CENTRO ALTI STUDI PER LA DIFESA
Centro Militare Studi Strategici (CeMiSS)
Osservatorio per la Sicurezza Nazionale (OSN)

- PANEL -
Strumenti di Indagine per il Cyber World: il GdL dell'OSN

CONVEGNO
"La sicurezza cibernetica nello scenario della cooperazione civile e militare"
Roma, 30 Novembre 2011

Aree di Analisi, Sottogruppi di Lavoro: Scenari Tecnologici

Relatore:
Raoul Chiesa, @ Mediaservice.net
GdL "Cyberworld" - Sottogruppo ROSA

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

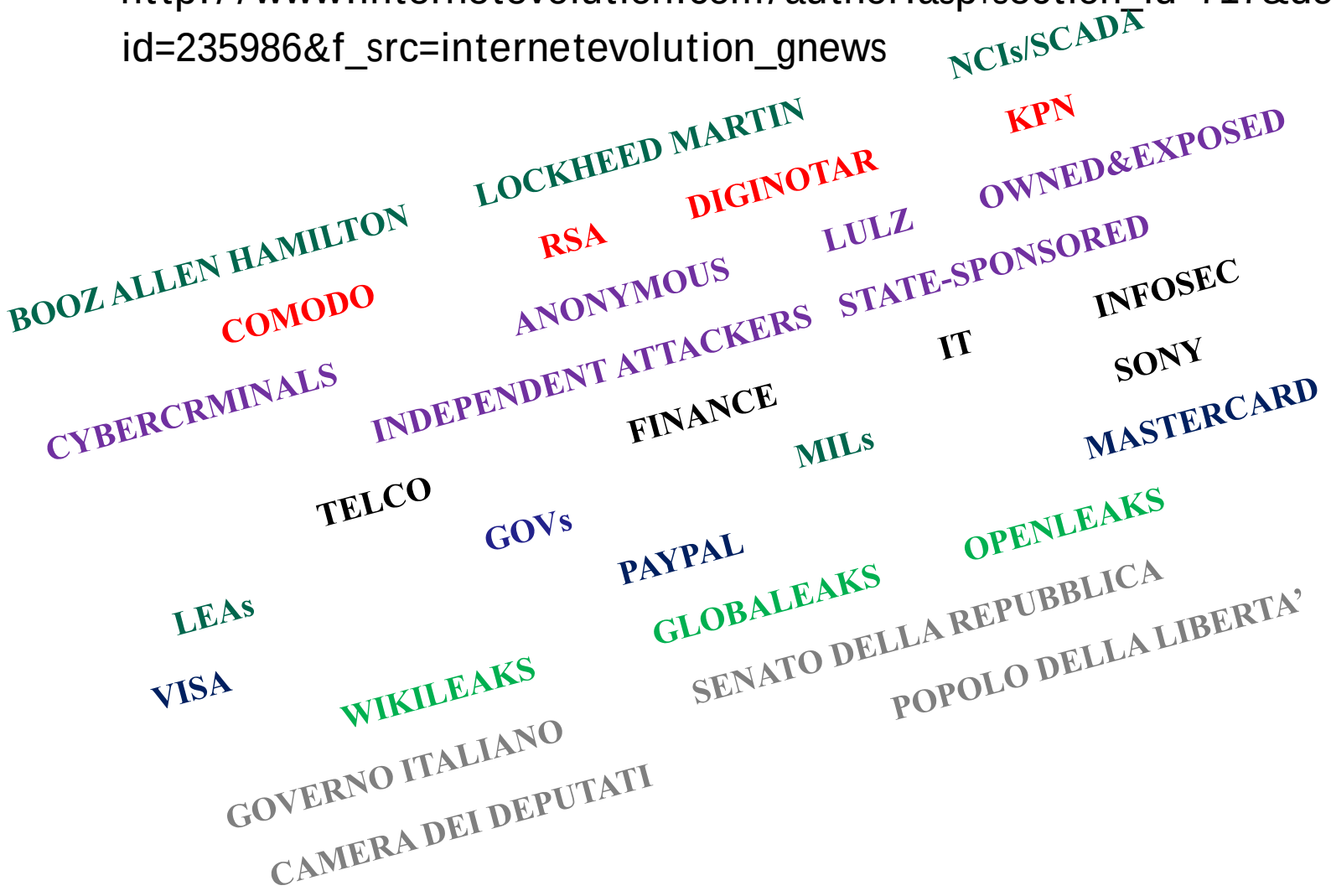
Sommario

- Il panorama attuale
  - Cybercrime: le risposte
  - Perché è essenziale la CO-CI-M
- Strategie di cyber sicurezza nazionale
- Sottogruppo Rosa: attività ed output prodotti
- Prossimi obiettivi
  - Idee e proposte
  - Il progetto di ACEA
- Contatti, Q&A

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Il panorama attuale

- **“Infrastructures Hacks call for Security Re-think” (Jart Armin)**
  - http://www.internetevolution.com/author.asp?section_id=717&doc_id=235986&f_src=internetevolution_gnews

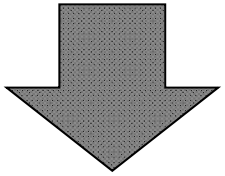


CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

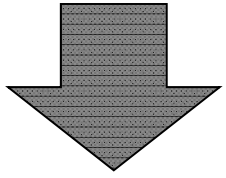
Il panorama attuale /2

- Come per la "corsa agli armamenti" al tempo della Guerra Fredda, in questi ultimi anni stiamo assistendo ad una **crescita esponenziale dell'interesse** verso le tematiche dell'**Information Warfare** e della **CyberWar**.
- Il **contrasto al Cybercrime** (decisamente meno recente e quindi con più esperienza sul campo) ci ha insegnato quanto segue:

"Da solo puoi vincere una singola battaglia, ma non l'intera guerra"



- Il **modello vincente** a livello mondiale è oggi rappresentato dalle VTF (**Virtual Task Forces**).



<u>Si sposa con la logica CO.CI.M !!!</u>

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Cybercrime: le risposte

- Il cybercrime è un reato tipicamente **transnazionale**, borderless, che vede **molteplici attori** e **differenti ruoli**.
