La Guerra Ibrida e il caso Stuxnet

Davide Pietrangeli
Master's student in Cybersecurity Management
Università Campus Bio-medico di Roma

9 luglio 2025

Indice

Capitolo 1

La Guerra Ibrida

1.1 Introduzione

La guerra ibrida è un conflitto che combina tattiche militari convenzionali con strategie non convenzionali. In questo approccio uno Stato impiega simultaneamente risorse politiche, economiche, informative e militari. La definizione della NATO sottolinea infatti che le minacce ibride «combinano mezzi militari e non militari, occulti e palesi»; vi rientrano campagne di disinformazione, attacchi informatici, pressioni economiche, nonché il ricorso contemporaneo a milizie irregolari e a forze convenzionali.

In sintesi, una guerra ibrida integra tattiche di natura diversa per conseguire un unico obiettivo strategico. Ciò comporta l'impiego simultaneo di leve politiche, economiche, informative e militari, spesso in modo sinergico e coordinato. Caratteristica fondamentale di queste operazioni è la sovrapposizione tra pace e guerra: i metodi ibridi puntano intenzionalmente a «confondere i confini tra guerra e pace» e a destabilizzare le società bersaglio, facendo ampio uso di azioni nel cosiddetto spazio grigio (grey zone).

La dottrina contemporanea enfatizza dunque la sincronizzazione degli attacchi su più fronti. Un caso emblematico è il malware Stuxnet (2010): esso si propagò su scala globale nelle reti Windows, ma il suo carico utile si attivava soltanto al rilevamento di specifiche apparecchiature di controllo industriale. In altre parole, sebbene Stuxnet infettasse in modo indiscriminato i sistemi, il suo effetto sabotante si manifestava solo sui bersagli programmati. Questo episodio dimostra come si possa combinare diffusione massiva e attivazione mirata, confermando l'importanza di operazioni cibernetiche coordinate e precise.

In conclusione, la guerra ibrida rappresenta una forma avanzata di conflitto asimmetrico, in cui le tradizionali distinzioni tra mezzi bellici e altre forme di coercizione risultano sfumate. L'aggressore sfrutta simultaneamente l'intero spettro di strumenti disponibili (politici, informatici, economici e militari) per conseguire vantaggi strategici senza ricorrere a uno scontro frontale convenzionale.

1.2 La storia

Sebbene il concetto di guerra ibrida sia emerso con forza soltanto nel discorso strategico del XXI secolo, le sue tattiche sono storicamente radicate. In varie forme, la combinazione di strumenti militari e non militari è stata applicata da numerosi attori statali e non statali nel corso dei conflitti moderni. Un esempio precoce è rappresentato dall'azione condotta da Hezbollah durante la guerra del Libano del 2006, la quale ha anticipato molte delle caratteristiche della guerra ibrida contemporanea. In quell'occasione, il gruppo sciita ha impiegato simultaneamente razzi, tunnel sotterranei, combattimenti irregolari e una campagna mediatica sofisticata per influenzare l'opinione pubblica regionale e internazionale. Diversi analisti militari considerano questa campagna una manifestazione embrionale di guerra ibrida, per l'uso integrato di strumenti convenzionali e asimmetrici.

La guerra ibrida è divenuta un tema centrale del pensiero strategico occidentale a partire dal 2014, quando la Federazione Russa ha annesso la Crimea e avviato il conflitto nel Donbas. In questo contesto, la Russia ha impiegato un'ampia gamma di strumenti: forze speciali senza insegne, campagne di disinformazione, attacchi informatici, agitazione di insorti locali e operazioni sotto falsa bandiera. La NATO, dinanzi a questa modalità di attacco non lineare e ambigua, ha ufficialmente riconosciuto la natura ibrida delle operazioni russe, elevando il concetto a priorità analitica e dottrinale.

Anche nel conflitto russo-georgiano del 2008 si ravvisano elementi ibridi significativi. La Russia, oltre a un intervento militare convenzionale rapido e mirato, ha condotto operazioni informatiche coordinate, come il blocco temporaneo delle reti e dei siti governativi georgiani, e ha manipolato l'informazione pubblica attraverso canali mediatici filo-russi. Questo episodio ha segnato uno dei primi esempi concreti di integrazione simultanea tra attacchi cibernetici e operazioni cinetiche, prefigurando dinamiche oggi ricorrenti.

La guerra civile siriana, iniziata nel 2011, costituisce un ulteriore caso paradigmatico. All'interno del complesso mosaico siriano, molteplici attori – tra cui Russia, Iran, Turchia e gruppi jihadisti come lo Stato Islamico – hanno fatto ampio ricorso a tattiche ibride. Tra queste si annoverano il sostegno a milizie proxy, l'impiego di combattenti irregolari, l'utilizzo sistematico della propaganda digitale, nonché attività di sorveglianza informatica e guerra psicologica. In Siria, l'interconnessione tra guerra convenzionale, insurrezione, terrorismo e conflitto per procura illustra la complessità multilivello della guerra ibrida.

Nel contesto ucraino, a partire dal 2015, si sono intensificati anche gli attacchi cibernetici. Sono stati registrati attacchi ransomware su infrastrutture critiche, sabotaggi informatici mirati (ad esempio contro centrali elettriche e ferrovie), e campagne di manipolazione dell'informazione, spesso condotte attraverso social media e botnet. La continuità e l'adattabilità di queste strategie rafforzano l'idea che la guerra ibrida non sia una fase transitoria del conflitto, bensì una forma strutturale

e persistente della competizione strategica moderna.

Questi casi dimostrano che la guerra ibrida, pur essendo una manifestazione moderna, si basa su principi strategici antichi: disorientare l'avversario, evitare lo scontro diretto su vasta scala, e perseguire obiettivi politici tramite una combinazione coordinata di mezzi militari e non militari. Ciò rende la guerra ibrida una strategia estremamente flessibile, capace di adattarsi ai diversi contesti geopolitici e tecnologici.

