# CYBERCRIMES:

Una panoramica

Montillo Antonio

I cybercrimes comprendono un'ampia varietà di attività illegali che sfruttano la potenza della tecnologia digitale. Questi atti criminali variano dall'attacco a dati riservati alla violazione dei diritti d'autore e dei contenuti (Krone, 2005). Essenzialmente, il cybercrime si caratterizza per l'uso improprio della tecnologia dell'informazione.

Questi crimini possono essere sinteticamente  categorizzati in due tipi:

1. **Crimini che hanno come obiettivo le reti digitali e i computer ad esse collegati**: Questo include attività dannose come la creazione e la diffusione di virus, che danneggiano direttamente i sistemi informatici e le reti.
2. **Crimini facilitati dalle reti digitali e dai computer collegati**: In questa categoria, l'infrastruttura digitale viene utilizzata come strumento per commettere o facilitare una varietà di attività criminali, piuttosto che essere il bersaglio diretto.

# Cybercrimes

Bruce Schneier, nel 2000, propose una classificazione dei crimini informatici in tre distinte categorie, offrendo una prospettiva articolata sul fenomeno del cybercrime. Queste categorie sono:

1. **Attacchi Criminali Propriamente Intesi**: Questa categoria include azioni che violano le leggi vigenti in modo chiaro e diretto. Esempi possono includere hacking, furto di dati, creazione e diffusione di malware, e frodi online. Questi crimini sono universalmente riconosciuti come illegali e sono perseguiti in base alle leggi esistenti.
2. **Attacchi Non Propriamente Criminali**: Questi attacchi si situano in una zona grigia dal punto di vista legale. Non sono necessariamente illegali secondo la lettera della legge, ma possono essere eticamente discutibili o dannosi. Esempi possono includere attività come il doxxing (divulgazione di informazioni private online senza consenso), o certe forme di hacktivism dove non ci sono danni diretti a persone o proprietà.
3. **Attacchi Basati su Sistemi Legali**: Questa categoria è particolarmente interessante in quanto coinvolge l'uso di sistemi legali per scopi illeciti o non etici. Ad esempio, potrebbe includere l'uso della legislazione sul copyright per sopprimere informazioni di interesse pubblico o la manipolazione delle leggi per proteggere pratiche ingiuste nel cyberspazio. Questo tipo di attacco sfrutta le lacune o le ambiguità delle leggi esistenti per ottenere vantaggi o per danneggiare altri soggetti.

# Cybercrimes

1. Attacchi Criminali Propriamente Intesi: Una Prospettiva su Violazioni e Guadagni Economici

Gli attacchi criminali propriamente intesi nel contesto del cybercrime sono quelli che coinvolgono una chiara violazione dei sistemi informatici. Il denominatore comune di queste azioni è l'obiettivo di ottenere un vantaggio economico attraverso l'uso illegale della tecnologia. A differenza del sabotaggio fisico, questi crimini si avvalgono di strumenti tecnologici avanzati, come i virus, e si focalizzano sull'exploit delle vulnerabilità dei sistemi informatici.

Questi attacchi possono manifestarsi in diverse forme, tra cui:

- **Hacking**: L'accesso non autorizzato a sistemi informatici per rubare dati sensibili o informazioni private.
- **Phishing e Frodi Online**: Truffe che mirano a ingannare gli utenti per ottenere dati personali, finanziari o di accesso.
- **Diffusione di Malware**: Programmi dannosi, come virus o trojan, creati per danneggiare o prendere il controllo di sistemi informatici.
- **Ransomware**: Un tipo di malware che cripta i dati della vittima, richiedendo un riscatto per il loro sblocco.

La peculiarità di questi attacchi è che, pur essendo virtuali, hanno effetti molto reali e concreti, sia in termini economici che di sicurezza informatica. La loro natura tecnologica permette ai criminali di operare a distanza, spesso eludendo facilmente le barriere geografiche e legali tradizionali.

