OSINT

(OPEN SOURCE INTELLIGENCE)

LA RILEVANZA DELLE INFORMAZIONI

Michele Dal Checco

E METODI INVESTIGATIVI

La Polizia Postale e delle Comunicazioni
Organo Centrale e Uffici Territoriali

Organizzazione interna Uffici

Competenze

Michele Dal Checco

POLIZIA POSTALE

C.N.C.P.O.

Centro Nazionale per il Contrasto della Pedopornografia On-line

C.N.A.I.P.I.C.

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Michele Dal Checco

POLIZIA POSTALE

N.O.S.C.
Nuclei Operativi Sicurezza Cibernetica

Aziende / Privati

3P – Public Private Partnership

Michele Dal Checco

POLIZIA POSTALE

Codice penale – normativa relativa ad attacchi informatici e ad altri specifiche ad essi collegati

Diversi ambiti criminali legati ai compiti dei N.O.S.C.

Business Intelligence – Terrorismo …

POLIZIA POSTALE

Alcuni esempi

Art. 615 Ter – Accesso abusivo a sistema informatico ed aggravanti

Cenni su altre fattispecie di reati

Michele Dal Checco

POLIZIA POSTALE

La Costante evoluzione tecnologica

Costringe il legislatore a continui adeguamenti normativi spesso non semplici e di immediata attuazione

Michele Dal Checco

POLIZIA POSTALE

Si deve considerare l'aspetto normativo in base al paese dove il reato di fatto viene compiuto

Differenze tra Italia / Europa e resto del mondo

Esempio i social-network come Facebook

Michele Dal Checco

POLIZIA POSTALE

POC – Punto di contatto 24/7 per l'A.G.

Contatti diretti con le Forze di Polizia in ambito europeo e paesi con accordi bilaterali

Michele Dal Checco

POLIZIA POSTALE

G.D.P.R.

General data protection regulation

Dal 25 maggio 2018 è entrato in vigore il regolamento europeo 2016/679 in materia di privacy, relativo alla protezione dei dati personali.

Sono tenuti ad osservare la normativa sulla privacy le aziende, gli enti pubblici, e gli individui che devono accedere, trattare, conservare, gestire, o trasferire dati personali di cittadini UE e che pertanto devono applicare le norme contenute nel regolamento GDPR.

Michele Dal Checco

POLIZIA POSTALE

Data-retention

Codice della privacy

Utilizzo dei dati per l'A.G. (Autorità Giudiziaria)

Michele Dal Checco

POLIZIA POSTALE

Per la costante evoluzione tecnologica

C'è bisogno di continui ed adeguati cambiamenti investigativi che integrino le indagine classiche

Compiti specifici "Postale" e metodi classici di Polizia

Michele Dal Checco

POLIZIA POSTALE

Indagini classiche

- *Necessità di informazioni*
- *Richieste – Banche dati – Decreti*
- *Intercettazioni Telefoniche/Telematiche*
- *Indagini Forensi a seguito di attività operativa*

Michele Dal Checco

POLIZIA POSTALE

E’ stato necessario adeguare le proprie capacità per reperire, gestire, valutare le fonti informative

Internet – (quasi scontato oggi)

Una mole sempre crescente di informazioni reperibili

POLIZIA POSTALE

Concetto di OSINT (OpenSource Intelligence)

Concetto di Fonte Aperta – cosa si intende?

Intelligence – Servizio Segreto di investigazione?
Intelligente – Si nasce intelligenti o si diventa?

Michele Dal Checco

POLIZIA POSTALE

Intelligence – alcuni elementi

- ***Conoscenza***
- ***Acutezza intellettiva – Capacità mnemoniche***
- ***Menti brillanti/reattive perspicaci***
- ***Attitudine a aggregare dati e rappresentarli***

POLIZIA POSTALE

OSINT – introduzione e metodo

Ciclo dell'intelligence

Michele Dal Checco

POLIZIA POSTALE

Ciclo dell'intelligence

- *La raccolta*
- *L'elaborazione*
- *La disseminazione*
- *La valorizzazione*

Il ciclo OSINT

POLIZIA POSTALE

Concetti:

- ***Dato***
- ***Notizia***
- ***Informazione***

Michele Dal Checco

POLIZIA POSTALE

Le fonti Aperte e Grigie

Vantaggi e svantaggi

Pertinenza/Rilevanza

Michele Dal Checco

POLIZIA POSTALE

Concetti:

- ***Web 1.0 – web tradizionale "web marketing"***
- ***Web 2.0 – web sociale "social media marketing"***
- ***Web 3.0 – web semantico "semantic search"***
- ***Web 4.0 – verso la "Realtà aumentata e Big Data"***

