Giacomo Assenza, Luca Faramondi, Roberto Setola
(Complex System & Security Lab Università Campus Bio-Medico di Roma)

Peculiarità e problematiche della cyber security per gli Industrial Control System

Peculiarities and challenges of cyber security for the Industrial Control Systems

Sommario: *Gli Industrial Control System (ICS) sono una parte integrante delle moderne Infrastrutture Critiche (IC) in quanto sovrintendono a tutte le operazioni connesse con la gestione e il controllo di settori vitali come quello elettrico, petrolchimico, energetico, ecc.. Tuttavia, tali sistemi espongono le IC alla minaccia cyber, e i recenti attacchi informatici hanno dimostrato che è possibile, attraverso delle manipolazioni malevoli dei processi produttivi, provocare danni cinetici con conseguenze potenzialmente catastrofiche. Questo articolo illustra i problemi di sicurezza che scaturiscono dall'integrazione negli ICS di elementi e prodotti standardizzati e connessione Internet. Verranno, inoltre, analizzati gli attacchi cyber più rilevanti e si fornirà una profilazione della minaccia cyber suggerendo alcuni aspetti difensivi.*

Abstract: *ICS have become an integral component of CI, facilitating operations in vital sectors such as electricity, nuclear, energy and petrochemical manufacturing. However, these systems expose CI to the cyberthreat, and recent attacks demonstrated that targeting industrial process via cyberspace for inducing mechanical break points and provoking kinetic impacts has become possible. This paper will illustrate how ICS business-driven trends such as adopting IT elements, employing standard products and increasing Internet connectivity, have affected the security of industrial processes. Also, the paper will analyse the most relevant ICS cyberattacks and will provide a profiling of the cyberthreat and suggest defensive aspects.*

1. Introduzione

Gli Industrial Control System (ICS) sono ormai parte integrante delle infrastrutture critiche moderne in quanto sovrintendono a tutte le operazioni connesse con la gestione e il controllo. Questi sistemi di controllo, che rientrano nella più amplia categoria delle OT (operational technologies) e che vengono impiegati fina dagli anni '60, hanno subito profonde trasformazioni tutte orientate verso la massimizzazione della loro efficienza. Gli ICS infatti, che erano un tempo isolati dall'ambiente esterno e che si servivano di sistemi di legacy propri, si servono oggi di soluzioni IT, *off-the-shelf* e sono connessi a Internet. Queste trasformazioni, oltre ad avere consentito significativi progressi tecnologici e riduzione dei costi di

esercizio, hanno introdotto vulnerabilità importanti negli ambienti OT che potrebbero comprometterne la sicurezza. Infatti, data la grande quantità di dati scambiati e il vincolo di *hard real-time* che caratterizza le OT risulta difficile integrare in questi sistemi le classiche soluzioni di sicurezza del mondo IT rendendoli suscettibili ad attacchi cyber.

L'aspetto più critico delle vulnerabilità degli ICS è che gli attacchi cyber potrebbero indurre un impatto cinetico con drammatiche conseguenze sulla salute delle persone e sull'ambiente oltre che produrre danni con costi e tempi di ripristino significativi. Infatti un aggressore può volontariamente alterare il normale operato di un processo fino a portare il sistema a un punto di rottura meccanico. Bisogna infatti considerare che gli ICS costituisco dei target strategici e rilevanti non solo per la funzione che svolgono nella società ma anche perché spesso maneggiano impianti e processi intrinsecamente pericolosi, e una loro manomissione potrebbe provocare danni ambientali e alla popolazione, oltre che meramente economici.

Questi timori si sono concretizzati a partire dal 2011 con la scoperta di Stuxnet, il primo malware in grado di "deteriorare" fisicamente una apparecchiatura meccanica (nel caso in specie le centrifughe per l'arricchimento dell'uranio in un impianto nucleare Iraniano). Ad oggi, si sono verificati almeno altri quattro attacchi con conseguenze cinetiche: Irongate (2014) che ha comportato il danneggiamento di un impianto metallurgico in Germaia, BlackEnergy3 (2015) e Crashoverride (2016) che hanno provocato l'uno a distanza di un anno dall'altro due blackout in Ucraina, e Trisis (2017) che ha causato lo shutdown di uno stabilimento petrolchimico in Medio Oriente. Sebbene tali attacchi abbiano avuto un impatto limitato, o comunque ben lontano da catastrofico, hanno dimostrato che operazioni offensive immateriali, dunque una sequenza di zeri e uno, sono potenzialmente in grado di ottenere i medesimi risultati di una carica esplosiva, con il vantaggio che l'azione può essere sferrata da migliaia di chilometri di distanza e, soprattutto, che la possibilità di attribuzione, ossia di risalire all'autore dell'attacco, sono ridotte o comunque non immediate.

Quest'articolo affronterà l'argomento e la trattazione è sviluppata come segue: le sezioni 1, 2 e 3 illustrano il ruolo che svolgono gli ICS nelle IC e illustrano, anche a seguito delle recenti trasformazioni, i loro punti di vulnerabilità; la sezione 4 traccia le caratteristiche della minaccia cyber per gli ambienti industriali e la 5 passa in rassegna i principali attacchi informatici contro le OT; infine, la sezione 6 introduce alcuni elementi che giocano a favore della difesa degli ICS.