# Cybercrimes

1. Attacchi Criminali Propriamente Intesi: Frode Informatica, Attacchi Distruttivi e Furto d'Identità

Nella categoria degli attacchi criminali propriamente intesi nel campo del cybercrime, possiamo identificare tre tipologie principali di azioni illecite:

- **Frode Informatica**: Questa tipologia di crimine comporta la manipolazione di servizi o processi di elaborazione dati per ottenere un profitto ingiusto. Gli esempi includono l'alterazione di transazioni finanziarie, l'uso fraudolento di dati di carte di credito, o la manipolazione di sistemi di contabilità per trarne vantaggi economici.
- **Attacchi Distruttivi**: A differenza della frode informatica, gli attacchi distruttivi non sono primariamente mirati al guadagno economico. Il loro scopo è quello di arrecare danno alla proprietà altrui, che può variare dal danneggiamento di un singolo computer alla distruzione di reti aziendali o di complessi sistemi di reti. Tali attacchi possono assumere forme come la diffusione di virus distruttivi, attacchi DDoS (Distributed Denial of Service), o altre forme di sabotaggio digitale.
- **Furto d'Identità**: Questo crimine implica l'acquisizione e l'uso non autorizzato di informazioni personali di un individuo. Può variare dall'uso di dati personali come nomi e indirizzi, fino all'impersonificazione totale, dove il criminale assume l'identità della vittima per accedere a risorse finanziarie, commettere frodi o perpetrare altri crimini. Il furto d'identità può portare a conseguenze gravi per le vittime, includendo la perdita finanziaria e danni alla reputazione.

Queste varie forme di attacchi criminali propriamente intesi illustrano la vasta gamma e la complessità dei crimini nel cyberspazio, ognuno con le sue specifiche modalità operative e implicazioni.

# Cybercrimes

2. Attacchi Non Propriamente Criminali: Attacchi a Scopo Pubblicitario

Gli attacchi non propriamente criminali nel campo del cybercrime spesso hanno una natura e finalità differente rispetto ai crimini tradizionali. Un esempio significativo sono gli attacchi a scopo pubblicitario:

- **Natura e Obiettivo**: Questi attacchi si caratterizzano per una violazione pubblica di un sistema informatico, con l'obiettivo primario di attirare l'attenzione dei media e generare un impatto mediatico. A differenza di altre forme di cybercrime, l'intento non è quello di procurare un guadagno economico diretto o di danneggiare in modo permanente il sistema.
- **Scopo Dimostrativo**: Spesso, il fine di questi attacchi è quello di evidenziare una vulnerabilità o un problema, solitamente legato alla sicurezza informatica. Gli autori di tali attacchi potrebbero voler dimostrare l'esistenza di una falla di sicurezza, sottolineare la necessità di miglioramenti, o anche solo mettere alla prova le proprie abilità tecniche in modo visibile.
- **Conseguenze Economiche**: Nonostante la mancanza di un intento criminalmente lucrativo, le conseguenze economiche di tali attacchi possono essere notevoli. Possono includere la perdita di fiducia dei clienti, danni all'immagine dell'azienda, costi legati al ripristino della sicurezza e della funzionalità dei sistemi, e persino la possibilità di cause legali a seguito della violazione.
- **Effetti Collaterali**: Oltre alle perdite economiche dirette, questi attacchi possono portare a un'ampia gamma di reazioni, dalla diffidenza degli utenti al deterioramento della reputazione pubblica dell'ente o dell'azienda colpita.

In sintesi, mentre questi attacchi non sono intrinsecamente motivati da scopi criminali, le loro ripercussioni possono essere significative e richiedere un'attenzione seria da parte delle organizzazioni colpite.

# Cybercrimes

3. Attacchi Basati su Sistemi Legali: Esplorazione delle Debolezze Giuridiche

Gli attacchi basati su sistemi legali rappresentano una categoria peculiare nel panorama del cybercrime. Diversamente dagli attacchi informatici classici, questi non mirano a sfruttare vulnerabilità tecniche, ma piuttosto lacune o debolezze nel sistema giudiziario e legale. Caratteristiche e finalità di questi attacchi includono:

