Conferenza Chimica 4.0:
la gestione della security nell'era della digitalizzazione

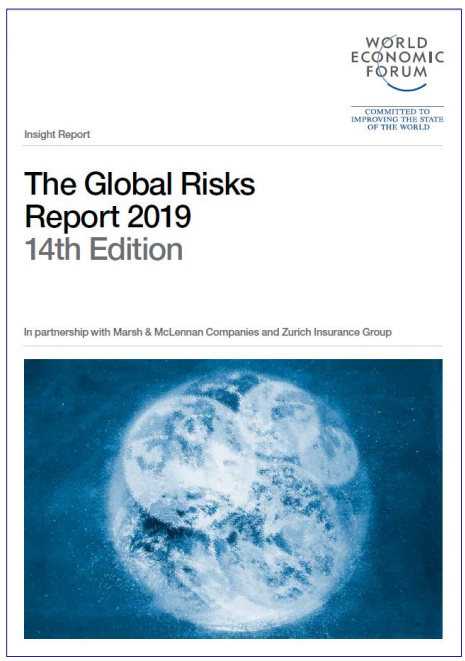
I rischi cyber

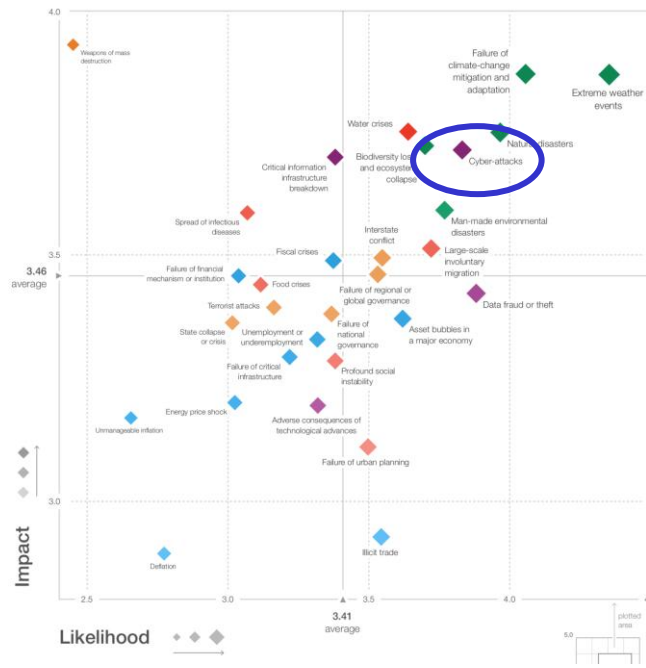
Corrado Giustozzi

Agenzia per l'Italia Digitale
CERT-PA