2. ICS e Infrastrutture critiche

L'acronimo ICS si riferisce a un insieme di tecnologie, sia software che hardware, che si interfacciano direttamente con i processi industriali e che svolgono attività di produzione, trasporto e trasformazione dei beni. Gli ICS, come gli SCADA (*Supervisor Control and Data Acquisition*), e i DCS (*Distributed Control Systems*) rientrano nella più amplia categoria delle Operational Technologies (OT), ossia quegli apparati e sistemi che impiegano network, protocolli di comunicazione ed elementi fisici per svolgere tre funzioni principali: l'acquisizione dei dati, le attività di controllo e supervisione, e l'esecuzione di comandi (Stouffer & Al., 2011).

Le società moderne dipendono in modo sempre più radicale dai dispositivi ICS. Infatti, tra i clienti dei principali fornitori di soluzioni OT (Rockwell Automation, Siemens, ABB, Mitsubishi) figurano soggetti che operano in campi quali il settore energetico, delle comunicazioni e dei trasporti. Tali campi sono considerati dalla maggior parte degli stati come settori critici, e i soggetti che vi operano sono identificati come infrastrutture critiche (IC) (Brunner & Suter, 2009). Sebbene non esista una caratterizzazione universale di infrastruttura critica, riflettendo questa l'identità geografica storica e culturale dei singoli soggetti (Setola, 2011), queste possono essere identificate come tutti quei sistemi e assetti, tanto fisici che virtuali, il cui malfunzionamento o interruzione avrebbe un impatto diretto e significativo sull'economia, sicurezza e salute nazionale, provocando un effetto domino di imprevedibili reazioni a catena in grado di compromettere la stabilità stessa di un paese (EPCP, 2005).

Le IC eseguono le funzioni essenziali della società moderna e costituiscono il loro cuore pulsante. Proprio come il cuore non può mai smettere di battere, gli assetti critici devono essere sempre disponibili, affidabili e operativi. Questo bisogno primario di disponibilità e performance ha comportato nel mondo degli ICS, presenti negli impianti industriali e manufatturieri già dagli anni '60, delle trasformazioni significative. Nel corso del tempo, infatti, le OT che tradizionalmente si affidavano a sistemi di legacy con protocolli proprietari e fisicamente isolate dall'ambiente esterno (Brunner & Suter, 2009; Galloway & Hancke, 2013), hanno fatto ricorso in modo sempre più massiccio alle tecnologie IT e a prodotti *off-the-shelf*. Inoltre, molti componenti di questi sistemi, che comunicavano un tempo attraverso network chiusi, sono stati integrati nel più generale trend del "*Industrial Internet of Things* (IIoT) con il risultato che gli odierni Cyber-Physical Sistems (CPS), ossia dispositivi informatici che controllano processi fisici, sono dotati non solo di un accesso diretto attraverso il corporate

network, ma anche di connessione internet (Sadeghi, Wachsmann & Waidner, 2015).

Da una parte, questo trend ha portato degli indubbi benefici che abbiamo potuto osservare nella nostra quotidianità in termini di miglioramenti generali della qualità della produzione e della sua efficienza ed economicità. Dall'altra, questo connubio ha implicato l'introduzione delle tradizionali vulnerabilità e minacce del settore IT nel dominio OT che, per le sue particolarità intrinseche, è un ambiente dove le misure di cyber-security risultano di difficile applicazione creando un problema di sicurezza non trascurabile (Nicholson & Al., 2012).

3. Sicurezza negli ambienti OT, il limite della disponibilità

Gli ambienti OT sono caratterizzati da peculiarità proprie che proiettano la necessità di proteggere questi apparati su un trade-off che vede l'opposizione di due elementi: la security e la safety. In primo luogo, gli ambienti ICS si caratterizzano per lo scambio di grandissime quantità di informazioni che vengono continuamente inviate e ricevute da una pletora complessa di fonti e soggetti, nel formato di pacchetti dalle piccole dimensioni dell'ordine di pochi byte.

Questo si lega all'altro aspetto essenziale degli ICS, ossia quello di dover rispondere a un vincolo di *hard real-time*. Infatti, gli impianti OT sono disegnati per interfacciarsi con "sistemi fisici" come reazioni chimiche, flussi di liquidi, processi di riscaldamento e raffreddamento, movimenti di oggetti etc. Gli impianti OT devono dunque operare ed adattarsi alle dinamiche e ai tempi richiesti dalla logica del processo supervisionato. Questo implica un alto livello di determinismo dove il meccanismo deve necessariamente passare attraverso una precisa sequenza di input, e in un intervallo di tempo ben determinato, per produrre l'output desiderato.

Ne consegue che l'applicazione di misure classiche di cyber-security quali cifratura, antivirus, firewalls e firma digitale, risulterebbe particolarmente problematica in quanto introdurrebbe controlli di routine che rischiano di compromettere il fluido funzionamento delle attività, generando un elevato overhead che, anche a causa della natura asincrona di tali processi, rischia di compromettere il normale ciclo di funzionamento introducendo pericolosi e inaccettabili ritardi dell'elaborazione del dato.