- **Focus sulle Debolezze Giuridiche**: Questi attacchi si concentrano sull'esplorazione delle debolezze nei sistemi legali piuttosto che su quelle dei sistemi informatici. Ciò può includere l'uso di leggi poco chiare, lacune normative o l'interpretazione ambigua delle leggi esistenti per perseguire obiettivi che, sebbene legalmente contestabili, non sono necessariamente considerati illegali.
- **Obiettivi Simili agli Attacchi Pubblicitari**: Come gli attacchi a scopo pubblicitario, anche questi tentativi hanno spesso l'obiettivo di attirare l'attenzione sui problemi o sulle incongruenze presenti nei sistemi di sicurezza informatica. Tuttavia, la differenza sostanziale risiede nel loro approccio, che è più orientato a sollevare questioni legali che a esporre vulnerabilità tecniche.
- **Strategia di Screditamento Legale**: Attraverso questi attacchi, gli autori cercano di dimostrare come alcune misure di sicurezza informatica, benché apparentemente solide, possano essere inefficaci o inadeguate quando si confrontano con le complessità e le ambiguità del sistema legale. Questo può includere la messa in discussione della validità legale di certe procedure di sicurezza o l'evidenziazione di come determinate politiche possano essere aggirate legalmente.
- **Implicazioni a Lungo Termine**: Sebbene questi attacchi non causino danni immediati ai sistemi informatici, possono avere importanti ripercussioni a lungo termine, sia per le organizzazioni che per gli individui coinvolti. Possono innescare dibattiti sulla normativa in materia di sicurezza informatica e sulla necessità di riforme legali, influenzando così il modo in cui le leggi vengono interpretate e applicate nel futuro.

In sintesi, gli attacchi basati su sistemi legali offrono una prospettiva diversa sui cybercrimes, sottolineando l'importanza di un approccio olistico alla sicurezza informatica che tenga conto non solo delle vulnerabilità tecniche ma anche delle complessità legali.

# Cybercrimes

La criminalità informatica sta vivendo un'espansione significativa a livello globale, e l'Italia, come molti altri paesi, non è esente da questo fenomeno. L'incremento degli incidenti, sia colposi che dolosi, nel campo della sicurezza informatica ha portato a un cambiamento sostanziale nel modo in cui studiosi e professionisti affrontano e comprendono questi crimini.

- **Aumento degli Incidenti Informatici**: In Italia, come nel resto del mondo, si è registrato un costante aumento degli episodi di criminalità informatica. Questo include una vasta gamma di attività illecite, dall'hacking e il furto di dati fino a frodi online e attacchi a infrastrutture critiche.
- **Impatto sui Professionisti e sugli Studiosi**: Di fronte a questa realtà in evoluzione, esperti di sicurezza informatica, ricercatori e professionisti del settore legale hanno dovuto adottare una "ristrutturazione cognitiva". Ciò significa un ripensamento degli approcci tradizionali alla sicurezza informatica, una maggiore enfasi sull'innovazione nella prevenzione e nella risposta agli incidenti, e un aggiornamento costante delle conoscenze per tenere il passo con le tattiche sempre più sofisticate dei criminali informatici.
- **Necessità di Aggiornamento e Innovazione**: L'aumento della criminalità informatica richiede un continuo aggiornamento delle strategie di difesa e una maggiore consapevolezza delle nuove minacce. Ciò comporta l'adozione di tecnologie avanzate, l'aggiornamento delle leggi e delle normative, e un rafforzamento della collaborazione tra enti governativi, aziende private e istituzioni accademiche.
- **Risposta Multidisciplinare**: Il fenomeno richiede un approccio multidisciplinare che coinvolga diversi settori, dalla tecnologia all'etica, dal diritto alla psicologia, per comprendere a fondo e contrastare efficacemente la criminalità informatica.

L'aumento della criminalità informatica in Italia riflette un trend globale e impone una ristrutturazione nell'approccio al problema. Questo passa attraverso l'aggiornamento delle competenze, l'innovazione tecnologica, e un approccio più olistico e integrato alla sicurezza informatica.

# Cybercrimes

Attualmente, la comprensione e il contrasto della criminalità informatica si basano in gran parte su conoscenze e competenze derivate dall'analisi di crimini tradizionali, ma con una particolare attenzione alle variabili introdotte dall'uso del computer. Questo approccio è in fase di continua evoluzione, adeguandosi al progressivo integrazione delle tecnologie digitali nella società.

