La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

1. Cosa significa TEMPEST;

La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

1. Cosa significa TEMPEST;
2. **La protezione delle informazioni nel contesto aziendale;**

1. Cosa significa TEMPEST;
2. La protezione delle informazioni nel contesto aziendale;
3. **La minaccia;**

1. Cosa significa TEMPEST;
2. La protezione delle informazioni nel contesto aziendale;
3. La minaccia;
4. **Metodi d’attacco per la cattura delle informazioni;**

La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

1. Cosa significa TEMPEST;
2. La protezione delle informazioni nel contesto aziendale;
3. La minaccia;
4. Metodi d’attacco per la cattura delle informazioni;
5. **La difesa;**

La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

1. Cosa significa TEMPEST;
2. La protezione delle informazioni nel contesto aziendale;
3. La minaccia;
4. Metodi d’attacco per la cattura delle informazioni;
5. La difesa;
6. **Impiego della tecnologia TEMPEST in azienda;**

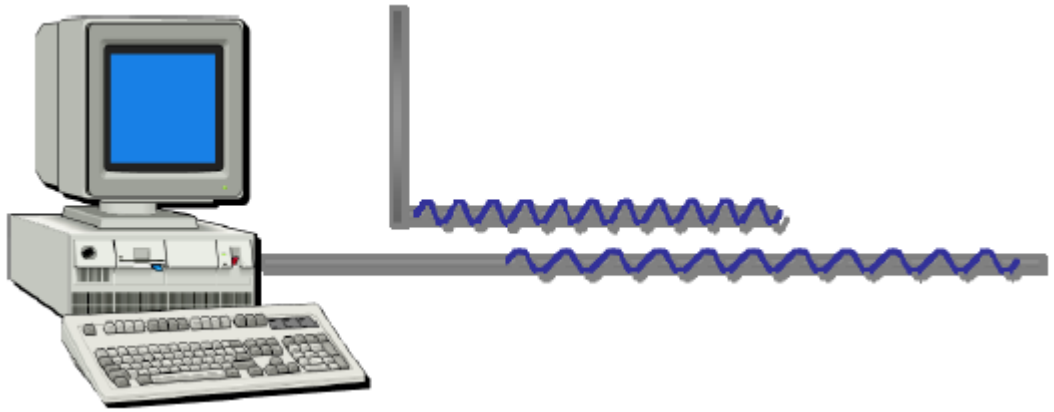
La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

1. Cosa significa TEMPEST;
2. La protezione delle informazioni nel contesto aziendale;
3. La minaccia;
4. Metodi d’attacco per la cattura delle informazioni;
5. La difesa;
6. Impiego della tecnologia TEMPEST in azienda;
7. **Esempi di alcuni materiali TEMPEST;**

La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

Ogni Hardware emette onde elettromagnetiche che possono essere intercettate da strumenti elettronici.

I possibili danni derivanti dalla cattura di informazioni “sensibili” possono vanificare gli investimenti in ricerca e sviluppo causando perdite finanziarie difficili da valutare.



1. Cosa significa TEMPEST

Transient ElectroMagnetic Pulse Emanation Standard

…..

…..

ecc. ecc

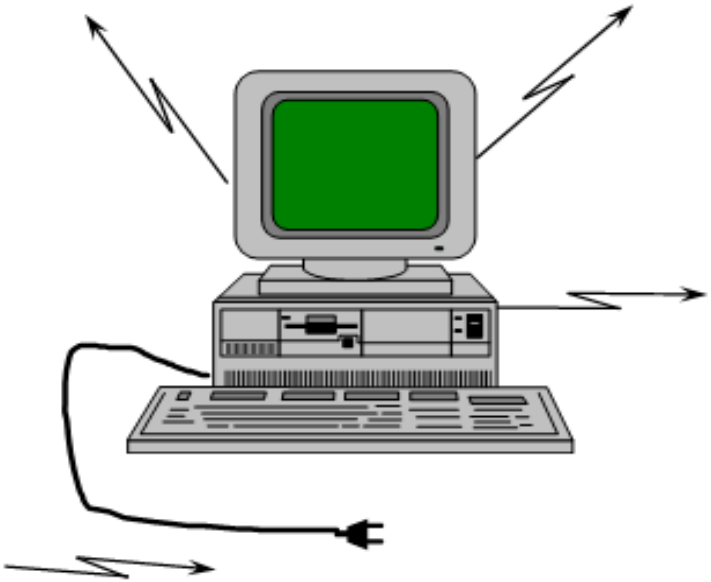
1. Cosa significa TEMPEST

TEMPEST è un nome in codice che si riferisce agli studi sulle emanazioni non intenzionali dei dispositivi elettronici, come computer, monitor, cavi di rete, etc, le quali possono compromettere la sicurezza dei dati trattati.
Tali emissioni, dette compromising emanations (emissioni compromettenti) o CE, consistono in energia elettrica, meccanica o acustica rilasciata intenzionalmente o meno da varie sorgenti all'interno dei dispositivi che manipolano le informazioni classificate o sensibili.

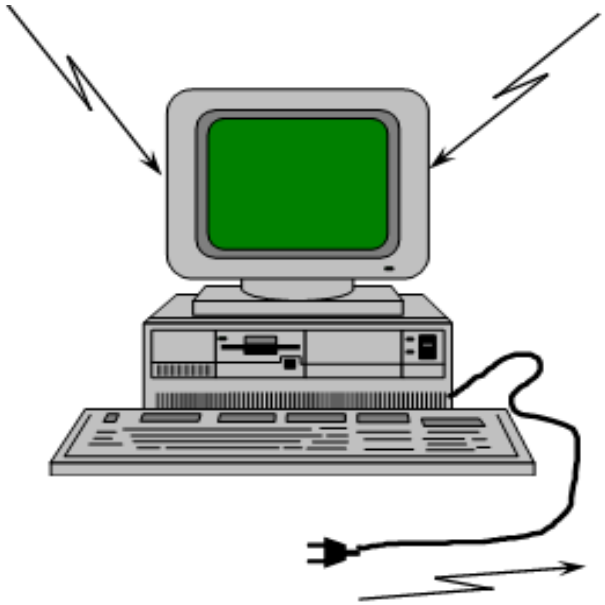
Le variazioni dell'energia rilasciata possono essere fatte risalire al messaggio originale, o alle informazioni che sono processate, in maniera da ricostruire l'originale. La possibilità di intercettare e decodificare tali informazioni dipendono da vari fattori, tra cui il "rumore", acustico o elettromagnetico, dell'ambiente, e la sicurezza intrinseca dei dispositivi.

1. Cosa significa TEMPEST (dove siamo vulnerabili?)

Emissione (EMI)



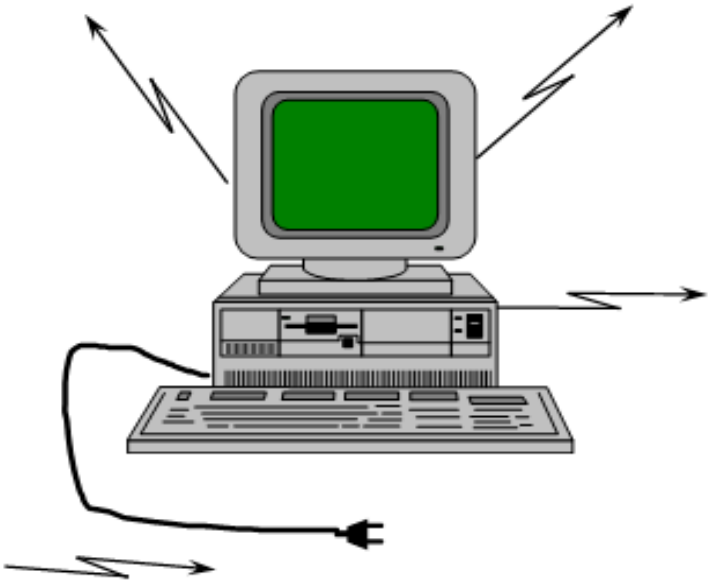
Suscettibilità (EMS)



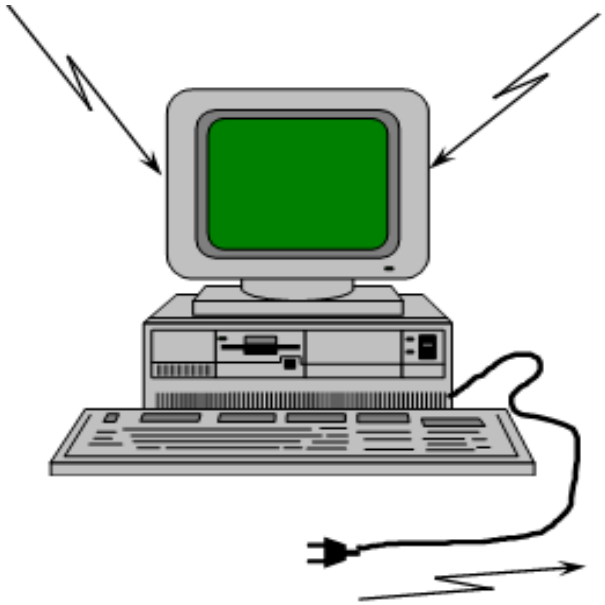
✓**Tipi di Misure EMC**

1. Cosa significa TEMPEST (dove siamo vulnerabili?)

Emissione (EMI)



Suscettibilità (EMS)

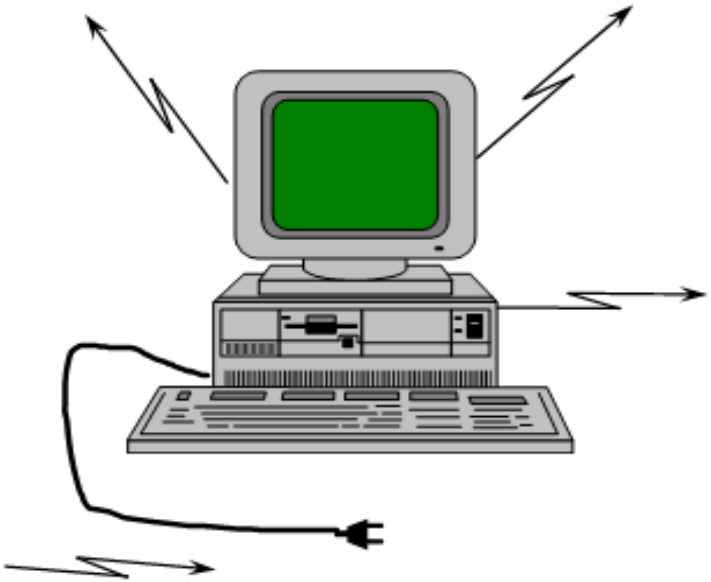


Tipi di Misure EMC

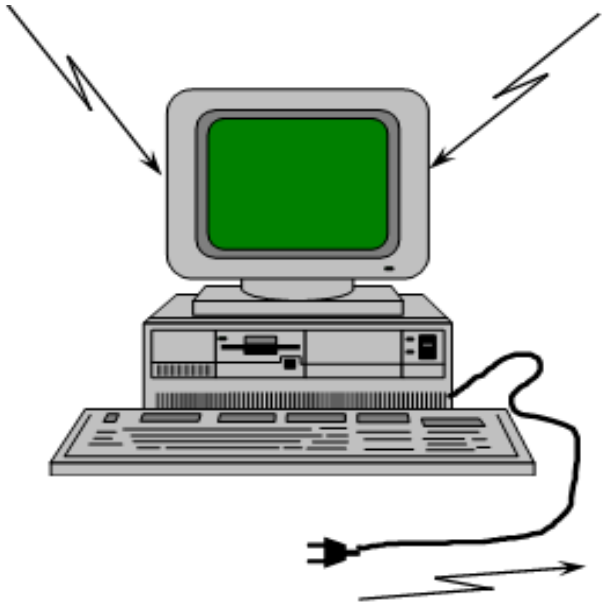
- ✓ **per conduzione**
- ✓ per radiazione