- Non è quindi ipotizzabile una **singola risposta**.
- E' invece necessario **pensare ed agire in forma distribuita**, mediante la creazione di **Task Forces Virtuali (Virtual Task Forces/VTF)**.
- E' **essenziale** la **collaborazione** tra PUBBLICO E PRIVATO: Law Enforcement – Governo – Militari / Internet community - Settore finanziario - ISP e carrier (voice & data) - Gruppi verticali di Lavoro
  - al fine di **individuare** ed **identificare** uno specifico gruppo, malware o facilitatore.

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Perché è essenziale la CO-CI-M

The UK government has today released its 2011 Cyber Security Strategy.

With an increased focus on cybercrime, and renewed focus on cyberspace as an engine of economic and social prosperity, the strategy continues to hone Whitehall's understanding of this vibrant, complex and increasingly global domain.

Many of the strategy objectives - in particular those related to securing critical infrastructure - will require close engagement with the private sector.

These public-private partnerships are essential, and, as noted in **a recent Chatham House report** on critical national infrastructure, they require awareness, engagement and trust among senior decision makers on all sides.

This is not an easy process and requires a keen understanding of the incentives that guide actions in the public and private sectors.

Links to business

The government will also have to balance the tension between building a more secure environment - which requires standards and regulation - and encouraging businesses to set up shop in the UK.

However there are signs that Whitehall is aware of these complexities and the need to experiment with potential solutions.

One new initiative is a three-month pilot scheme among five business sectors: defence, finance, telecommunications, pharmaceuticals, and energy.