1.3 Caratteristiche operative della guerra ibrida: ambiguità e multi-dominio

Uno degli aspetti distintivi della guerra ibrida è il ricorso sistematico all'ambiguità strategica e agli effetti multi-dominio. A differenza della guerra convenzionale, essa si sviluppa simultaneamente in più sfere – fisica, informativa, economica, legale e cibernetica – con l'obiettivo di saturare le capacità di risposta del nemico, sfruttando i punti deboli del suo sistema decisionale e istituzionale.

Le tattiche ibride possono spaziare da intrusioni informatiche contro infrastrutture critiche (come reti elettriche, acquedotti, ospedali e sistemi di trasporto) a sabotaggi clandestini delle catene logistiche, fino a forme più sofisticate di coercizione indiretta, quali la manipolazione dei mercati finanziari o l'impiego strumentale del diritto internazionale, fenomeno noto come "lawfare". A queste si affianca anche l'eventuale impiego aperto, ma negabile, di forze speciali e milizie paramilitari, spesso non ufficialmente riconducibili allo Stato aggressore.

Gli analisti descrivono questa varietà di strumenti come un "cassetto degli attrezzi ibrido" (hybrid toolbox), che comprende azioni coordinate di natura:

- **politica**, come l'infiltrazione di élite locali o la strumentalizzazione di movimenti secessionisti;
- **economica**, inclusi embargo mirati, guerre valutarie e interruzioni nei flussi energetici;
- **giuridica**, attraverso il ricorso strategico a norme e trattati per ostacolare l'azione avversaria o legittimare interventi;
- **informativa**, tramite campagne di disinformazione, deepfake, uso di social media e narrazioni ostili;
- **militare non convenzionale**, mediante l'impiego di forze irregolari, milizie proxy o truppe "non contrassegnate", volte a creare negabilità plausibile (plausible deniability) e confondere l'identità dell'aggressore.

Esempi concreti di azioni ibride includono:

- attacchi informatici contro servizi pubblici o infrastrutture sanitarie;

- campagne di disinformazione tese a influenzare l'opinione pubblica interna o internazionale;
- pressioni economiche, come embarghi energetici, interruzioni delle forniture o speculazioni destabilizzanti;
- utilizzo di gruppi armati non statali o mercenari per destabilizzare aree di confine o fomentare conflitti civili.

L'efficacia della guerra ibrida risiede nella sua capacità di sfumare i confini tra guerra e pace, rendendo difficile l'attribuzione immediata della responsabilità e ritardando eventuali risposte. In questo modo, si paralizza il processo decisionale del Paese bersaglio, che si trova a fronteggiare una crisi distribuita e opaca, ma priva di un chiaro casus belli. L'obiettivo non è la vittoria militare tradizionale, bensì il logoramento strategico: destabilizzare, dividere, confondere, senza superare formalmente la soglia del conflitto armato dichiarato.

Capitolo 2

La guerra cibernetica come dominio strategico autonomo

La guerra cibernetica può essere definita come l'impiego di operazioni offensive e difensive all'interno del dominio informatico da parte di Stati o attori non statali (proxy), al fine di conseguire obiettivi strategici di natura militare, politica o economica. A differenza dei conflitti convenzionali, caratterizzati da strumenti tangibili quali carri armati, artiglieria o missili, la guerra cibernetica si svolge nel cyberspazio, un ambiente virtuale ma con impatti reali e crescentemente significativi.

2.1 Componenti tecniche e tattiche

Dal punto di vista tecnico, la guerra informatica si basa sull'utilizzo di una vasta gamma di strumenti:

- **malware**(software maligni finalizzati all'infiltrazione o alla distruzione di sistemi);
- **exploit zero-day**(vulnerabilità non ancora note ai produttori di software);
- **botnet**(reti di dispositivi compromessi utilizzati per condurre attacchi coordinati);
- **attacchi DDoS**(Distributed Denial of Service, mirati a rendere indisponibili servizi essenziali);
- **phishing e social engineering** impiegati per ottenere accesso non autorizzato a sistemi sensibili.

Queste tecniche possono essere impiegate per interrompere, degradare, spiare o assumere il controllo remoto di infrastrutture avversarie. Obiettivi comuni includono sistemi elettrici, telecomunicazioni, reti sanitarie, trasporti e comunicazioni militari.

Gli attori statali particolarmente avanzati come gli Stati Uniti, la Russia, la Cina, la Corea del Nord e l'Iran, ricorrono frequentemente a exploit personalizzati, certificati digitali rubati per eludere le misure di sicurezza, e architetture C2

(command-and-control) che consentono il controllo continuo degli attacchi in corso. Il cyberspazio consente inoltre un'esecuzione pressoché istantanea e a basso costo su scala globale, rendendo la guerra cibernetica un efficace moltiplicatore di forza (force multiplier) all'interno di operazioni militari congiunte.

2.2 Finalità strategiche e limiti operativi

Dal punto di vista strategico, la guerra cibernetica ha finalità che vanno ben oltre il semplice sabotaggio tecnico. Essa può servire a:

- **disattivare infrastrutture critiche**, riducendo la resilienza del sistema paese colpito;
- **sottrarre informazioni classificate**, con impatti su intelligence, sicurezza nazionale e competitività economica;
- **manipolare il flusso e la percezione delle informazioni**, interferendo con i processi democratici e l'opinione pubblica.

Tuttavia, la guerra informatica presenta alcune distinzioni fondamentali rispetto alla guerra convenzionale. In primo luogo, la difficoltà di attribuzione: spesso non è possibile identificare con certezza l'origine dell'attacco, il che complica eventuali risposte politiche o militari. In secondo luogo, gli effetti degli attacchi cyber raramente si traducono in distruzione fisica immediata o nella conquista di territori, e generalmente non comportano perdite umane dirette, almeno nel breve periodo.

Come osservano numerosi studiosi, la guerra informatica "spesso manca delle componenti centrali della guerra tradizionale: distruzione fisica su larga scala, violenza di massa e costrizione diretta di un attore alla volontà di un altro". Per questo motivo, le sole operazioni cyber difficilmente possono determinare la capitolazione del nemico, ma possono comunque esercitare una forte pressione strategica, soprattutto se integrate in una campagna più ampia.