ENISA Advisory Group

AGID Agenzia per l'Italia Digitale





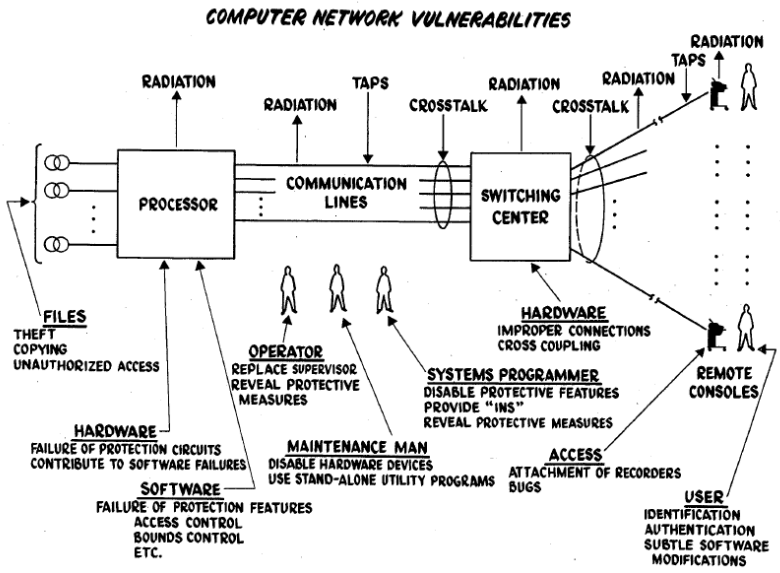


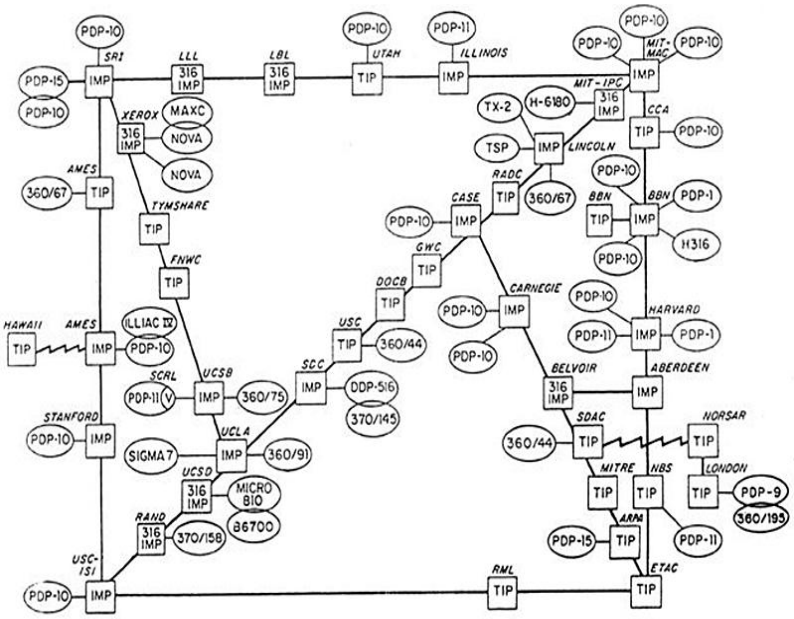
Figure 3

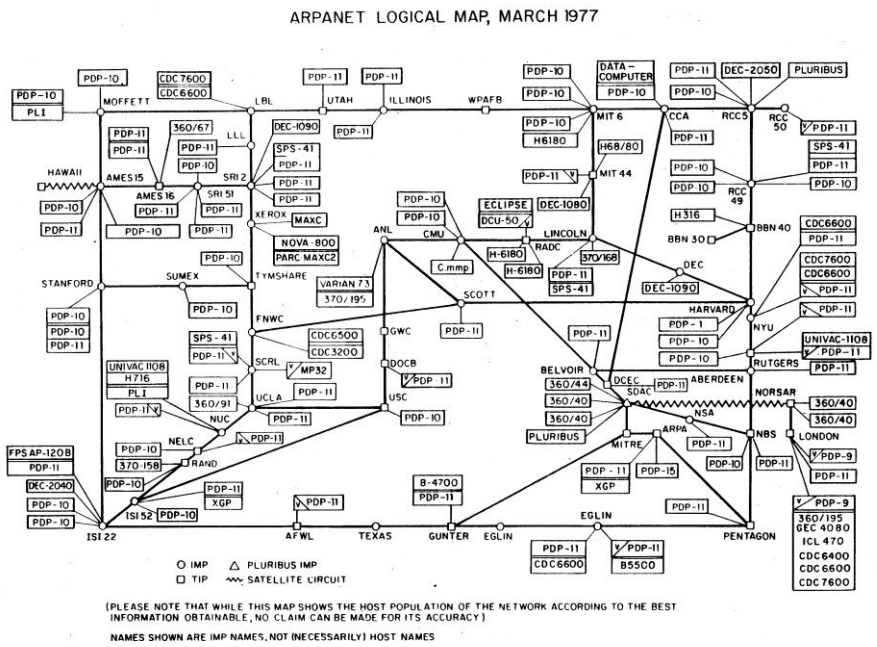
Fonte: "The Ware report", Rand Corp., 1970