Infine, un altro fattore che limita l'introduzione di misure di sicurezza, è la difficoltà di operare azioni di manutenzione del sistema. Gli ICS infatti sono disegnati per operare a ciclo continuo

24x365, o almeno fino a quando il processo controllato è attivo. Ne consegue che gli interventi di aggiornamento, upgrade e patching, che richiedono un periodo di downtime dell'infrastruttura, devono essere pianificati con largo anticipo e non possono seguire pedissequamente le innovazioni in ambito di sicurezza (Cook & Al., 2017). Inoltre, tali attività sono considerate rischiose in quanto qualsiasi modifica del sistema, in un ambiente complesso e caratterizzato dal requisito di hard real-time, potrebbe creare effetti inaspettati. Gli interventi sul software dunque richiedono intense attività di testing, generalmente indicate come processo di convalida, il cui costo in termini monetari e di tempo è significativo oltre che, in molti casi, imposto e regolato da specifiche norme e procedure pensate in modo quasi esclusivo con un'ottica di salvaguardia dell'integrità e tracciabilità del processo e della safety dei lavoratori e degli utenti (McLaughlin & Al., 2016).

In altre parole, una volta istallati e certificati, gli ICS rimangono operativi per più di 20 anni con interventi di manutenzione sui sistemi controllo ridotti al minimo, il che implica in molti casi l'utilizzo di software obsoleti sui quali il processo di patching e aggiornamento non è effettuato in modo sempre tempestivo. Per esempio uno studio condotto alcuni anni fa da una società specializzata negli USA ha evidenziato che il tempo medio per l'applicazione di una patch di sicurezza era di 350 giorni con alcuni episodi nei quali l'istallazione era stata effettuata solo 3 anni dopo il rilascio della patch. Una diversa ricerca ha, addirittura evidenziato, che solo il 10% degli operatori installa patch e aggiornamenti mentre il restante lascia i propri sistemi suscettibili di essere attaccati (Bodenheim, 2014). Inoltre la maggior parte dell'apparecchiature presenti in ambito industriale a non è in grado di gestire misure di sicurezza sofisticate, infatti la maggior parte dei PLC (*Programmable Logic Controller*) istallati sono dimensionati rispetto al ciclo di funzionamento proprio del processo da controllare e non hanno capacità di calcolo per elaborare ulteriori informazioni (Higgins & Jan, 2013). Infine, nel 2011 Symantec ha pubblicato un report in cui evidenziava 129 vulnerabilità che interessano i prodotti ICS (Symantec, 2011), mentre solo un anno dopo ne sono state individuate 171, mostrando un trend di crescita di oltre il 40% in un sol anno e che difficilmente subirà delle inversioni in futuro.

4. Una crescente superficie di attacco

In questo contesto di vulnerabilità intrinseche, l'unica barriera che ha garantito per un lungo periodo di tempo un livello accettabile di protezione era costituita dalla così detta *security through obscurity*. Tale concetto fa della complessità dei sistemi OT un elemento di difesa volto a dissuadere un eventuale attaccante dall'agire. Infatti, per compromettere un ICS basato su protocolli propri e senza connettività esterna erano necessari non solo una conoscenza estensiva del software utilizzato, ma anche un punto di accesso fisico all'ambiente industriale. A questo andava aggiunta la necessità di conoscere il processo sotteso al fine di individuare qurgli elementi e quelle azioni atte a indurre rischio significativi al processo. Di conseguenza, le OT erano viste ragionevolmente immuni da attacchi esterni, e la minaccia principale era considerata quella interna (Byres & Lowe, 2004) proveniente da "addetti ai lavori" scontenti e mossi da motivi personali (Galloway & Hancke, 2013).

Non è un caso che fino al 2010 l'unico episodio di cui si ha notizia riguarda un attacco portato contro i sistemi di gestione delle acque nella cittadina di Maroochy Shire (una provincia australiana) che provocò la dispersione di 800.000 litri di liquami grezzi con significativi danni ambientali ed economici. In questo caso l'autore dell'attacco era uno degli sviluppatori del sistema che aveva poi cercato di mettere in piedi una estorsione (Slay & Miller, 2007).

È evidente che oggi, come diretta conseguenza della maggiore connettività e dell'utilizzo di soluzioni predefinite, la strategia di *security through obscurity* non è più ragionevole.

Da una parte, questi cambiamenti hanno dato la possibilità di sferrare attacchi da remoto, scavalcando quindi il vincolo della necessità di accesso fisico (Drias & Al., 2015), dall'altra hanno significativamente facilitato le attività di *reconnaissance*. La *reconnaissance* costituisce uno step propedeutico essenziale nella preparazione delle operazioni cyber (Assante & Lee, 2015) nel quale gli attaccanti raccolgono intelligence e informazioni riguardo al target prescelto al fine di identificarne le debolezze e i punti di rottura da sfruttare per compromettere il sistema e indurlo in una configurazione non-safe. Oggi, gli attori malintenzionati possono soddisfare in buona parte le loro esigenze di raccolta di informazioni e documentazione impiegando strumenti di intelligence open source (OSINT). La piattaforma Shodan, per esempio, è un motore di ricerca liberamente utilizzabile e dai costi limitati, in grado di tracciare tutte le porte di comunicazione connesse a Internet, incluse quelle dei dispositivi OT. Gli utenti possono facilmente individuare quale specifico ICS è utilizzato in

un impianto e, una volta identificato, posso mappare il sistema al fine di individuarne le vulnerabilità e i punti di ingresso sfruttabili (Bodenheim, Butts, Dunlap & Mullins, 2014; Bodenheim, 2014).

5. Evoluzione della minaccia

Gli sviluppi del mondo delle OT hanno portato anche a una trasformazione effettiva del panorama delle minacce cyber. Infatti, se tra il 1982 e il 2000 il 70% degli attacchi era di natura interna, tra il 2000 e il 2003 si è verificata una progressiva inversione del trend che ha portato l'ammontare delle azioni con origine esterna fino al 70% degli attacchi totali (Byres & Lowe, 2004; Iversen, 2004), ed è improbabile che questa tendenza diminuisca in futuro.

