# 1. Introduzione

## Le principali minacce informatiche

Oggi, le principali minacce informatiche, ordinate per **frequenza degli incidenti**, sono

**Negligenza, errore umano e frodi da parte di insider**

- Incidenti causati internamente dall'organizzazione.
- Comprendono errori non intenzionali e atti fraudolenti.

**Cybercrime transnazionale organizzato**

- Genera profitti di circa **60 miliardi di dollari all'anno** (dati del 2018).
- Causa danni diretti e indiretti per quasi **800 miliardi di dollari** a livello globale.
- Operazioni condotte da gruppi criminali organizzati a livello internazionale.

**Cyber Espionage e Cyber Warfare**

- **Cyber Espionage (Spionaggio Cibernetico):** Attività mirate alla raccolta non autorizzata di informazioni sensibili attraverso mezzi digitali. Queste informazioni possono riguardare segreti di stato, proprietà intellettuale, dati militari o informazioni personali.
- **Cyber Warfare (Guerra Cibernetica):** Uso di tecnologie informatiche per attaccare le infrastrutture digitali di uno Stato o di un’organizzazione, con l’obiettivo di causare danni, interruzioni o influenzare decisioni politiche e militari.

**Nota:** Se si inverte l'ordine si ottiene un **ordinamento per gravità** degli incidenti

## La nascita dell'hacking

La storia dell'hacking può essere suddivisa in diverse generazioni, ognuna caratterizzata da motivazioni e contesti specifici.

Alla fine degli anni '70, la **prima generazione** di hacker era guidata da una profonda sete di sapere. Questi pionieri erano spinti dal desiderio di esplorare e comprendere le nuove tecnologie emergenti.

Negli anni '80, la **seconda generazione** era alimentata dalla curiosità e dalla continua ricerca di conoscenza. In un'epoca in cui molti sistemi operativi e reti potevano essere appresi solo penetrandoli, l'hacking divenne un mezzo per imparare. Verso la metà di questo decennio, il fenomeno iniziò a intrecciarsi con tendenze di moda e trend culturali.

Durante gli anni '90, la **terza generazione** di hacker era mossa dalla pura voglia di fare hacking. Questo significava coltivare curiosità, desiderio di imparare cose nuove, violare sistemi informatici e condividere informazioni con la comunità underground. In questo periodo nacquero i primi gruppi di hacker.

Nel 2000, la **quarta generazione** era spinta dalla rabbia e dall'interesse economico. Spesso si trattava di individui con conoscenze tecniche limitate, attratti dall'idea di essere hacker perché considerato affascinante o alla moda. Molti di loro non conoscevano né erano interessati alla storia, alla cultura e all'etica del phreaking e dell'hacking. In questa fase, l'hacking iniziò a mescolarsi con la politica, dando origine al "Cyber-Hacktivism", o con attività criminali, sfociando nel "Cybercrime".

Originariamente, era possibile identificare tre tipologie di hacker:

- **Black-hat**: coloro che violano i sistemi informatici, con o senza vantaggio personale. Si schierano dalla parte "cattiva", oltrepassando la chiara linea di demarcazione tra "amore per l'hacking" e l'esecuzione deliberata di azioni criminali. Per questi attori, è normale violare un sistema informatico e penetrare nei suoi meandri più segreti, rubando informazioni e, dato il loro profilo di hacker, rivendendole a paesi esteri.
- **Grey-hat**: coloro che non vogliono essere etichettati come "neri o bianchi" e possono considerarsi "hacker etici". Spesso potrebbero aver effettuato intrusioni in sistemi informatici, ma hanno deciso di non utilizzare questo approccio.
- **White-hat**: anche definiti "cacciatori", hanno le competenze necessarie per essere un black-hat, ma hanno deciso di schierarsi con “i buoni”. Collaborano con le autorità e la polizia, sono in prima linea nelle operazioni anticrimine informatico, sono consulenti per governi e aziende; nella loro vita di solito non violano sistemi informatici, o se lo fanno, non è mai per scopi criminali o per guadagno economico.

# L'hacking oggi

Il libro *"Profiling Hackers: Applied Research Project"* rappresenta uno dei più importanti progetti di ricerca applicata nel campo del profiling degli hacker.