The UK government plans "unprecedented co-operation" with businesses to improve cybersecurity

Related Stories

- Cyber plan 'to protect UK online'
- FBI downplays water supply 'hack'
- Russia and China 'top cyberspies'

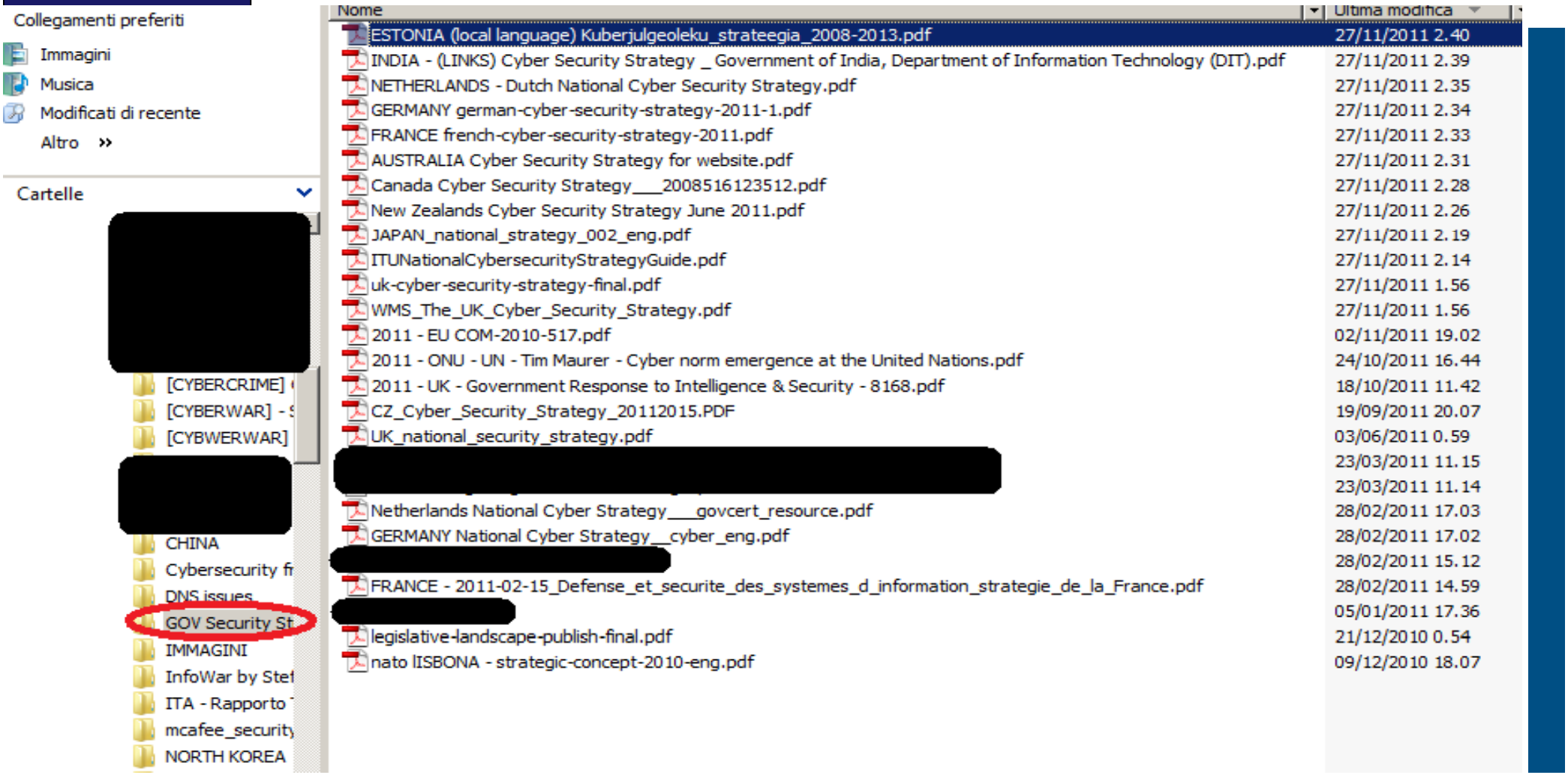
CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Strategie di Cyber-Security Nazionali

CENTRO ALTI STUDI PER LA DIFESA

Strategie di Cyber-sicurezza

Australia / Canada / Czech Republic / EU COM / Estonia / France / Germany / India / Japan / Netherlands / NATO / New Zealand / UK / UN (UNODC, UNICRI, ITU) ….



CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Sottogruppo Rosa: attività ed output prodotti al 30-11-2011

- Individuazione e selezione degli **obiettivi** effettivamente realizzabili
- Scambio **documentazione, Early Warning, Awareness**
- **Collaborazioni inter-subgroups:**
  - **Sottogruppo Giallo/Aspetti Giuridici (Prof.ssa Vassalli) -> R.Chiesa, Stefano Mele**
  - **Review incrociati, scambio di opinione e brainstorming ("Social Networks" Alfonso Montagnese; "Dark Networks: l'approccio topologico", Vinicio Pelino)**
  - Creazione **servizio FTP** per i Coordinatori del GdL e per i Referenti dei Sottogruppi (C. Lausi, E. Sampaolesi, G. Esposito)
- **Dizionario Terminologico Condiviso** aka "Glossario" (R. Chiesa)
  - Terminologie comuni, condivise ed integrabili da tutti i Sottogruppi
  - Profilazione degli attaccanti
- Video "**Rilevazione di attacchi**" (R. Chiesa)
  - **Categorizzazione** tipologie attacchi informatici

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Prossimi obiettivi: idee e proposte

- Call **nuovi membri**
  - **IT Security Industry**
  - **Istituzioni/PA**
- **Report** del Sottogruppo ROSA (2012)
  - Include il **Glossario**, che verrà **aggiornato** ove necessario
  - Include il "**progetto ACEA**" (cfr. prossima slide)
  - Struttura in via di **rivisitazione** e **possibile ampliamento**
- **Progetto ACEA**
- Utilizzo del **simulatore satellitare** (Prof. M. Luglio)
  - In contatto con ricercatori esteri per pianificazione attività di attacco e security testing

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Prossimi obiettivi: il progetto di ACEA

- Come detto questa mattina, **in origine** si era pensato di **produrre alcuni attacchi** per **pesarne l'effettivo impatto** e le conseguenze.

- L'idea è rimasta per gli **aspetti teorici**.

- ACEA ha quindi proposto una **tabella:** "Simulazioni di Attacco VS Tipologia di Attacco", alla quale i membri del Sottogruppo Rosa hanno lavorato.
  - Il Sottogruppo tornerà su questa idea con alcune **migliorie** ed **aggiornamenti**.

Il progetto di ACEA: la tabella

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Tipologia di Attacco	Impatto su Aspetti Giuridici, Normativi, Umanitari	Impatto su aspetti (Terminologici) Tecnologici	Impatto su Aspetti Economici e Finanziari	Impatto su Aspetti Sociali e Geopolitici
Spam Abuse (MX Open Relay, etc. from the Target Infrastructure)	X	X	X	
Phishing Attacks towards employees		X	X	X
Whaling (targeted Phishing) Attacks towards Executives & Management		X	X	
Botnet Abuse (from the Target Infrastructure) for DDoS attacks	X	X	X	
Botnet Abuse (from the Target Infrastructure) for Industrial Espionage (keyloggers, etc)		X	X	X
Web Applications Exploiting/Hacking onto the Target Infrastructure		X	X	X
Perimeter Infrastructure Hacking onto the Target Infrastructure (in-house)	X	X	X	X
Perimeter Infrastructure Hacking onto the Target Infrastructure (outsourced [Hosting/Housing/Cloud])	X	X	X	X
Internal Network Hacking (private IP classes)	X	X	X	X
DDoS (towards the Target Infrastructure)		X	X	X
Physical Security Violations	X	X	X	X
SCADA related Attacks (i.e. water quality sensors)	X	X	X	X

CENTRO ALTI
STUDI PER
LA DIFESA
CeMiSS

CONTATTI

CENTRO ALTI STUDI PER LA DIFESA
CeMiSS

Contatti, Q&A

- **Grazie per l'attenzione**!
  - **Domande**?