1. Cosa significa TEMPEST (dove siamo vulnerabili?)

Emissione (EMI)



Suscettibilità (EMS)

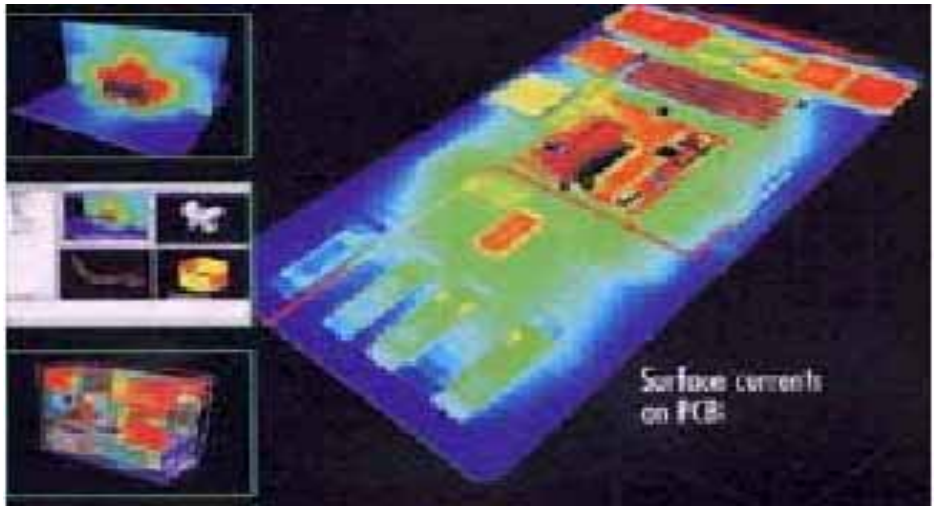


Tipi di Misure EMC

- ✓ per conduzione
- ✓ **per radiazione**

1. Cosa significa TEMPEST

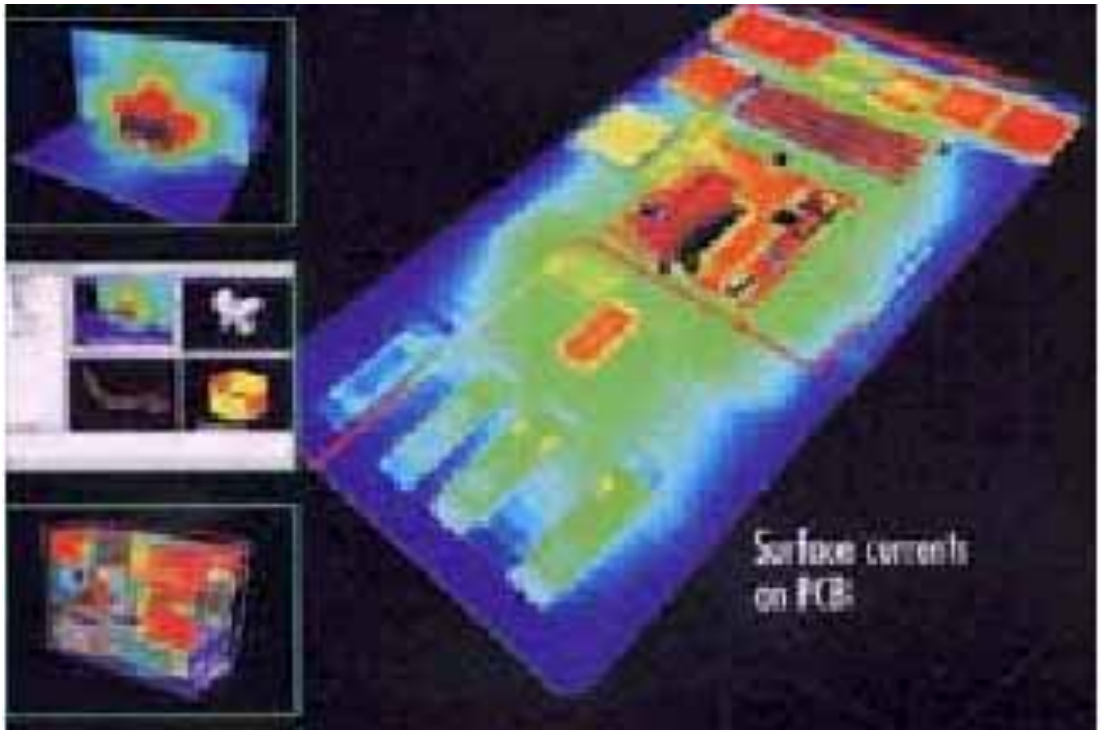
Fonti d'emanazione compromissorie



1. Cosa significa TEMPEST

Fonti d'emanazione compromissorie

✓**Monitor**

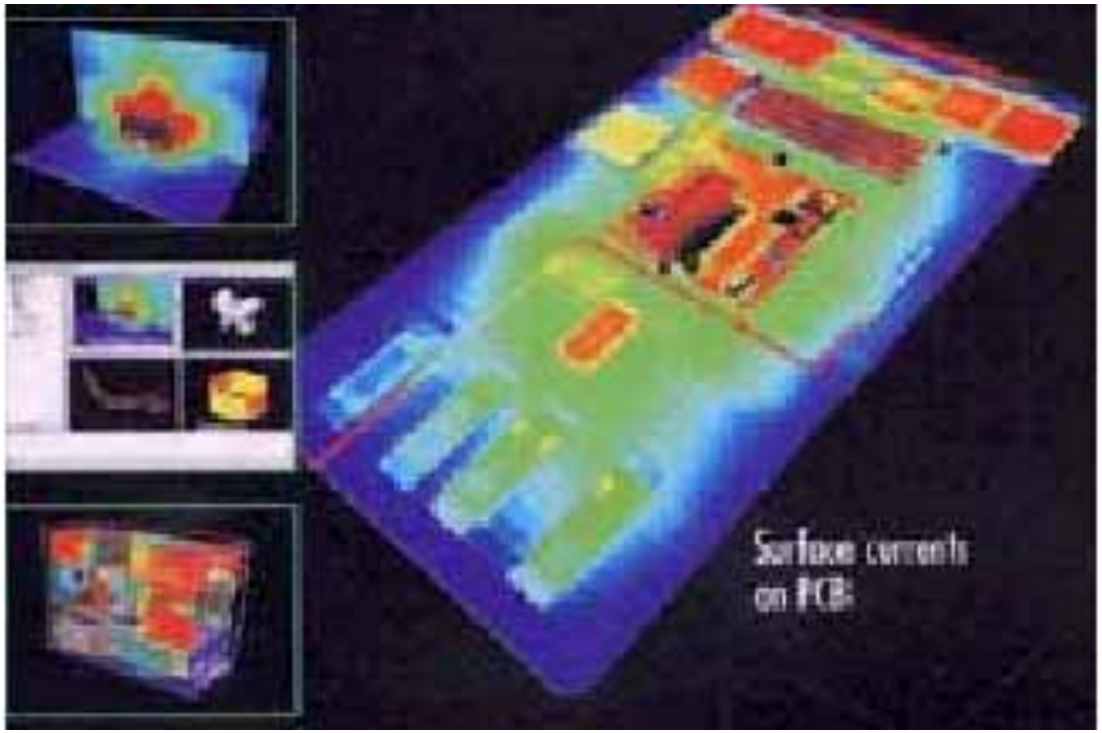


1. Cosa significa TEMPEST

Fonti d'emanazione compromissorie

✓Monitor

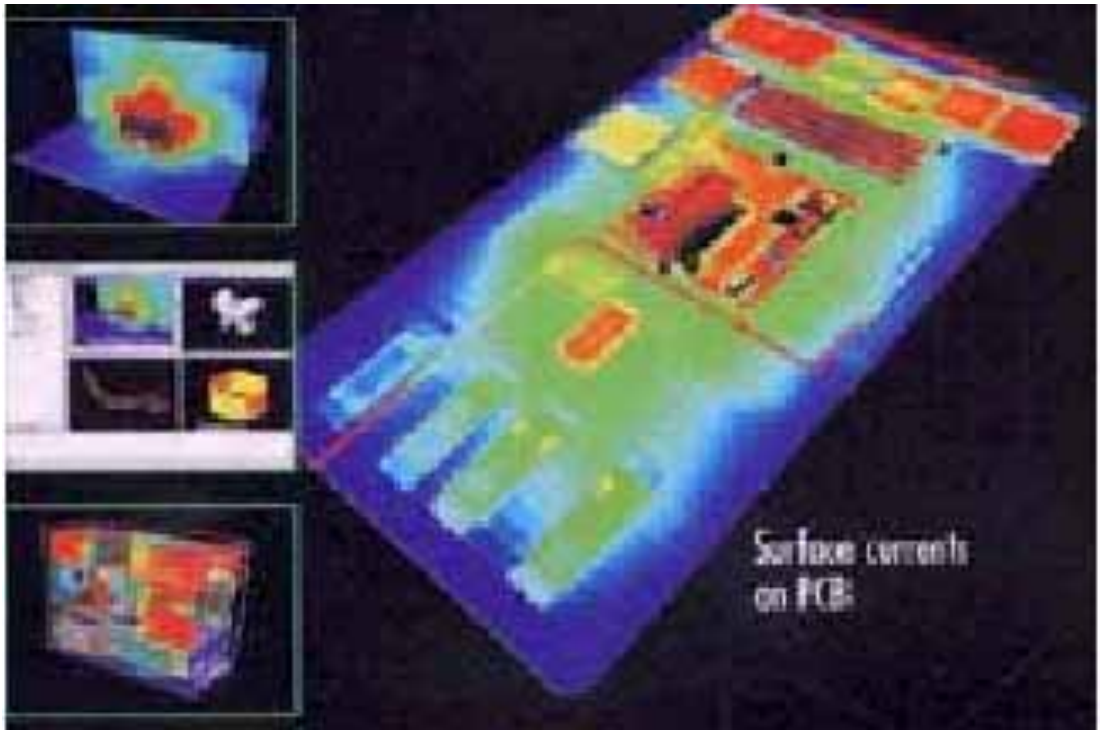
✓**Computers**



1. Cosa significa TEMPEST

Fonti d'emanazione compromissorie

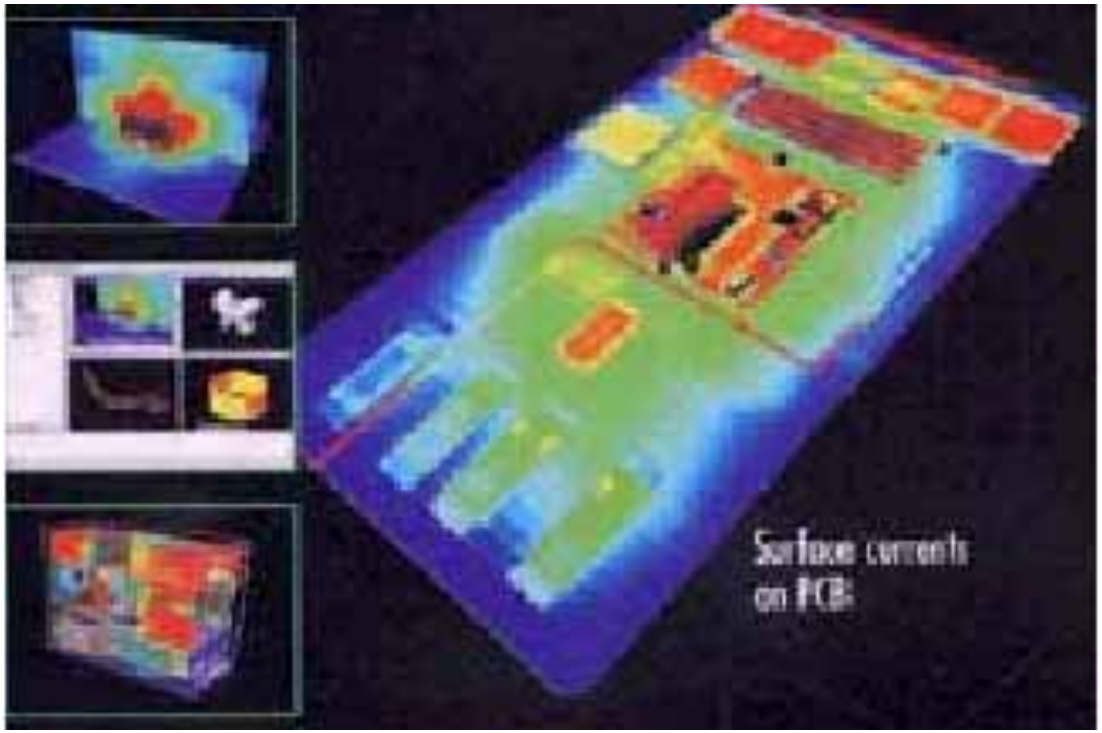
- ✓Monitor
- ✓Computers
- ✓**Tastiere**



1. Cosa significa TEMPEST

Fonti d'emanazione compromissorie

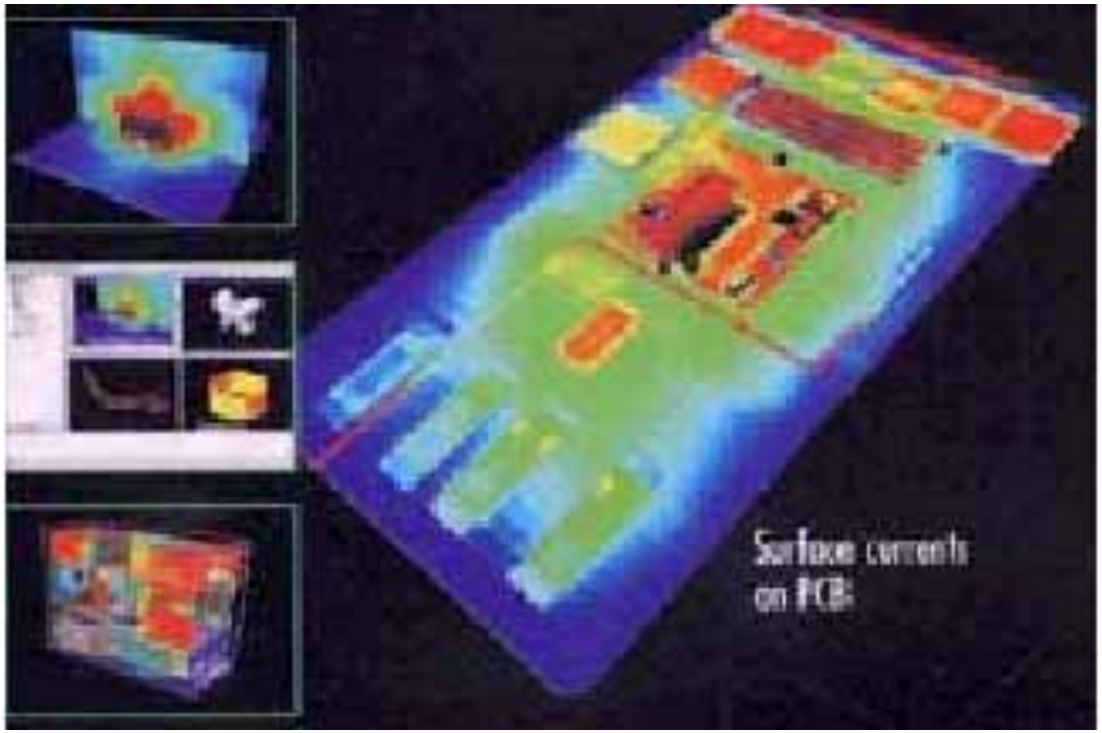
- ✓Monitor
- ✓Computers
- ✓Tastiere
- ✓**Porte I/O e cavi**



1. Cosa significa TEMPEST

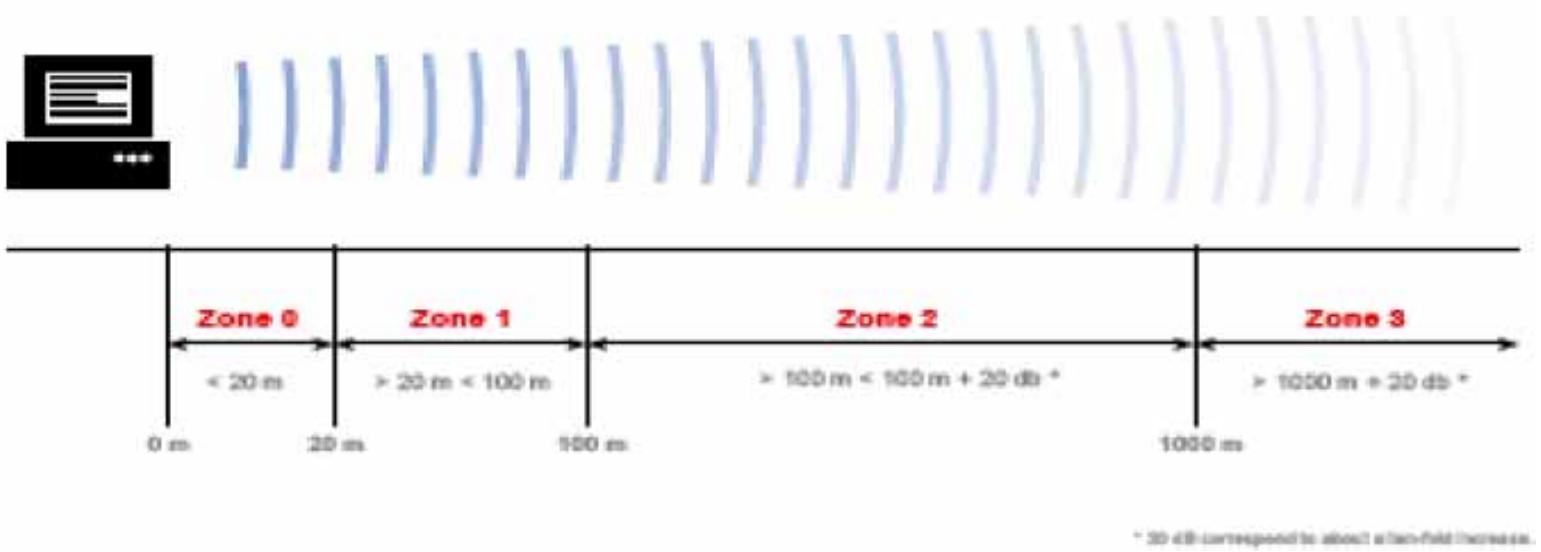
Fonti d'emanazione compromissorie

- ✓Monitor
- ✓Computers
- ✓Tastiere
- ✓Porte I/O e cavi
- ✓**Periferiche**



1. Cosa significa TEMPEST (dove siamo vulnerabili?)

Distanze d'intercettazione TEMPEST



1. Cosa significa TEMPEST

TEMPEST standards

NATO SDIP-27 Standards	Former NATO AMSG Standards	USA NSTISSAM 1-92 Standards	NATO Tempest Zoning Standards