Questi dati, accompagnati da un aumento generale della frequenza degli attacchi informatici (Kaspersky lab ICS-CERT, 2017) hanno sollevato una grande preoccupazione per le minacce derivanti dal cyberspazio. Nel 2009, un sondaggio che coinvolgeva oltre 600 IT security manager di imprese operanti in settori critici ha evidenziato che la maggior parte degli intervistati riteneva probabile, se non imminente, un'operazione cyber di larga scala in grado di degradare le IC del paese (McAfee, 2009). Lo stesso anno, l'ex presidente americano Barack Obama, ha definito gli attacchi cibernetici "*una delle più gravi minacce alla sicurezza statale ed economica che le nostre nazioni stanno affrontando*" (Napolitano, 2009) e, secondo uno studio recente, le minacce informatiche detengono la quarta posizione dopo quelle legate al terrorismo, vandalismo e furto fisico (Moreno & Al., 2018).

L'aspetto più critico delle vulnerabilità degli ICS è che gli attacchi informatici potrebbero avere non solo un impatto economico, ma anche uno cinetico. Un aggressore può introdurre guasti e alterare il normale operato di un processo fino a portare il sistema a un punto di rottura meccanico. A questo timore è stato dato fondamento pratico nel 2007 con il progetto Aurora, condotto dall'Idhao National Lab, nel quale una squadra di hacker etici simulò un attacco informatico per distruggere un gruppo elettrogeno da 27 tonnellate (Cárdenas, Amin & Sastry, 2008). L'esperimento Aurora dimostrò che un attacco immateriale ipoteticamente sferrabile da migliaia di kilometri di distanza è in grado di creare danni meccanici potenzialmente paragonabili a quelli ottenibili da una carica esplosiva, con il vantaggio che la possibilità di attribuzione, ossia di risalire all'autore dell'attacco, sono ridotte o comunque non immediate.

Questo comporta che un attacco informatico contro le IC potrebbe creare danni all'ambiente, problemi alla salute delle

persone e gravi disagi per la società (ARIA, 2015). Questo anche perché occorre considerare che il ripristino e la riparazione delle componenti meccaniche dei sistemi OT possono richiedere tempi dilatati dell'ordine di mesi se non addirittura di anni.

Oggi, la necessità di difendere le OT da attacchi cyber è riconosciuta a livello italiano e mondiale. In Italia la relazione dei Servizi di Intelligence al Parlamento del 2016 avverte della possibilità che un'operazione cyber può danneggiare oggetti fisici e, come affermato nel 2012 dall'ex Segretario alla Difesa statunitense Leon E. Panetta, un'operazione di successo potrebbe portare a un "cyber-Pearl Harbor" se un gruppo di aggressori acquisisse il controllo degli "interruttori critici" (Bumiller & Shanker, 2012).

6. I principali attacchi

Il Progetto Aurora era solo una simulazione e fu ampliamente considerato con scetticismo in quanto gli hacker avevano una conoscenza estensiva dell'impianto che gli ha concesso di eseguire una manipolazione mirata del processo, mentre, in uno scenario realistico, si riteneva improbabile che un avversario disponesse di informazioni tanto precise e dettagliate.

Tuttavia, l'apparizione del worm Stuxnet nel 2010, ha cambiato radicalmente non solo lo scenario, ma anche la percezione della minaccia cyber (Langner, 2011; 2013). Questo worm era specificatamente progettato per attaccare i PLC Siemens in uso in uno stabilimento nucleare nel Natanz, una regione dell'Iran. Nello specifico, Stuxnet era programmato per alterare la velocità di rotazione di alcuni motori facendoli girare in modo anomalo (Albright, Brannan, Walrond, 2011, Langner, 2011; 2013). L'attacco provocò la deteriorazione di circa 1,000 turbine che di conseguenza rallentò significativamente il programma nucleare iraniano (Lindsay, 2013).

Stuxnet non è stato un caso isolato, ma ha segnato il punto di inizio di una serie di operazione cyber volte a compromettere la sicurezza fisica dei processi industriali fra i quali è importante ricordare: Irongate (2014), Black Energy 3 (2015), Crashoverride (2016) e Trisis/Triton (2017).

L'attacco Irongate del 2014 prese di mira un'acciaieria tedesca. I malintenzionati ottennero l'accesso alla rete degli impianti e, impedendo il corretto spegnimento di una fornace, furono in grado di causare "danni fisici enormi" a vari componenti critici del sistema, comportando la sospensione della produzione e costi significativi per ripristinare l'operabilità (Lee & Al., 2014).

