

OSINT & Critical Infrastructure Protection: approcci e prospettive

Alessandro Distefano

adistefano@fub.it

Area: Procedure critiche per la Pubblica Amministrazione e le
Organizzazioni complesse
Referente: Ing. Daniele Perucchini



Outline:

- › **Area & interessi di ricerca;**
- › **Open Source INTelligence;**
- › **Critical Infrastructure Protection;**
- › **Approcci & Prospettive;**
- › **Formazione;**
- › **Interventi;**
- › **Pubblicazioni.**

Area & interessi di ricerca

Presso FUB:

- › Infrastrutture Critiche: modellazione, simulazione ed analisi delle interdipendenze.

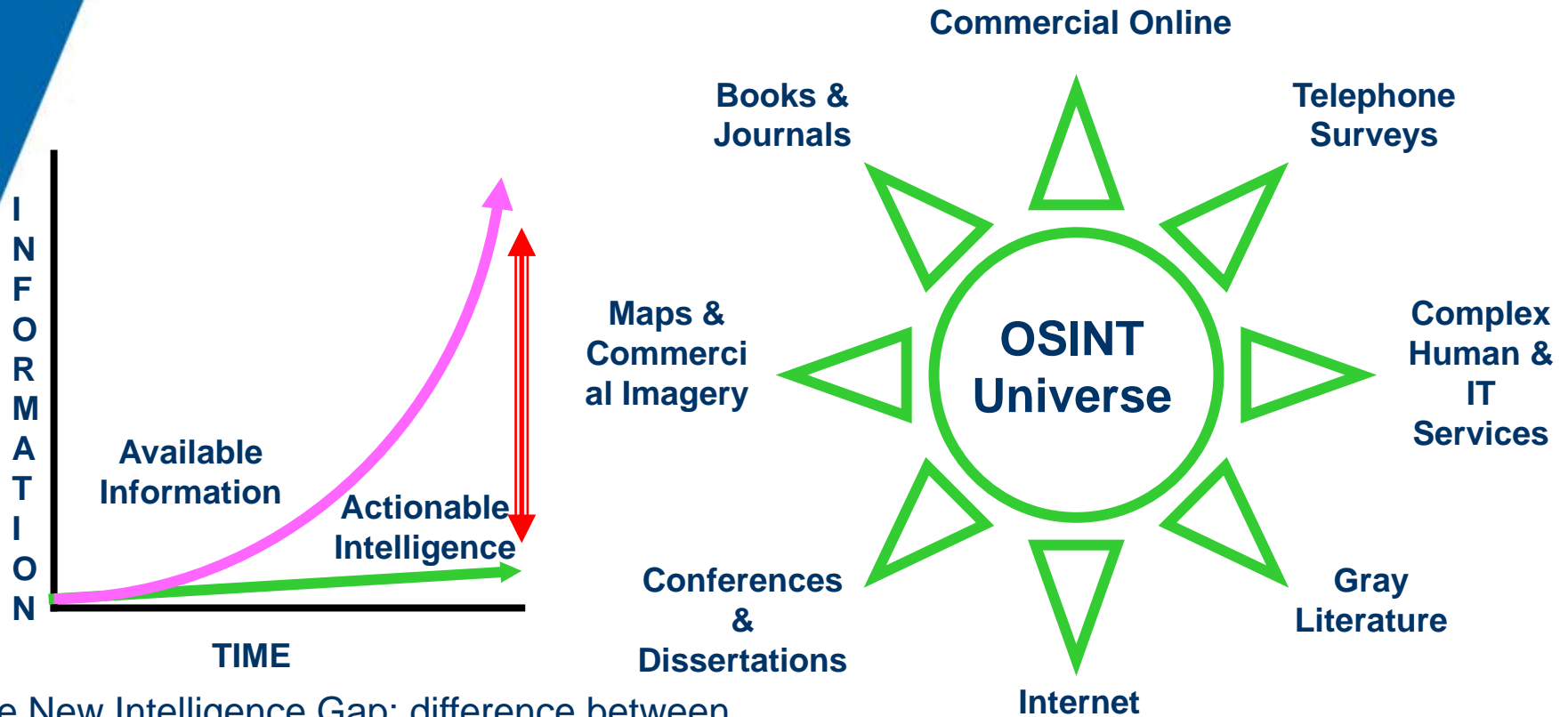
Presso Università di Roma "Tor Vergata":

- › Gruppo Computer Security: Prof. G.F. Italiano;
- › Computer & Mobile Security;
- › Computer & Mobile Forensics.

Open Source INTelligence (OSINT)

- › Open Source INTelligence: raccolta di informazioni mediante fonti di pubblico accesso;
- › Open Source si riferisce a fonti pubbliche, liberamente accessibili in contrapposizione a fonti segrete o coperte;
- › Rilevanza:
 - Dinamicità della moderna Intelligence;
 - Base comprensione per materiale classificato;
 - Protezione delle fonti di informazione;
 - Mantenimento di cronologie;
 - Correlazione e collegamento di più fonti.