Level A	AMSG 720B	Level I	Zone 0
Level B	AMSG 788A	Level II	Zone 1
Level C	AMSG 784	Level III	Zone 2

SECAN Doctrine and Information Publication
SDIP- 27 Level A, B, C

2. La protezione delle informazioni nel contesto aziendale

2. La protezione delle informazioni nel contesto aziendale

a. Individuazione delle risorse da proteggere;

2. La protezione delle informazioni nel contesto aziendale

a. Individuazione delle risorse da proteggere;
b. Valutazione dell'entità del rischio;

2. La protezione delle informazioni nel contesto aziendale

a. Individuazione delle risorse da proteggere;
b. Valutazione dell'entità del rischio;
c. Valutazione del possibile danno economico;

2. La protezione delle informazioni nel contesto aziendale

a. Individuazione delle risorse da proteggere;
b. Valutazione dell'entità del rischio;
c. Valutazione del possibile danno economico;
d. Ricerca delle soluzioni per la riduzione del rischio;

2. La protezione delle informazioni nel contesto aziendale

a. Individuazione delle risorse da proteggere;
b. Valutazione dell'entità del rischio;
c. Valutazione del possibile danno economico;
d. Ricerca delle soluzioni per la riduzione del rischio;
e. Armonizzazione della/e soluzioni con il piano generale di sicurezza aziendale;