Le attività di ricerca sul campo sono iniziate nel 2006 e sono tuttora in corso. L'approccio adottato è stato molto apprezzato da forze dell'ordine e agenzie governative, tanto da essere considerato una lettura obbligatoria dagli agenti speciali dell'FBI specializzati in crimini informatici. Il testo è disponibile presso la biblioteca dell'FBI Academy a Quantico, Virginia, ed è anche riconosciuto dall'Agenzia di Intelligence Italiana (DIS) come riferimento ufficiale sui profili degli hacker.

Questo libro rappresenta una pietra miliare che supera l'approccio tradizionale, fornendo una prospettiva più avanzata e dettagliata sul profiling degli hacker. Di seguito sono riportati i 9 profili di hacker che possono essere identificati in base alle loro motivazioni, età, target e modalità di azione:

**Wanna Be Lamer**
Questi individui, generalmente di età compresa tra i 9 e i 16 anni, aspirano a diventare hacker ma mancano delle competenze tecniche necessarie. Operano solitamente in gruppo e il loro target è costituito dagli utenti finali. Le loro motivazioni sono prevalentemente sociali, desiderano sentirsi parte di un gruppo "cool" e si dedicano a piccole attività di hacking più per vantarsi che per realizzare attacchi significativi.

**Script Kiddie**
I "Script Kiddies" sono giovani hacker, tra i 10 e i 18 anni, che utilizzano strumenti e script creati da altri, senza avere una vera comprensione tecnica di come funzionano. Spesso agiscono da soli ma fanno parte di gruppi online più ampi. Il loro target principale sono le piccole e medie imprese (PMI) o le vulnerabilità specifiche di software. Le loro azioni sono motivate dalla rabbia o dalla voglia di attirare l'attenzione dei media di massa, spesso in modo sconsiderato.

**Cracker**
I "Crackers" sono hacker distruttivi di età compresa tra i 17 e i 30 anni che agiscono da soli. Il loro scopo è danneggiare le aziende, creando scompiglio per dimostrare il loro potere o per attirare attenzione mediatica. Non sono interessati a rubare informazioni, ma piuttosto a compromettere sistemi per il gusto della distruzione.

**Ethical Hacker**
Conosciuti anche come hacker etici, questi individui, di età compresa tra i 15 e i 50 anni, operano sia da soli che in gruppo. Sono motivati dalla curiosità e agiscono per imparare e contribuire al miglioramento della sicurezza informatica. Il loro target sono i fornitori di tecnologia o i sistemi vulnerabili che vogliono rendere più sicuri, non per scopi maliziosi ma per scopi altruistici. Tuttavia, alcuni hacker etici agiscono solo per divertimento.

**Quiet, Paranoid, Skilled Hacker**
Questi hacker, che hanno tra i 16 e i 40 anni, sono estremamente abili e spesso agiscono in modo paranoico, preferendo lavorare da soli. Il loro target varia a seconda delle necessità, e il loro scopo principale è la curiosità e l'apprendimento, ma con intenti più egoistici. Sono esperti nel nascondere le loro tracce e lavorano in modo silenzioso e metodico.

**Cyber-Warrior**
I "Cyber-Warrior" sono hacker di età compresa tra i 18 e i 50 anni, che spesso agiscono da soli. Questi individui vedono l'hacking come una forma di guerra digitale, e il loro obiettivo sono le aziende "simbolo" o gli utenti finali. Operano per profitto, spesso come mercenari, vendendo le loro competenze al miglior offerente o a gruppi con interessi geopolitici o economici.

**Industrial Spy**
Gli "Industrial Spy", che hanno tra i 22 e i 45 anni, si specializzano nello spionaggio industriale. Agiscono da soli e il loro target sono le aziende o le grandi corporazioni, da cui

cercano di rubare informazioni preziose per rivenderle o utilizzarle per ottenere vantaggi competitivi. Il loro scopo è esclusivamente il profitto economico.