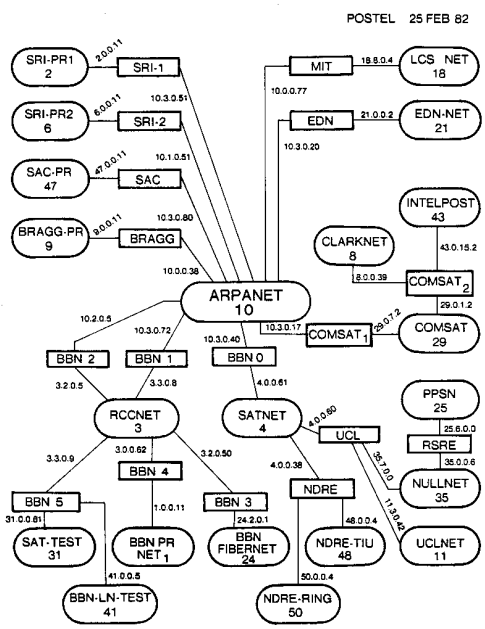
Il cyberspace

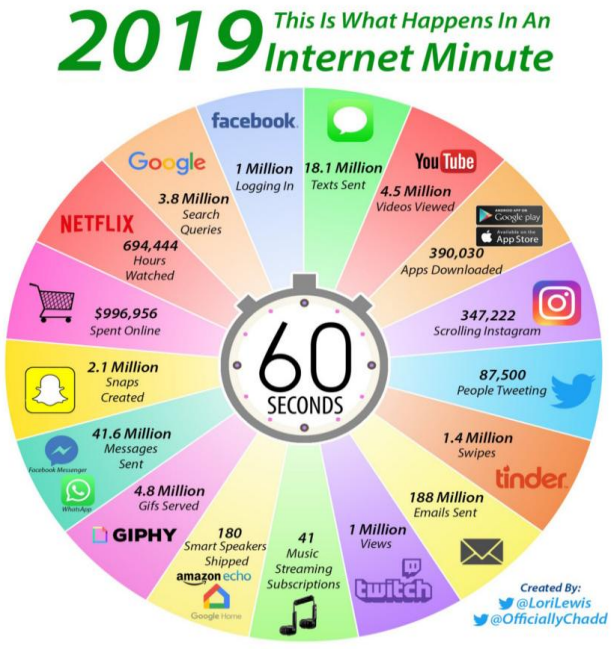
«Un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. **Impensabile complessità.** Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...].»

William Gibson
Neuromante (1984)