2. La protezione delle informazioni nel contesto aziendale

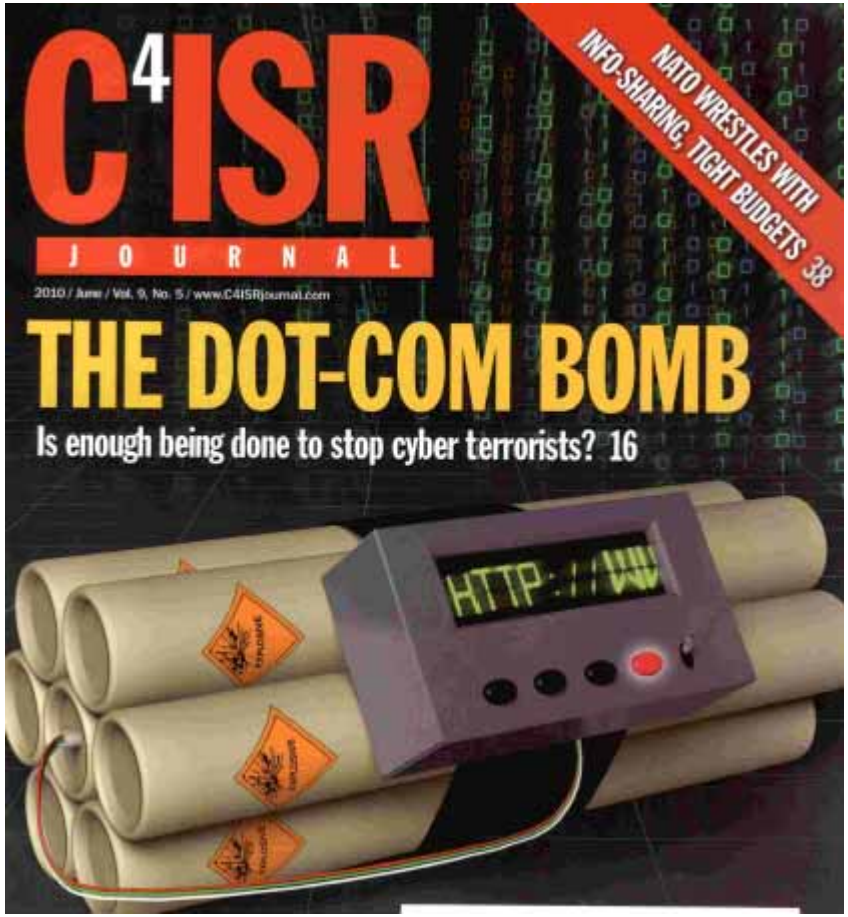
a. Individuazione delle risorse da proteggere;
b. Valutazione dell'entità del rischio;
c. Valutazione del possibile danno economico;
d. Ricerca delle soluzioni per la riduzione del rischio;
e. Armonizzazione della/e soluzioni con il piano generale di sicurezza aziendale;
f. Pianificazione degli interventi (costi, tempi, impatti sui lavori correnti, ecc. ecc.)

2. La protezione delle informazioni nel contesto aziendale

a. Individuazione delle risorse da proteggere;
b. Valutazione dell'entità del rischio;
c. Valutazione del possibile danno economico;
d. Ricerca delle soluzioni per la riduzione del rischio;
e. Armonizzazione della/e soluzioni con il piano generale di sicurezza aziendale;
f. Pianificazione degli interventi (costi, tempi, impatti sui lavori correnti, ecc. ecc.)
g. Addestramento del personale ai nuovi criteri di sicurezza;

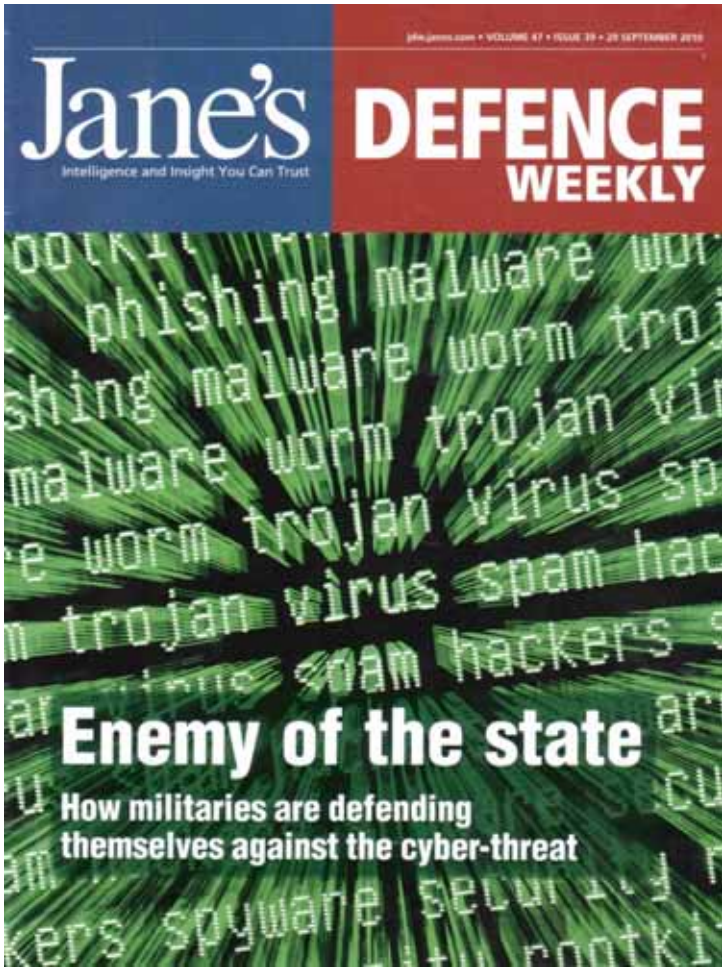
3. La minaccia (Spionaggio industriale)

L’allarme di C4ISR, rivista statunitense del settore



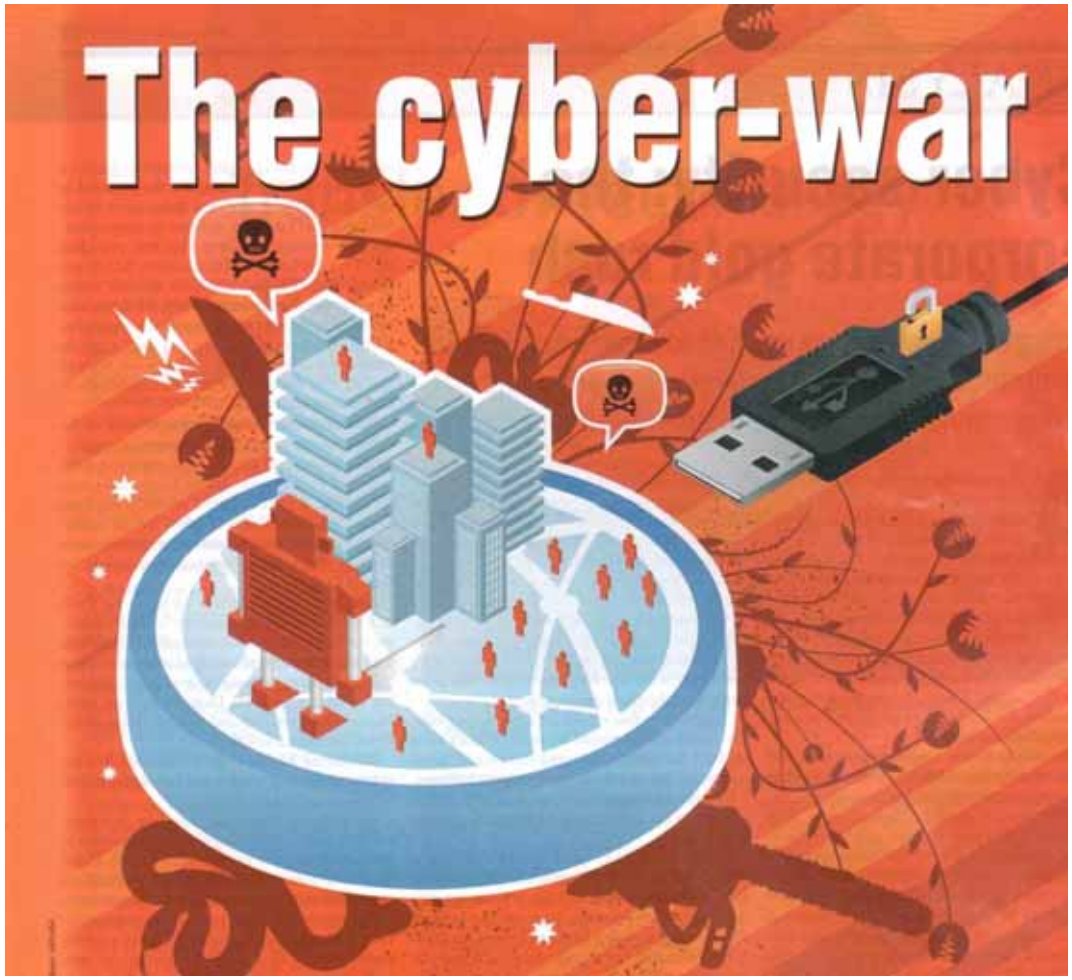
3. La minaccia
(Spionaggio industriale)

… sul settimanale inglese di difesa Jane's Defence Weekly del 29 settembre…
…l'industria è uno degli obiettivi



3. La minaccia
(Spionaggio industriale)

… il 29 u.s. su Jane's Defence Weekly



3. La minaccia (Spionaggio industriale)

… e il nostro Sole24ore

Il Sole 24 Ore
Mercoledì 23 Giugno 2010 - N. 171

Germania. Nel rapporto annuale dei servizi segreti allarme sulla protezione del know-how del paese

Berlino attacca le spie industriali

Da Russia e Cina i rischi maggiori per le imprese tedesche

La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

3. La minaccia
(Spionaggio industriale)

… e il
nostro
Sole24ore

Beda Romano

FRANCOFORTE. Dal nostro corrispondente

Nel 2007, il governo federale denunciò il clamoroso tentativo di alcuni hacker cinesi di introdursi nei computer della Cancelleria. La vicenda, ormai dimenticata, appare oggi come il segnale di un fenomeno in forte crescita. Per decenni, lo spionaggio ha colpito soprattutto i governi: attualmente a farne le spese sono anche le imprese, in particolare quelle tedesche così proiettate sui grandi mercati internazionali.

Nel suo rapporto annuale pubblicato questa settimana, l'Ufficio federale per la protezione della Costituzione, vale a dire i servizi segreti tedeschi, ha avvertito che due sono i rischi principali per la democrazia tedesca: l'estremismo politico di sinistra e lo spionaggio industriale. «Quest'ultimo tema è sempre più sentito nei piani alti delle grandi imprese tedesche», ha sottolineato Thomas de Maizière, il ministro dell'Interno.

In un rapporto di oltre 300 pagine che minuziosamente fa il punto sulla violenza politica e non in Germania, i servizi segreti puntano il dito in particolare contro la Cina e la Russia, due paesi alla ricerca disperata di know-how tecnologico e che vedono nelle imprese tedesche, piccole e grandi, una straordinaria cassaforte di dati e invenzioni di cui impadronirsi in un modo o nell'altro.