- **Fase Attuale di Transizione**: Nel momento presente, la lotta contro il cybercrime è ancora fortemente ancorata alle teorie e alle pratiche tradizionali di criminologia, adattate per affrontare le sfide poste dall'elemento digitale. Questo include l'adattamento di vecchi schemi investigativi e legali per affrontare crimini in cui il computer gioca un ruolo chiave.
- **Adattamento alle Nuove Tecnologie**: Si sta assistendo a un processo di adattamento dove le nuove tecnologie stanno diventando sempre più integrate nella nostra vita quotidiana. Man mano che questo processo procede, il ruolo dei computer e delle tecnologie digitali diventa più diffuso e meno distintivo in termini di comportamento criminale.
- **Futuro della Criminalità Informatica**: In un futuro non troppo lontano, quando l'adattamento alle nuove tecnologie sarà più completo, potrebbe non essere più rilevante considerare il computer come una variabile distinta nello studio del comportamento criminale. Invece, l'uso del digitale potrebbe essere considerato un aspetto intrinseco e onnipresente del crimine moderno, richiedendo un approccio più integrato che non fa distinzione tra crimini "tradizionali" e "informatici".
- **Verso un Approccio Integrato**: Questo potrebbe portare a un approccio più olistico alla criminologia, dove la tecnologia digitale è vista come parte integrante del panorama criminale, anziché come un fattore esterno o aggiuntivo. In tale scenario, le tecniche di investigazione, prevenzione e contrasto del crimine dovranno essere profondamente integrate con la comprensione delle tecnologie digitali e delle loro implicazioni nella società.

# Cybercrimes

Nella società contemporanea, l’informatica la tecnologia digitale stanno già diventando elementi centrali in molti aspetti della vita quotidiana. Questo progressivo intreccio sta influenzando significativamente la nostra percezione del crimine informatico.

- **Integrazione Attuale della Tecnologia**: Oggi, computer e tecnologie digitali sono onnipresenti nelle organizzazioni, influenzando la struttura sociale, l'antropologia e la psicologia degli individui. Questa pervasività sta modificando il modo in cui interagiamo, lavoriamo e viviamo.
- **Redefinizione del Crimine Informatico**: Nel contesto attuale, il crimine informatico sta iniziando a essere percepito meno come una categoria a sé stante e più come una faccetta del panorama criminale più ampio. Con l'incremento della digitalizzazione, la distinzione tra crimini "tradizionali" e crimini "digitali" si sta attenuando.
- **Implicazioni per Legislazione e Società**: Questa evoluzione sta già sfidando le attuali strutture legali e di sicurezza. Gli investigatori, i legislatori e i professionisti della sicurezza devono ora avere una solida comprensione sia delle dinamiche umane che della tecnologia per affrontare efficacemente il crimine nell'era digitale.
- **Sfide e Opportunità Emergenti**: La crescente fusione della tecnologia nella vita quotidiana presenta nuove sfide in termini di privacy e sicurezza informatica, ma anche nuove opportunità per utilizzare la tecnologia al fine di prevenire e contrastare il crimine.

In sintesi, nella società attuale, con la tecnologia digitale che diventa sempre più intrinseca in tutti gli aspetti della vita, il crimine informatico sta evolvendo da una categoria distinta a una parte integrante del più ampio spettro criminale. Questo richiede un approccio più integrato e olistico nella gestione e nella comprensione del crimine, considerando sia le sue dimensioni digitali che umane.

# CYBER INTELLIGENCE E PROFILING

Ronconi Giovanni

# LA CYBER INTELLIGENCE

Si può descrivere come un insieme complesso di attività programmate e applicate per identificare, seguire, misurare e monitorare informazioni sulle minacce digitali, dati sulle intenzioni e attività di entità avversarie. È rilevante notare che la Cyber Intelligence non si limita solo alla componente informatica, ma incorpora anche le logiche dell'intelligence classica. Questo implica la necessità di analizzare i dati raccolti con metodologie specifiche derivanti dall'intelligence classica, che utilizza l'intelligenza umana per fare valutazioni appropriate e/o previsioni

Non bisogna confondere la Cyber Intelligence con la Cyber Threat Intelligence.

# IL CICLO DELLA CYBER INTELLIGENCE

**Direzione**: Questa fase riguarda la definizione degli obiettivi e delle priorità della raccolta di informazioni. Nella Cyber Intelligence, ciò può includere specifici tipi di minacce digitali o attività di entità avversarie.