In Ucraina invece, due attacchi informatici importanti hanno preso di mira il settore energetico. BlackEnergy 3 è il primo attacco cyber conosciuto che è stato in grado di interferire con le operazioni di un operatore elettrico provocando un blackout il 23 dicembre del 2015 che è durato per 6 ore tenendo al buio circa 225,000 utenti nella regione. Il malware, dopo aver imparato il corretto funzionamento del sistema sfruttando le informazioni visualizzate tramite la HMI (*Human Machine Interface*), è stato capace di inviare comandi "leciti" con l'obiettivo di disconnettere alcune sottostazioni dalla rete elettrica e successivamente rendere non operativo l'apparato di telecontrollo cancellando alcuni file di sistema (Lee, 2017a; E-ISAC, 2016). A distanza di un anno, nel dicembre 2016, un secondo blackout ha colpito l'Ucraina, e in questo caso il gestore elettrico ha esplicitamente dichiarato che la causa è da ricercare in interferenze illecite nella rete di controllo industriale derivanti dall'esterno, ovvero in un attacco cyber condotto tramite il malware CrashOverride. Attraverso il malware, anche conosciuto come Industroyer, gli attaccanti hanno potuto prendere il controllo degli interruttori di alcune sottostazioni, che sono poi stati aperti provocando una perdita di energia di circa un'ora in vari sobborghi di Kiev (Lee, 2017a ESET, 2017).

Una peculiarità interessante di questi due attacchi è che i malware hanno funto da mero vettore per accedere e prendere controllo dei dispositivi di gestione delle operazioni, e soltanto la malevola interazione degli attaccanti con il sistema ha provocato i due blackout (Conway & Al., 2016; Lee, 2017a; Cherepanov, 2017). Questo indica che il focus principale dell'operazione non è tanto nella payload dei due malware, ma piuttosto nella conoscenza degli attaccanti e nella loro capacità di sfruttare il processo per portarlo in una condizione di malfunzionamento. Il che implica che questo tipo di attacchi non sono limitati a un particolare vendor o impianto ma possono essere riproposti altrove (Lee, 2017a). Per esempio, il CERT USA ha evidenziato che malware come BlackEnergy 3 e Crashoverride sono stati rinvenuti in diversi sistemi di controllo di utility americane (Larson, 2018) e che in alcuni casi sono rimasti latenti nei sistemi anche per più di cinque anni (Setola & Al., 2019).

Infine, l'ultimo attacco OT in ordine cronologico è il malware scoperto nel dicembre 2017 in un impianto petrolchimico in Medio Oriente, e conosciuto con il nome di Trisis o Triton. La particolarità di questo malware è che il suo target sono i sistemi SIS (Safety Instrumental System) ovvero quella porzione dei sistemi ICS, generalmente separata dai normali sistemi di gestione di processo, che sono utilizzati per prevenire eventi catastrofici (Lee, 2017b; Johnson & Al., 2017). I SIS supervisionano le

operazioni critiche assicurando che il processo industriale mantenga un livello minimo di sicurezza. Se la soglia necessaria non viene soddisfatta, i controllori SIS entrano in modalità *safe-failed* interrompendo le operazioni produttive (Higgins, 2018). In questo caso, gli aggressori sono riusciti a penetrare il dispositivo SIS e nel tentativo di riprogrammare il controller hanno involontariamente attivato lo stato di errore provocando l'arresto del processo industriale.

Prendere di mira i SIS è strategicamente rilevante in relazione a due scenari plausibili. Una prima strategia, classificabile come fake attack, consiste nel riprogrammare il SIS affinché il sistema rilevi dei falsi positivi. In altre parole, parametri o situazioni del tutto normali vengono segnalate come anomale e potenzialmente pericolose inducendo il sistema ad adottare misure di recovery, se non addirittura lo shutdown del processo. Una seconda tipologia di attacco, decisamente più critica e perniciosa, implica la riprogrammazione dei dispositivi SIS affinché il sistema non sia più in grado di rilevare situazioni di emergenza, e dunque di intraprendere le necessarie azioni di "protezione" per riportare i processi in configurazione di sicurezza. In tale scenario il processo produttivo perde la capacità di prevenire l'insorgenza di situazioni pericolose per cui un ulteriore evento anomalo, sia esso accidentale o indotto dall'attaccante, può degenerare in un incidente con impatti significativi in termini di danni fisici e ambientali (Johnson & Al., 2017; Assante, 2018).

L'impatto di questi attacchi, pur rimanendo limitato e ben al di sotto della soglia di un "cyber-Pearl Harbour", ha dimostrato che operazioni cibernetiche con conseguenze cinetiche non sono più una mera speculazione teorica o l'oggetto di esperimenti militare ma, al contrario, gli strumenti offensivi di questo genere sono diventati "possibili, accessibili, incisivi e capaci di interrompere il corretto funzionamento delle società sviluppate" (Tabansky, 2011). Non è un caso che anche il Global Risks Report del 2019 enfatizza il rischio cyber come una minaccia con un impatto potenziale non lontano da quello di calamità e disastri naturali maggiori (figura 1) (WEF, 2019). È tuttavia da considerare che gli attacchi informatici, a differenza delle catastrofi ambientali, sono minacce artificiali di cui la mano umana è la prima responsabile e, in quanto tali, sono più facilmente difendibili e mitigabili.