2.3 Integrazione con il conflitto cinetico e ridefinizione dei domini

Nel contesto dei conflitti moderni, gli attacchi cibernetici sono sempre più spesso sincronizzati con operazioni cinetiche. Ad esempio, durante un'invasione armata, le reti di comunicazione del nemico possono essere neutralizzate in anticipo attraverso cyberattacchi, riducendo la capacità di coordinamento e risposta. Questa commistione ha contribuito a sfumare ulteriormente la linea di demarcazione tra guerra e pace, poiché tali atti non comportano necessariamente una dichiarazione formale di ostilità.

Di fronte a queste dinamiche, numerosi Stati hanno iniziato a riconoscere il cyberspazio come un dominio operativo autonomo, alla pari dei domini tradizionali

(terra, mare, aria, spazio). Sono stati istituiti comandi cibernetici dedicati (come il U.S. Cyber Command o il NATO Cooperative Cyber Defence Centre of Excellence), ed elaborate dottrine specifiche per l'impiego integrato delle capacità informatiche all'interno della strategia militare complessiva.

2.4 Esempi di Cyberwarfare

Diversi incidenti verificatisi negli ultimi due decenni illustrano con chiarezza l'evoluzione e le applicazioni pratiche della guerra cibernetica come strumento strategico, spesso inquadrato all'interno di contesti geopolitici più ampi.

2.4.1 Estonia (2007): il primo caso emblematico di cyberattacco politico

Nel 2007, l'Estonia fu vittima di una serie coordinata di attacchi informatici di tipo DDoS (Distributed Denial of Service), che colpirono siti istituzionali, bancari e mediatici. Gli attacchi ebbero luogo a seguito di una controversia con la Russia circa la rimozione di un monumento sovietico a Tallinn. Provenienti da reti bot controllate da ambienti filorussi, gli attacchi paralizzarono per settimane i servizi digitali del paese, tra cui l'e-government, provocando il primo blackout informatico su scala nazionale in Europa. Questo episodio è considerato il primo caso documentato di cyberattacco su base geopolitica e segnò una svolta nella percezione della vulnerabilità delle infrastrutture digitali statali.

2.4.2 Georgia (2008): sinergia tra guerra cinetica e cyber

Nel corso dell'invasione russa della Georgia nell'agosto 2008, furono registrati attacchi informatici paralleli all'offensiva militare convenzionale. Diversi siti governativi, mediatici e finanziari georgiani furono presi di mira con campagne di defacement e DDoS. L'aspetto significativo fu la simultaneità degli attacchi digitali e fisici, che rivelò la crescente integrazione tra il dominio cibernetico e le operazioni belliche tradizionali.

2.4.3 Ucraina (2015–2017): cyberattacchi alle infrastrutture critiche

Tra il 2015 e il 2017, l'Ucraina fu teatro di ripetuti attacchi cibernetici contro le sue infrastrutture energetiche, attribuiti a gruppi legati ai servizi di intelligence russi. In particolare, il malware BlackEnergy e successivamente Industroyer furono impiegati per penetrare nei sistemi di controllo industriale (ICS/SCADA) e causare blackout che lasciarono centinaia di migliaia di cittadini senza elettricità. Questi episodi rappresentano una delle prime manifestazioni concrete degli effetti fisici diretti derivanti da operazioni informatiche.

2.4.4 NotPetya (2017): l'escalation della guerra cibernetica globale

Nel 2017, il worm NotPetya, attribuito a un'operazione russa contro l'Ucraina, si diffuse rapidamente oltre i confini del conflitto, sfruttando un aggiornamento compromesso del software fiscale ucraino MeDoc. L'attacco causò danni stimati in oltre 10 miliardi di dollari a livello globale, colpendo aziende multinazionali, infrastrutture critiche e sistemi bancari, con effetti su larga scala in Europa, Asia e Nord America. NotPetya ha dimostrato che le armi cibernetiche, pur concepite per obiettivi locali, possono generare impatti sistemici transnazionali.

2.4.5 Invasione dell'Ucraina (2022–): operazioni informatiche a supporto del conflitto armato

L'invasione russa dell'Ucraina nel 2022 è stata accompagnata da numerosi episodi di guerra informatica, tra cui:

- **attacchi DDoS e defacement**contro siti governativi e media ucraini;
- **disturbo delle comunicazioni satellitari**, come nel caso dell'attacco alla rete Viasat, che comprometteva i sistemi di controllo militare e civile;
- **tentativi di penetrazione nei sistemi delle centrali nucleari**, evidenziando il rischio di incidenti catastrofici.

Tuttavia, l'uso della cyberwarfare in questo conflitto è stato più contenuto rispetto alle aspettative iniziali. La Russia ha evitato il danneggiamento irreversibile delle infrastrutture critiche, probabilmente per ragioni strategiche legate alla futura occupazione o al costo politico di un'escalation incontrollata.

2.5 Potenzialità e limiti della guerra informatica

Questi casi dimostrano le potenzialità della guerra informatica come strumento offensivo per:

- **influenzamento delle capacità decisionali e comunicative dell'avversario**;
- **disgregazione dei servizi essenziali**, con impatti sulla resilienza e sulla psicologia della popolazione civile;
- **influenza indiretta su teatri bellici convenzionali**.

Tuttavia, permangono significativi limiti strutturali e strategici. Gli esperti sottolineano che, ad oggi, non si è ancora verificato un evento equivalente a una "Pearl Harbor cibernetica", ovvero un attacco informatico di scala tale da determinare una risposta militare diretta o una trasformazione immediata dell'ordine geopolitico. Inoltre, la guerra informatica non sostituisce le forme tradizionali di coercizione militare, ma piuttosto le completa, agendo come moltiplicatore di forza o strumento di guerra asimmetrica.