**Government Agent**
Gli hacker governativi, di età compresa tra i 25 e i 45 anni, operano sia da soli che in gruppo e lavorano per agenzie come la CIA, Mossad o FBI. Il loro compito è lo spionaggio o il controspionaggio, il monitoraggio di attività sospette, la conduzione di test di vulnerabilità o la sorveglianza di individui o organizzazioni strategiche. Le loro azioni sono spesso giustificate come necessarie per la sicurezza nazionale.

**Military Hacker**
Infine, i "Military Hacker" sono individui di età compresa tra i 25 e i 45 anni che operano da soli o in gruppo per conto di governi o aziende strategiche. Sono coinvolti in operazioni di monitoraggio e controllo di sistemi digitali, e in alcuni casi, nel sabotaggio di reti o infrastrutture. Le loro azioni sono motivate da necessità geopolitiche e militari, e possono includere la distruzione o la compromissione di infrastrutture critiche.

# Dall'hacking al cybercrime

Il **cybercrime** può essere definito come l'uso di strumenti informatici e reti di telecomunicazione per commettere reati di diversa natura. Alla base di questo modello si trova un assioma chiave: *l'obiettivo principale è acquisire insiemi di dati (informazioni) che possono essere trasformati in denaro*. I criminali informatici cercano di ottenere profitti attraverso attività illegali come il furto di dati, la frode, il ricatto o la vendita di informazioni rubate. Gli obiettivi principali del cybercrime sono **privati cittadini**, **aziende** e **istituzioni finanziarie**.

Il panorama del cybercrime è estremamente complesso e in continua evoluzione. Gli attori coinvolti sono variegati e cambiano costantemente, rendendo difficile delineare profili stabili. Anche le loro motivazioni possono variare: alcuni cercano fama, altri sono mossi dal desiderio di guadagno economico, mentre altri ancora agiscono per ideali o, in alcuni casi, senza una motivazione apparente. Possono essere **hackers indipendenti**, **gruppi organizzati** o reti di **cybercrime-as-a-service** che vendono strumenti e servizi di hacking.

Dal punto di vista legislativo, esistono gravi carenze, poiché non tutti i Paesi dispongono di normative adeguate per affrontare ogni tipologia di crimine informatico. La cooperazione internazionale è spesso insufficiente e limitata. Il cybercrime trova poi terreno fertile in paesi con problematiche interne, come lacune legislative, budget limitati, una formazione inadeguata delle forze dell’ordine o alti livelli di corruzione.

Alcuni punti salienti caratterizzano questo fenomeno:

- **Virtualità**: Il cybercrime si basa su un modello “a piramide” che sfrutta l'anonimato, le infrastrutture di comando e controllo (C&C) che sono altamente flessibili e scalabili. È caratterizzato dalla capacità di spostarsi rapidamente e ricostruirsi, con un utilizzo "cross" di prodotti e servizi in differenti scenari e modelli di business.

- **Transnazionale**: Le attività criminali informatiche non sono limitate da confini geografici, operano su scala globale.
- **Multi-mercato**: Il cybercrime coinvolge acquirenti provenienti da diversi settori e mercati, creando una rete complessa di transazioni e compravendite illegali.
- **Diversificazione**: I prodotti e i servizi offerti dai criminali informatici sono altamente diversificati e spaziano su più livelli, da
- lla vendita di dati rubati a servizi di hacking personalizzati.
- **Basso costo di ingresso**: Le barriere per entrare nel mondo del cybercrime sono estremamente basse, permettendo a molti di partecipare senza grandi investimenti iniziali.
- **Alto ritorno sugli investimenti (ROI)**: Ogni operazione criminale può generare profitti elevati, e se queste attività vengono industrializzate, il ritorno sugli investimenti può crescere esponenzialmente.
- **Paradisi fiscali e legali**: Esistono Paesi che non solo offrono vantaggi fiscali ma sono anche considerati paradisi legali per i criminali informatici, rendendo difficile perseguirli e fermare le loro operazioni

Gli attacchi cybercriminali includono principalmente **phishing**, **malware**, **ransomware**, furti di identità e **frodi finanziarie**

# Dal cybercrime alla cyberwar

La cyberwar è condotta principalmente per ragioni **politiche**, **strategiche** o **militari**. Gli attacchi cibernetici in questo contesto mirano a minare o distruggere le infrastrutture critiche di una nazione, compromettere le sue capacità difensive o destabilizzare il governo e la società.