Le autorità tedesche non vogliono dare stime ufficiali su quanto ogni anno le imprese perdono a causa di un fenomeno in crescita. Associazioni di categoria calcolano però che il danno possa essere tra i 20 e i 50 miliardi di euro. Dietro allo spionaggio industriale si nasconde il successo delle società tedesche nel settore manifatturiero e la loro forte esposizione internazionale attraverso anche una crescente delocalizzazione.

In questo senso, alcuni dati societari fanno impressione. Nel 2009 Siemens contava 176 centri di R&D in tutto il mondo; la società ha registrato l'anno scorso 7.700 nuove invenzioni che sono andate ad aggiungersi agli oltre 56mila brevetti tutt'ora attivi. Sempre nel 2009, Bosch ha speso in ricerca 3,6 miliardi di euro, su un fatturato di 38 miliardi, mentre il gigante della chimica Basf aveva a livello mondiale 385 siti di produzione.

Secondo il governo tedesco, lo spionaggio industriale può avvenire in modi diversi. Non bisogna sospettare soltanto diplomatici o giornalisti. Anche i professori a contratto, gli studenti e gli stagisti potrebbero essere delle spie. Dalla Cina l'interesse riguarda i processi produttivi, le scoperte scientifiche e i nuovi prodotti. Dalla Russia, invece, lo sguardo corre al grande settore energetico, tradizionale e alternativo.

La Germania sta cavalcando la forte ripresa economica dei paesi emergenti grazie a una produzione manifatturiera di qualità. Come le imprese italiane, i gruppi tedeschi devono battere la concorrenza straniera, spesso meno costosa, grazie a prodotti sempre più innovativi. Il ministro de Maizière ha quindi esortato le imprese a lavorare insieme al governo per meglio difendersi dallo spionaggio industriale.

Heinz Schulte, il direttore della rivista Griephan Global Security dedicata ai problemi di sicurezza nelle aziende, sottolinea che il problema riguarda soprattutto le imprese più piccole: «Non sempre ci si rende conto che quando si costruisce, per esempio, un componente anche piccolo di un sistema aerospaziale molto complesso vi è dall'altra parte del mondo un'azienda concorrente che potrebbe esservi interessata».

L'analisi di Schulte è condivisa da altri. Mentre molte grandi imprese hanno uno staff dedicato alla sicurezza e non esitano a dedicarvi una parte notevole del bilancio, quelle più piccole sono in ritardo. Mario Ohoven, il presidente dell'associazione che raggruppa le piccole e medie aziende tedesche Bvmw, ha avvertito che «molte società sottostimano ancora il pericolo di diventare vittime di spionaggio».

Il ministro. Thomas de Maizière

L'IMPATTO ECONOMICO

Danni potenziali fino a 50 miliardi e la delocalizzazione aggrava il fenomeno

Pericoli con ricercatori a contratto e studenti

3. La minaccia (Spionaggio industriale)

Il Sole 24 Ore
Mercoledì 23 Giugno 2010 - N. 171

Germania. Nel rapporto annuale dei servizi segreti allarme sulla protezione del know-how del paese

Berlino attacca le spie industriali

Da Russia e Cina i rischi maggiori per le imprese tedesche

… e dall'articolo:

✓BND: «*due sono i rischi principali per la democrazia tedesca: l'estremismo politico di sinistra e lo spionaggio industriale* »

3. La minaccia (Spionaggio industriale)

Il Sole 24 Ore
Mercoledì 23 Giugno 2010 - N. 171

Germania. Nel rapporto annuale dei servizi segreti allarme sulla protezione del know-how del paese

Berlino attacca le spie industriali

Da Russia e Cina i rischi maggiori per le imprese tedesche

… e dall'articolo:

✓BND: «*due sono i rischi principali per la democrazia tedesca: l'estremismo politico di sinistra e lo spionaggio industriale* »

✓Associazioni di categoria calcolano però che il **danno** possa essere tra i **20 e i 50 miliardi di €**.

3. La minaccia (Spionaggio industriale)


Il Sole 24 Ore
Mercoledì 23 Giugno 2010 - N. 171

Germania. Nel rapporto annuale dei servizi segreti allarme sulla protezione del know-how del paese

Berlino attacca le spie industriali

Da Russia e Cina i rischi maggiori per le imprese tedesche

… e dall'articolo:

✓BND: «*due sono i rischi principali per la democrazia tedesca: l'estremismo politico di sinistra e lo spionaggio industriale* »

✓Associazioni di categoria calcolano però che il **danno** possa essere tra i **20 e i 50 miliardi di €**.

✓Mario Ohoven,il presidente dell'associazione delle piccole e medie aziende tedesche Bvmw (Confapi tedesca), ha avvertito che «*molte società sottostimano ancora il pericolo di diventare vittime di spionaggio*».

3. La minaccia (Spionaggio industriale)

… da Il Monferrato On Line:

2008-02-14 il caso **DimSport**

✓FOTO. Investigatori, titolari dell'azienda di Camino e materiale informatico sequestrato.

3. La minaccia (Spionaggio industriale)

… da Il Monferrato On Line:

2008-02-14 il caso **DimSport**

✓FOTO. Investigatori, titolari dell'azienda di Camino e materiale informatico sequestrato.

✓in meno di due anni un **danno** alla società stessa di circa **€ 1.100.000**

3. La minaccia (Spionaggio industriale)

… da Il Monferrato On Line:

2008-02-14 il caso **DimSport**

✓FOTO. Investigatori, titolari dell'azienda di Camino e materiale informatico sequestrato.

✓in meno di due anni un **danno** alla società stessa di circa **€ 1.100.000**

✓La PMI occupa una sessantina di dipendenti e studia, progetta e produce apparati elettronici per la messa a punto di motori montati su autoveicoli, motoveicoli, camion ecc.

3. La minaccia (Spionaggio industriale)

3. La minaccia (Spionaggio industriale)

a. **Tecnologica (ELINT, SIGINT, EMSEC e COMSEC)**;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC);
b. Umana (HUMINT);

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC)
b. Umana (HUMINT);
c. Subdola;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC)
b. Umana (HUMINT);
c. Subdola;
d. Difficile da individuare e da contrastare;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC)
b. Umana (HUMINT);
c. Subdola;
d. Difficile da individuare e da contrastare;
e. Imprevedibile;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC);
b. Umana (HUMINT);
c. Subdola;
d. Difficile da individuare e da contrastare;
e. Imprevedibile;
f. Senza limiti temporali;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC)
b. Umana (HUMINT);
c. Subdola;
d. Difficile da individuare e da contrastare;
e. Imprevedibile;
f. Senza limiti temporali;
g. Senza limiti geografici;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC)
b. Umana (HUMINT);
c. Subdola;
d. Difficile da individuare e da contrastare;
e. Imprevedibile;
f. Senza limiti temporali;
g. Senza limiti geografici;
h. Mirata;

3. La minaccia (Spionaggio industriale)

a. Tecnologica (ELINT, SIGINT, EMSEC ed INFOSEC);
b. Umana (HUMINT);
c. Subdola;
d. Difficile da individuare e da contrastare;
e. Imprevedibile;
f. Senza limiti temporali;
g. Senza limiti geografici;
h. Mirata;

Ecc. ecc.

4. Metodi d’attacco per la cattura delle informazioni

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;

b. Intercettazione ambientale;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;
b. Intercettazione ambientale;
c. Intercettazione elettromagnetica;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;
b. Intercettazione ambientale;
c. Intercettazione elettromagnetica;
d. Internet, intranet, WIFI;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;
b. Intercettazione ambientale;
c. Intercettazione elettromagnetica;
d. Internet, intranet, WIFI;
e. **Fotografie**;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;
b. Intercettazione ambientale;
c. Intercettazione elettromagnetica;
d. Internet, intranet, WIFI;
e. Fotografie;
f. **Registratori**;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;
b. Intercettazione ambientale;
c. Intercettazione elettromagnetica;
d. Internet, intranet, WIFI;
e. Fotografie;
f. Registratori;
g. **Garbage collection**;

4. Metodi d'attacco per la cattura delle informazioni

a. Intercettazione telefonica;
b. Intercettazione ambientale;
c. Intercettazione elettromagnetica;
d. Internet, intranet, WIFI;
e. Fotografie;
f. Registratori;
g. Garbage collection;

ecc. ecc.;

5. La difesa

5. La difesa

a. **Attiva**;

5. La difesa

a. Attiva;

b. **Passiva**;.

5. La difesa

a. Attiva;
b. Passiva;
c. **Complessa**;

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. **Articolata**;

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. **Fluida**;

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. Fluida;
f. **Riservata**;

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. Fluida;
f. Riservata;
g. **In costante aggiornamento**;

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. Fluida;
f. Riservata;
g. In costante aggiornamento;
h. **Tecnologica (INFOSEC);**.

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. Fluida;
f. Riservata;
g. In costante aggiornamento;
h. Tecnologica (INFOSEC);
i. **Omnidirezionale**;.

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. Fluida;
f. Riservata;
g. In costante aggiornamento;
h. Tecnologica (INFOSEC);
i. Omnidirezionale;
j. Nella coscienza degli attori in azienda;

5. La difesa

a. Attiva;
b. Passiva;
c. Complessa;
d. Articolata;
e. Fluida;
f. Riservata;
g. In costante aggiornamento;
h. Tecnologica (INFOSEC);
i. Omnidirezionale;
j. Nella coscienza degli attori in azienda;