2.6 Attribuzione, diritto e governance: le sfide emergenti

Uno degli aspetti più critici nella gestione della guerra informatica riguarda la complessità dell'attribuzione, sia sul piano tecnico che su quello politico e giuridico. A differenza delle forme convenzionali di attacco, in cui la provenienza è spesso immediatamente rilevabile, nel cyberspazio gli aggressori possono sfruttare tecniche di obfuscation, spoofing e proxying, rendendo difficile, se non impossibile, determinare in tempi rapidi e con certezza l'autore di un attacco. Questa ambiguità strategica mina i principi tradizionali della responsabilità statale e complica la possibilità di rispondere con misure proporzionate e legittime, come previsto dal diritto internazionale.

In tale contesto, la comunità internazionale ha cercato di colmare il vuoto normativo e interpretativo attraverso iniziative dottrinali e accademiche. Tra queste, il Manuale di Tallinn, elaborato sotto la supervisione del NATO Cooperative Cyber Defence Centre of Excellence e giunto alla sua seconda edizione nel 2017 (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations), rappresenta uno dei tentativi più significativi di applicare il corpus del diritto internazionale umanitario e del diritto dei conflitti armati (IHL e jus ad bellum/jus in bello) al dominio cibernetico. Il Manuale, redatto da un gruppo di esperti internazionali, non costituisce uno strumento legalmente vincolante, ma si propone come standard di riferimento interpretativo per governi, forze armate e decisori politici. Tra i punti salienti affrontati figurano la soglia per qualificare un attacco cibernetico come "uso della forza" ai sensi dell'art. 2(4) della Carta ONU, la legittima difesa in cyberspazio (art. 51), e l'obbligo di distinzione, proporzionalità e necessità negli attacchi contro infrastrutture critiche.

In un'ottica più ampia, l'emergere della guerra cibernetica ha sancito la piena affermazione del cyberspazio come "quinto dominio operativo", accanto a terra, mare, aria e spazio. Tale riconoscimento è stato formalizzato anche da organizzazioni come la NATO e il Dipartimento della Difesa degli Stati Uniti, che integrano ormai strutture cibernetiche nelle rispettive dottrine militari (Cyber Commands, Joint Cyber Operations, ecc.). Tuttavia, la guerra nel cyberspazio non rappresenta una cesura netta rispetto alla tradizione strategica: essa si configura piuttosto come un'estensione e una riformulazione delle modalità di proiezione del potere, particolarmente efficace in scenari ibridi e sotto soglia, dove l'ambiguità è uno strumento funzionale alla coercizione e alla denegabilità.

Infine, la natura del dominio cibernetico, decentralizzato, asimmetrico e fortemente interconnesso, ha spinto gli Stati a rivedere le proprie posture difensive e offensive. La resilienza delle infrastrutture critiche, la cooperazione pubblico-privato, il monitoraggio delle minacce emergenti e lo sviluppo di capacità di deterrenza cibernetica credibile sono oggi elementi centrali nella strategia di sicurezza nazionale di numerosi Paesi. In questo quadro, la guerra informatica non è solo una questione tecnologica, ma un fenomeno intrinsecamente politico e strategico, che ridefinisce le

frontiere tra guerra e pace, tra sicurezza e vulnerabilità, tra responsabilità statale e accountability internazionale.

Capitolo 3

Il caso Stuxnet: un precedente strategico di guerra informatica mirata

Il caso Stuxnet rappresenta uno degli esempi più emblematici e sofisticati di attacco informatico mirato, nonché una svolta nell'impiego del cyberspazio come dominio operativo di guerra. Scoperto nel 2010, Stuxnet è stato progettato per sabotare il programma di arricchimento dell'uranio iraniano presso il sito nucleare di Natanz, nel contesto delle crescenti tensioni geopolitiche legate alla proliferazione nucleare in Medio Oriente.

3.1 Genesi e obiettivi dell'attacco

Secondo diverse fonti di intelligence, lo sviluppo del malware sarebbe riconducibile a una cooperazione segreta tra Stati Uniti e Israele, all'interno dell'operazione denominata "Olympic Games", avviata sotto l'amministrazione Bush e proseguita con il presidente Obama. L'obiettivo strategico era quello di ritardare il progresso nucleare iraniano senza ricorrere a un'azione militare convenzionale, evitando così un'escalation regionale o una rottura diplomatica irreversibile.

Il sito di Natanz, pur essendo fisicamente isolato da Internet (air-gapped), impiegava sistemi Windows con software Siemens Step7 per la programmazione dei Programmable Logic Controller (PLC) che regolavano la velocità delle centrifughe per l'arricchimento dell'uranio. Stuxnet fu concepito per infettare questi sistemi in modo mirato, alterare il funzionamento dei PLC e compromettere così le centrifughe a livello meccanico, senza essere rilevato.

3.2 Cronologia e scoperta

Le indagini di cyber-forensics collocano la fase di ingegnerizzazione iniziale del codice intorno al 2005-2006, con la scrittura del modulo di attacco per i PLC verso la fine del 2007. Il malware fu distribuito per la prima volta in Iran il 1° apri-

le 2009, mentre la sua presenza fu identificata pubblicamente nel giugno 2010 dal laboratorio bielorusso VirusBlokAda, che individuò un worm anomalo denominato "Rootkit.Tmphider", in seguito riconosciuto come Stuxnet.

Nel corso del 2010, Stuxnet si evolse in diverse varianti, aumentando le proprie capacità di infiltrazione e sabotaggio. Nella seconda metà dell'anno, circa un quinto delle centrifughe iraniane operative (stimate tra 5.000 e 9.000 unità) risultava danneggiato o inutilizzabile. L'Iran denunciò l'incidente come un vero e proprio "cyberattacco nucleare", sebbene né gli Stati Uniti né Israele abbiano mai rivendicato ufficialmente la responsabilità.

3.2.1 Infrastrutture e meccanismi tecnici

Stuxnet fu il primo malware noto a colpire con successo un impianto industriale fisico, progettato per operare su sistemi Windows dotati di software Siemens WinCC/Step7, targettizzando i PLC Siemens S7-315 e S7-417. Una volta infettata la macchina, il worm:

- cercava dispositivi compatibili;
- sovrascriveva i blocchi di codice dei PLC;
- **modificava i cicli di rotazione delle centrifughe**, facendole accelerare e rallentare in modo anomalo e intermittente.