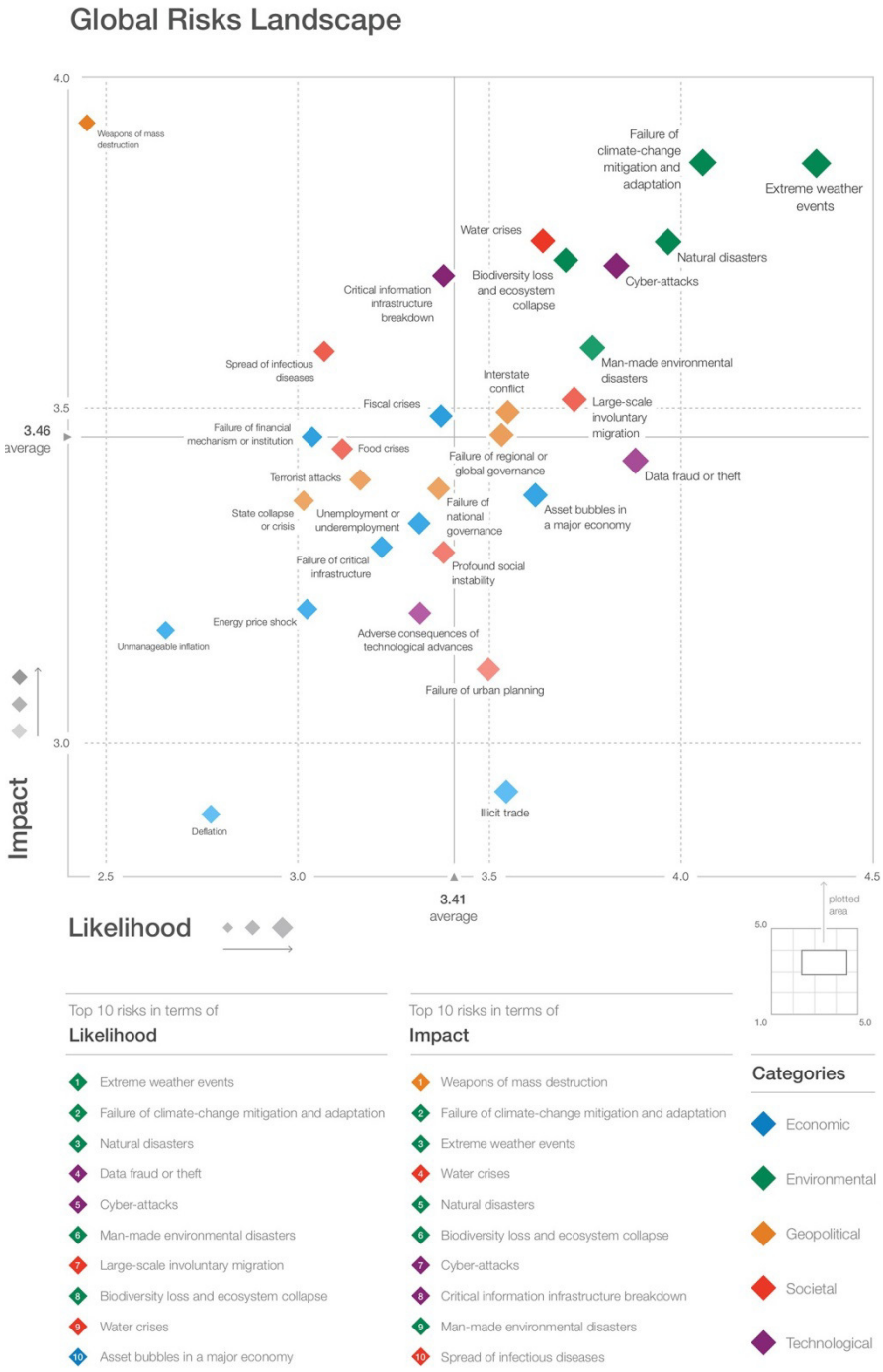

Figura 1 Thrath Landscape, Global Risk Report 2019

7. Aspetti difensivi degli ICS

Sebbene la loro intrinseca vulnerabilità e l'alta esposizione alla minaccia cyber, gli attacchi contro le OT sono risultati limitati sia in termini di frequenza (ad oggi se ne possono annoverare solo cinque che hanno avuto conseguenze fisiche), sia in termini di

impatto, e questo suggerisce che gli aggressori non hanno ancora sviluppato la capacità o l'intenzione di infliggere danni significativi.

In primo luogo, bisogna considerare che a partire dalla scoperta di Stuxnet sono state proposte varie misure difensive per proteggere gli ICS. Una delle strategie migliori è il così detto approccio a "cipolla" o *defence in depth*. Questo metodo è organizzato sulla base di una gerarchia di rilevanza delle minacce nei vari sistemi e mira a creare filtri e barriere che ostacolino l'attaccante nel tentativo di accedere ai settori critici del processo, ossia quei livelli del sistema che garantiscono la safety dell'intero ambiente. La *defence in depth*, introdotta con lo standard ANIS/ISA 99 (Byres & Al., 2012) e ripresa in modo più dettagliato dall'ICS Cyber Emergency Response Team statunitense (DHS, 2016), prevede di segmentare la rete ICS in zone, dove sono raggruppati gli asset logici e fisici che presentano requisiti di sicurezza comuni in termini di criticità e conseguenze in caso di un eventuale manomissione. Tutte le unità che compongono un settore sono considerate trust e possono dunque scambiare dati e informazioni senza restrizioni. Al contrario, il dialogo tra entità afferenti a zone diverse deve essere concentrato in un numero limitato di snodi, generalmente chiamati *conduits*, e in corrispondenza di ognuno di essi è bene che vengano inseriti sistemi di monitoraggio, come firewall o dispositivi analoghi, per verificare la correttezza e regolarità dei flussi. Inoltre, in un'architettura a cipolla si tende a raggruppare gli asset più critici nei settori più interni del sistema. In tale contesto, una misura che aumenterebbe notevolmente la sicurezza dell'intero sistema potrebbe essere quella di adottare soluzioni di comunicazioni data diode, ossia basate su device che consentono un flusso dell'informazione esclusivamente unidirezionalmente dall'interno (campo) verso l'esterno (rete aziendale). Tuttavia, limitare il flusso informativo risulta particolarmente problematico in quanto occorre sia ricevere informazioni dal campo sia definire set-point, strategie e attività di manutenzione. Questo impone la presenza di sistemi di by-pass del data diode con conseguente limitazione dell'efficienza di quest'ultimi rendendone l'adozione poco utile in tutti quei casi in cui le attività di controllo sono in volume paragonabili al flusso di monitoraggio.