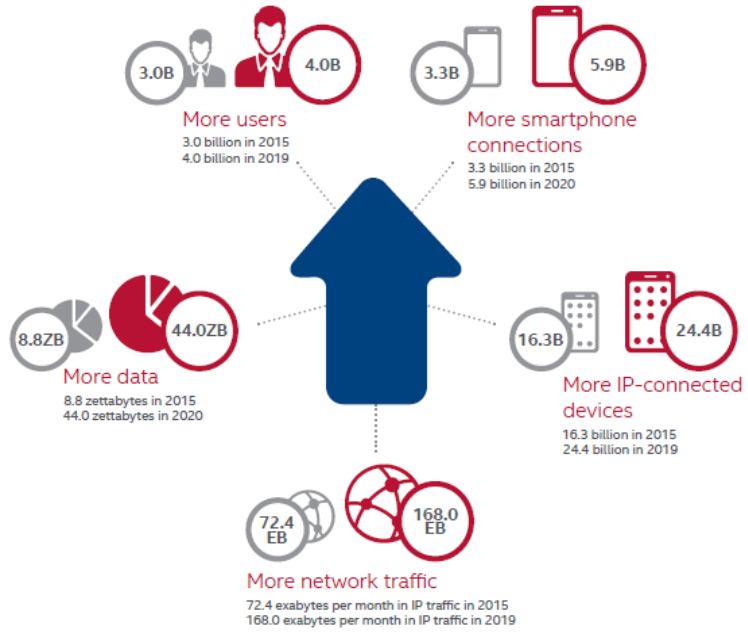

ARPA NETWORK, LOGICAL MAP, SEPTEMBER 1973
SRI
LLL
LBL
UTAH
ILLINOIS
MIT-MAC
MIT-IPC
XEROX
AMES
TYMSHARE
FNWC
CASE
GWC
DOCB
CARNEGIE
HARVARD
HAWAII
USC
UCSB
SCC
BELVOIR
ABERDEEN
SCRL
STANFORD
UCLA
SDAC
NORSAR
UCSD
MITRE
NBS
LONDON
RAND
ARM
USC-ISI
RML
ETAC
BBN
RADC
CCA
LINCOLN


ARPANET LOGICAL MAP, MARCH 1977
MOFFETT
LBL
UTAH
ILLINOIS
WPAFB
MIT 6
CCA
RCC 50
HAWAII
AMES 15
AMES 16
SRI 2
SRI 51
XEROX
MAXC
NOVA-800
PARC MAXC2
ANL
CMU
ECLIPSE
DCU-50
DEC-1080
LINCOLN
RADC
H-6180
370/168
C.mmp
DEC
DEC-1090
MIT 44
H68/80
H6180
H316
BBN 30
BBN 40
RCC 49
CDC6600
CDC7600
STANFORD
SUMEX
TYMSHARE
VARIAN 73
370/195
SCOTT
HARVARD
NYU
FNWC
CDC6500
CDC3200
GWC
SCRL
MP32
DOCB
UNIVAC 1108
H716
PLI
UCLA
USC
BELVOIR
360/44
360/40
DCEC
SDAC
ABERDEEN
RUTGERS
NORSAR
NSA
NUC
NELC
RAND
ARPA
MITRE
NBS
LONDON
PLURIBUS
FPS AP-120B
DEC-2040
370-158
ISI 22
ISI 52
AFWL
TEXAS
GUNTER
EGLIN
PENTAGON
B-4700
XGP
B5500
CDC6400
CDC6600
CDC7600
DEC 4080
ICL 470
O IMP
□ TIP
△ PLURIBUS IMP
SATELLITE CIRCUIT
(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