Contestualmente, Stuxnet impiegava un sofisticato meccanismo di falsificazione dei dati di monitoraggio, facendo apparire i sistemi in condizioni normali, mentre in realtà subivano danni fisici. Questo sabotaggio indiretto portò alla distruzione stimata di circa 1.000 centrifughe, compromettendo il programma nucleare iraniano per mesi. Il worm conteneva inoltre un rootkit per PLC, una tecnica senza precedenti all'epoca, che ne mascherava completamente l'azione agli occhi degli operatori locali.

3.3 Attribuzione e implicazioni strategiche

Benché nessun governo abbia mai ammesso pubblicamente la paternità dell'attacco, l'attribuzione a una operazione statale congiunta tra Stati Uniti e Israele è ampiamente accettata nella comunità degli analisti e dei ricercatori di sicurezza. Secondo Kaspersky Labs e Symantec, la complessità tecnica, l'impiego di exploit zero-day, l'uso di certificati digitali rubati (a Realtek e JMicron) e la natura del target indicano senza ambiguità un progetto statale sostenuto da ingenti risorse umane, economiche e operative.

Fonti giornalistiche autorevoli, come il New York Times, hanno confermato l'esistenza dell'Operazione Olympic Games e il coinvolgimento diretto delle agenzie di intelligence americane (NSA, CIA) e israeliane (Mossad, Unit 8200). Di conseguenza, Stuxnet è considerato il primo caso documentato di arma cibernetica progettata

per distruggere fisicamente infrastrutture industriali, aprendo una nuova fase nei conflitti asimmetrici e nello sviluppo delle dottrine di cyber deterrence.

Il caso Stuxnet ha rappresentato una svolta epocale nel panorama della guerra informatica. Per la prima volta, un malware ha dimostrato la capacità non solo di compromettere sistemi digitali, ma anche di infliggere danni fisici misurabili a infrastrutture strategiche, il tutto mantenendo una negabilità plausibile per gli attori coinvolti. Stuxnet ha aperto la strada a nuove tipologie di operazioni cibernetiche offensive, evidenziando l'intersezione tra cyberspazio, sicurezza nazionale e geopolitica nucleare.

Capitolo 4

Architettura tecnica

Dal punto di vista tecnico, Stuxnet rappresenta uno dei malware più sofisticati mai realizzati, grazie alla sua architettura modulare avanzata e alla combinazione di capacità di infezione, persistenza e sabotaggio. Il worm si articolava in più componenti principali, tra cui un dropper eseguibile (wrapper) e una libreria dinamica (DLL) centrale, che fungeva da payload operativo.

Il dropper, ossia il modulo iniziale di esecuzione, conteneva al suo interno tutti gli altri componenti in una sezione "stub" incorporata. Una volta attivato su un sistema target, estraeva in memoria una DLL di circa 90 KB, avviando quindi una delle numerose funzioni esportate integrate nel file. Questo design ha permesso a Stuxnet di eseguire operazioni in modo furtivo ed efficiente, senza scrivere necessariamente file sul disco, riducendo così la tracciabilità.

La DLL principale conteneva decine di routine esportate, ciascuna responsabile di un segmento specifico del ciclo di vita del worm:

- la funzione esportata 1 era incaricata di infettare dispositivi rimovibili (es. chiavette USB), sfruttando meccanismi di autorun e tecniche di lateral movement;
- le funzioni 22 e 24 gestivano la propagazione attraverso reti locali, identificando host vulnerabili e trasmettendo il malware in ambienti Windows;
- la funzione 15 fungeva da punto di ingresso iniziale per l'esecuzione del payload;
- le esportazioni 28 e 29 implementavano la logica di comando e controllo (C2), stabilendo comunicazioni remote con i server degli attaccanti per ricevere aggiornamenti o nuovi comandi.

Una delle tecniche più ingegnose utilizzate da Stuxnet riguardava la evasione del monitoraggio delle API di sistema. Il malware, infatti, agganciava la libreria NTDLL.dll, caricando DLL con nomi appositamente manipolati direttamente dalla memoria, bypassando il file system tradizionale. Questa strategia riduceva ulteriormente la visibilità dell'attacco da parte degli strumenti di sicurezza e degli operatori umani.

Nel complesso, la modularità di Stuxnet non solo facilitava l'aggiornamento o la disinstallazione remota del worm, ma ne potenziava anche la resilienza e la capacità di adattamento ai diversi ambienti. Tale livello di complessità e finezza esecutiva è tipico di operazioni sponsorizzate da Stati nazionali, e ha elevato Stuxnet al rango di prototipo per armi cibernetiche moderne.

4.1 Sfruttamento di vulnerabilità zero-day

Uno degli aspetti più notevoli di Stuxnet è il ricorso a quattro vulnerabilità zero-day di Microsoft Windows, due delle quali all'epoca erano completamente sconosciute alla comunità di sicurezza. Questo livello di sofisticazione ha reso il malware estremamente furtivo e difficile da contenere, rafforzando l'ipotesi di una sponsorizzazione statale.

Nello specifico, Stuxnet ha sfruttato le seguenti falle:

- **MS10-046** Una vulnerabilità nei file di collegamento LNK di Windows, che consentiva l'esecuzione automatica di codice maligno quando un dispositivo USB infetto veniva semplicemente visualizzato in Esplora risorse. Questa tecnica ha facilitato l'infezione tramite supporti rimovibili, anche senza esecuzione manuale da parte dell'utente.
- **MS10-061** Una vulnerabilità nel servizio di spooler di stampa di Windows, utilizzata da Stuxnet per propagarsi all'interno di reti locali (LAN), sfruttando meccanismi di stampa condivisa per l'esecuzione remota di codice.
- **MS08-067** Una falla critica nel servizio server di Windows (nota ma ancora sfruttabile in molti sistemi non aggiornati), che permetteva la diffusione attraverso condivisioni di rete SMB, un metodo già usato in attacchi come Conficker.
- **MS10-073** Una vulnerabilità di escalation dei privilegi in Win32k.sys, utilizzata per ottenere diritti di amministratore anche su macchine completamente aggiornate, aggirando le protezioni utente standard.