POLIZIA POSTALE

Oltre al Web "tradizionale":

- *Hidden web – metamori di ricerca*
- *Darkweb – Anonimizzazione (TOR)*

Michele Dal Checco

POLIZIA POSTALE

Necessaria <u>Conoscenza</u> protocolli e strumenti:

- ***Funzionamento protocolli (http/https ...)***
- ***Strumenti a disposizione***

POLIZIA POSTALE

Esempi

Motori di ricerca / Metamotori

Diversi “tool” opensource

Tool autoprodotti es. script python ed altri

POLIZIA POSTALE

- *Google dorks*
- *Metamotori specifici*
- *Tool opensource*
- *Mappe mentali / Mappe concettuali*

Michele Dal Checco

POLIZIA POSTALE

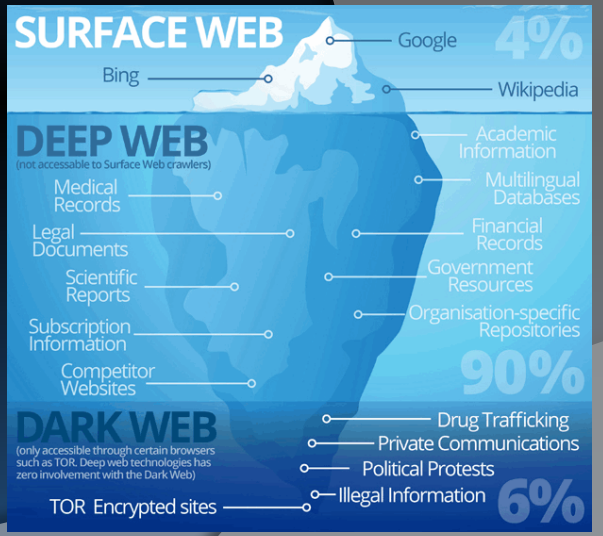
- *Va un po' di moda parlare di OSINT*
- *Disponibilità di Documentazione ma da valutare*
- *Molte agenzie investigative si propongono*

POLIZIA POSTALE

Ricerca informazioni nelle darknet

No motori di ricerca nel darkweb

No reti convenzionali
(es. no DNS) – domini onion



POLIZIA POSTALE

In ambito OSINT

Ricerca/Lettura, ma chi scrive?

Consapevolezza delle informazioni che rilasciamo

C’è chi ascolta? (es. exit node TOR)

POLIZIA POSTALE

Cenni sugli strumenti base

Browser pregi e difetti (attenzione ai cookies)

Scelta e metodo di lavoro (attenzione ai plugin)