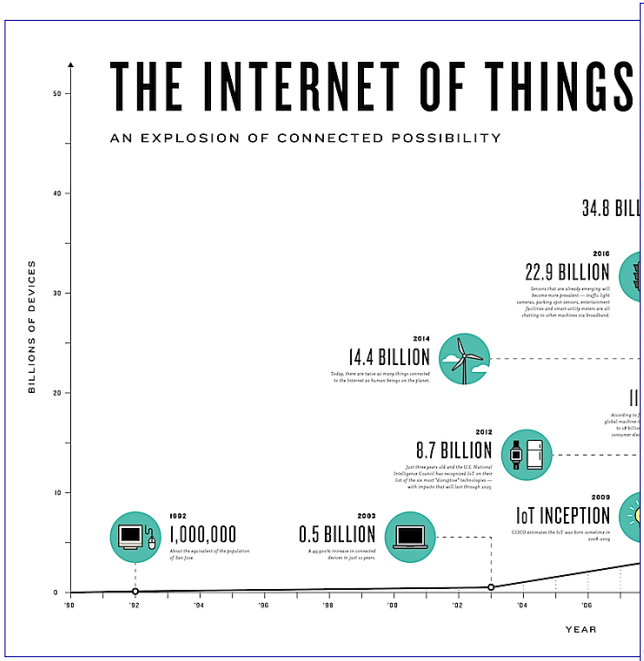


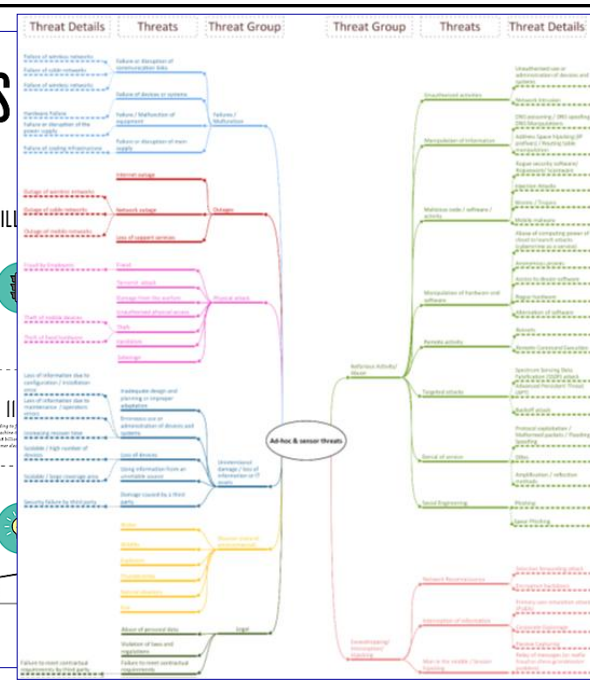


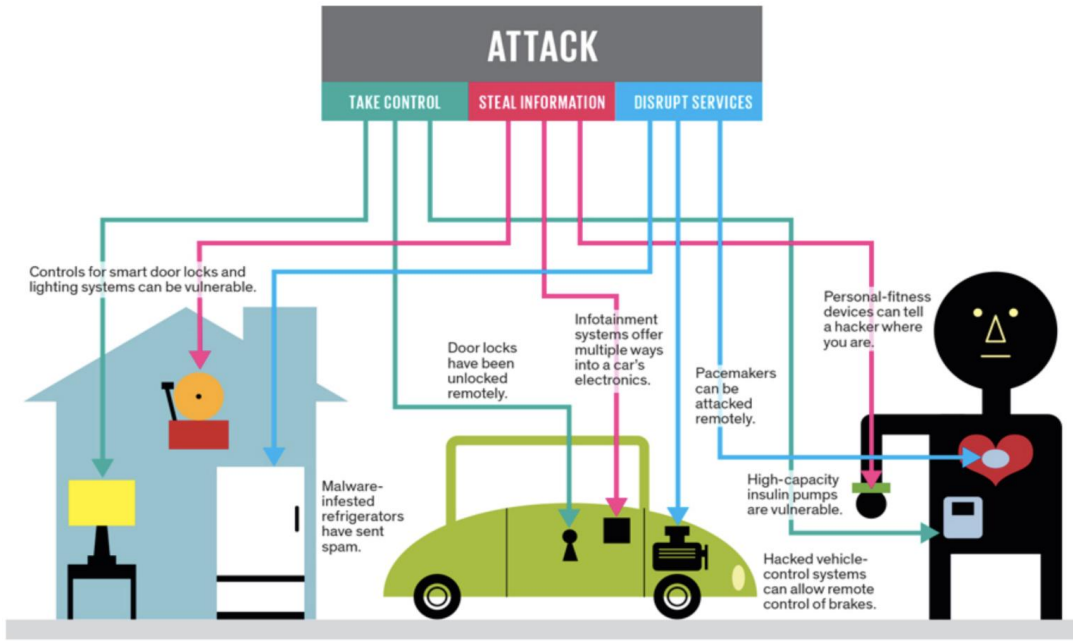
- **Oggetti**: nel 2019 i dispositivi connessi in Rete saranno un numero pari a tre volte e mezza la popolazione della Terra.
- **Traffico**: il traffico IP nel 2015 è stato di 72,4 HByte al mese. Nel 2019 sarà di 168,0 HByte al mese.
  (1 HByte = 10^{18} Byte, ossia un milione di TByte).
- **Utenti**: erano 3 miliardi nel 2015, saranno 4 miliardi nel 2019.