La combinazione simultanea di più exploit zero-day in un singolo worm ha rappresentato un evento senza precedenti nella storia della sicurezza informatica. Secondo Symantec, "Stuxnet sfrutta un totale di quattro vulnerabilità Microsoft non patchate, due delle quali non erano mai state divulgate pubblicamente", confermando così l'elevato livello di risorse e competenze impiegato nello sviluppo.

In sintesi, il successo della propagazione autonoma e silenziosa di Stuxnet è dipeso in larga parte dalla sua capacità di sfruttare falle di sicurezza precedentemente ignote, garantendo una profonda penetrazione in ambienti industriali altamente protetti, come quelli del programma nucleare iraniano.

4.2 Meccanismo di propagazione

Stuxnet adottava molteplici vettori di infezione, progettati per massimizzare la penetrazione iniziale e la persistenza all'interno di ambienti industriali isolati. Il vettore primario di infezione sembra essere stato costituito da unità USB infette, tramite le quali il worm si trasmetteva utilizzando un file .LNK malevolo denominato Shortcut to.lnk. Questo file sfruttava la vulnerabilità MS10-046 nei collegamenti di Windows per eseguire automaticamente il codice maligno al semplice accesso visivo alla directory, senza necessità di esecuzione manuale da parte dell'utente. Una volta introdotto all'interno della rete di destinazione, Stuxnet si propagava lateralmente attraverso diverse tecniche avanzate:

- Exploiting del servizio di spooler di stampa (MS10-061) per l'esecuzione remota di codice attraverso meccanismi di stampa condivisa;
- Sfruttamento del protocollo SMB tramite la vulnerabilità MS08-067, già nota ma ancora efficace su molte reti vulnerabili;
- Diffusione attraverso condivisioni di file aperte, includendo directory condivise e repository interni;
- Accesso diretto ai database WinCC di Siemens, sfruttando credenziali hard-coded e comunicazioni su rete LAN.

Una tecnica particolarmente insidiosa consisteva nella manomissione dei file di progetto del software Siemens Step7: ogni volta che un ingegnere apriva un progetto compromesso, Stuxnet si auto-eseguiva, reinfezionando il sistema anche dopo una rimozione apparente del malware, rafforzando così la resilienza del worm all'interno degli ambienti di sviluppo SCADA.

Infine, Stuxnet implementava un meccanismo di aggiornamento peer-to-peer altamente sofisticato. I computer infetti attivavano un server RPC locale, permettendo la comunicazione con altri host compromessi nella stessa rete. In tal modo, i nodi infetti potevano condividere tra loro versioni aggiornate del worm, garantendo un flusso continuo di aggiornamenti del codice senza necessità di contatto con server esterni di comando e controllo. Questa strategia contribuiva a mantenere l'autonomia dell'infezione, specialmente in ambienti non connessi a Internet, e dimostra il livello avanzato di progettazione e di sostenibilità operativa dell'attacco.

4.3 Evasione delle difese tramite certificati digitali rubati

Per aggirare i meccanismi di sicurezza dei sistemi operativi e ottenere un'apparenza di legittimità, Stuxnet impiegava una tecnica altamente sofisticata: la firma digitale del proprio codice malevolo mediante certificati rubati da aziende affidabili. In particolare, nel gennaio 2010, una prima variante del malware fu firmata digitalmente

con un certificato appartenente alla società taiwanese Realtek Semiconductor Corp. Successivamente, nel luglio 2010, una nuova variante utilizzò un certificato appartenente alla JMicron Technology Corp., un altro fornitore di hardware anch'esso con sede a Taiwan.

Questi certificati, validi al momento dell'attacco, permettevano a Stuxnet di caricare driver e componenti (come MRxNet.sys) su sistemi Windows a 32 bit senza attivare avvisi di sicurezza, in quanto il sistema operativo considerava affidabili le firme digitali provenienti da enti certificati. L'uso di firme valide rappresentava un'importante tecnica di evasione: non solo superava i controlli degli antivirus, ma eludeva anche le restrizioni imposte da Microsoft sui driver kernel-mode, che richiedevano firme certificate per l'installazione automatica.

I certificati in questione furono revocati dalle autorità di certificazione (CA) una volta scoperta la loro compromissione, ma fino a quel momento avevano garantito a Stuxnet una notevole furtività operativa. L'acquisizione di questi certificati compromessi implica una compromissione fisica o remota dei sistemi aziendali di Realtek e JMicron, evidenziando il coinvolgimento di attori statali con notevoli capacità di intelligence informatica. Secondo numerosi esperti di sicurezza, tale capacità indica non solo la complessità tecnica dell'operazione, ma anche il livello di risorse e accesso compatibile con operazioni condotte da agenzie governative.

4.4 Meccanismo di Command-and-Control (C2)

Oltre alle sue capacità di propagazione e sabotaggio autonomo, Stuxnet integrava un sistema di comunicazione con server C2 (command-and-control) al fine di mantenere una certa interattività con gli attori che lo avevano distribuito. Una volta installato su un sistema compromesso, il worm eseguiva un processo di ricognizione locale, raccogliendo informazioni tra cui la versione del sistema operativo Windows e la presenza di software Siemens Step7 o WinCC, utilizzati per il controllo industriale.

Se il sistema era connesso a Internet, Stuxnet tentava di stabilire una connessione HTTP in uscita sulla porta 80 verso uno dei due domini preconfigurati: mypremierfutbol.com e todaysfutbol.com. Questi domini, ospitati su server localizzati in Malesia e Danimarca, fungevano da nodi C2 per ricevere telemetria dai dispositivi infetti e, potenzialmente, inviare aggiornamenti o nuovi moduli malevoli. Le informazioni inviate includevano fingerprint del sistema target, e le risposte dai server potevano contenere payload aggiornati, configurazioni modificate o persino nuovi indirizzi C2, memorizzabili in file locali per utilizzi futuri.