Gli obiettivi della cyberwar sono generalmente **infrastrutture governative**, militari, energetiche, di telecomunicazioni, finanziarie o altre componenti chiave di un Paese. L'obiettivo è spesso sabotare, danneggiare o spiare per ottenere vantaggi geopolitici o militari.

La cyberwar è condotta da **stati nazionali** o da attori sponsorizzati da governi, come **military hackers** o **cyber-warriors**. Si tratta di un conflitto tra nazioni o tra stati e gruppi organizzati con agende politiche o ideologiche.

Gli attacchi possono includere **attacchi DDoS** (Distributed Denial of Service), **sabotaggio informatico**, infiltrazioni nelle reti militari e civili, e altre forme di spionaggio e sabotaggio digitale. Possono essere utilizzati anche per propaganda o disinformazione.

Gli effetti della cyberwar possono essere devastanti e avere un impatto duraturo su **infrastrutture critiche**, **settori economici** e **sicurezza nazionale**. Gli attacchi possono scatenare crisi politiche e militari reali.

# Underground economy

L'**underground economy**, o economia sommersa, si riferisce a un mercato non regolamentato dove vengono scambiati beni e servizi illegali o illeciti. Nel contesto digitale, è un ecosistema nascosto, accessibile attraverso canali come il **dark web**, che coinvolge attività criminali e transazioni illegali, spesso correlate al **cybercrime**.

Questa economia digitale sommersa include una vasta gamma di operazioni illecite, tra cui:

- **Commercio di dati rubati**: come numeri di carte di credito, credenziali di accesso a conti bancari e identità personali
- **Vendita di malware e exploit**: strumenti informatici per compromettere la sicurezza di sistemi e reti
- **Servizi di hacking su richiesta**: assunzione di hacker per violare sistemi specifici o per attività di spionaggio
- **Mercati di droga e armi**: piattaforme anonime per l'acquisto di droghe illegali, armi, documenti falsi, ecc.
- **Riciclaggio di denaro**: schemi complessi per ripulire il denaro proveniente da attività criminali, spesso attraverso criptovalute

In questo contesto, i metodi di pagamento riflettono l'anonimato e la difficoltà di tracciamento che caratterizzano queste attività illecite. Le transazioni possono avvenire in contanti, spesso in incontri faccia a faccia (F2F), un metodo tradizionale che permette di evitare qualsiasi traccia digitale. Un'altra opzione sono i conti bancari offshore, utilizzati per nascondere l'origine e la destinazione dei fondi, grazie alla segretezza garantita da alcune giurisdizioni.

**Nota:** Le banche offshore ( lett. "**fuori dalle acque territoriali"**) sono banche che hanno sede legale in paesi, cosiddetti paradisi fiscali, che applicano legislazioni in campo fiscale e creditizio più convenienti, rispettando inoltre il segreto bancario

Tuttavia, uno degli strumenti più utilizzati per i pagamenti nell'economia sommersa sono le valute digitali. Pur essendo il **bitcoin** la criptovaluta più conosciuta, non è l'unica utilizzata.

In realtà, l'underground economy fa uso di un'ampia varietà di valute digitali alternative, molte delle quali sono state progettate specificamente per aumentare l'anonimato e la sicurezza delle transazioni. Hawala (o hewala, noto anche come hundi), è un sistema informale di trasferimento di denaro che si basa sull'affidabilità e l'integrità di una vasta rete di mediatori. Questo sistema è particolarmente diffuso in Medio Oriente, Nord Africa, Corno d'Africa e nel subcontinente indiano. Funziona al di fuori dei tradizionali canali bancari e dei sistemi finanziari convenzionali, offrendo un metodo alternativo per l'invio di rimesse e trasferimenti di valore.

Molti sistemi di pagamento elettronico si ispirano al modello Hawala e sono stati sviluppati con strutture simili, ora supportate da un'infrastruttura digitale. Questo approccio finanziario non lascia tracce nelle reti bancarie tradizionali: il denaro scompare da un luogo e riappare in un altro, rendendo difficile il tracciamento dei trasferimenti.