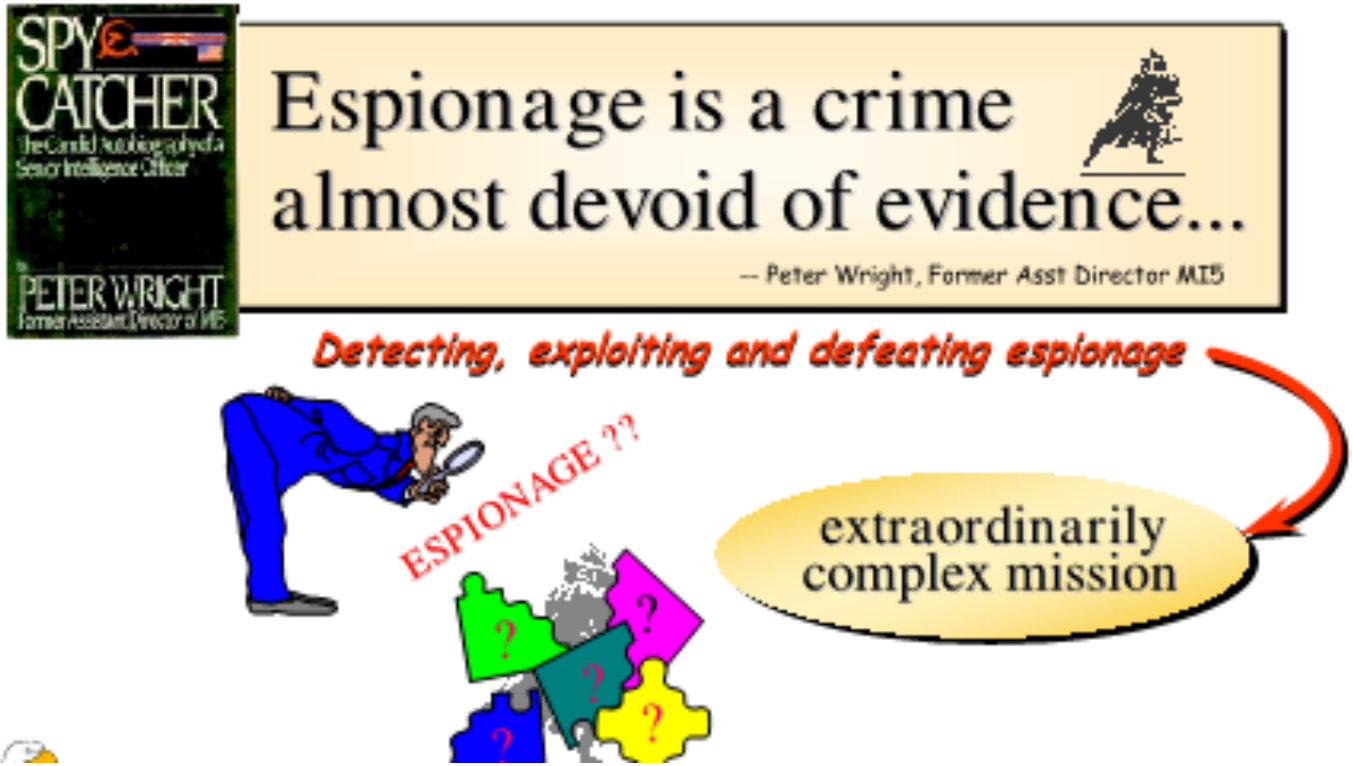
ecc. ecc.

5. La difesa

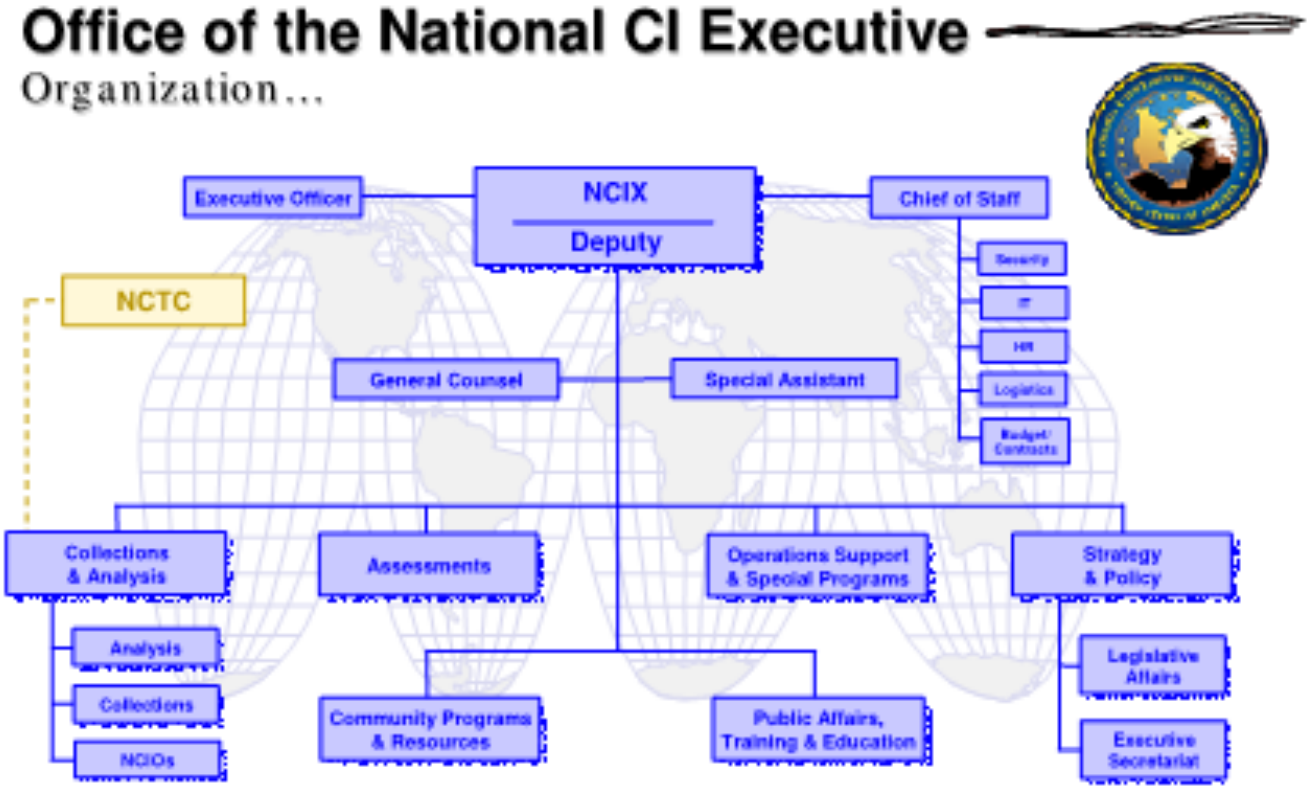
Counterintelligence versus Security

	COUNTERINTELLIGENCE	SECURITY
Activities	• CI Investigations • CI Operations (Defensive & Offensive) • CI Collection/Liaison • CI Analysis/Production • CI Services to include TSCM, CI polygraphs, CI training & awareness, etc.	• Physical Security/Facilities Protection • Industrial & Personnel Security • Personnel Security Investigations • AIS/Information Systems Security • Information Security/Document Control • Personnel Protection Operations • Security Education & Training
Focus:	Sword directed at the adversary collector… identify/understand/counter adversary collection efforts *…mission driven*	Shield to protect friendly activities… establish/adhere to standards; fix system weaknesses *…rule driven*
Objective:	deter/detect/disrupt/control adversary collection *…reduce or control "threat"*	deny/prevent unauthorized access *…reduce "vulnerability"*
Perspective:	adversary's perspective *…looking "outside - in"*	internal perspective *…looking "inside - out"*
Concern:	clandestine & covert threats	unauthorized access
Key Authorities:	EO 12333; NSPD-1; PDD-24; PDD-75; PDD-63; CI Enhancement Act of 2002; DoDD 5240.2; and DoDI 5240.1	EO 12958, 12968 & 12829; PDD-63; NSSD-298; DoDD 5200.1/.8/.28; DoD 5200.1-R/.2-R; 5200.8-R; & 5220.22-R/-M
Nat'l Board:	National CI Policy Board (NCIPB)	**PCC/RA & IS** (Records Access & Info Security) Security Policy Board (SPB) originally established Sep 94 (PDD-29) was abolished via NSPD-1 (13 Feb 2001)

5. La difesa


SPY CATCHER
PETER WRIGHT
Espionage is a crime almost devoid of evidence...
-- Peter Wright, Former Asst Director MI5
Detecting, exploiting and defeating espionage
ESPIONAGE ??
extraordinarily complex mission

5. La difesa (sembra facile…)



La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

5. La difesa

Dal **Manuale di controspionaggio industriale**
Ministero della Difesa USA

CHAPTER 11
Miscellaneous Information

Section 1. TEMPEST

11-100. General. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

11-101. TEMPEST Requirements.

a. TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security should the information be intercepted and analyzed by a foreign intelligence organization. It is the responsibility of the GCA to identify in writing what TEMPEST countermeasures may be required. The GCA will identify any TEMPEST requirements within the United States to the CSA for approval prior to imposing requirements for TEMPEST countermeasures on contractors. Contractors may not impose TEMPEST countermeasures upon their subcontractors without GCA and CSA approval.

b. The government is responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed to TEMPEST collection.

c. Contractors will assist the GCA in conducting threat and vulnerability surveys by providing the following information upon request:

(1) The specific classification and special categories of material to be processed/handled by electronic means.

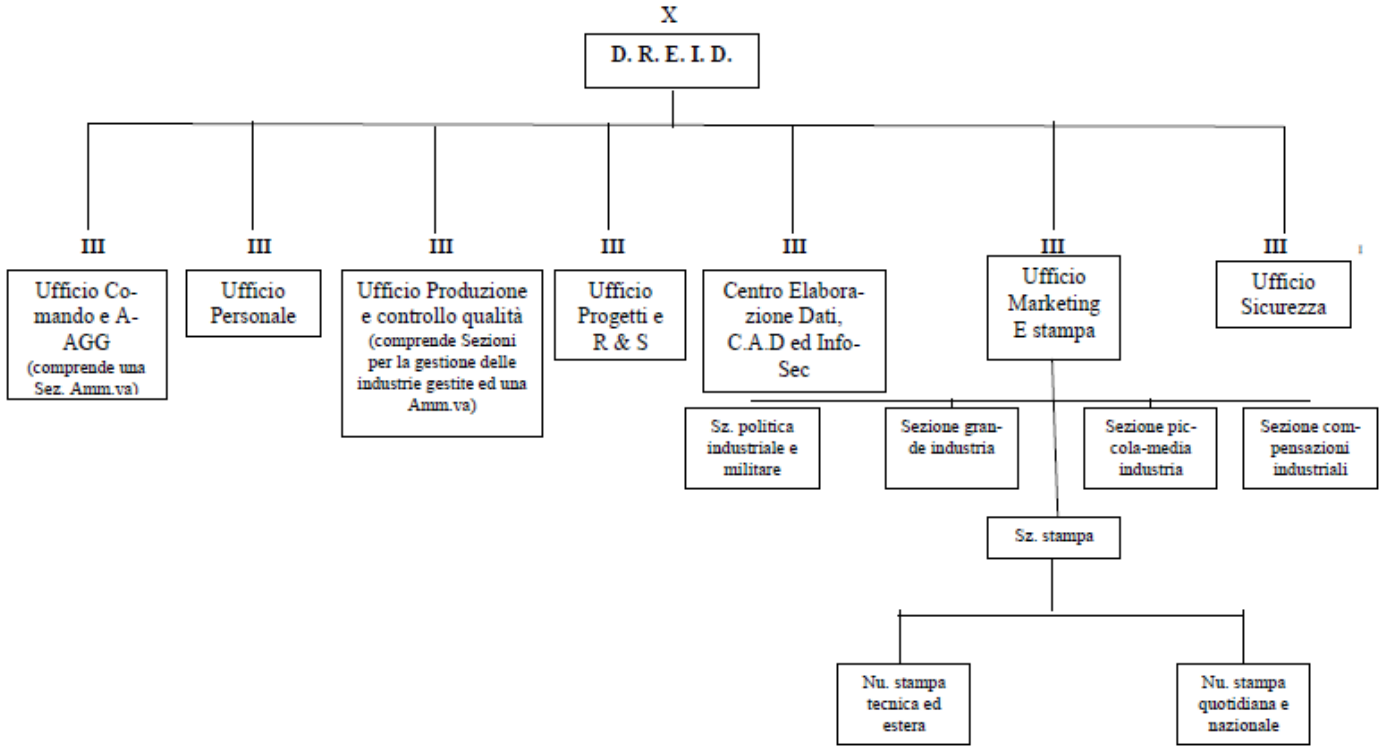
(2) The specific location where classified processing will be performed.