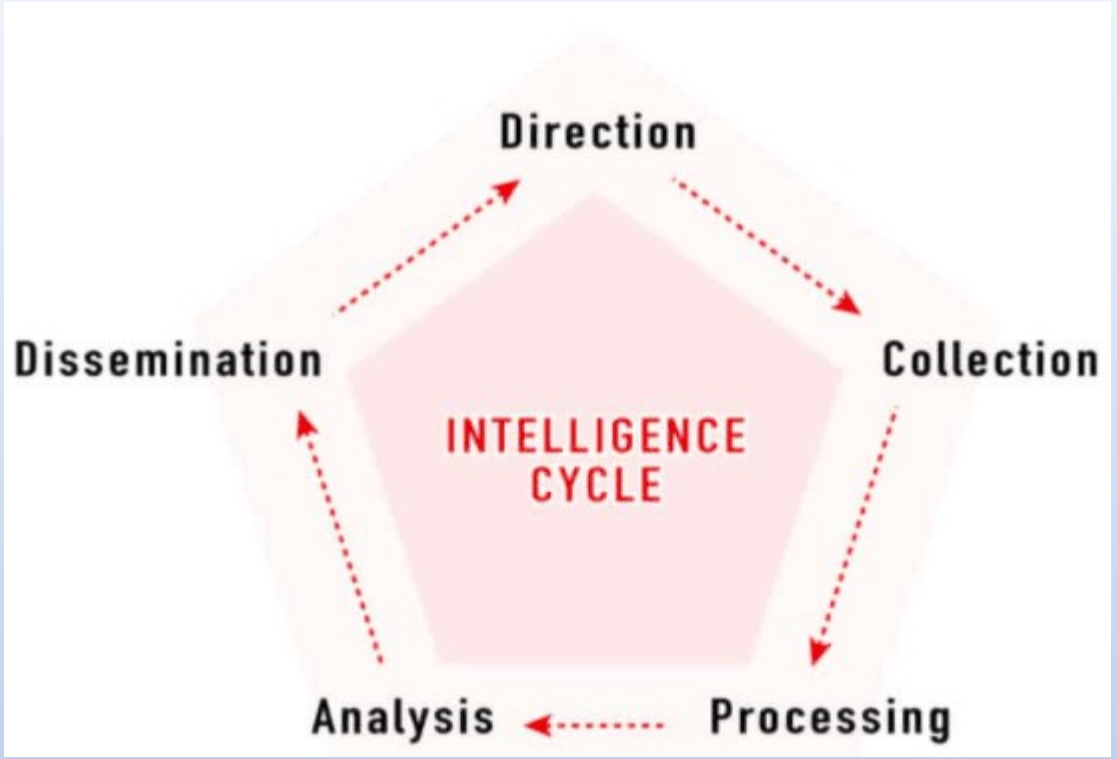
**Raccolta**: In questa fase, si raccolgono dati e informazioni dai sistemi informatici, reti e dal cyberspazio. Questo può includere la sorveglianza di reti, il monitoraggio del traffico di dati, e l'infiltrazione in sistemi avversari.

**Elaborazione e sfruttamento**: Le informazioni raccolte vengono elaborate e trasformate in formati utilizzabili. Nella Cyber Intelligence, ciò potrebbe comportare la decrittografia dei dati, l'analisi del malware, o l'analisi di grandi set di dati.

**Analisi e produzione**: Gli analisti interpretano le informazioni elaborate, identificando schemi, intenzioni, capacità e potenziali minacce. Questo può includere l'analisi di comportamenti sospetti nelle reti e la valutazione delle vulnerabilità.

**Diffusione e integrazione**: Le informazioni analizzate vengono distribuite ai decisori e agli operatori di campo. Nella Cyber Intelligence, ciò può comportare la comunicazione di avvertimenti su minacce imminenti, la condivisione di intelligenza con altre agenzie o la realizzazione di raccomandazioni per azioni difensive.

**Feedback**: Questa fase prevede la valutazione dell'efficacia del ciclo di intelligence. Nella Cyber Intelligence, il feedback può riguardare l'accuratezza delle previsioni sulle minacce digitali o l'efficacia delle misure di difesa implementate.