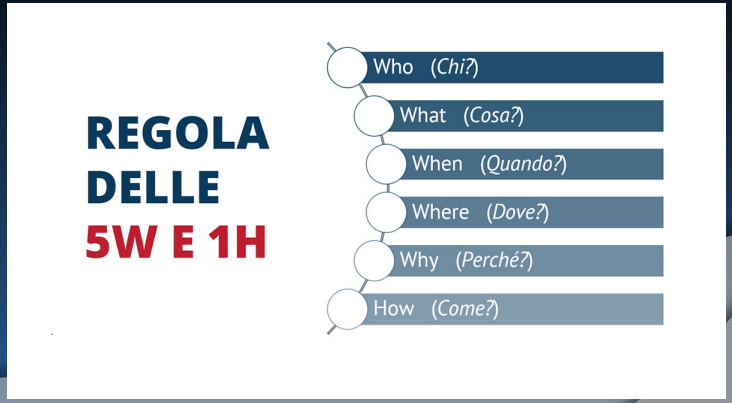
Michele Dal Checco

POLIZIA POSTALE

Metodo

Seguendo l'iter del ciclo dell'intelligence

La regola delle 5 W



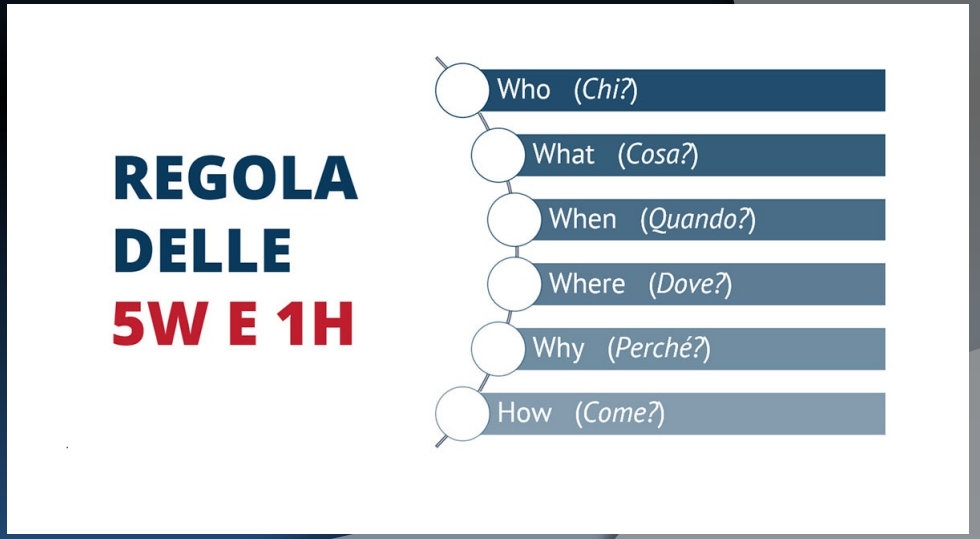
Michele Dal Checco

POLIZIA POSTALE

Metodi

Seguendo l'iter del ciclo dell'intelligence

La regola delle 5 W



POLIZIA POSTALE

Metodi

Presuposti assunti dal Decisore

Definire i Target

Michele Dal Checco

POLIZIA POSTALE

Metodi

Analisi e definizione di eventuali nuovi target

Rischio ciclo infinito – risultati soddisfacenti

Michele Dal Checco

POLIZIA POSTALE

Metodi

Ciclo infinito – "livello di paranoia"

La costante tempo

Michele Dal Checco

POLIZIA POSTALE

Metodi

Sintesi:
“Sapere dove cercare”
“Conoscere chi conosce”

es. Social

Michele Dal Checco

POLIZIA POSTALE

Metodi e Rischi

- ***Obbiettività***
- ***Vizi di analisi***
- ***Tesi che avvalorano i miei pregiudizi***

Michele Dal Checco

POLIZIA POSTALE

Metodi

Gruppi di analisi

BrainStorm

Fondamentale che siano disomogenei

Michele Dal Checco

POLIZIA POSTALE

Metodi

Verso l'Analisi predittiva

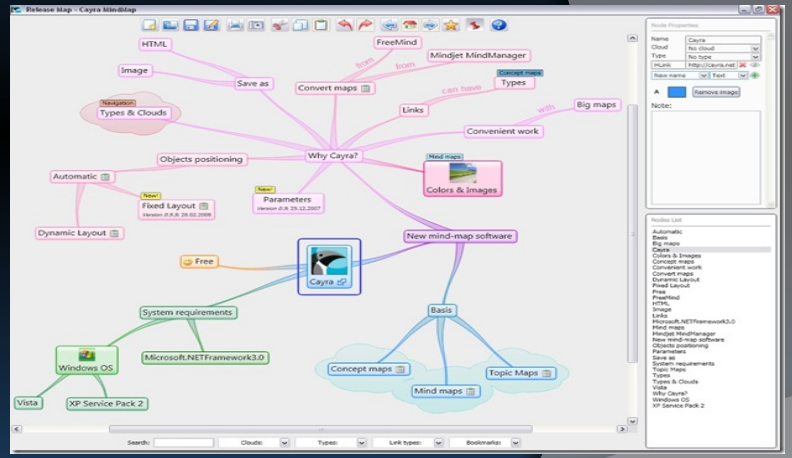
Molti ambiti di attualizzazione

Michele Dal Checco

POLIZIA POSTALE

Metodi

Organizzazione dei risultati



- *Visualizzazione*
- *Archiviazione*
- *Comparazione nel tempo dei risultati*
- *Presentazione*

Michele Dal Checco

POLIZIA POSTALE

Cenni su attacchi informatici

- ***Malware – Virus***
- ***RAT** (Remote Access Trojan)*
- ***Sql-injection***
- ***BOF** (Buffer overflow)*
- ***BEC** (Business email Compromise)*
- ***Ransomware***

Michele Dal Checco

POLIZIA POSTALE

Ingegneria sociale

Anonimato

Michele Dal Checco

POLIZIA POSTALE

Attacchi informatici contromisure

- *Situazione in italia*
- *Alfabetizzazione digitale*
- *Error config e valutazione del rischio*
- *Aspetti culturali*

Michele Dal Checco

POLIZIA POSTALE

Collaborazione Polizia Postale

- ***C.N.A.I.P.I.C. - N.O.S.C.***
- ***Protocolli d'intesa – 3 P – (IOC)***
- ***Ambiente Universitario***

Michele Dal Checco

POLIZIA POSTALE

Domande / Chiarimenti

Grazie per l'attenzione ...

michele.dalchecco@poliziadistato.it