Open Source INTeelligence (OSINT)

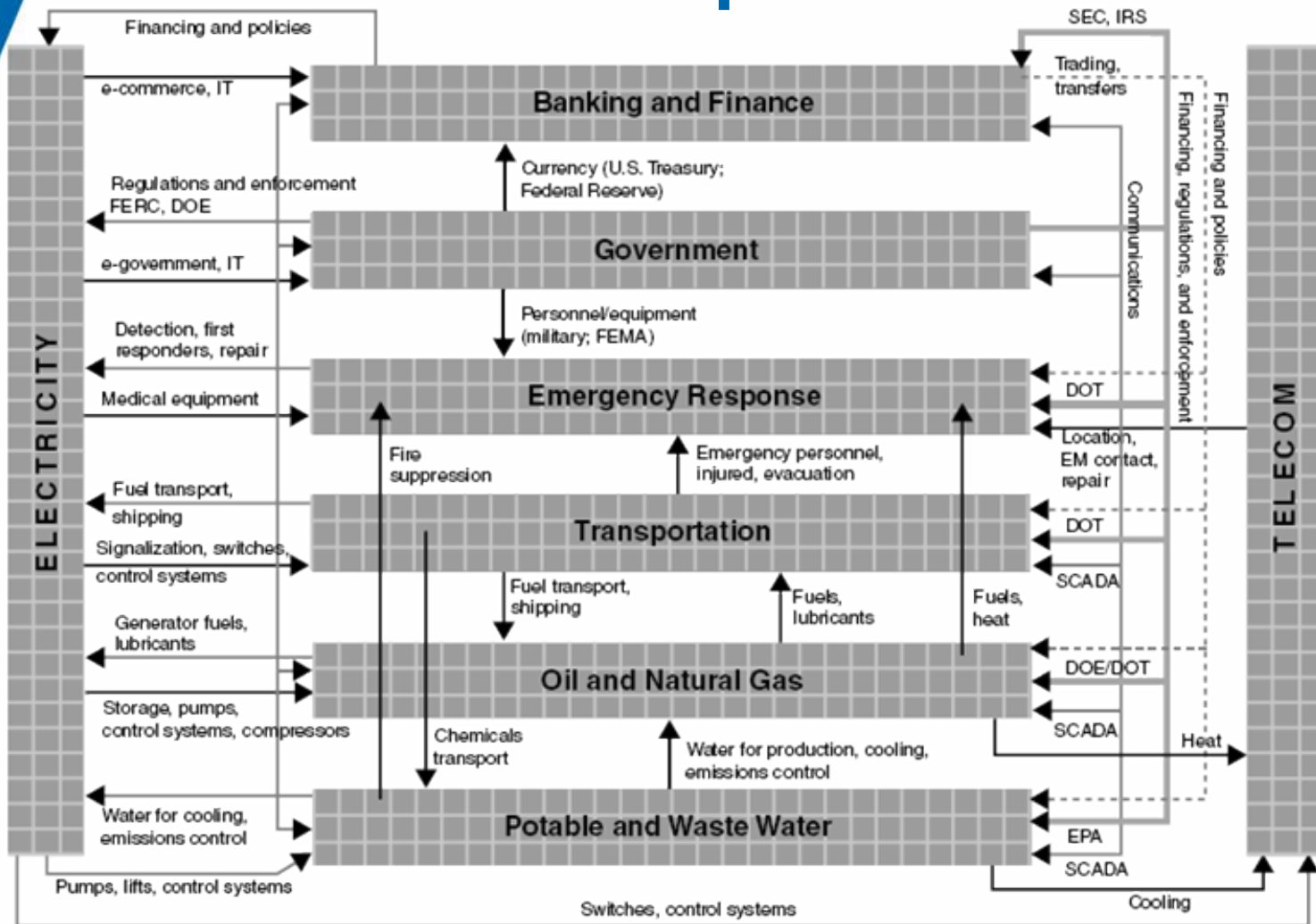


The New Intelligence Gap: difference between what you can know and what you can use!