# LE FONTI

In ambito di Cyber Intelligence, una "fonte" si riferisce a qualsiasi origine da cui è possibile estrarre informazioni sotto forma di dato strutturato facilmente utilizzabile dai sistemi di correlazione utili per l'intelligence. Questo può includere, ma non è limitato a, dati digitali, comunicazioni, documenti, report, database, traffico di rete, sistemi informatici compromessi, attività sui social media, forensica digitale, malware e altri software dannosi, nonché sistemi di rilevamento e prevenzione delle intrusioni. Le fonti in Cyber Intelligence sono fondamentali per raccogliere dati che, una volta analizzati e interpretati, possono rivelare insight sulle minacce, vulnerabilità e comportamenti degli attaccanti nel cyberspazio.

# VALUTAZIONE DELLE FONTI

Nell'ambito dell'intelligence, la valutazione delle fonti avviene seguendo criteri ben definiti che si concentrano sulla credibilità e l'affidabilità. Questo processo può essere riassunto con l'acronimo inglese "ADMIRALTY", che sta per:

**Authenticity (Autenticità)**: Verifica dell'autenticità della fonte.

**Date (Data)**: Data dell'informazione, per valutarne la pertinenza temporale.

**Meaning (Significato)**: Comprensione del contenuto dell'informazione.

**Intelligence (Intelligenza)**: Valutazione dell'utilità dell'informazione per scopi di intelligence.

**Relevance (Rilevanza)**: Pertinenza dell'informazione rispetto alla richiesta o all'obiettivo.

**Accuracy (Accuratezza)**: Correttezza e precisione dei dettagli.

**Lawfulness (Legalità)**: Acquisizione dell'informazione in modo legale.

**Tendency (Tendenza)**: Bias potenziale o obiettività della fonte.

**Yield (Rendimento)**: Quantità e qualità delle informazioni fornite dalla fonte nel tempo.

# VALUTAZIONE DELLE FONTI

**Valutazione della Fonte**: Analizzare la credibilità della fonte basandosi su esperienze passate e sulla conoscenza della sua affidabilità.

**Valutazione del Contenuto**: Esaminare il contenuto dell'informazione per la sua coerenza, accuratezza e dettaglio.

**Correlazione con Altre Informazioni**: Confrontare l'informazione ricevuta con altre fonti per verificare la sua validità.

**Analisi del Contesto**: Considerare il contesto in cui l'informazione è stata raccolta, inclusi i potenziali bias o le motivazioni della fonte.

**Classificazione del Grado di Fiducia**: Assegnare un punteggio o un livello di fiducia basato sull'analisi complessiva.

**La valutazione delle fonti è essenziale per garantire che le informazioni siano affidabili prima di utilizzarle in analisi e rapporti di intelligence**.

# ANALISI FINALE

è il processo di integrazione e interpretazione di informazioni che provengono da fonti cyber-specifiche per produrre intelligence rilevante per decisioni strategiche. Questa analisi si propone di fornire una comprensione olistica delle attività, delle capacità, delle intenzioni e delle minacce potenziali nel cyberspazio e creare un profilo atto all'identificazione. Tale processo comprende la correlazione di dati, la valutazione di affidabilità e rilevanza delle informazioni, e la produzione di valutazioni che possano guidare azioni di politica estera, difesa, e altre strategie nazionali.

IL DOCUMENTO DI ANALISI FINALE E' UN ELEMENTO DA INSERIRE IN UN CONTESTO PIU AMPIO DI INTELLIGENCE

# PROFILING

il profiling si riferisce all'identificazione e all'analisi delle caratteristiche e dei comportamenti degli attori, sia che si tratti di individui, gruppi, organizzazioni o persino di entità statali. Il profiling in questo contesto si focalizza su un'analisi più ampia e multidimensionale che va oltre il mero aspetto tecnico, includendo aspetti psicologici, sociali e culturali per costruire un profilo completo dell'attore o dell'entità di interesse.

IL PROFILING NON E’ MAI SINGLE SOURCE

# PROFILING

**Dall’analisi effettuata attraverso varie fonti oltre la quelle attribuite alla Cyber Intelligence si prendono in esame anche:**

**Analisi Comportamentale**: Valutare le azioni dell'attaccante per comprendere motivazioni, obiettivi e metodi.

**Analisi Psicologica**: Tentare di comprendere la psicologia del target.

**Valutazione Geopolitica**: Considerare il contesto geopolitico in cui l'attaccante opera, che potrebbe influenzare le sue azioni.