(3) The name, address, title, and contact information for a point-of-contact at the facility where processing will occur.

11-102. Cost. All costs associated with applying TEMPEST countermeasures, when such countermeasures are imposed upon the contractor by a GCA, shall be recoverable by direct charge to the applicable contract. The GCA should provide TEMPEST shielding and shielded equipments as government-furnished equipment (GFE) when such extreme countermeasures are deemed essential to the protection of the information being processed.

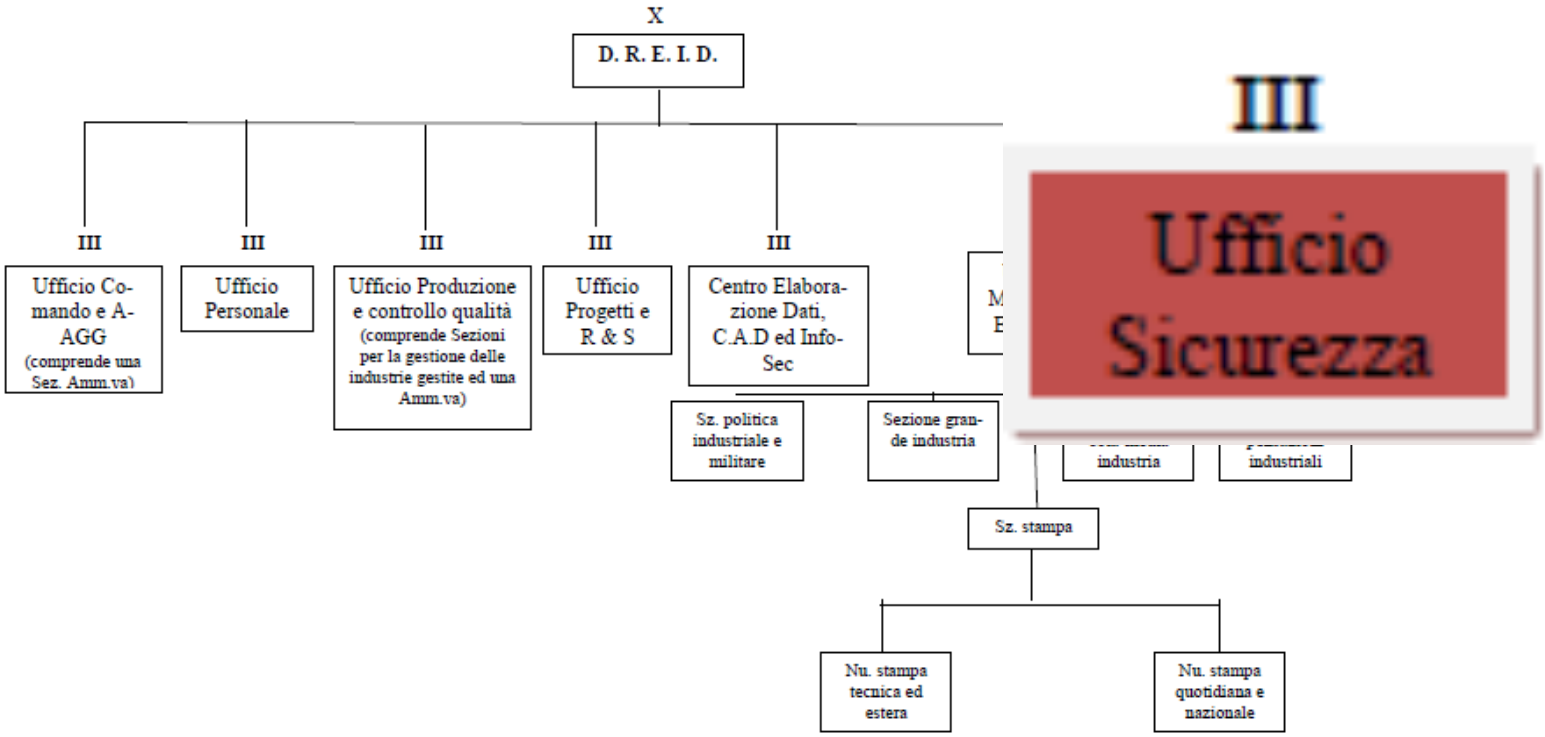
5. La difesa

Una **possibile soluzione italiana:** Delegazione Regionale Equipaggiamenti ed Industria per la Difesa **DREID**



5. La difesa

Una **possibile soluzione italiana:** Delegazione Regionale Equipaggiamenti ed Industria per la Difesa **DREID**



6. Impiego della tecnologia TEMPEST in azienda

6. Impiego della tecnologia TEMPEST in azienda

a. **Efficace ed immediata come protezione**;.

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. **Omnidirezionale**;

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. **Difficile da attaccare**;.

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. **Facile da impiegare**;

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. **Non aggiunge ritardi ai ritmi aziendali**;

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. Non aggiunge ritardi ai ritmi aziendali;
f. **Rapporto costo/efficacia vantaggioso**;.

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. Non aggiunge ritardi ai ritmi aziendali;
f. Rapporto costo/efficacia vantaggioso;
g. **Include altre forme di protezione**;

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. Non aggiunge ritardi ai ritmi aziendali;
f. Rapporto costo/efficacia vantaggioso;
g. Include altre forme di protezione;
h. **Integrabile con sistemi esistenti**;

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. Non aggiunge ritardi ai ritmi aziendali;
f. Rapporto costo/efficacia vantaggioso;
g. Include altre forme di protezione;
h. Integrabile con sistemi esistenti;
i. **Articolabile**.

6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. Non aggiunge ritardi ai ritmi aziendali;
f. Rapporto costo/efficacia vantaggioso;
g. Include altre forme di protezione;
h. Integrabile con sistemi esistenti;
i. Articolabile
j. **Previene attacchi SIGINT**;.

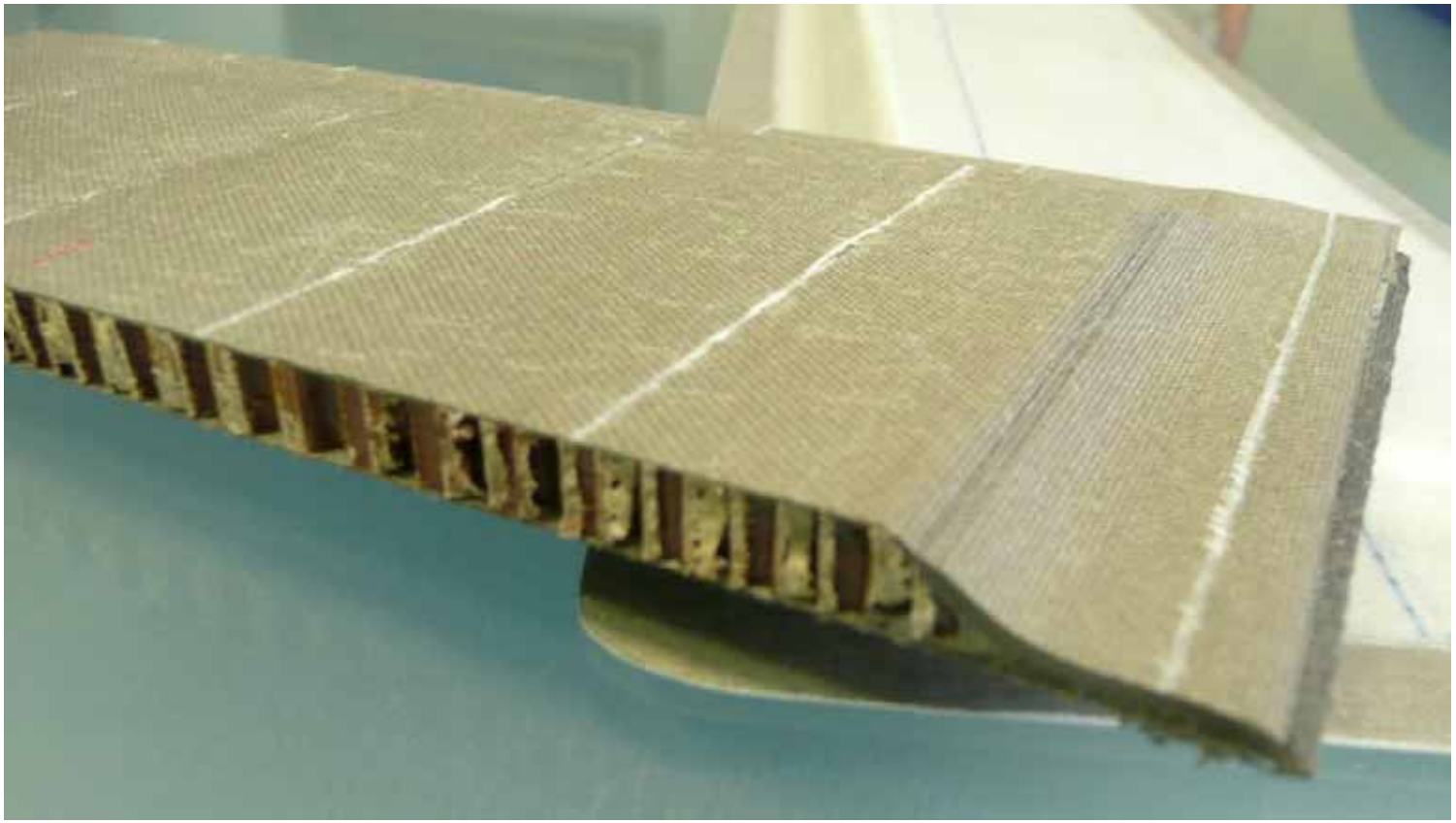
6. Impiego della tecnologia TEMPEST in azienda

a. Efficace ed immediata come protezione;
b. Omnidirezionale;
c. Difficile da attaccare;
d. Facile da impiegare;
e. Non aggiunge ritardi ai ritmi aziendali;
f. Rapporto costo/efficacia vantaggioso;
g. Include altre forme di protezione;
h. Integrabile con sistemi esistenti;
i. Articolabile
j. Previene attacchi SIGINT;
k. Fondamentale nella strategia INFOSEC.