Tuttavia, in molti casi pratici, i sistemi industriali bersaglio — tra cui le centrali iraniane — erano isolati fisicamente da Internet tramite misure di air gap, riducendo significativamente l'efficacia del canale C2. Nonostante ciò, la presenza di questa funzionalità dimostra che Stuxnet non era progettato come un semplice malware statico, ma come un'arma cibernetica dinamica e modulare, capace di ricevere istruzioni post-deployment, aggiornarsi autonomamente e adattarsi a nuove condizioni

operative.

L'infrastruttura C2 di Stuxnet è stata disattivata dopo la scoperta pubblica del worm, con il blocco dei domini da parte delle autorità e delle società di sicurezza informatica. Tuttavia, la sua architettura flessibile e resiliente, unita alla capacità di auto-aggiornamento tramite canali laterali (come la comunicazione peer-to-peer tra host infetti), conferma l'elevato livello di progettazione, più coerente con un'operazione militare sponsorizzata da uno Stato che con una campagna malware convenzionale.

4.5 Il Carico Offensivo: Attacco ai PLC e Sabotaggio Ciberfisico

Il nucleo dell'efficacia distruttiva di Stuxnet risiedeva nel suo payload mirato contro i Programmable Logic Controller (PLC) Siemens impiegati per il controllo delle centrifughe a gas nell'impianto nucleare iraniano di Natanz. Il worm agiva sostituendo dinamicamente una DLL critica all'interno del software Siemens Step7, comunemente utilizzato dagli ingegneri per programmare i PLC. In particolare, Stuxnet rimpiazzava la libreria s7otbxdx.dll con una propria versione malevola (nota come risorsa 208), mantenendo la stessa interfaccia e struttura per non destare sospetti.

Questa DLL sostitutiva consentiva a Stuxnet di intercettare e manipolare tutte le operazioni di lettura e scrittura tra il PC e i PLC Siemens. Di conseguenza, il worm era in grado di iniettare blocchi di codice dannoso direttamente nei PLC al momento della programmazione da parte dell'utente, senza che questi se ne accorgesse. Inoltre, ogni modifica introdotta nel codice ladder o nei blocchi funzione veniva mascherata durante i processi di lettura: il malware mostrava una versione "pulita" del codice al software Step7 o WinCC, nascondendo così la presenza dell'infezione in modo simile a un rootkit tradizionale, ma applicato ai controllori industriali.

Una volta installato, il payload agiva attraverso blocchi funzione maligni che modificavano impercettibilmente il comportamento delle centrifughe. In particolare, le routine alteravano la frequenza di rotazione dei motori in modo ciclico: Stuxnet causava accelerazioni e rallentamenti controllati, fuori specifica, che portavano a stress meccanico, usura prematura e rottura fisica delle centrifughe. Allo stesso tempo, il malware falsificava i dati di ritorno verso l'interfaccia operatore, mostrando valori normali nei grafici e nei registri di sistema. In questo modo, l'attacco non solo era efficace nel danneggiare i macchinari, ma lo faceva in maniera subdola, prolungata e invisibile agli occhi degli operatori.

I ricercatori di sicurezza hanno confermato che Stuxnet implementava una sofisticata forma di attacco ciberfisico, in cui il codice digitale compromette direttamente l'integrità dei dispositivi fisici controllati. Questo approccio, all'epoca senza precedenti, ha segnato un punto di svolta nella storia della guerra informatica, dimostrando per la prima volta che un malware poteva alterare con precisione il funzio-

namento di infrastrutture critiche attraverso la manipolazione dei sistemi SCADA (Supervisory Control and Data Acquisition) e dei dispositivi embedded.

4.6 Meccanismi di Stealth ed Evasione di Stuxnet

Uno degli aspetti più notevoli di Stuxnet è rappresentato dalla sua sofisticata architettura stealth, progettata per evitare il rilevamento sia da parte degli utenti umani che degli strumenti di sicurezza informatica. A livello di host Windows, il worm ha installato un driver in modalità kernel denominato MRxNet.sys, firmato con un certificato digitale rubato a Realtek, che fungeva da rootkit di sistema. Questo driver intercettava le chiamate al file system e filtrava dinamicamente l'output delle directory, nascondendo tutti i file che corrispondevano a pattern specifici, come Shortcut to.lnk e WTRxxxx.tmp, ovvero i file utilizzati per l'autopropagazione via USB. Ciò faceva apparire completamente innocue le unità USB infette, impedendo che un'ispezione manuale o automatica potesse rilevare elementi sospetti.

Stuxnet implementava inoltre tecniche di hooking delle API di sistema a livello kernel, con l'obiettivo di oscurare i processi in esecuzione, le voci nel registro di sistema e altri indicatori di compromissione. Questo livello di persistenza e invisibilità era estremamente raro all'epoca nei malware industriali, indicando un investimento considerevole in capacità tecniche e risorse.

Sul fronte dei PLC, l'occultamento era altrettanto avanzato: sfruttando la comunicazione legittima del software Siemens Step7, il malware intercettava e manipolava le operazioni di lettura/scrittura ai PLC. In particolare, Stuxnet mascherava i blocchi di codice dannoso iniettati nei controllori, facendo apparire ai tecnici solo i blocchi originali o "attesi". In tal modo, anche controlli regolari del codice ladder o dei blocchi funzione non rivelavano alterazioni, rendendo di fatto Stuxnet il primo esempio noto di rootkit applicato ai sistemi di controllo industriale (ICS).

Infine, Stuxnet integrava diverse funzionalità anti-analisi e anti-debugging. Tra queste figuravano il controllo dell'ambiente per rilevare l'esecuzione in macchine virtuali (sandbox), l'uso di configurazioni cifrate per rendere ardua la decodifica manuale, e una whitelist geografica: il worm evitava intenzionalmente di infettare host con configurazioni linguistiche associate ad alcuni Paesi (tra cui Israele), al fine di limitare la diffusione collaterale e ridurre il rischio di scoperta prematura.