Al di là delle misure difensive poste in essere, le operazioni cibernetiche sono *scale sensitive* e la difficolta di preparare e sferrare un attacco con successo aumenta in parallelo con la complessità del sistema preso di mira. I sistemi industriali sono tra i target più complessi e quindi tra i più ardui da compromettere. La grande difficoltà risiede nel fatto che un malintenzionato, per portare un processo al punto di rottura, deve essere in grado non

solo di comprendere e padroneggiare il linguaggio dell'ICS per mandare comandi legittimi, ma deve anche sapere quali comandi mandare, a quali componenti del sistema e quali reazioni fisiche provocare per mandare il processo in una configurazione erronea (Setola & Al., 2019). In altre parole, un attaccante deve combinare skills di diversa natura che comprendono non solo articolate abilità informatiche ma anche avanzate conoscenze ingegneristiche del processo che si vuole compromettere.

Oggi, gli attori che raggiungono questo livello di sofisticazione vengono definiti come *Advanced Persisten Threath* (APT) (NIST, 2011), ossia un team di avversari determinati e dotati di risorse consistenti (basti pensare che lo sviluppo di Stuxnet è costato oltre venti milioni di dollari) che trascendono il regno digitale comprendendo anche aspetti istituzionali ed organizzativi quali la capacità di acquisire conoscenze di intelligence precise e dettagliate, e la possibilità di mobilitare capitale umano di prima qualità (Rid & Mc Burney, 2012; Lindsay, 2013; Liff, 2012).

È evidente che la soglia di risorse necessarie per poter prendere di mira gli ambienti ICS è ben al di fuori della portata degli attori più deboli e, al contrario, rimane una prerogativa di attori di altissimo profilo probabilmente sponsorizzati e supportati da entità statali che usano le APT come *proxies* nel cyberspace (Maurer, 2018). Da una parte, questo aspetto taglia fuori gli attori più comuni, come i criminali o gli attivisti (Craig & Valeriano, 2018). Dall'altra suggerisce che le operazioni offensive contro gli OT sono volontariamente circoscritte nel loro impatto e sono progettate più per raggiungere vantaggi geopolitici, economici o militari, che per infliggere danni "economici" o reputazionali alla vittima.

8. Conclusioni

Negli ultimi anni si è assistito a una crescita non solo della frequenza, ma anche della qualità degli attacchi cyber contro gli ICS. Da una parte, questo è dovuto a un aumento sostanziale della vulnerabilità esposte da questi sistemi, che per ragioni di efficienza hanno integrato in modo sempre più massiccio strumenti e prodotti propri del mondo IT. Dall'altra, si è registrato un generale aumento e diffusione delle capacità offensive cyber che ha portato al verificarsi di almeno cinque attacchi informatici (Stuxnet, Irongate, BlackEnergy3, Crashoverride, Trisis) con conseguenze cinetiche.

L'impatto di questi attacchi è risultato limitato e distante dalle previsioni catastrofiche di un "Cyber Pearl-Harbour". Inoltre, le OT costituiscono i target più complessi e comprometterli richiedere il

lavoro delle APT, ossia team altamente sofisticati che dispongono di risorse tecnico organizzative al di fuori della portata degli hacker più comuni. Come riconosciuto dal summit NATO del 2016, che elegge il cyberspace come quinto dominio delle operazioni (NATO, 2019), si pensa che le APT vengano sponsorizzate da entità statali che se ne servono per avanzare i propri interessi geopolitici.

Tuttavia, è da notare come le capacità offensive cyber si stiano sviluppando più velocemente delle contromisure per arginarne la minaccia (WEF, 2018), è dunque urgente e necessario che gli operatori delle IC, in sinergia con i soggetti pubblici deputati, si preparino per ridurre le vulnerabilità delle OT e per proteggersi rispetto a questa classe di attacchi.

Bibliografia

[1] Albright, D., Brannan, P., & Walrond, C. (2011). Stuxnet malware and natanz: Update of isis december 22, 2010 report. *Institute for Science and International Security*, *15*, 739883-3

[2] ARIA - Analysis, Research and Information on Accidents database (2015). Ministry of Environment / General Directorate for Risk Prevention, the BARPI (Bureau forAnalysis of Industrial Risks and Pollutions). At: https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en

[3] Assante, M. (2018). Triton/TriSIS – In Search of its Twin. *SANS Industrial Control Systems*. 29 January. Available at: https://ics.sans.org/blog/2018/01/29/tritontrisis-in-search-of-its-twin

[4] Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, *1*

[5] Bodenheim, R. C. (2014). *Impact of the Shodan computer search engine on internet-facing industrial control system devices* (No. AFIT-ENG-14-M-14). AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT

[6] Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*, *7*(2), 114-123

[7] Brunner, E.M. & Suter, M. (2009). International CIIP Handbook 2008/2009, *CRN handbooks,* 4(1)

[8] Bumiller, E. and Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S, *The New York Times*, 11 October 2012 available at: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

[9] Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218)