# Cyber Espionage

Nel 2011, lo spionaggio industriale e commerciale ha raggiunto livelli senza precedenti, portando alla luce una serie di attività di intelligence mirate a importanti aziende, principalmente occidentali. Queste operazioni sono state realizzate tramite intrusioni sofisticate condotte da team di specialisti altamente qualificati.

Tra le più note vi sono *Operation Nitro* e *Operation Night Dragon*, che hanno colpito numerose multinazionali nei settori chimico, energetico e oil & gas. Gli attacchi sono stati condotti principalmente attraverso tecniche di spear phishing, con cui gli aggressori hanno preso il controllo dei computer portatili di alcuni dipendenti. In questo modo, hanno potuto sfruttare le legittime connessioni VPN delle vittime per accedere in remoto agli applicativi e ai server interni aziendali, installando malware e monitorando le attività.

Questi attacchi furtivi, che possono protrarsi per mesi o addirittura anni prima di essere scoperti, sono estremamente insidiosi e difficili da prevenire. Nessuna organizzazione, infatti, può oggi considerarsi completamente al riparo da tali minacce.

La complessità e i costi legati allo spionaggio, in senso lato, sono diminuiti drasticamente nel corso degli anni, a causa della rivoluzione informatica. Oggi, gran parte delle informazioni si trova su supporti digitali e viene trasmessa attraverso le reti, rendendo più facile il loro accesso non autorizzato.

Un effetto importante di questa trasformazione è il superamento del concetto tradizionale di "furto" proprio del crimine, sostituito dalla centralità del concetto di "copia", tipico dello spionaggio. Dal momento che ciò che "è sempre lì" sembra essere "al sicuro", la scoperta di tali attività viene ritardata, mentre il tempo necessario per smercio e cash-out viene notevolmente ridotto.

Gli incidenti di spionaggio toccano sia il mondo civile che quello militare e coinvolgono diverse tipologie di attori:

- **Insider**, motivati da ragioni politiche, etiche, religiose, corruzione, ricatto, fama o semplice ignoranza
- **Contractor**, come fornitori esterni, consulenti
- **Competitor**, sia civili che militari, sponsorizzati dallo Stato o indipendenti

# Cyber Terrorism

Il cyber terrorismo rappresenta una delle minacce più insidiose dell'era digitale. Si tratta dell'uso intenzionale della tecnologia informatica, delle reti di comunicazione e delle infrastrutture digitali per compiere attacchi che possono causare danni fisici, psicologici o economici. Gli obiettivi dei cyber terroristi possono includere il sabotaggio di sistemi critici, la diffusione di panico e disinformazione, o la destabilizzazione di interi settori strategici, come l'energia, i trasporti, le finanze e la sanità.

A differenza del terrorismo tradizionale, il cyber terrorismo non richiede la presenza fisica degli aggressori e può essere condotto da qualsiasi parte del mondo. Questo lo rende estremamente difficile da prevenire e contrastare. Tra le tecniche più comuni usate dai cyber terroristi ci sono gli attacchi DDoS (Distributed Denial of Service), il malware, il ransomware, il furto di dati e l'hacking di infrastrutture critiche.

Le motivazioni dietro il cyber terrorismo sono molteplici e possono spaziare dal perseguimento di ideologie politiche o religiose, alla volontà di danneggiare gli interessi economici di specifici Paesi o organizzazioni. Uno degli aspetti più preoccupanti è il fatto che tali attacchi possono essere compiuti da singoli individui o piccoli gruppi, grazie alla disponibilità di strumenti e risorse online a costi relativamente bassi.

Gli effetti di un attacco cyber terroristico possono essere devastanti: interruzioni di servizi essenziali, danni economici ingenti, furto di dati sensibili e, in casi estremi, anche rischi per la sicurezza e la vita delle persone. Le infrastrutture critiche, come le reti elettriche, gli ospedali, le reti di comunicazione e i sistemi di controllo dei trasporti, sono tra i principali bersagli. La crescente dipendenza dalle tecnologie digitali ha aumentato la vulnerabilità delle società moderne a questo tipo di minaccia.