**Ricerca Storica**: Analizzare le attività passate per identificare schemi o cambiamenti nel comportamento.

# PROFILAZIONE DI UN CYBER CRIMER

*Brasi Cristina*

Un cyber crimer è un individuo che a tutti gli effetti delinque.

L’unica differenziazione concerne lo strumento utilizzato per agire

# LA CONDOTTA CRIMINALE

La costruzione del profilo nasce dal confronto con le caratteristiche di altri offender che hanno compiuto reati di natura similare.

La personalità è un'organizzazione più o meno durevole di forze che agiscono nell'ambito dell'individuo. Tale forze persistenti forniscono coerenza nel comportamento.

sia di ordine verbale

sia di ordine non verbale

Le emozioni e gli impulsi hanno il potere di determinare il comportamento, e risultano variabili da individuo a individuo

Nel corso dello sviluppo si acquisiscono quelli che sono definiti «*pattern* comportamentali»

schemi comportamentali appresi in tenera età di cui non si ha consapevolezza

Tali caratteristiche esplicitano come ogni individuo abbia una struttura cognitiva, emotiva, comportamentale unica, facendo emergere la grande limitazione di questa metodologia di profilazione.

Sono proprio le caratteristiche di unicità che consentono di delineare il profilo dell'*offender*

- Si può identificare, in ogni *offender*, un *modus operandi*

  ↓

  metodologia utilizzata per compiere il reato → armi utilizzate, tipologia di attacco e di controllo, eventuali tentativi di dissimulazione del reato, ecc.

- la firma criminale (*criminal signature*)

- le caratteristiche demografiche, socioculturali…

È anche possibile identificare i tratti di personalità a partire da come un individuo ha organizzato il proprio dispositivo digitale

# IL DIGITAL PROFILING

È un nuovo strumento di indagine e applica sulla memoria digitale specifiche tecniche di *intelligence* e di *profiling* allo scopo di ottenere tutta una serie di informazioni, dalla descrizione delle modalità con cui è stato compiuto il reato, all'identificazione dell'autore o degli autori del reato in oggetto

Il processo si svolge attraverso la ricerca e l'analisi delle informazioni che si possono trarre dalle «tracce digitali»: il computer è una macchina, ma il suo utilizzatore è un essere umano e, come tale tende a personalizzare l'ambiente con cui interagisce

reale virtuale

Con *Intelligence* si intende quel procedimento che, attraverso la raccolta, la valutazione e l'analisi delle informazioni, consente di dare un significato all'insieme delle informazioni esaminate

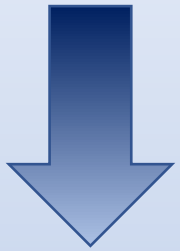
Il processo è composto da 4 fasi:

- Individuazione dell'obiettivo
- Raccolta mirata delle informazioni e la loro valutazione
- Analisi delle informazioni
- Utilizzazione del prodotto finale

Le principali aree di ricerca di dati da cui è possibile trarre gli indicatori uniti alla creazione del profilo digitale all'interno di un sistema informatico sono:

- Analisi degli utenti
- Analisi dei file di testo
- Analisi delle cartelle di *file* personali
- Analisi dell'organizzazione delle cartelle
- Analisi del nickname
- Analisi dei file di *log* e della cronologia delle connessioni
- Analisi delle installazioni hardware
- Analisi delle installazioni *software*
- Analisi dei listati di codice
- Analisi della *timeline*
- Analisi della macchina virtuale
- Analisi del *modus operandi*

Davide Bassani, esperto digitale forense, ragionando sul paradigma relativo al fatto che, un individuo, nel momento in cui utilizza un dispositivo, lo modifica, ha creato un *software* in grado di riconoscere, con certezza, se un soggetto, nella fattispecie il reo, dopo un'analisi del dispositivo in uso, abbia utilizzato altri dispostivi



L'individuo lascerebbe quindi un'impronta digitale in grado di identificarlo, per mezzo del *software* in questione, su qualsiasi dispositivo che egli abbia utilizzato

# FINE

GRAZIE PER
L'ATTENZIONE