[10] Byres, E., Eng, P., & Fellow, I. S. A. (2012). Using ANSI/ISA-99 standards to improve control system security. *White paper, Tofino Security*

[11] Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. In *HotSec*

[12] Cherepanov, A. (2017). WIN32/INDUSTROYER, A new threat for industrial control systems. *White paper, ESET (June 2017)*

[13] Conway, T., Lee, R. M., & Assante, M. J. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electricity Information Sharing and Analysis Center*. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[14] Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. *Computers & Security*, *70*, 467-481

[15] Craig, A. J., & Valeriano, B. (2018) Realism and Cyber Conflict: Security in the Digital Age. *Realism in Practice*, 85

[16] DHS (2016). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. *Industrial Control Systems Cyber Emergency Response Team*. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [20/05/2019]

[17] Drias, Z., Serhrouchni, A., & Vogel, O. (2015). Analysis of cyber security for industrial control systems. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on* (pp. 1-8). IEEE

[18] E-ISAC (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.

[19] ESET, (2017). ESET discovers dangerous malware designed to disrupt industrial control systems. *ESET – Enjoy Safer Technology*. 12 June, Available at: https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-dangerous-malware-designed-to-disrupt-industrial-control-systems/

[20] European Commission (2005). Green Paper on a European programme for critical infrastructure protection, Com. 576 final. Available at: https://eur-lex.europa.eu/legal-content/EN-FR/TXT/?uri=CELEX:52005DC0576&from=BG

[21] Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, *15*(2), 860-880.

[22] Higgins, K. J., & Jan, D. (2013). The SCADA patch problem. *Information Week*. Available at: https://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979

[23] Higgins, K.J. (2018). FireEye Finds New Clue in TRITON/TRISIS Attack. Dark Reading, 6 August. Available at: https://www.darkreading.com/operations/fireeye-finds-new-clues-in-triton-trisis-attack/d/d-id/1332008

[24] Iversen, W. (2004). Hackers Step Up SCADA Attacks. AutomationWorld. 12 october. Available: https://www.automationworld.com/article/technologies/networking-connectivity/switches-gateways-routers-modems/hackers-step-scada

[25] Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., Glyer, C., (2017). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. FireEye. 14 December. Available at: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[26] Kaspersky lab ICS-CERT, (2017). Threat Landscape for Industrial Automation Systems In The Second Half Of 2016, Kaspersky Lab. Available: https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

[27] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49-51.

[28] Langner, R. (2013). To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve. *The Langner Group*

[29] Larson, S. (2018). Threats to Electric Grid are Real; Widespread Blackouts are Not. Dragos, 6 August. Available at: https://dragos.com/blog/20180806ElectricGridThreats.html

[30] Lee, R. (2017 a). CRASHOVERRIDE: Analysis of the threat to electric grid operations. *Dragos Inc., March*

[31] Lee, R. (2017 b). TRISIS Malware: Analysis of Safety System Targeted Malware. Dragos Inc. available at: https://dragos.com/blog/trisis/

[32] Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber-attack. *Industrial Control Systems*, *30*, 62

[33] Liff, A. P. (2012). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401-428

[34] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404

[35] Maurer, T. (2018). *Cyber Mercenaries*. Cambridge University Press

[36] McAfee, (2009). In the Crossfire: Critical Infrastructure in the Age of Cyber War. McAfee report. Available at: https://img.en25.com/Web/McAfee/CIP_report_final_uk_fnl_lores.pdf

[37] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039-1057

[38] Moreno, V. C., Reniers, G., Salzano, E., & Cozzani, V. (2018). Analysis of physical and cyber security-related events in the chemical and process industry. *Process Safety and Environmental Protection*, *116*, 621-631

[39] Napolitano, J. (2009) A New Challenge for Our Age: Securing America Against the Threat of Cyber Attack. Department of Homeland security. 20 October. Available: https://www.dhs.gov/news/2009/10/20/secretary%E2%80%99s-web-address-cybersecurity

[40] NATO (2019). NATO's role in cyberspace. *NATO Review Magazine*, 2019. Available: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

[41] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418-436

[42] NIST (2011). *Managing Information Security Risk: Organization, Mission, and Information System View* (No. Special Publication (NIST SP)-800-39)

[43] Rid, T., & McBurney, P. (2012). Cyber-weapons. *the RUSI Journal*, *157*(1), 6-13

[44] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE* (pp. 1-6). IEEE

[45] Setola, R. (2011), *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*, Centro Militare di Studi Strategici CEMISS, At: http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/Lastrategiaglobalediprotezione.aspx

[46] Setola R., Faramondi L., Salzano E., & Cozzani, V.(2019). An overview of Cyber Attack to Industrial Control System. *Chemical Engineering Transactions vol.75,2019*

[47] Slay, J., & Miller, M. (2007, March). Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection* (pp. 73-82). Springer, Boston, MA

[48] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security, NIST special publication 800-82, *National Institute of Standards and Technology*

[49] Symantec (2011). Symantec. "SCADA (Supervisory Control and Data Acquisition) security threat landscape". Available at: https://www.symantec.com/security-center/threat-report

[50] Tabansky, L. (2011). Critical Infrastructure Protection against cyber threats. *Military and Strategic Affairs*, *3*(2) 61-68

[51] World Economic Forum (2018), The Global Risks Report 2018, https://www.weforum.org/reports/the-global-risks-report-2018

[52] World Economic Forum (2019). Global Risks Report 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf