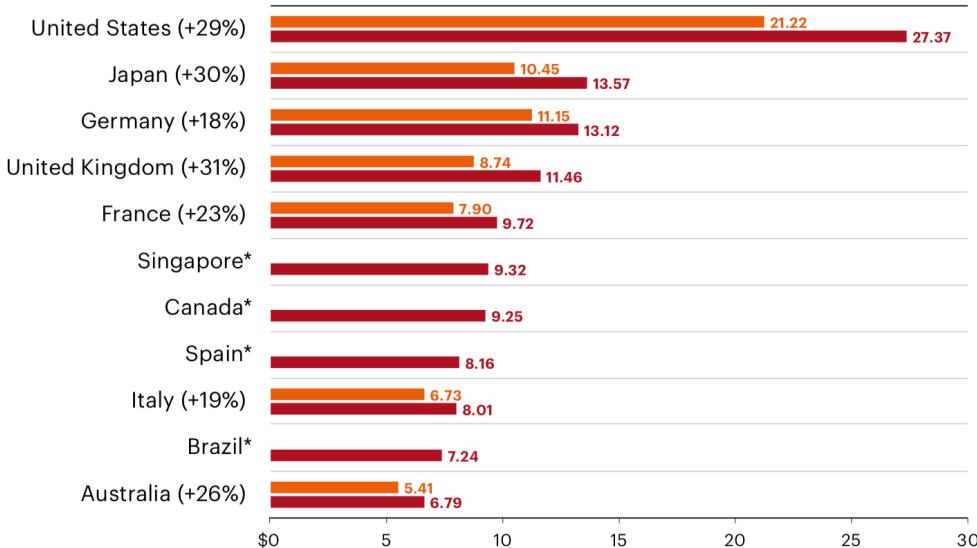
Esfiltrare  
db, credenziali, carte...

Estorcere  
ransomware, ddos, breach...

Creare Botnet  
zombie

# Impatto economico e valore a rischio

The average annual cost of cybercrime by country



Fonte: Accenture - ANNUAL COST OF CYBERCRIME STUDY

# I costi associati alle minacce

## Social Engineering (Phishing)



## Vulnerability Exploit



## Infezioni Malware



### Le battaglie perse

- Inevitabilità degli errori umani
- Nuove vulnerabilità emergono di continuo in sistemi ed applicazioni
- 85% delle nuove violazioni non rilevate<sup>2</sup>
- Le infezioni si propagano rapidissime
- Le contromisure richiedono troppo tempo

**Seri dubbi sulla sostenibilità di un tale trend**

## Attuazione Di frodi



## Perdite economiche



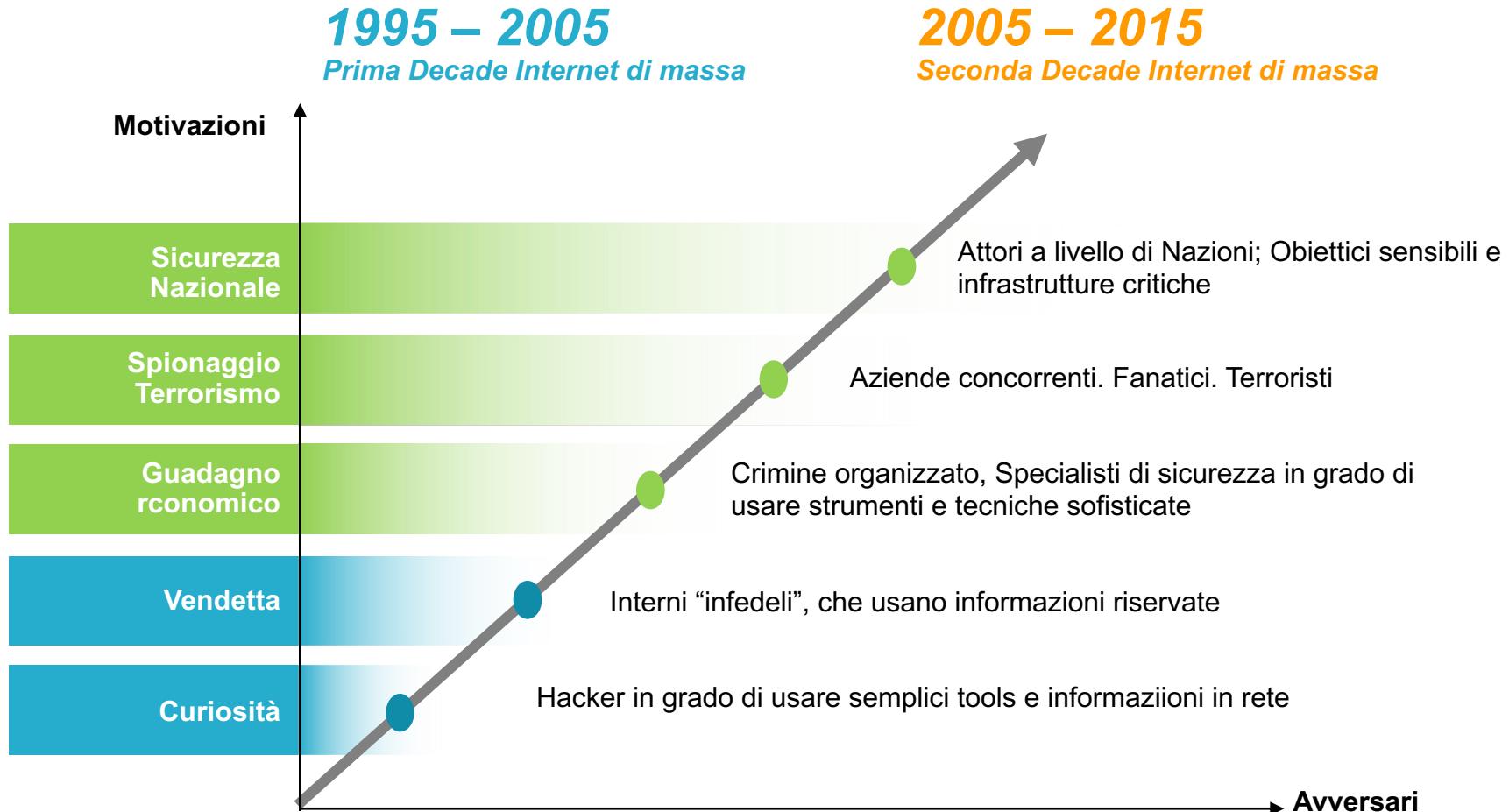
## Furto di Dati

## Siti compromessi

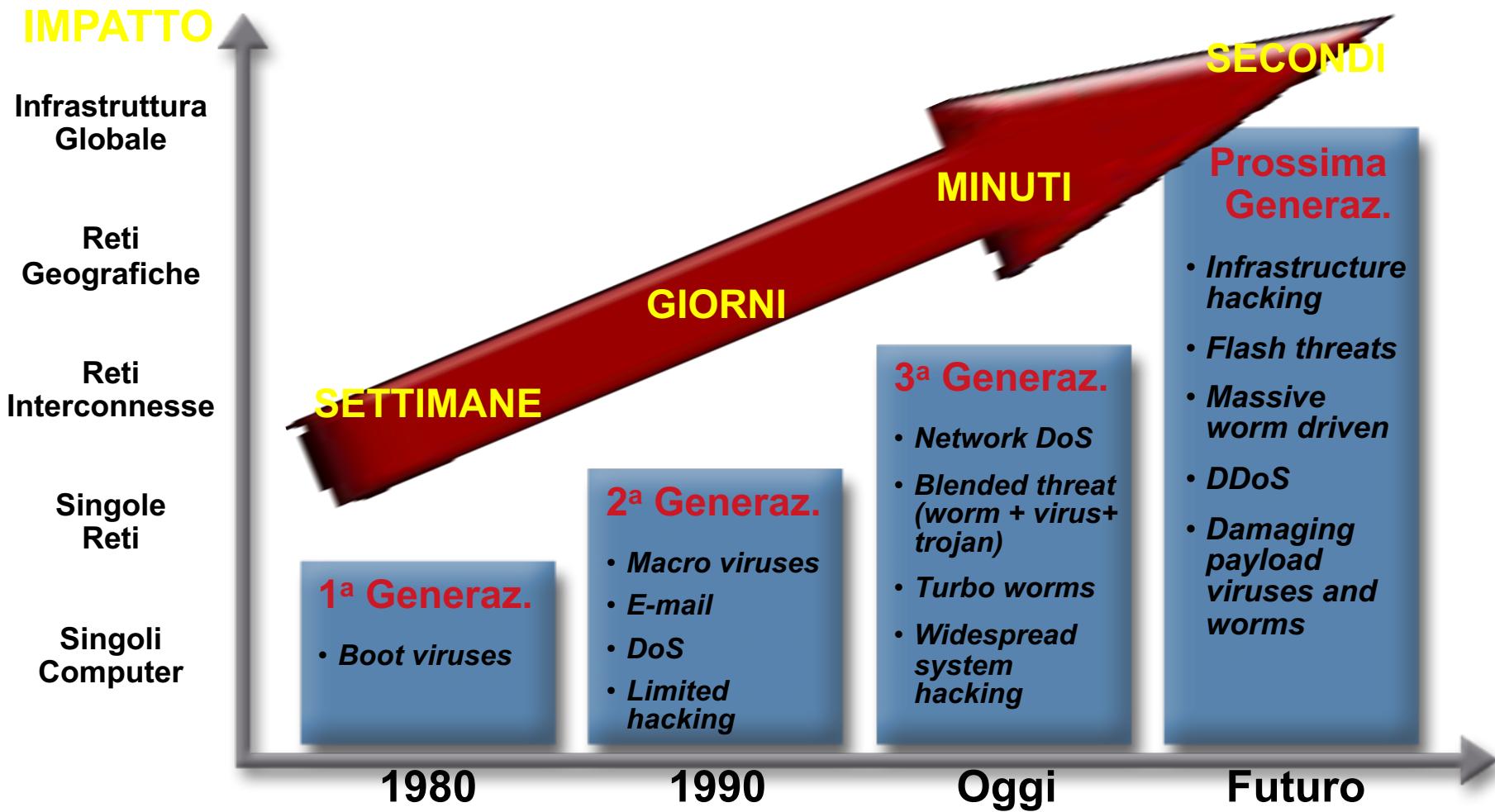
### I costi

- **\$3.4B:** perdite per frodi anno<sup>1</sup>
- **\$8.9M:** costo medio di un attacco<sup>3</sup>
- **\$18B:** Mercato della security
  - tasso di crescita : 12/15% anno
- **\$50B:** Danni complessivi da violazioni
  - tasso di crescita : 45% anno

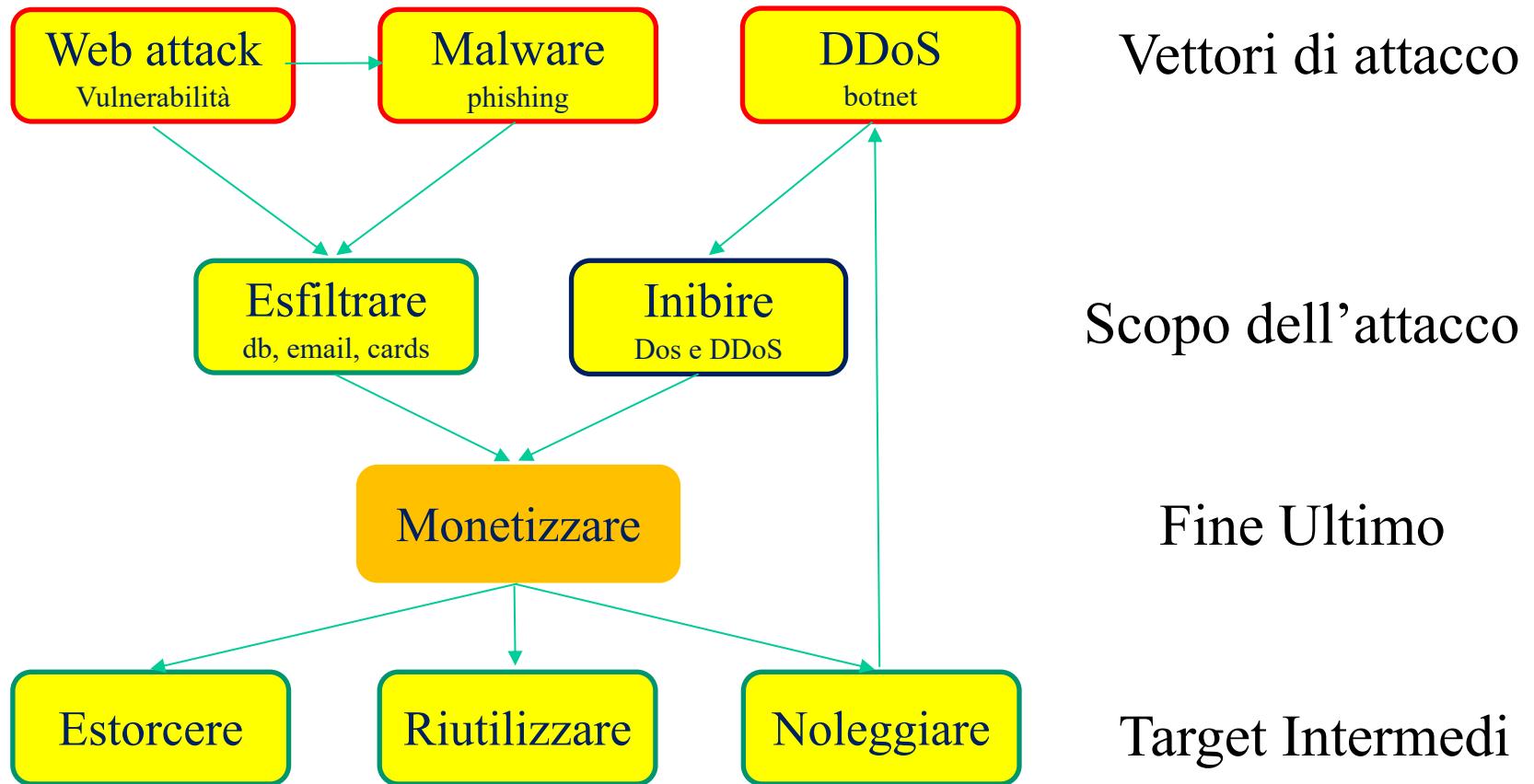
# Obiettivi e motivazioni degli attacchi



# Evolvono strumenti e dinamiche



# Gli attacchi: flusso operativo



# I soggetti coinvolti

## Le vittime ↴

- Scelte o casuali
- Sistemi informatici **esposti** e **vulnerabili**
- Personale **non** adeguatamente preparato
- Eventi di interesse **nazionale**

### Vittime selezionate

- Target mirato
- Selezione per brand e per categoria

### Vittime casuali

- Non esiste un target specifico
- Attacchi massivi

## Gli attaccanti ↴

- Criminali di strada, **assoldati** o in **autonomia**, singoli o in gruppo
- Hacktivisti
- Terroristi
- Paesi (ostili?)

Espionage	Sabotage
Suveillance	Warfare



# Gli obiettivi “sensibili”

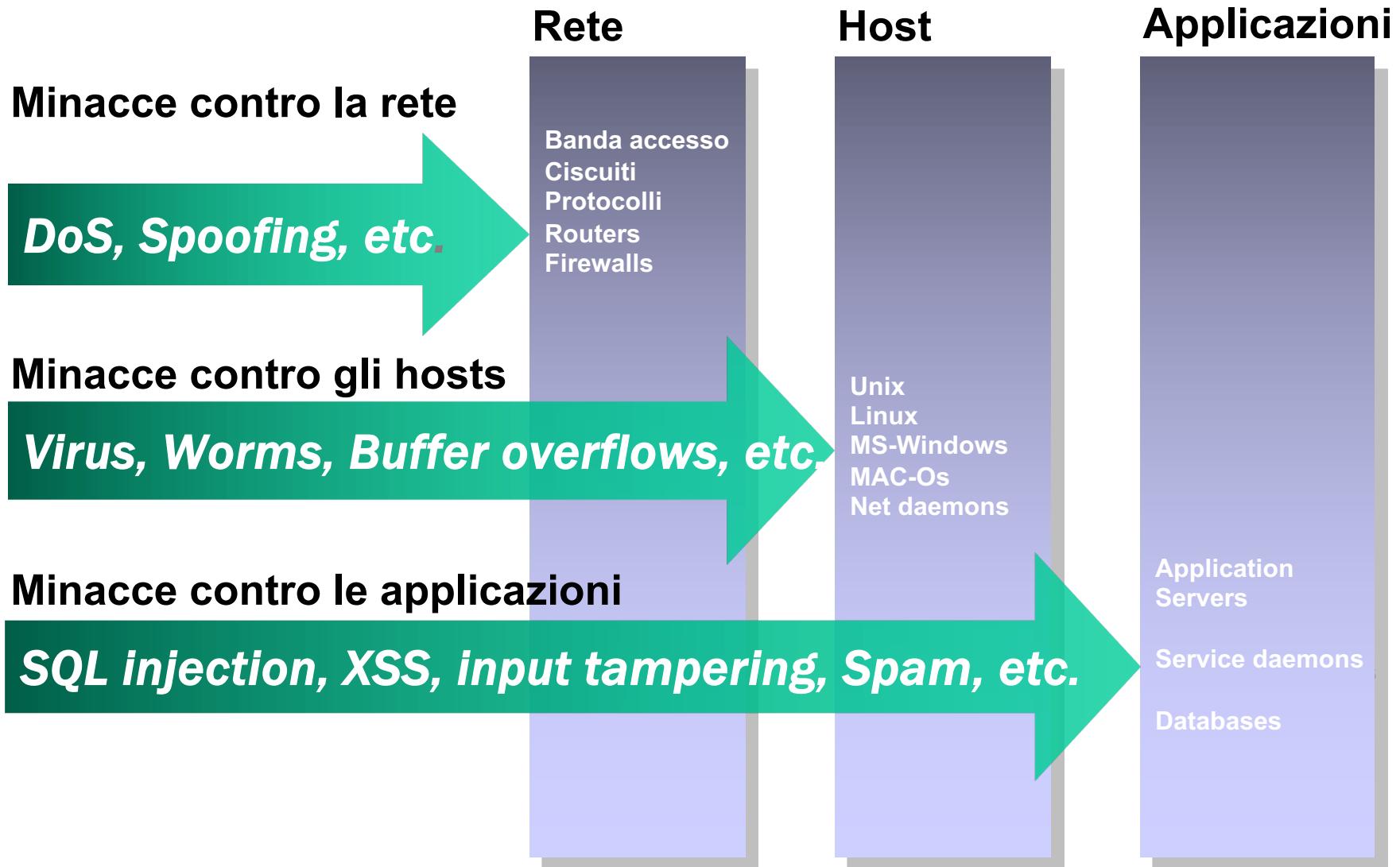
- La stabilità generica della rete: DoS, Worms e Virus
- I grandi portali servizi WWW (governativi, e-business, e-banking, informativi etc.)
- I meccanismi di base dell' infrastruttura Internet
  - DNS (Domain Name System)
  - BGPv4 (Border Gateway Protocol)
  - MPLS e servizi MPLS-based (VPN, FRR etc.)



## I BERSAGLI DIVENTANO

- *Non l'e-economy*
  - *Ma tutta l'economia*
- **Non un settore**
  - **Ma tutti i settori**
- **Non solo le aziende**
  - **Ma tutta la nazione**

# Classificazione delle minacce

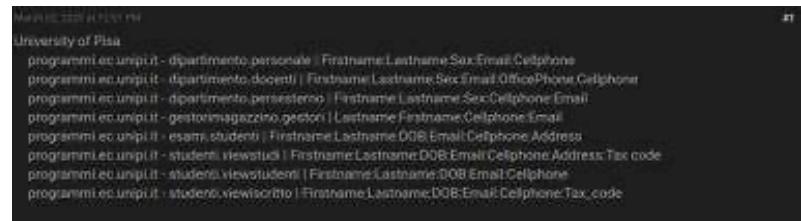
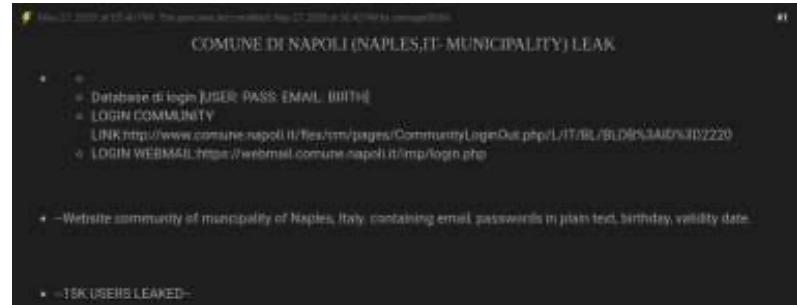


# Data Leaks

- Sono sempre esistiti ma oggi è diventata una moda
- È nato un mercato di nicchia in forte crescita
- I blackmarket sono migrati dal darkweb al deepweb
- Prezzi sempre più accessibili

## Quali dati in vendita?

- Dati anagrafici
- Email
- Credenziali
- Carte di credito



# Data Leaks

Fondazione Arena di Verona - Full dump (100%)

<https://www.arena.it>

● [Arena](#) ● [Cystic Fibrosis](#)

---

## Total Info

---

Phone +39 02 70001111

Fax +39 02 82220000

Email [arena@arena.it](mailto:arena@arena.it)

Address Via Mario Andretti 66 - 35131 Verona

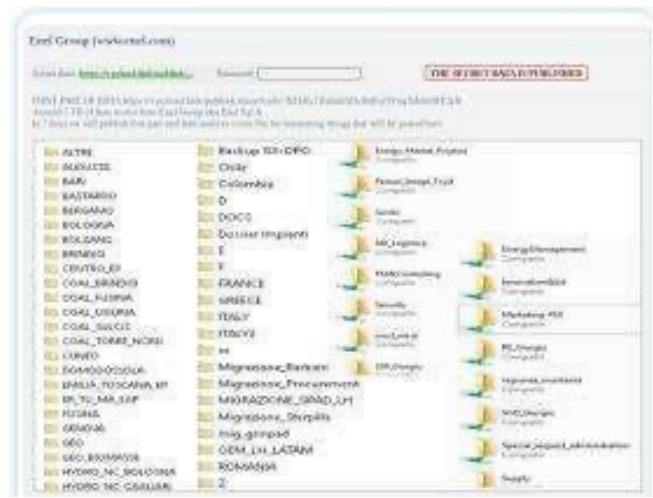
---

## Proofs

---

[Facebook](#) [Twitter](#) [LinkedIn](#) [Instagram](#) [YouTube](#)

Comments 3 | Likes 789 | Posts 11 | 22 | 14 | 18 | 16 | 27 | 21 | 16 | 16 | 21 | 22 | 21 | 24 | 25 | 26 | 27 | 28 | 29 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45



CORPORATE LEAKS

[HOME](#) | [ACTIVE](#) | [FINISHED](#) | [ABOUT](#) | [CONTACT](#)

Printed on MyPrints on 7/20/20 by user\_johnn

LUXOTTICA\_human\_Results\_part\_3.xlsx

LUXOTICA Banking part 4 Heastie

LUXOTICA = core part 5\_emarketing

LUXÓTICA\_other\_part\_1\_Siebert.tif

LUXOTICA Human Resources

LIXOTICA training plan 4.0

LUXOTICA e-commerce 5 star

LUDOTICA. www.juan-luis

Luxottica Group S.p.A. is an Italian e-

company in the eyewear industry.

For a seriously integrated company, it's time to make a serious commitment.

#### 10.3.3.1.2.3.1.1

1930. Larger Upview. Eyed and winged.

Wu, Ray-Chan, Purnell, and Gaskins

Lipottica also makes sunglasses an

Chanel, Prada, Giorgio Armani, But

Burch

In January 2017, Lipotica announced

# Il problema dell'anonimato

- Gli attacchi possono essere celati nascondendosi nell' anonimato dei miliardi di hosts presenti sulla rete
- L'eccesso di informazione disponibile crea disinformazione
- E' quasi impossibile tracciare attacchi intermittenti di breve durata che cambiano spesso origine o hanno origini inattendibili o compromesse



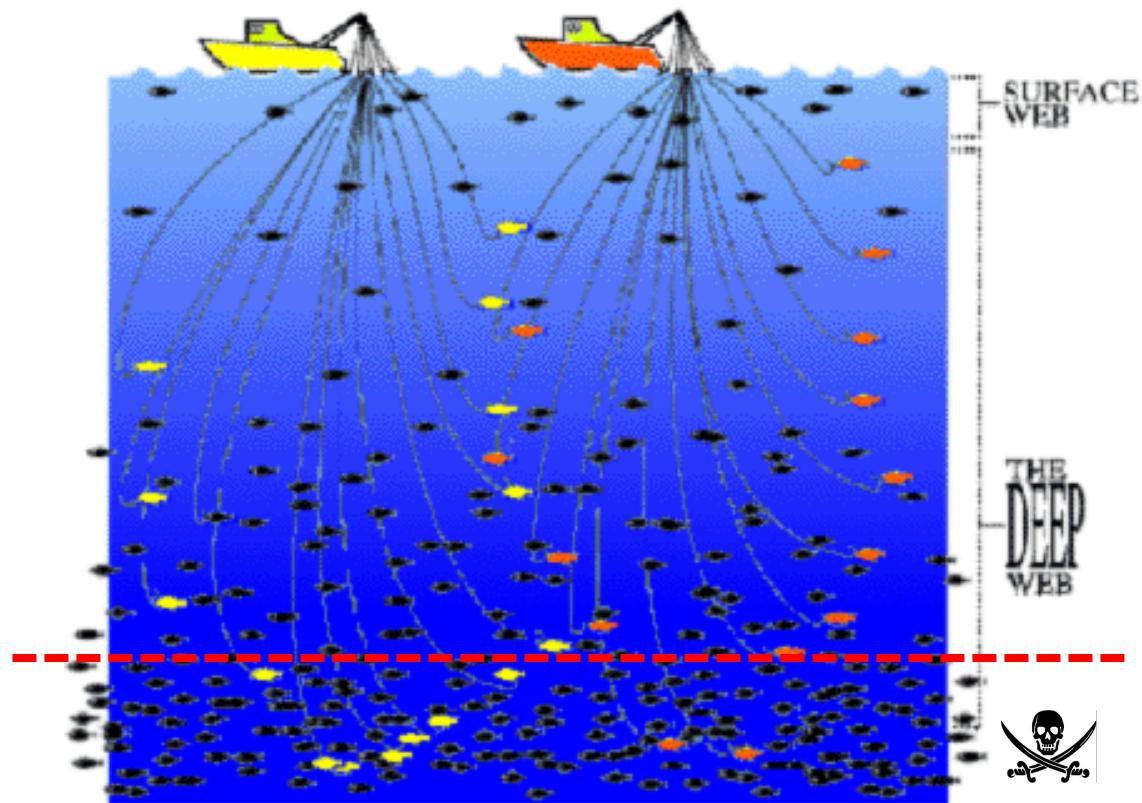
# Anonimato e accessi WiFi

- La diffusione capillare della tecnologia WiFi introduce ulteriori aggravi al generico ambito della sicurezza in rete
- Scarsa cultura della sicurezza negli installatori
- Il **60%** degli AP rilevati risulta aperto del tutto
- Un rimanente **50%** usa tecniche di protezione facilmente aggirabili



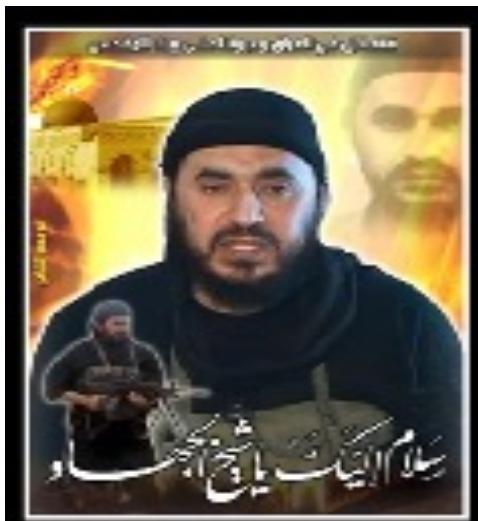
# Dark Web: il lato oscuro (1)

- **Il deep web contiene 500 volte** i contenuti accessibili attraverso motori di ricerca tradizionali
- Molti petabytes di informazioni
- Centinaia di miliardi di documenti
- Milioni di siti nascosti
- Una parte di questi siti costituisce il Dark Web



# Dark Web: il lato oscuro (2)

- Uso terroristico della rete
- Contatti e reclutamento
- Controllo Web-based di cellule terroristiche
- Canali di comunicazione nascosti e non intercettabili



Raythaytka Hoban

Majless Shora

Aboumos3ab

**BERG**



Azzam

Awal Afgan arab I

Awal Afgan arab II

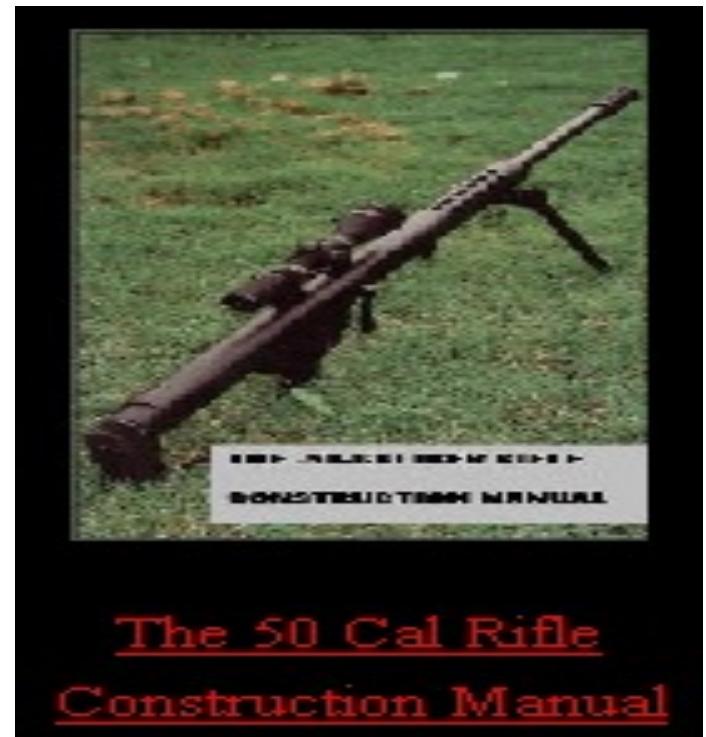
Dourous

# Dark Web: il lato oscuro (3)

- Risorse e istruzione per la costruzione di armi fatte in casa

A screenshot of a dark web website for a gun store. The header reads "Guns - Number one guns dealer in ...". Below it, there's a navigation bar with links for Products, FAQs, Register, and Login. The main content features a product listing for a "Walther PPK, Kal.7,65". The image shows a black Walther PPK pistol with its magazine. The text "New and unused!" is visible next to the image. Below the image is a table with columns for Product, Price, and Quantity. The first row shows "Walther PPK, Kal.7,65" with a price of "600 EUR = 8.091 ₦" and a quantity of "1" with a "Buy now" button. The second row shows "Ammo, 50 Rounds" with a price of "40 EUR = 563.9 ₦" and a quantity of "1" with a "Buy now" button.

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 8.091 ₦	1 <input type="button" value="Buy now"/>
Ammo, 50 Rounds	40 EUR = 563.9 ₦	1 <input type="button" value="Buy now"/>



- Vendita diretta di armi senza controlli

# Dark Web: il lato oscuro (3)

- Affitto di killers – Omicidi su commissione



# Dark Web: il lato oscuro (4)

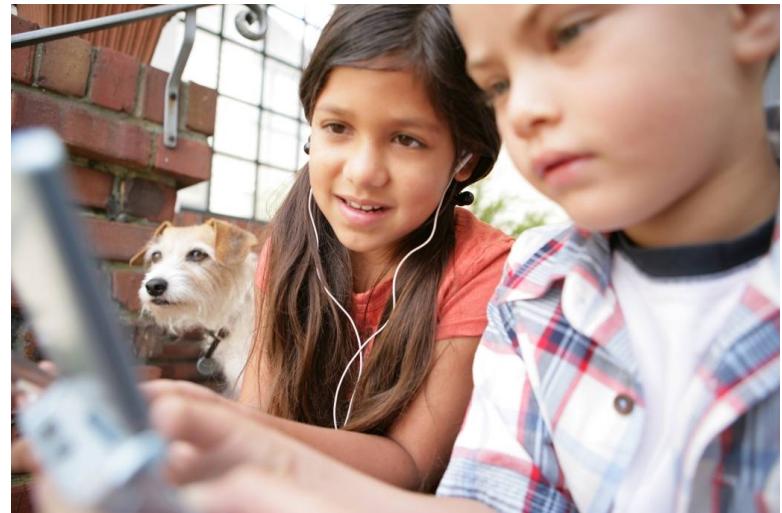
- Vendita di droghe
- Documenti falsificati
- Nuove identità
- Carte di credito clonate
- SIM telefoniche clonate
- Botnets per attacchi

The screenshot shows the homepage of the BlackMarket Reloaded website. At the top, there's a navigation bar with links for Home, Your Account, Your Purchases, Forum, Deposit Address, Account Balance (showing 0.00000 BTC), and Logout/Help. A sidebar on the left lists categories: Drugs (2883), Services (1108), Beta (371), Weapon (223), Collectedibles (21), Metals/Stones (26), Other (347), Software (164), Movies (23), Tobacco (144), Counterfeits (237), Alcohol (13), Blobs (237), Weight Loss (15). Below this is an Exchange section with a button labeled "Exchange". The main area displays a grid of 12 product cards:

- Drugs > Cannabis > Hash Tea, Blownmecrack (greenhouse) 100g carabinato (1kg) - Seller: Nek (228) 1.45209 BTC
- Drugs > Other - UNLIMITED STEALTH PAYPAL ACCOUNTS AND HOW TO WITHDRAW Seller: Nek (228) 0.17336 BTC
- Services > Documents Random legit SSN + DOB + DL USA only. Seller: v3c\_9f6\_810 0.10000 BTC
- Drugs > Cannabis > Hash 10g Super Amnesia Hash Organza - Herbed Grade AAA Seller: marmos (262) 1.73359 BTC
- Drugs > Psychedelic > Other Jumbo cactus clusters 5 grams 440 (desiccated) Seller: Dr. Ehardt (28) 0.22222 BTC
- Drugs > Cannabis > Hash 10g Sativas (Kali-Pain), medical grade Seller: myth (28) 1.19168 BTC
- Services > Other - we have the best ones UV & Zebra's USA Europe Canada Seller: Nek (228) 0.05993 BTC
- Drugs > Other 857 - Hone The Honey Service Seller: Prof\_Honey\_Service (7) 0.04627 BTC
- Drugs > Non-psychoactive (Entomological - Telescope version) Seller: Uncle Murphy (52) 0.33333 BTC
- Services > Ammunition calibre .223 (CE standard velocity 23 rounds) Seller: HellfireTeam (23) 0.17336 BTC
- Drugs > Smoking ExtremeTech - Hacking BlackBerry Seller: e4D\_059 (27) 0.25681 BTC
- Services > Money - I sell you fast cash (27) 0.25000 BTC

# I requisiti degli utenti...

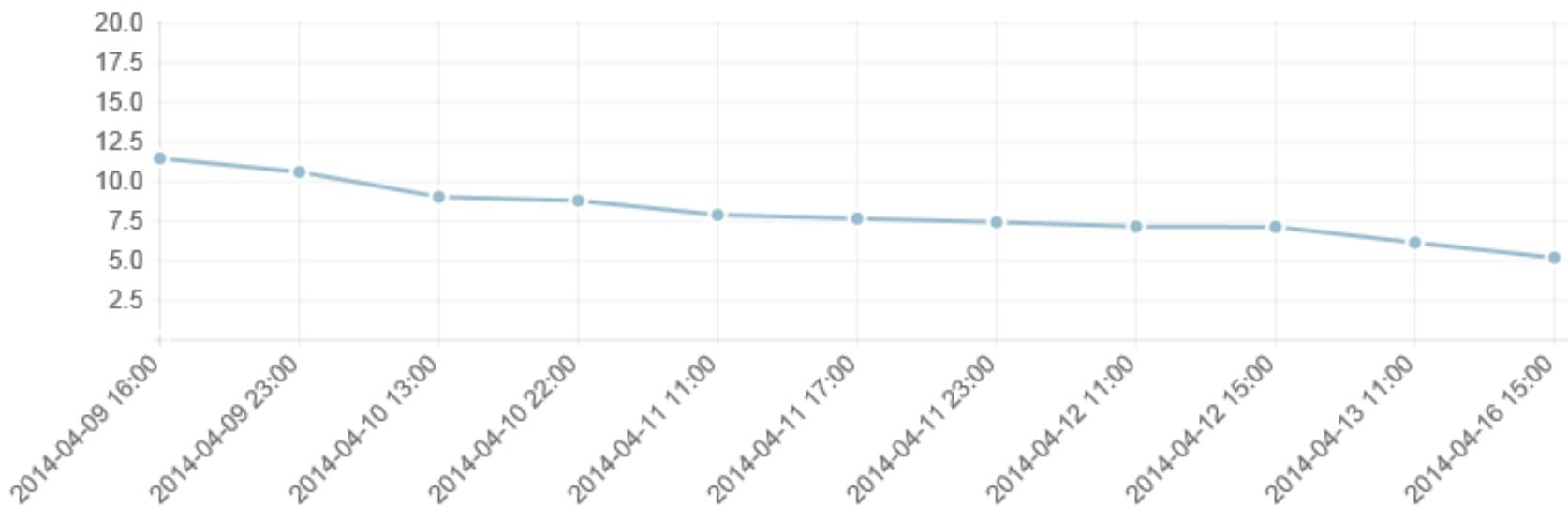
- I requisiti sono chiari
  - **Integrità**
  - **Riservatezza**
  - **Autenticazione**
  - **Non ripudiabilità**
- Dovremmo disporre di strumenti abbastanza maturi
  - **Crittografia**
  - **Firma digitale**
  - **SSL**



# L'esperienza di HeartBleed

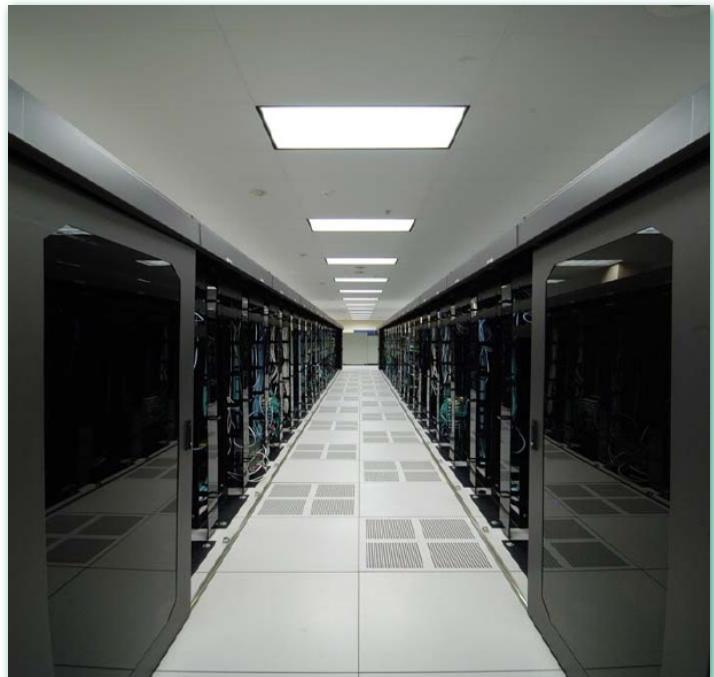


Historical Trend of Vulnerable HTTPS Enabled Alexa Top 1 Million Websites



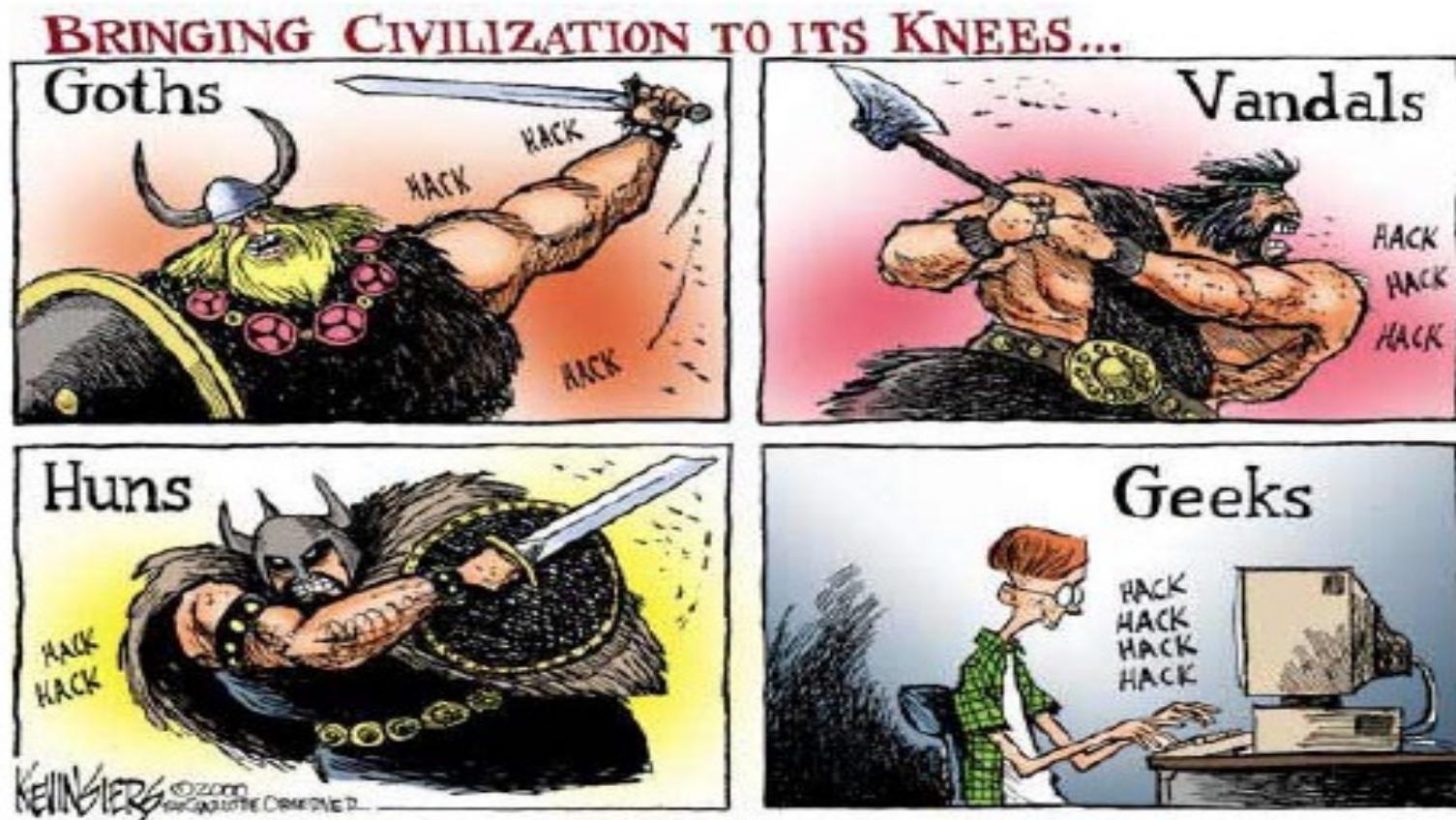
# Per chi eroga servizi...

- Cambiano i requisiti
  - **Continuità**
  - **Disponibilità**
  - **Resilienza**
- Scenari molto più complessi
  - **Infrastrutture critiche in rete**
  - **Elevata sofisticazione**
  - **Costi elevati**



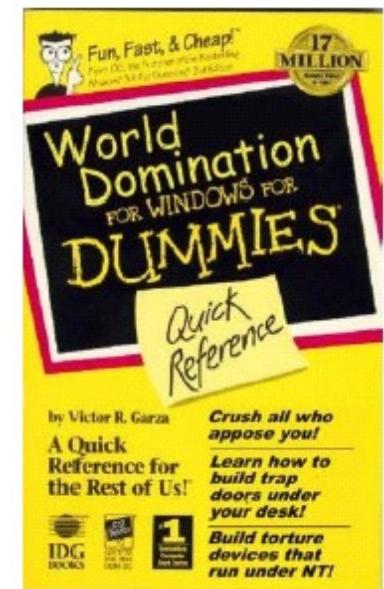
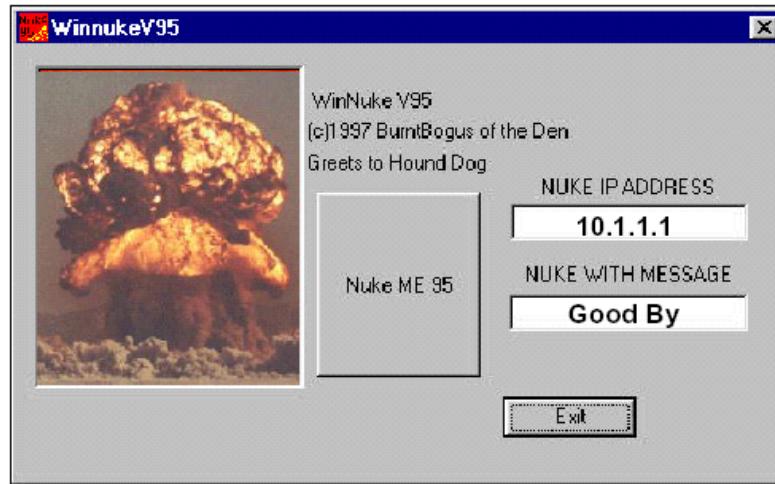
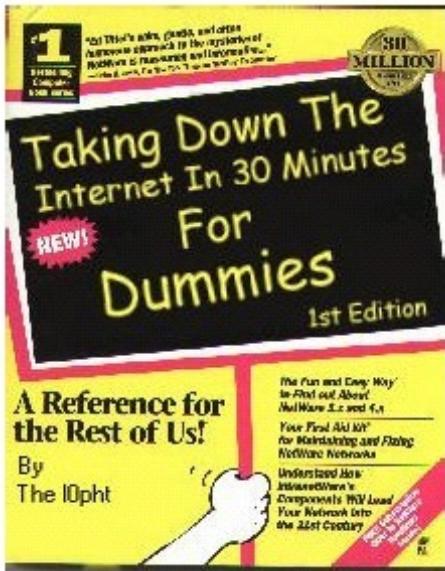
# Il Denial of Service

- Si moltiplicano gli episodi di *vandalismo informatico*
- Il danneggiamento o la *negazione (DoS) della connettività* è ora il principale problema di sicurezza



# Come funziona?

- Ora le tecniche di attacco sono alla portata di tutti anche grazie alla diffusione di massa, attraverso la stessa rete, di informazioni, strumenti e metodologie per il danneggiamento e lo sfruttamento illecito di risorse altrui
- Lo sviluppo di nuove tecniche e metodi di attacco e offesa procede più velocemente della ricerca e diffusione di nuovi paradigmi di sicurezza



# Il mercato delle tecnologie di offesa

L'attività sta assumendo **connotati professionali**, anche grazie alla notevole domanda finalizzata a **danneggiare il mondo dell'industria**

Nasce un **florido mercato** degli attacchi informatici

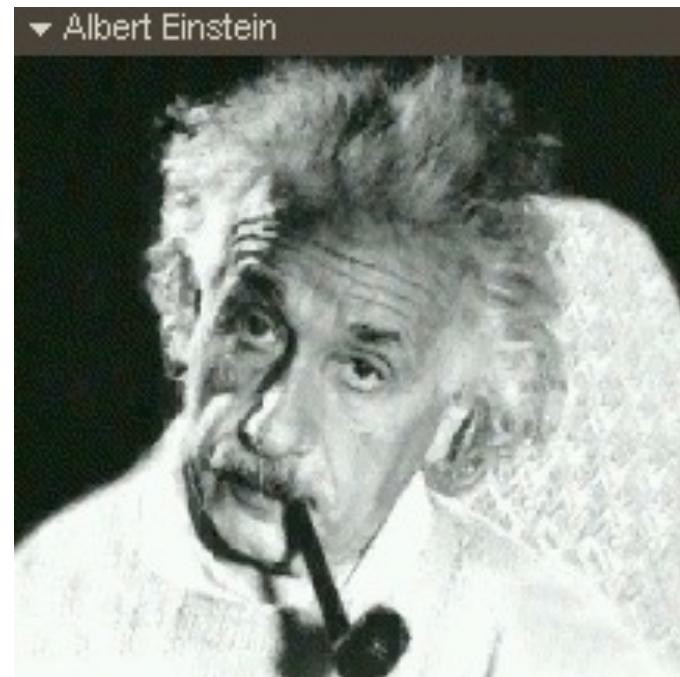


# I pro e contro della diffusione dell'informazione

Il paradigma “security through obscurity” è concettualmente discutibile ma il rendere alla portata di tutti determinate tecnologie offensive comporta la necessità di una maggiore attenzione per tutti coloro che gestiscono la sicurezza

Albert Einstein ha detto:

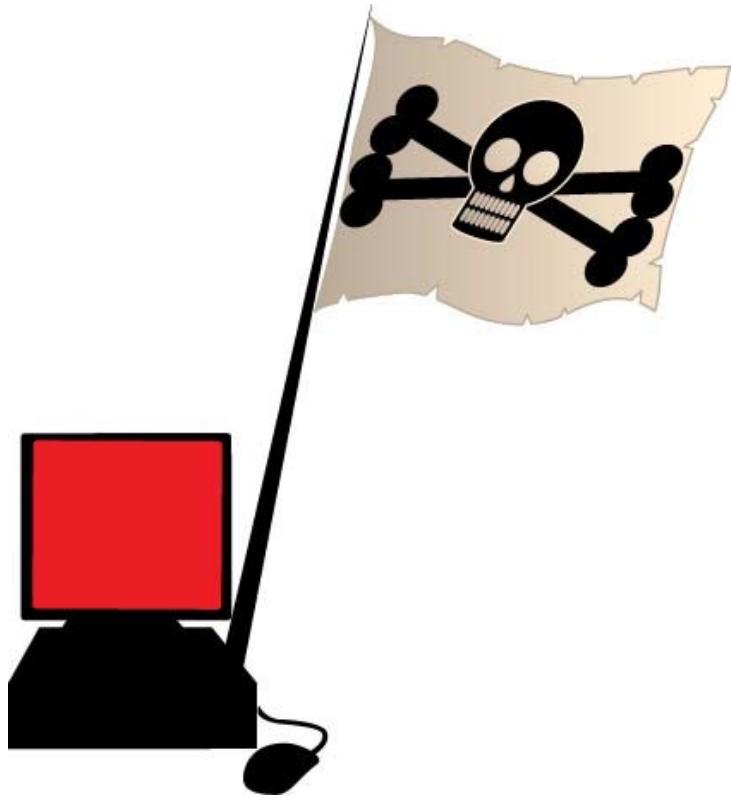
*“Il progresso tecnologico a volte può essere paragonabile a un’ascia nelle mani di un criminale psicopatico.”*



# Botnets in affitto

Fonte: Technology Review, 24 Settembre 2014

- Nasce un florido mercato delle macchine in rete compromesse
- Botnets di molte centinaia di hosts in affitto a circa 100\$/ora
- Utilizzate per l' invio di SPAM, per sferrare attacchi DDOS, per distribuire materiale pedo-pornografico, etc.
- L' attività sta assumendo connotati professionali, anche grazie alla notevole domanda finalizzata a danneggiare il mondo dell' industria



# Potenzialità delle Botnets

September 6th, 2007

## Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

**Categories:** [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox](#).....

**Tags:** [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



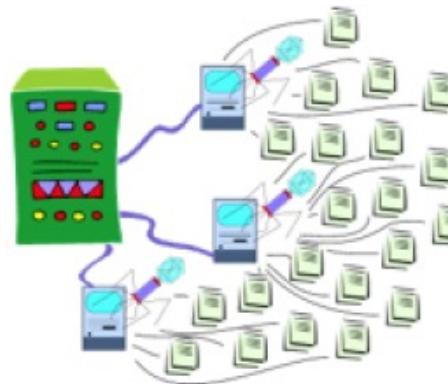
**150** TalkBacks

[ADD YOUR OPINION](#)



+97

WORTHWHILE? 115 VOTES



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

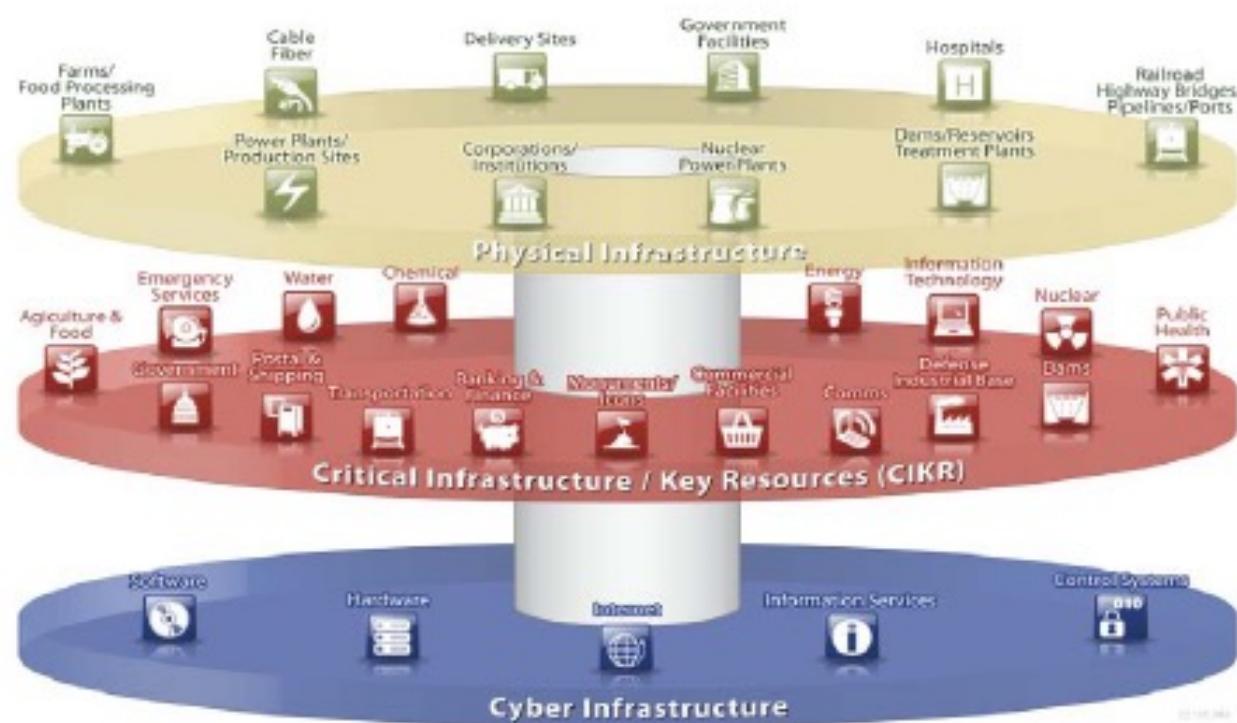
# Cyberterrorismo

- La minaccia terroristica contro cittadini ed infrastrutture critiche diventa uno degli obiettivi fondamentali della cybersecurity
- La cyber security assume un ruolo fondamentale per buona parte delle nazioni maggiormente industrializzate



# Cyber-infrastructure e Infrastrutture critiche

- La nostra vita dipende sempre di più dalla disponibili di sistemi critici
- Le infrastrutture critiche includono gas, **rete elettrica**, sistemi bancari e **finanziari**, sistemi di **difesa**, **trasporti** e **telecomunicazioni**
- Tutti dipendono fortemente dalla rete e da sistemi informatici



# Attacchi a infrastrutture critiche

TECHNOLOGY | APRIL 21, 2009

## Computer Spies Breach Fighter-Jet Project

Article

Comments

Email  
Printer Friendly

Share:  
Yahoo Buzz

Save This

Text

By SIOBHAN GORMAN, AUGUST COLE and YOCHI DREAZEN

WASHINGTON -- Computer spies have broken into the Pentagon's \$300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks.

Similar incidents have also breached the Air Force's air-traffic-control system in recent months, these people say. In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft.

NETWORK

Espresso

LE INCHIESTE



## Tecnologia

News

App

Social Network

Mobile

Videogiochi

Sicurezza

Vodafone Super ADSL Family. Parli e navighi senza limiti a solo 32 euro al mese.

Consiglia

Condividi

781

Twee

# "Cellulari, c'è una falla in Gsm e Umts: a rischio comunicazioni in intere aree geografiche"

Un bug nella tecnologia dei telefoni di seconda e terza generazione

## Defence Talk

Global Defense & Military Portal

HOME PICTURES FORUM REPORTS NEWS WEAPONS

You are here » Home » Defense & Security News » Chinese, Russian hackers probing US power grid: report

## Chinese, Russian hackers probing US power grid: report

DEFENSE & SECURITY NEWS — BY AGENCIE FRANCE-PRESSE ON APRIL 13, 2009 AT 6:45 AM

★★★★★ (No Ratings Yet)

Washington: Chinese and Russian hackers are attempting to seed viruses in the US power grid that could one day plunge major cities into chaos, a report warned Wednesday.

The report in the Wall Street Journal quotes intelligence officials saying that cyber-spies last year repeatedly gained access to the system powering everything from financial institutions to sewage systems.

BBC NEWS | Europe | Estonia hit by '



BBC

http://news.bbc.co.uk/2/hi/europe/6665145.stm

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

E-mail this to a friend

Printable version

## Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state



# Attacchi a infrastrutture critiche

- Le infrastrutture critiche includono gas, **rete elettrica**, sistemi bancari e **finanziari**, sistemi di **difesa**, **trasporti** e **telecomunicazioni**
- Tutti dipendono fortemente dalla rete e da sistemi informatici



# U.S. Critical Infrastructure Full of Security Holes

By Ann R. Thryft 06.04.2020 □ 0

Share Post

f Share on Facebook

t Share on Twitter

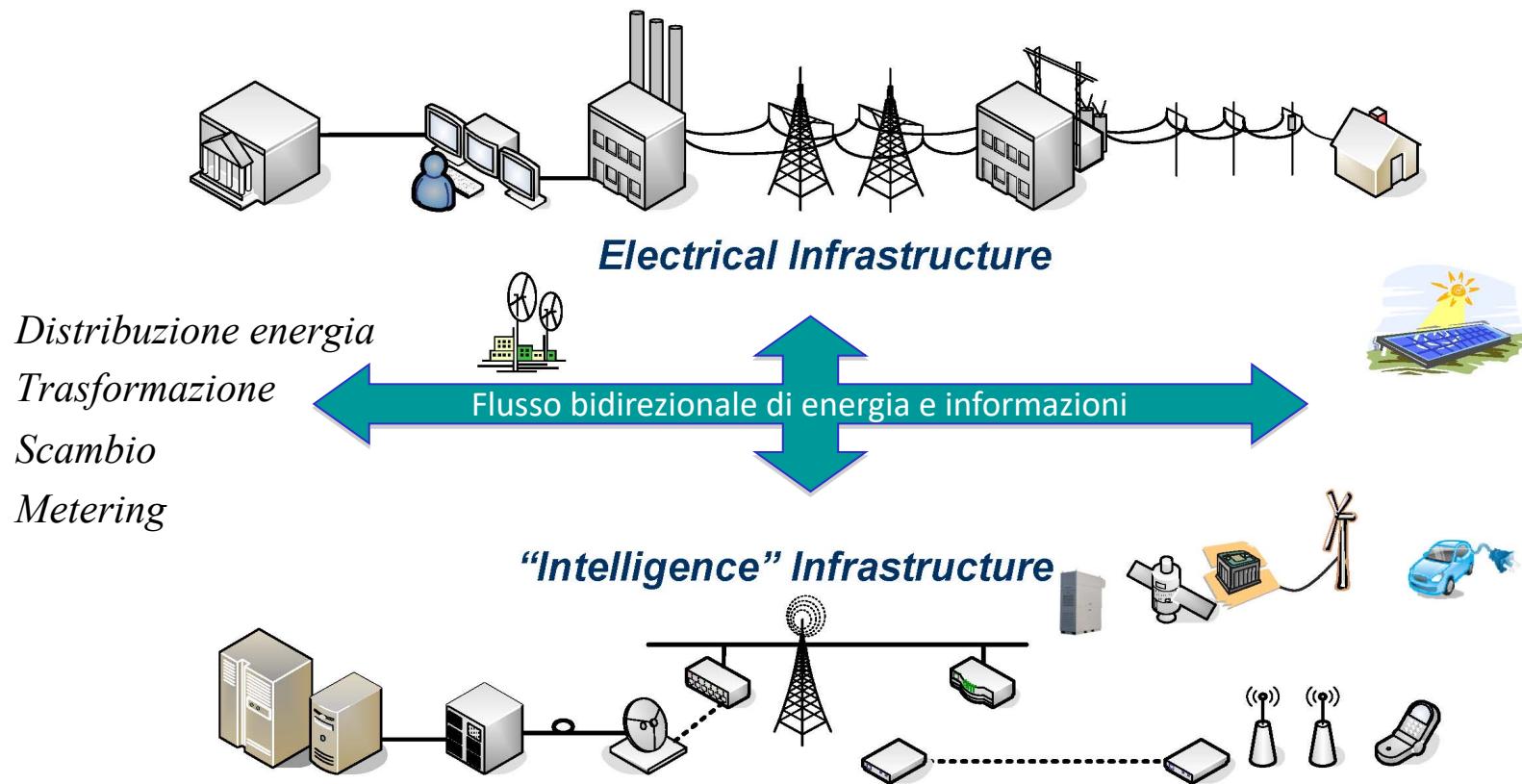
in

The coronavirus pandemic has spawned a huge increase in cyberthreats and attacks. While much of this is aimed at consumers, a lot has also targeted companies whose employees must now access critical infrastructure, such as industrial control systems (ICS) and operational technology (OT) networks, from home.

But that critical infrastructure, which keeps modern society going even during a pandemic, is seriously under-protected against cyberattacks, say recent reports from cybersecurity companies.

# Smart Power Grid: “Energy Internet”

- Sistemi SCADA basati su tecnologie legacy
- Limitati controlli e meccanismi di protezione con rischi di:
  - Accesso a SW di controllo
  - Alterazione del carico
  - DOS e destabilizzazione



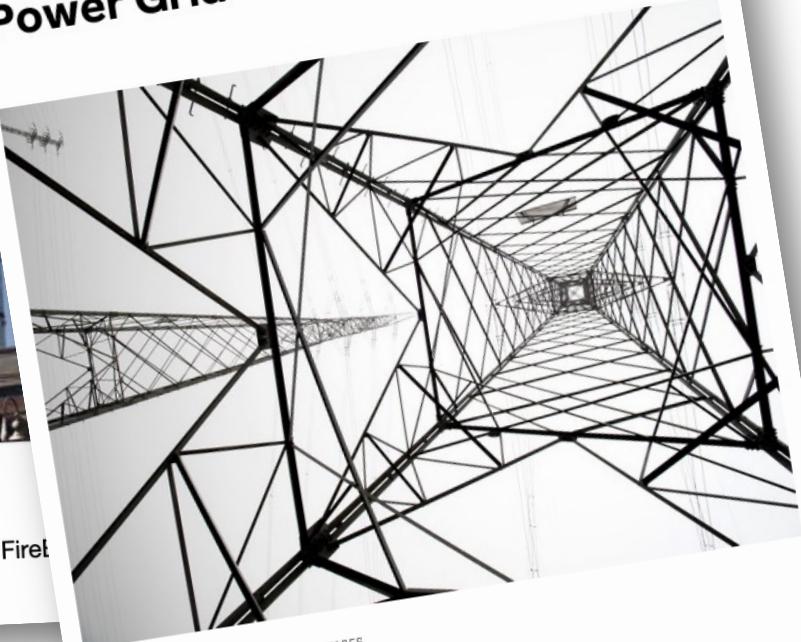
New: Security researchers say Triton, a powerful malware that once tried to blow up a Saudi chemical plant, has been found in a second facility.



**A powerful malware that tried to blow up a Saudi plant strikes again**  
A highly capable malware reportedly used in a failed plot to blow up a Saudi petrochemical plant has now been linked to a second compromised facility. Fire at

[techcrunch.com](https://techcrunch.com)

## Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



© JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their

HACKING | Di [Joseph Cox](#) | gen 12 2016, 10:18am

# La rete elettrica in Ucraina è stata attaccata da degli hacker

Gli hacker hanno attaccato anche i centri telefonici cercando di impedire ai clienti di notificare alle compagnie le interruzioni di corrente.

## Johannesburg residents left in the dark after a ransomware attack at City Power

July 26, 2019 By Pierluigi Paganini

---

South African electric utility City Power that provides energy to the city of Johannesburg, has suffered serious disruptions after a ransomware attack.

A ransomware infected systems at City Power, an electricity provider in the city of Johannesburg, South Africa, and some residents were left without power.

The energy utility informed its customers via Twitter of the ransomware attack that encrypted its network, including all its databases and applications.

# Hackers targeted ICS/SCADA systems at water facilities, Israeli government warns

---

April 27, 2020 By [Pierluigi Paganini](#)

---

The Israeli authorities are alerting organizations in the water industry following a series of cyberattacks that hit water facilities in the country.

The Israeli government has issued an alert to organizations in the water sector following a series of cyberattacks that targeted the water facilities.

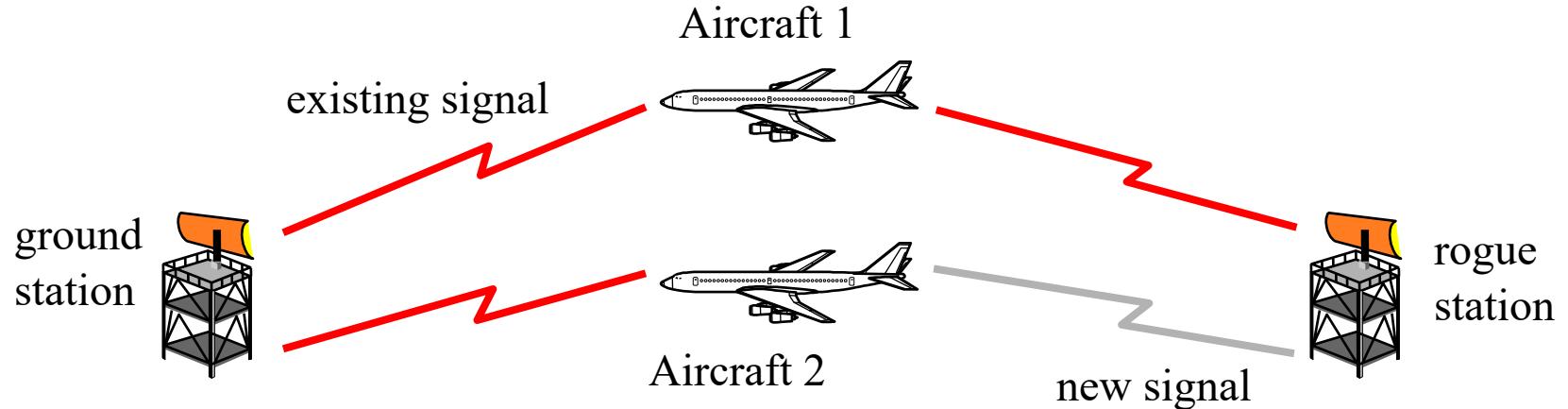
# Controllo del traffico aereo (ATC)



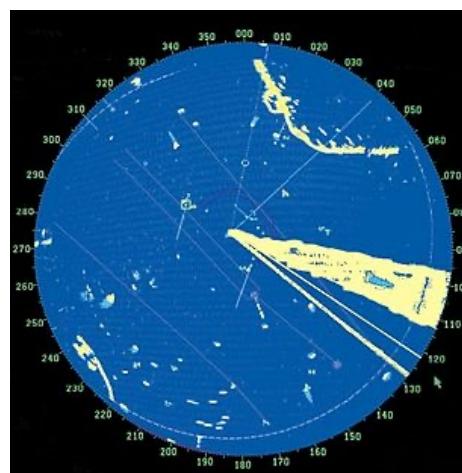
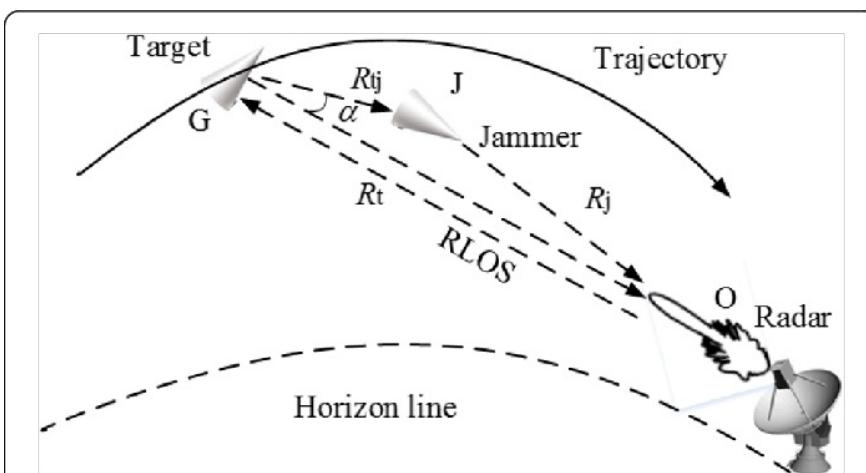
- Funzioni di:
  - Tracciamento
  - Localizzazione
  - Segnalazione
  - Comunicazione
- Garantito da una rete su cui viaggiano:
  - messaggi coordinamento fra controllori
  - dati radar
  - dati meteorologici
  - messaggi di volo e informativi

# Possibili rischi

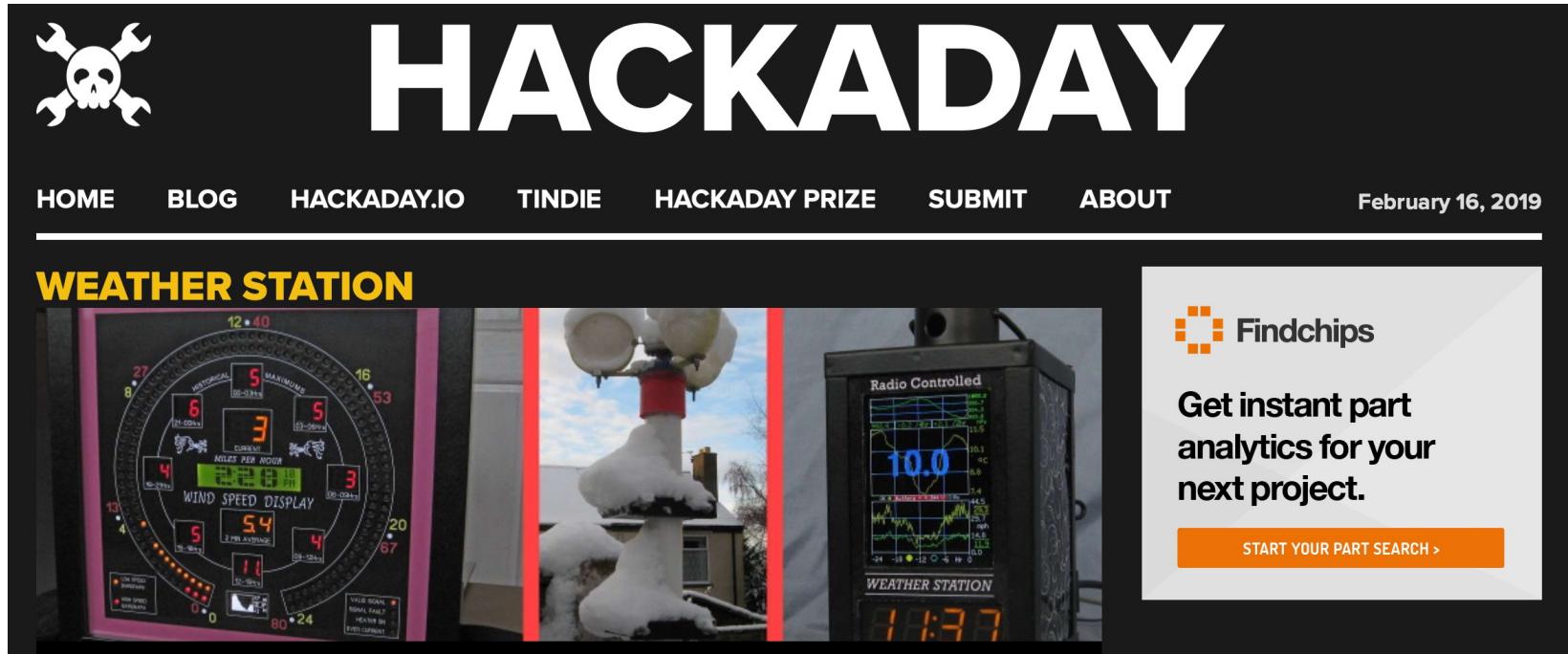
- Transponder spoofing



- Radar Jamming



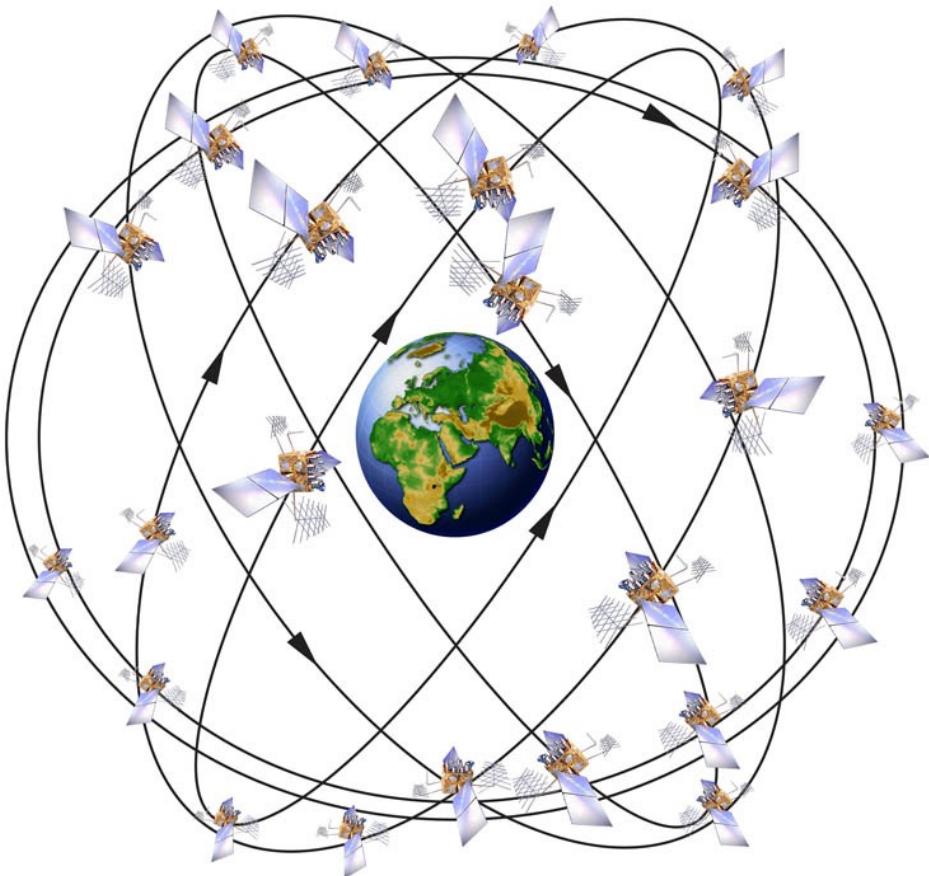
# Altri obiettivi...



The screenshot shows the Hackaday homepage with a prominent skull and wrench logo. The main title "HACKADAY" is displayed in large white letters. Below the title, there are navigation links: HOME, BLOG, HACKADAY.IO, TINDIE, HACKADAY PRIZE, SUBMIT, and ABOUT. To the right, the date "February 16, 2019" is shown. A horizontal line separates the header from the content area. In the content area, there is a section titled "WEATHER STATION" with three images: a circular control panel with various buttons and displays, a wind vane and anemometer mounted on a pole covered in snow, and a close-up of a weather station unit with a digital display showing "10.0" and "1:37". To the right of the weather station images is an advertisement for Findchips. The ad features the Findchips logo (an orange stylized 'F') and the text "Findchips" followed by "Get instant part analytics for your next project." Below this is a button with the text "START YOUR PART SEARCH >".

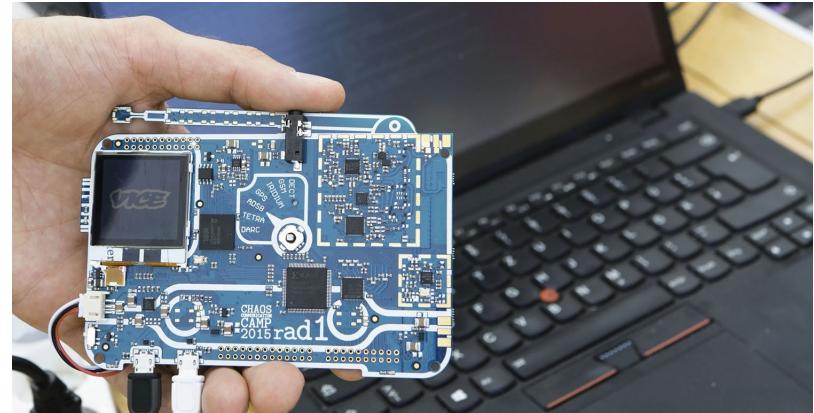
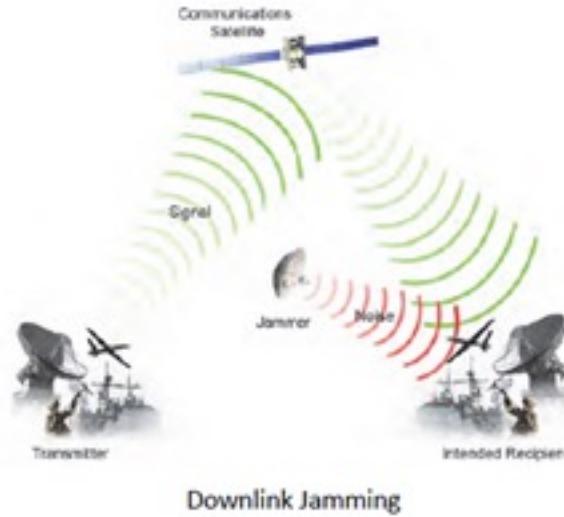
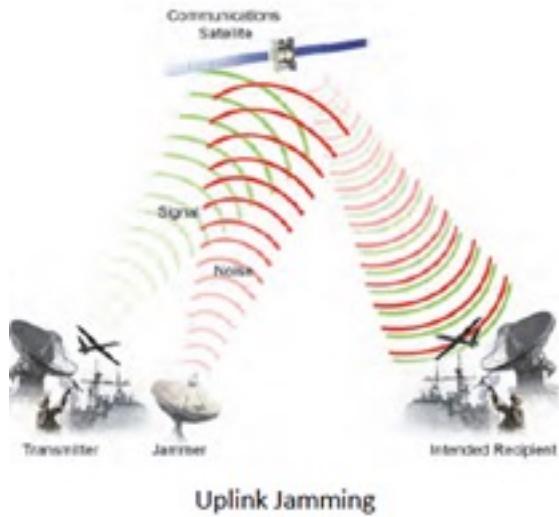
- Spoofing radiofrequenze su reti di raccolta dati meteo
- DoS o iniezione dati contraffatti

# Global Positioning System

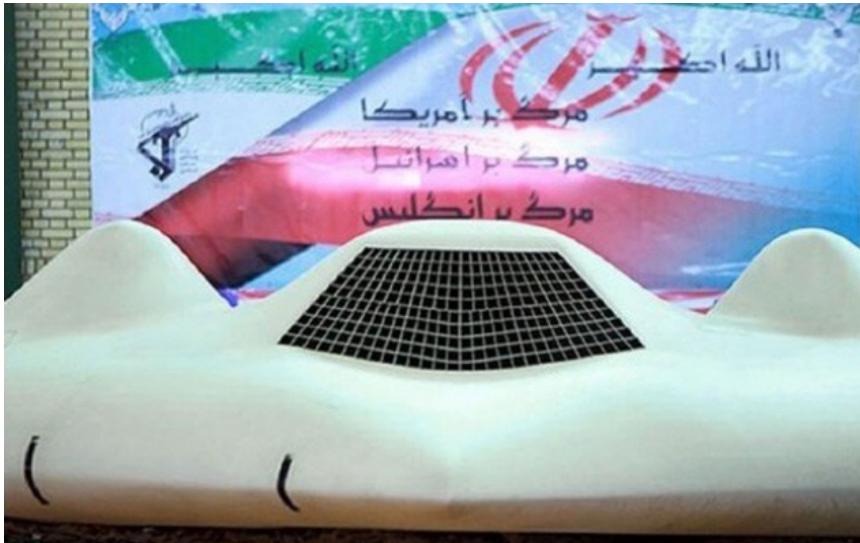


- Fondamentale per
  - Navigazione Satellitare
  - Guida assistita
  - Guida autonoma
  - Gestione flotte
  - Controllo droni
  - Controllo crociera
- Vulnerabile ad attacchi:
  - Jamming
  - Spoofing

# GPS Jamming



# Dirottamento Droni



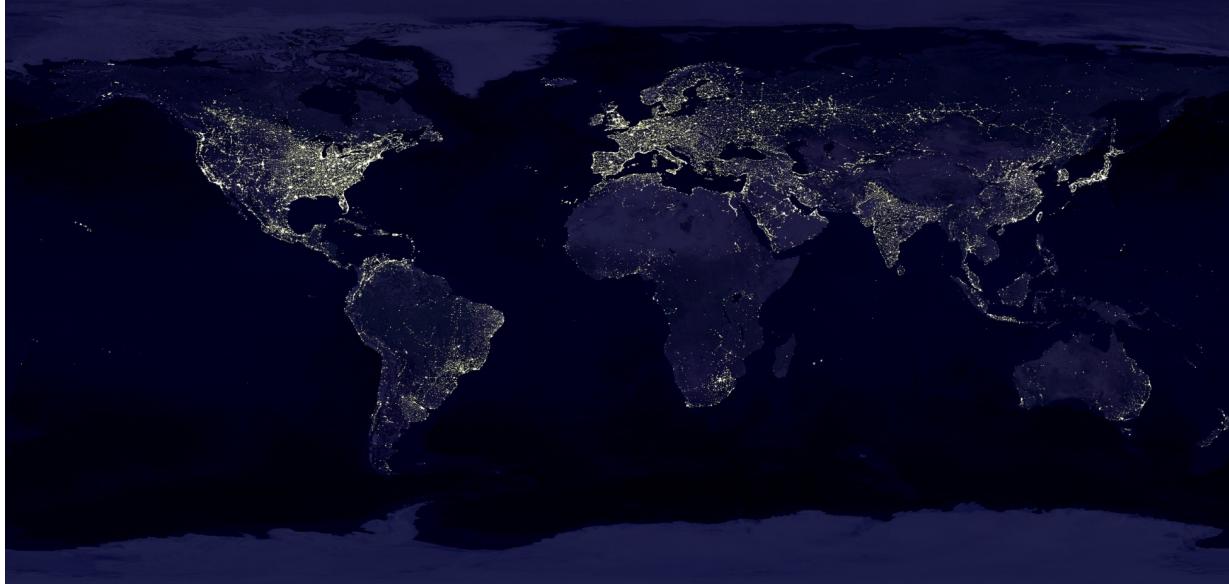
# GPS Spoofing via SDR

- Da quando Realtek ha rilasciato il chip RTL2832U un paio di anni fa sono comparsi tantissimi dispositivi SDR (Software Defined Radio)
  - un dispositivo in grado di trasmettere su una grande varietà di frequenze al costo di 15\$
  - al posto di un circuito commerciale integrato troviamo un software Open Source atto a produrre il calcolo della posizione dell'antenna del ricevitore ad un determinato istante
- Diventa banale riprodurre il segnale generato da un satellite risultando in una sorgente ad elevata potenza e precisione



# Conseguenze attacchi alle Power Grids

- Esplorando vulnerabilità delle smart grids è possibile:
  - Privare di energia intere aree geografiche
  - Creare sovraccarichi e danni alle apparecchiature
  - Creare danni economici a gestori e soggetti terzi
  - Bloccare la funzionalità di sistemi di protezione



SHODAN search results for power grid equipment.

Search term: power grid

Number of results: 1000

Map view: World Map

Download results

Create report

My Account

Results:

- 108.152.91.145  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 178.22.117.242  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 94.112.158.199  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 78.25.94.194  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 5.209.188.52  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 89.182.77.165  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 80.123.340.226  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 153.142.212.108  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 77.216.175.133  
Copyright: Original Source: Siemens  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...
- 188.65.85.219  
Copyright: Original Source: Digital Telecommunication Services  
Power type: 3PH-3W-4P-2P  
Voltage: 230V, 480V, 11kV, 13.2kV  
Basic Firmware: v.3.2.4  
Model: S7-300  
Serial number of module: 0.0000000000  
Plant identification: 0007-007000...  
Power Verbal name: 0007-007000...

Next

© 2013-2016. All Rights Reserved - SHODAN.NET

# Uno scenario apocalittico...

- Immaginiamo un ipotetico cyberattacco in grado di prendere il controllo di arsenali nucleari



[Ovviamente la foto è finta, solo per evidenziare la criticità di un tale momento]  
Source: <http://www.armscontrolwonk.com/1955/missile-palooza>

# Cyberterrorism o Activism?...

**Continuing pro-Wikileaks DDOS actions, Anonymous takes down PayPal.com**

Xeni Jardin at 7:10 PM Wednesday, Dec 8, 2010



**Operation Payback**

22 minutes ago

Target: [www.Paypal.com](http://www.Paypal.com) FIRE NOW!!!!!!111 #DDOS  
#PAYBACK #WIKILEAKS



**Operation Payback**

27 minutes ago

HIVE MIND LOIC: server loic.anonops.net Backup server  
irc.anonops-irc.com IRC port 6667 Channel #loic FAQ:  
<http://bit.ly/fGHDib> #ddos



**Operation Payback**

40 minutes ago

Next Target: [www.paypal.com](http://www.paypal.com) ETA: 20 minutes! Get  
ready! #ddos #wikileaks #payback

# Cyberterrorismo: da semplici defacing...

Zone-H.org – Unrestricted Information – dodtravelregs.hqda.pentagon.mil defaced by Agd\_Scorp

H [http://www.zone-h.org/component?option=com\\_mirrorwp&Itemid,0/id,777](http://www.zone-h.org/component?option=com_mirrorwp&Itemid,0/id,777) Google

Wednesday, 10 September 2008

Mirror saved on: 2008/08/18 01:30

Defacer: Agd\_Scorp

Domain: <http://dodtravelregs.hqda.pentagon.mil/>

IP address: 141.116.10.20

System: Win 2003

Web server: Unknown

[Attacker stats](#)

Terrorist Crew



~ Hi Master ~

Hacked by | Agd\_Scorp , JeXToXiC , Wh0!, Starturk, Rx5, AntiW4R, Security-Terror

# Ad un uso militare degli attacchi informatici...

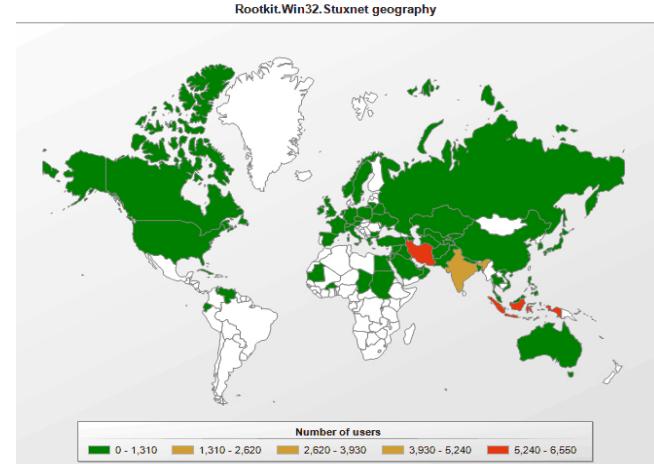
Il cyberspazio diventa lo scenario ideale per nuove forme di conflitto:



- Cyber Warfare
- Cyber Weapons
- Cyber Attacks



# Un worm come arma: Stuxnet



- Settembre 2010: generici “ritardi” nel programma nucleare iraniano
- Ottobre 2010: “spie” accusate di sabotaggio nel programma
- Novembre 2010: Iran riconosce che le centrifughe per l’arricchimento sono state attaccate da un worm
- Attacco selettivo a specifici sistemi SCADA SIMATIC PCS 7 Siemens deputati al controllo delle centrifughe
- Il worm si è propagato su gran parte della rete senza alcun danno per i sistemi infettati



# Cyber Warfare

- Attacchi Computer-based contro l'integrità o la disponibilità, di sistemi critici in grado di costituire una minaccia per la sicurezza nazionale
- Accompagnano gli attacchi fisici
- Crescono in volume, sofisticazione e coordinamento



# I 4 Scenari Bellici

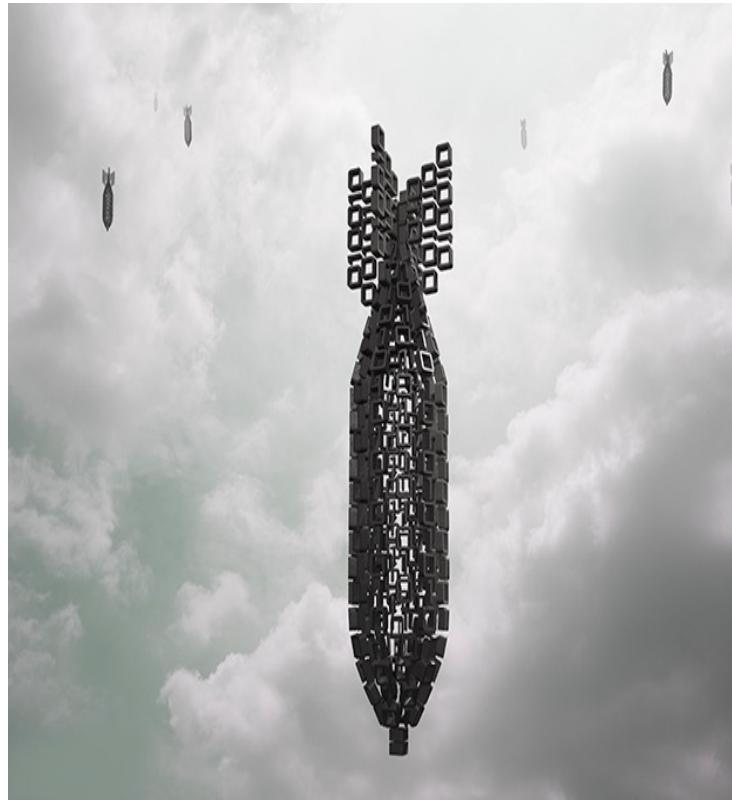
- Terra
- Mare
- Cielo
- Cyberspace

} Attività Cinetiche



# Cyber Attacchi

- Un cyberattacco su larga scala è altamente probabile nei prossimi anni, potenzialmente in grado di causare la perdita di decine di milioni di euro o minacciare la sicurezza di intere nazioni e la loro capacità di difendersi, o peggio, causare significative perdite di vite umane



# Attacchi da parte di paesi

## Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima  
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

### THIS STORY

- » Google attack part of vast campaign
- [Google hands China an Internet dilemma](#)
- [Statement from Google: A new approach to China](#)
- [+ View All Items In This Story](#)

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and [Dow Chemical](#) -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail



People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

[+ Enlarge Photo](#)

### What Google might miss out on

Google said it may exit China,

# Fino a parlare di CyberWars

## Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
  - Nato experts sent in to strengthen defences

**Ian Traynor** in Brussels  
The Guardian, Thursday 17 May 2007  
[Article history](#)



Bronze Soldier, the Soviet war memorial removed from Tallinn Affairs undertaking a desperate step in order to disseminate real-time Nisametdinov/AP

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

August 11th, 2008

## Coordinated Russia vs Georgia cyber attack in progress

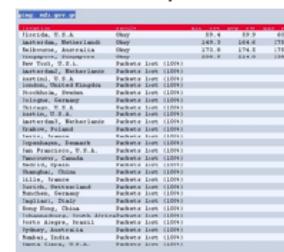
- Posted by Dancho Danchev @ 4:23 pm

**Categories:** [Black Hat](#), [Botnets](#), [Denial of Service \(DoS\)](#), [Governments](#), [Hackers..](#)

**Tags:** Security, Cyber Warfare, DDoS, Georgia, South Ossetia.



In the wake of the **Russian-Georgian conflict**, a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S., with **Georgia's Ministry of Foreign Affairs**.



# Sistemi tattici di jamming

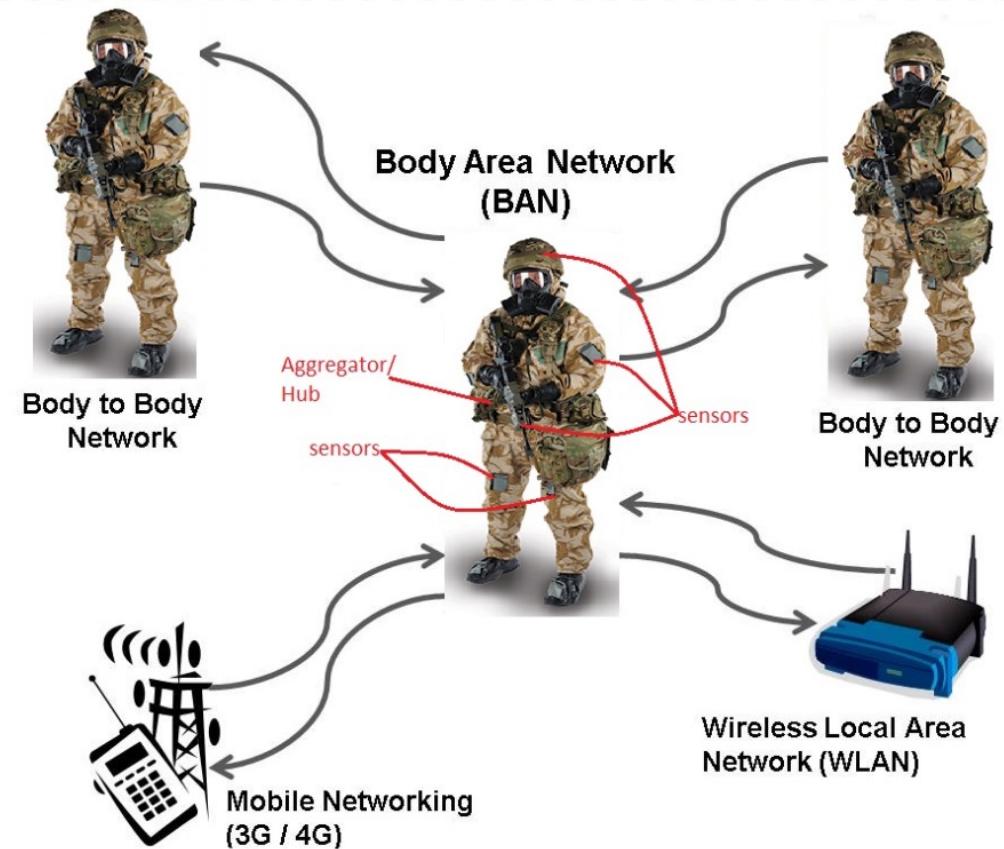
- Krasukha-4
  - Fino a 300 km di copertura
  - jamming radar e canali di controllo droni



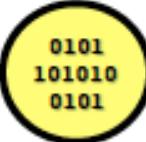
- EC-130H Compass Call
  - Aereo tattico
  - Noise jamming vs comunicazioni C&C



# In grado di condizionare l'attività di terra...



# Dalla Cold War alle Code Wars

- Atomic 
- Biological 
- Chemical 
- Digital 

“Cold War” → “Code War”

Non-State Actors

Asymmetric Attack

# Azione e reazione

**U.S. cyber counterattack: Bomb 'em one way or the other**

**National Cyber Response Coordination Group establishing proper response to cyberattacks**

*By [Ellen Messmer](#), Network World, 02/08/07*

San Francisco — If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source.

# Tirando le somme

Numero utenti +  
Confini territoriali +  
Problematiche tecniche +  
Disponibilita' informazioni =

---

**Probabilita' di subire un'attacco**

# La sfida

- Una soluzione realmente efficace a questi problemi richiede una combinazione delle giuste tecnologie e politiche di sicurezza da applicare a livello nazionale ed internazionale
- Ciò comporta una presa di coscienza da parte dei governi, delle organizzazioni coinvolte e degli utenti finali

**Questa è la vera sfida della cybersecurity**

# Verso soluzioni concrete

- **Come ottenere un reale successo e affrontare bene la sfida della cybersecurity?**
- **Vanno considerati 4 fattori fondamentali:**
  - Tecnologia
  - Costi e fattori economici (obiettivi per gli stakeholders e meccanismi di incentivo)
  - Influenza sociale (e resistenza a fenomeni di controllo di massa)
  - Politiche locali, nazionali ed internazionali

# Esiste una ricetta???

- E' una necessità affrontare la cybersecurity come **emergenza globale**, e non affidarsi solo a prodotti, elementi o indagini generiche
- E' necessaria la **consapevolezza** dei problemi da affrontare con le **competenze adeguate**
- **Non esisterà mai** una soluzione **definitiva** o standard per tutti: la security è un processo **in divenire** che va gestito affrontando i problemi secondo **nuovi schemi di pensiero** e **paradigmi** di intervento



# Consapevolezza: mirare al problema