Fonte: McAfee Labs, 2015





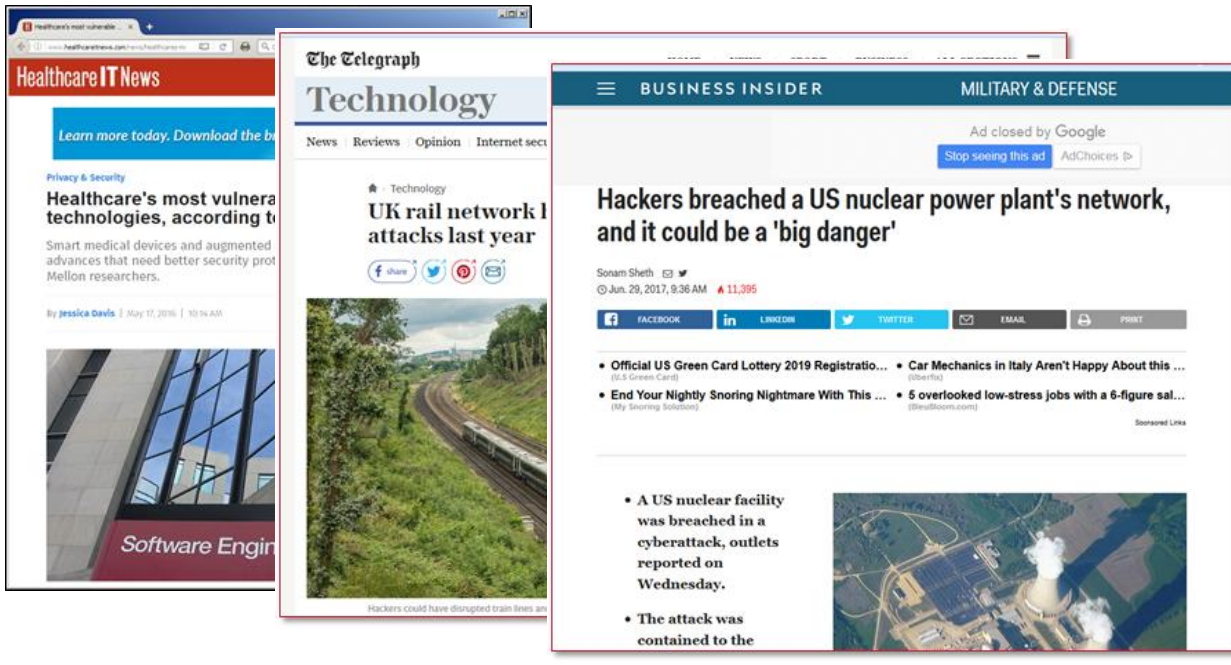


Cybersecurity dei sistemi industriali (1/2)

- I sistemi SCADA sono da sempre progettati per essere **safe** ma non per essere **secure**
- La sicurezza nel mondo SCADA è tradizionalmente stata basata su:
  - il fatto che i sistemi **non fossero accessibili da reti esterne** (*isolation*)
  - il fatto che i sistemi **fossero molto specifici, complessi e oscuri** (*security by obscurity*)
- Poi è arrivato **Stuxnet** (2010):
  - mirato al Siemens Simatic S7-300 (SO WinCC e PCS 7)
  - propagato sia off-line (USB key) che on-line (rete locale)
  - rimasto attivo per mesi fino a che non è uscito all'esterno per errore
  - per rilasciare la patch Siemens ha impiegato 675 giorni!