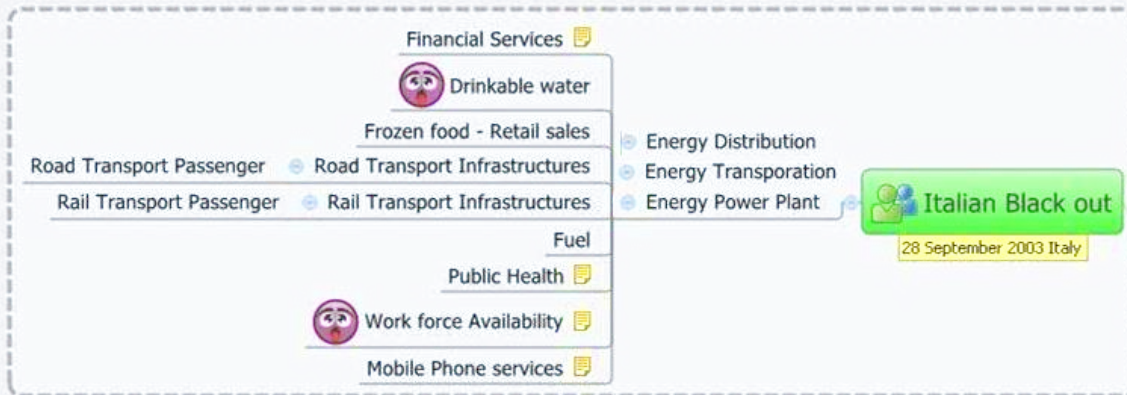
Critical Infrastructure Protection

- › Critical Infrastructure Protection (CIP): attività proattiva e reattiva per gestione di gravi incidenti (scala regione, nazione) legati ad Infrastrutture Critiche;
- › Infrastruttura Critica: asset essenziale per una società/economia (e.g., fornitura energia/alimenti, sanità, ICT, trasporti).
- › La direttiva presidenziale americana (PDD-63 Maggio 1998) ha generato un programma nazionale di CIP;
- › L'Europa dal 2004 è attiva (a livello comunitario) con proposte e programmi in ambito CIP.

CIP - Interdipendenze



CIP - Interdipendenze



Past Event
Cascading
Effect
Analysis

Approcci & Prospettive

- › Tipicamente le statistiche (preziose) su IC non sono facili da ottenere:
 - Problemi di reputazione;
 - Problemi legati a SLA/QOS da contratto.
- › Alcuni studi su relazioni OSINT – CIP:
 - Utilizzo di fonti pubbliche per ottenere dati su CI;
 - Molti incidenti/malfunzionamenti sono riportati spontaneamente (e.g., forum, news).

Approcci & Prospettive

- › Grande quantità di informazioni di pubblico dominio;
 - Qualità da verificare (e.g., notizie non autorevoli, errate);
 - Dipendenza dal tempo;
 - Collegamento tra fonti.
- › Approcci:
 - Esame manuale delle fonti;
 - Esame automatico supervisionato delle fonti;
 - Esame automatico non-supervisionato delle fonti.

Approcci & Prospettive

- › Classificazione automatica di notizie su incidenti/failure dalla rete:
 - Supporto a esame di grandi moli di dati testuali.
- › Compilazione automatica di vocabolari di dominio:
 - Identificazione di vocaboli chiave.
- › Identificazione automatica di gruppi (cluster) di notizie:
 - Separazione (e intersezione) di notizie con argomenti differenti.

Interventi che ho tenuto

- › Speaker al “Workshop on Advanced technologies for law enforcement use” organizzato per EUROPOL, Settembre 2008, Università Tor Vergata, Roma.
- › Speaker a “ISACA Rome Chapter”, Ottobre 2008, Università La Sapienza, Roma.
- › Seminario “MIAT: Mobile Internal Acquisition Tool.” nel corso di perfezionamento in Computer Forensics e Investigazioni Digitali, Febbraio 2009, Università Statale di Milano, Milano.
- › Seminario “Mobile security & vulnerabilities” nel corso di aggiornamento presso RayTalk Industries, Maggio 2009, Repubblica di SanMarino.
- › Speaker a “Exploring Cyberspace Law 2009”, Giugno 2009, Università degli Studi G. D’Annunzio, Pescara.

Publicazioni

Accettate:

1. A. Distefano, G. Me, *“An overall assessment of Mobile Internal Acquisition Tool”*, Proc. of 2008 Digital Forensic Research Workshop (DFRWS), Journal of Digital Investigation, vol. 5;
2. A. Distefano, R. Galbani, A. Grillo, A. Lentini, G. Me, *“Exploitation of Secrets Injected in Java Midlets”*, Proc. of 5° International Conference of Global Security, Safety & Sustainability, ICGS3 2009.

Publicazioni

Work in Progress:

1. A. Distefano, G. Me, D. Tulimiero, *“Mobile Forensics Data Integrity Assessment by Event Monitoring”*;
2. A. Distefano, G. Me, F. Pace, *“Android OS: Forensics & Anti-forensics”*;
3. A. Distefano, G. F. Italiano, G. Me, *“Digital Signature: from RSA to ECDSA”*;
4. A. Distefano, A. Grillo, A. Lentini, G. Me, *“Mobile Threats: Privacy & Security Issues”*.

OSINT & Critical Infrastructure Protection: approcci e prospettive

Q&A



Università degli Studi di Roma "Tor Vergata"