Nel complesso, Stuxnet ha ridefinito il paradigma dell'"invisibilità" in ambito malware, combinando tecniche avanzate di rootkit, firme digitali autentiche, exploit zero-day, evasione comportamentale e stealth su più livelli (host, rete, PLC). Questi elementi lo rendono di gran lunga più sofisticato del malware convenzionale, e ne confermano la natura di arma cibernetica di livello statale progettata con cura strategica e precisione tecnica.

Capitolo 5

Conclusione

5.1 Implicazioni Strategiche e Geopolitiche della Scoperta di Stuxnet

La scoperta di Stuxnet ha avuto implicazioni profonde e durature per il panorama della sicurezza informatica globale, ridefinendo radicalmente le percezioni circa il potenziale delle armi digitali. Dal punto di vista tecnico, Stuxnet ha dimostrato in maniera inequivocabile che un worm informatico può causare danni fisici intenzionali e controllati a infrastrutture industriali reali, inaugurando la categoria degli attacchi ciber-fisici. Prima del 2010, nessun malware conosciuto aveva manipolato processi industriali con una tale precisione operativa. Questo precedente ha provocato una revisione urgente delle politiche di sicurezza nelle infrastrutture critiche, con particolare attenzione ai sistemi SCADA (Supervisory Control and Data Acquisition) e ai controllori logici programmabili (PLC), soprattutto in settori come l'energia, la manifattura e la difesa.

Sul piano politico e militare, Stuxnet è stato considerato un "game changer" nella dottrina della guerra cibernetica. Esso ha consolidato l'idea che gli attacchi informatici non siano semplici episodi di sabotaggio, bensì strumenti di potere statale e proiezione strategica, parte integrante della diplomazia coercitiva e delle operazioni militari non convenzionali. In risposta, molte nazioni hanno istituito comandi cibernetici dedicati (come l'US Cyber Command), incorporando la dimensione cyber nelle esercitazioni interforze e nelle strategie di difesa congiunta. La guerra cibernetica è oggi trattata come un dominio operativo paritario rispetto a terra, mare, aria e spazio.

Dal punto di vista strategico, Stuxnet ha mostrato che un'operazione informatica può raggiungere obiettivi di alto valore con un costo inferiore e rischi politici contenuti rispetto agli attacchi cinetici convenzionali. Diversi analisti hanno sottolineato come simili operazioni possano persino essere percepite come eticamente preferibili, in quanto minimizzano le vittime collaterali e i danni indiscriminati. Alcuni studiosi hanno paragonato Stuxnet a una forma di operazione speciale digitale, condotta con precisione chirurgica e finalizzata a neutralizzare un'infrastruttura critica avversaria

senza dover impiegare forze militari sul campo.

Tuttavia, l'attacco ha anche generato preoccupazioni legate all'escalation e alla proliferazione. In particolare, la problematica dell'attribuzione, ovvero la difficoltà di identificare con certezza gli autori di un attacco, complica la risposta politica e giuridica: l'Iran ha considerato Stuxnet un atto di guerra, ma nessun attore statale ha mai rivendicato ufficialmente la responsabilità. Questa ambiguità erode i meccanismi tradizionali di deterrenza e diritto internazionale, rendendo più difficile distinguere tra stato di pace e stato di ostilità. Inoltre, vi è il timore che la pubblica esposizione del codice e delle tecniche di Stuxnet possa incentivare altri attori, statali o non statali, a sviluppare armi simili, aumentando il rischio di attacchi contro infrastrutture civili.

In risposta, molte nazioni hanno rafforzato le strategie di cyber-resilienza, focalizzandosi sulla protezione dei sistemi industriali. Sono aumentati gli investimenti in standard di sicurezza ICS, monitoraggio delle anomalie comportamentali, condivisione di informazioni tra governi e settore privato, e capacità di risposta rapida agli incidenti. Ad esempio, negli Stati Uniti la CISA (Cybersecurity and Infrastructure Security Agency) emette bollettini periodici dedicati alle minacce contro ambienti OT/ICS, mentre nel contesto NATO sono emerse iniziative come C4IRCYBER per supportare rapidamente le infrastrutture cyber degli alleati, come nel caso del conflitto in Ucraina.

5.2 L'Eredità Strategica di Stuxnet

In definitiva, Stuxnet rappresenta una svolta epocale nella storia della guerra informatica. Ha dimostrato che il codice può essere un'arma con effetti reali e strategici, ma ha anche rivelato che simili operazioni richiedono capacità tecniche eccezionali, intelligence mirata e risorse statali ingenti. Il suo sviluppo, stimato in milioni di dollari, e la conoscenza dettagliata richiesta sull'infrastruttura bersaglio suggeriscono che solo un ristretto numero di Stati possa oggi replicare un'operazione di pari portata.

Tuttavia, la sua esistenza ha ridefinito la percezione della minaccia informatica, spostando l'attenzione dalla semplice prevenzione alla resilienza strutturale delle reti critiche. In questo contesto, Stuxnet non è solo un'arma, ma anche un catalizzatore per l'evoluzione della cyber-difesa globale.

Capitolo 6

Riferimenti Bibliografici

- Anderson, H. S., Roth, P. (2018). *EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models.* arXiv:1804.04637
- Ucci, D., Aniello, L., Baldoni, R. (2019). *Survey of machine learning techniques for malware analysis.* Computers & Security, 81
- Kolosnjaji, B. et al. (2016). *Deep learning for classification of malware system call sequences.* AI Conference.
- Rigaki, M., Garcia, S. (2018). *Bringing a GAN to a Knife-Fight.* IEEE Euro S&P Workshops.
- Szor, P. (2005). *The Art of Computer Virus Research and Defense.* Addison-Wesley.
- Goodfellow, I., Bengio, Y., Courville, A. (2016). *Deep Learning.* MIT Press.
- Russell, S., Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*, 4th Ed. Pearson.