Cybersecurity dei sistemi industriali (2/2)

- Le vecchie assunzioni di «sicurezza» non sono più valide:
  - i sistemi SCADA sono generalmente **connessi**, e spesso a reti non sicure
  - i sistemi e i protocolli SCADA attuali sono **intrinsecamente insicuri**
  - la conoscenza delle architetture e dei protocolli SCADA non è più un «segreto professionale» di pochi addetti ai lavori
- Il risultato: lo sviluppo e la circolazione di malware «generici» che prendono di mira nativamente i sistemi SCADA
- **Industroyer** (CrashOverride), responsabile di attacchi alle centrali energetiche Ucraine (dicembre 2016):
  - implementa direttamente i protocolli IEC 60870-5-101, IEC 60870-5-104, IEC 61850, e OLE for Process Control Data Access (OPC DA)
  - è in grado di lanciare attacchi DoS contro i sistemi Siemens SIPROTECT, sfruttandone una nota vulnerabilità (CVE-2015-5374)



Dallo spazio cibernetico al dominio ciber-fisico

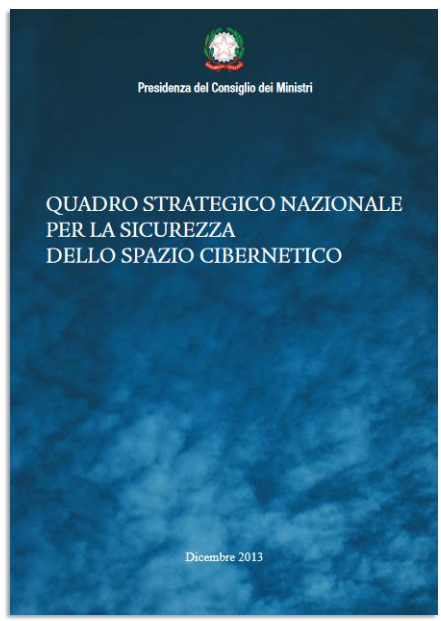
- Il cyberspace non è una dimensione a parte, ma **l'insieme connesso di tutti i sistemi e le reti del pianeta**:
  - le minacce cyber sono globali e pervasive, e il loro bersaglio non è il cyberspace in sé ma sono le infrastrutture del «mondo reale», il cosiddetto **dominio ciber-fisico**
- Il cyberspace è spesso considerato «terra di nessuno» per via dell'assenza di confini evidenti e della mancanza di una chiara giurisdizione:
  - è piuttosto una sorta di «portale» che consente a chiunque di proiettare la sua presenza e le sue attività nel cuore dei sistemi di un'altra nazione senza dover attraversare alcun reale confine: **il cyberspace non è uno spazio topologico**
- Il rapporto costo-benefici di un attacco terroristico o di una campagna criminale di tipo cibernetico diventa sempre migliore perché è sempre più facile raggiungere il bersaglio desiderato e sfruttarne le vulnerabilità

Il cyberspace vulnerabile

- Debolezze **tecniche**:
  - insecurity by design: autenticazione debole, nessuna crittografia, …
  - errori di progetto: protocolli difettosi, algoritmi inadeguati, …
  - errori di implementazione: buffer overflow, codici insicuri, …
- Debolezze date dalla **complessità**:
  - la complessità dei sistemi e delle reti è sempre più elevata
  - il numero di utenti/dispositivi e il volume di traffico sono enormi
  - reti che prima erano separate sono ora interconnesse ed interdipendenti
- Debolezze del **fattore umano** e comportamentale:
  - scarsa consapevolezza e cultura da parte dell'utente finale
  - errata percezione dei rischi delle azioni nel ciberspazio
  - l'assunzione fondamentale (sbagliata…) è che tutti siano in buona fede

Cosa facciamo: attività di prevenzione e contrasto

- Cyberstrategy europea in continua evoluzione:
  - 2013: «An open, safe and secure cyberspace»
  - 2017: «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU»
- Regolamento eIDAS
- Regolamento EU sulla protezione dei dati personali
- Direttiva NIS (Network and Information Security):
  - protezione delle "infrastrutture critiche" (OSE e FSD)
- Cybersecurity Act:
  - certificazione di sicurezza per i prodotti consumer
- Azioni operative:
  - costituzione della rete dei CERT e del CERT-EU
  - European Cyber Security Month
  - esercitazioni cyber europee



Grazie per l'attenzione

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Il Paese che cambia passa da qui.

corrado.giustozzi@agid.gov.it
@cgiustozzi

agid.gov.it