7. Esempi di materiali TEMPEST

7. Esempi di materiali TEMPEST

SOLIANI emc s.r.l.
Protezioni Interferenze Elettromagnetiche
EMI - RFI - ESD - TEMPEST



7. Esempi di materiali TEMPEST

7. Esempi di materiali TEMPEST

SOLIANI emc s.r.l.
Protezioni Interferenze Elettromagnetiche
EMI - RFI - ESD - TEMPEST

7. Esempi di materiali TEMPEST

PRINTERS




Based on HP
SDIP-27 Level A, B, C

SCANNERS


Based on Pentax Dsmobile 600
SDIP-27 Level A, B, C

Based on HP SJ8300
SDIP-27 Level A, B, C

Siltec

NETWORK EQUIPMENT



Based on HP, SUN, AT
SDIP-27 Level A, B, C

7. Esempi di materiali TEMPEST

Siltec

TEMPEST PRODUCTS

SHIELDED CABINETS

La tecnologia TEMPEST per la sicurezza e protezione dei dati aziendali

Non sottovalutare la minaccia è un ottimo investimento!

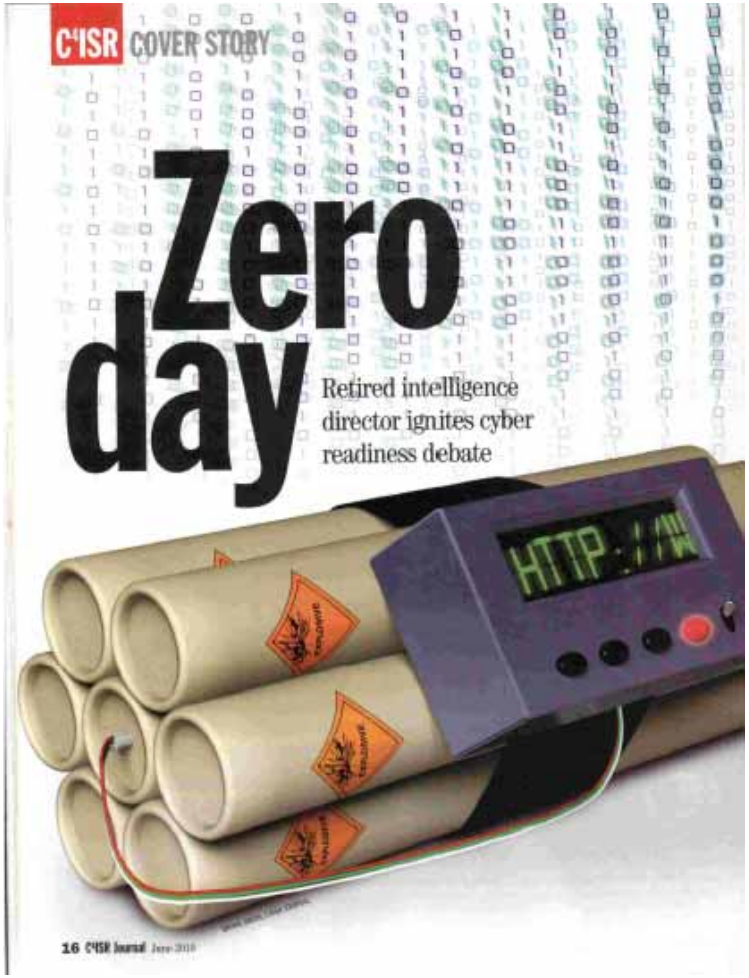
Counterintelligence

A word from the wise…

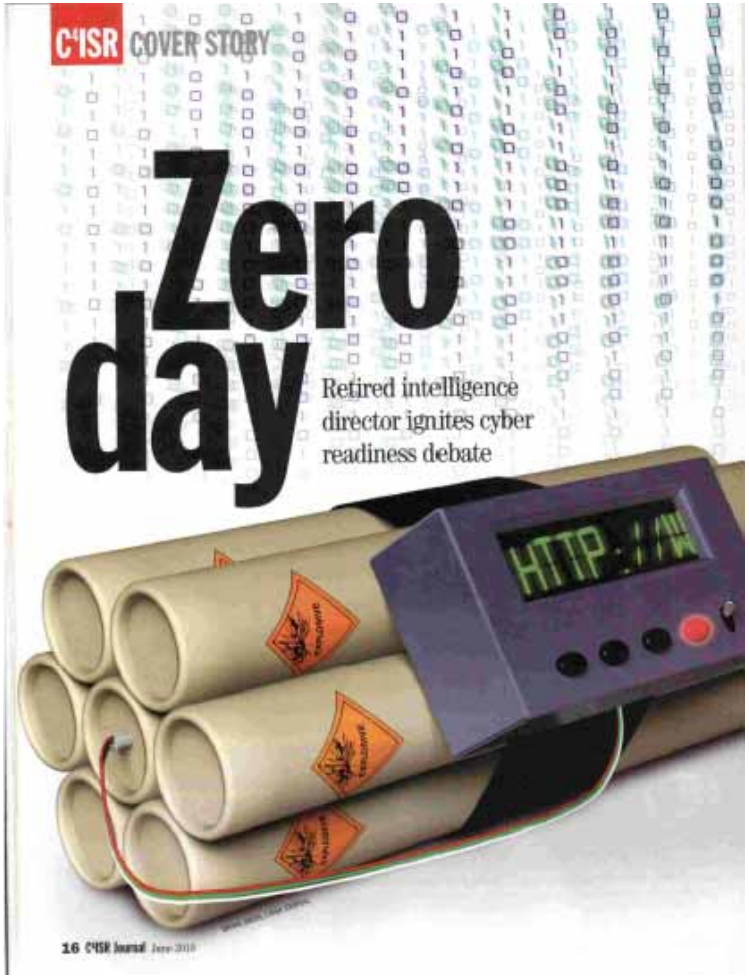
Be generous with counterintelligence

-- Sun Tzu
circa 500 B.C.

Quote cited by Angelo Codevilla in Informing Statecraft: Intelligence for a New Century

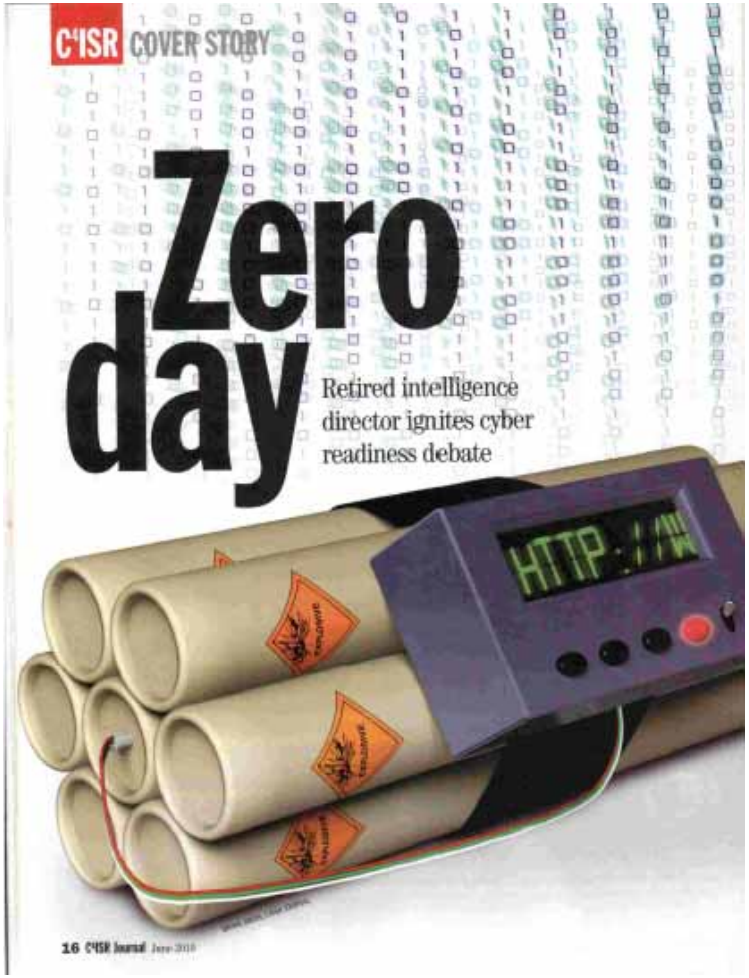


Grazie per la vostra attenzione



Grazie per la vostra attenzione

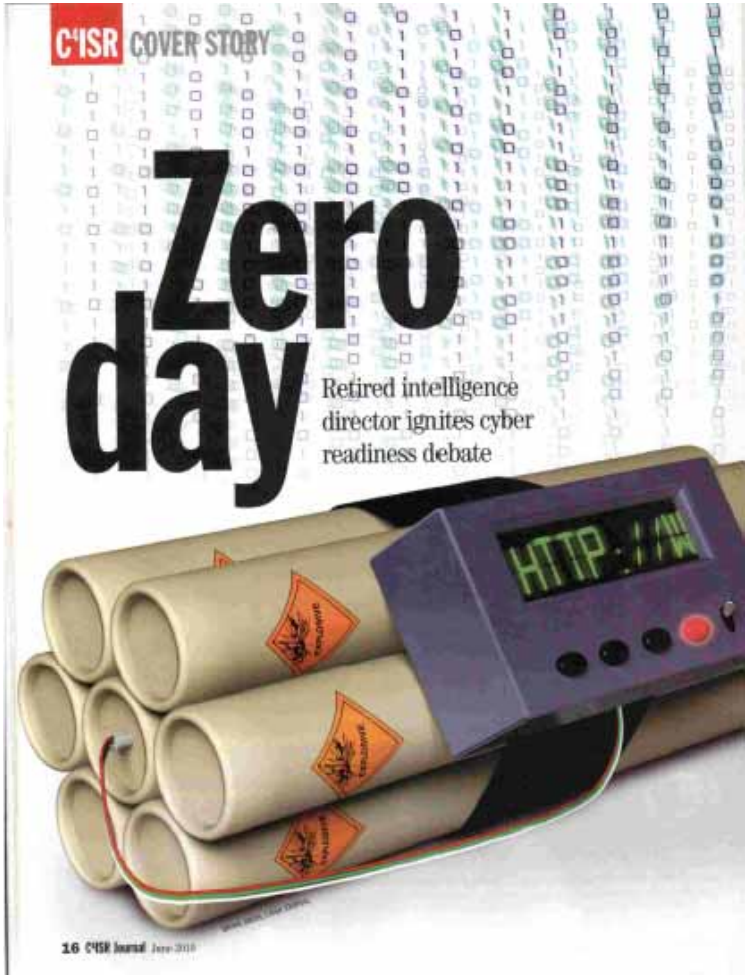
Questions ??????????



Grazie per la vostra attenzione

Questions?????????

Domande ??? ??????



Grazie per la vostra attenzione
Questions??????????
Domande ??????????

m.lopez@sigintsrl.it