Università degli Studi di Salerno

DIPARTIMENTO DI SCIENZE AZIENDALI - MANAGEMENT & INNOVATION SYSTEMS - DISA-MIS

DOTTORATO DI RICERCA IN
MANAGEMENT & INFORMATION TECHNOLOGY
XV° ciclo (XXIX° nazionale)

TESI di DOTTORATO in

CYBER SECURITY RISK MANAGEMENT NEI SERVIZI PUBBLICI STRATEGICI

Coordinatore
Chiar. mo Prof.
Andrea DE LUCIA

Tutor
Chiar. mo Prof.
Roberto PARENTE

Candidato
Valter RASSEGA
Matr. 8887600012

A.A. 2016/2017

Indice

INTRODUZIONE

L'arena digitale, con la sua capacità di stabilire contatti diretti e in tempo reale tra persone in ogni parte del pianeta, rappresenta uno strumento formidabile per sviluppare relazioni e realizzare scambi di informazioni e di conoscenza, oltre che di beni e di servizi. Le potenti tecnologie elettroniche ed informatiche hanno determinato una vera e propria rivoluzione cibernetica, con la connessione in rete della quasi totalità della superficie del pianeta, e il controllo diretto di una miriade di dispositivi fisici tra i più vari, dagli Smartphone ai dispositivi indossabili, dai sistemi di controllo del traffico cittadino alle infrastrutture di produzione e distribuzione di energia elettrica. E' la c.d. "Internet of Things" o Internet delle cose, in cui anche i dispositivi elettronici acquisiscono intelligenza, comunicano dati e contribuiscono a tracciare una mappa a livello virtuale di ciò che accade nel mondo reale.

Questa pervasività non ha risparmiato il settore pubblico che deve garantire le regole di convivenza civile, affermando la propria sovranità, anche nel cyberspace e che, pertanto, è chiamato a fornire risposte su numerosi fronti, non ultimo quello normativo, garantendo, per quanto possibile, il rispetto delle regole presenti nel mondo reale, anche nello spazio cibernetico. Più specificatamente, il settore pubblico deve farsi carico di garantire la sicurezza fisica e informatica delle c.d. infrastrutture critiche nazionali, che includono tutti quei servizi essenziali per la sicurezza nazionale, il buon funzionamento del Paese e la sua crescita economica e, non ultimo, il benessere della popolazione, quali il sistema elettrico ed energetico, le reti di comunicazione in genere, le reti e le infrastrutture di trasporto di persone e merci (navale, ferroviario, aereo e stradale), il sistema sanitario pubblico, i circuiti economici e finanziari, le reti del Governo nazionale, delle Regioni, quelle per la gestione delle emergenze e della Protezione Civile. Sono proprio le Infrastrutture Critiche, indispensabili ad una Nazione per mantenere il suo modo di vivere, ma vulnerabili a causa della loro necessaria interconnessione, interdipendenza e gestione informatizzata, a risultare gli obiettivi sensibili dei cyber conflitti dei nostri tempi, in cui il controllo dello spazio cibernetico, determina il predominio di una Potenza sulle altre.

La sfida è complessa e la Pubblica Amministrazione da sola non sembra in grado di poter rispondere in modo efficace agli attacchi informatici sempre più sofisticati che, quotidianamente, colpiscono il mondo civile, industriale ed economico. Su questo tema, i Governi occidentali hanno da tempo avviato una stretta collaborazione con il settore privato, ed è emersa la necessità di definire una strategia e un modus operandi condiviso e di qualità tra i vari attori coinvolti.

Questo lavoro si propone di affrontare in maniera sistematica il tema "caldo" del Cyber Security Risk Management, un ambito che coinvolge l'erogazione di servizi pubblici, il sistema economico e il mondo delle imprese nel suo complesso e, via via e a vario titolo e grado di interesse, ogni singolo cittadino del mondo.

In questo scenario inedito, fortemente connotato da incertezza e variabilità delle minacce, l'applicazione sic et simpliciter delle tecniche "tradizionali" di valutazione del rischio di derivazione aziendale risulta inadeguata allo scopo, nonostante un certo grado di adattamento al nuovo scenario sia già in corso.

L'analisi si concentra sulla parte relativa all''evoluzione adattativa' che sta interessando il risk management nel campo della cyber security e dello stato dell'arte nel panorama accademico e scientifico mondiale nell'introduzione di nuovi e più evoluti strumenti per l'analisi del Cyber Risk.

Il lavoro si conclude con un caso di studio effettuato su di una grande azienda italiana che fornisce un servizio pubblico strategico quale l'energia elettrica.

L'UNIVERSO CYBER

Dalla Cibernetica di Wiener alla società dell'informazione

A partire dal secondo dopoguerra, grazie al notevole sviluppo delle conoscenze, soprattutto in ambito elettronico, informatico e telematico, il nostro mondo si è caratterizzato per una forte spinta all'innovazione tecnologica. La c.d. terza rivoluzione industriale, con il passaggio dall'analogico al digitale, ha permesso nuove modalità di comunicazione e di trasmissione e la creazione del mercato globale dell'informazione. L'epoca che stiamo vivendo – in cui tutti possediamo orologi, bracciali, termostati, telefoni e svariati altri oggetti connessi alla Rete per ottenere una serie di servizi e contenuti ulteriori - era stata profetizzata nei racconti fantascientifici di Gibson, agli inizi degli anni ottanta, quando lo stesso neologismo "cyberspace", coniato dallo scrittore canadese, coincideva, nel romanzo del 1984, *Neuromancer*, con una definizione futuristica e, a quel tempo, improbabile di *"...un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano..."*. Lo spazio cyber è descritto dallo scrittore canadese come un territorio anarchico che non può non preoccupare chi si occupa di cybercrime, cyberwar e netwar, dove gli hackers sono una sorta di cow-boys della consolle, le lobbies economico-finanziarie travalicano i confini geografici degli Stati e determinano il destino del mondo, e i computer e la cibernetica permettono di creare universi paralleli rispetto al nostro e altrettanto reali.

I racconti fantascientifici di quegli anni si sono rivelati profetici e hanno saputo interpretare l'indagine scientifica precedente, prevedendo gli scenari che si sarebbero manifestati in seguito. Già nel 1948, il matematico americano Norbert Wiener aveva usato, per la prima volta, il termine "cibernetica" (Wiener, 1948; Wiener, 1968 trad.), per indicare un ramo di indagine interdisciplinare, dalle scienze umane, all'ingegneria, passando per la biologia e l'economia, finalizzato allo studio unitario di sistemi, viventi e non-viventi, attraverso l'utilizzo degli strumenti del calcolo matematico. La definizione

primigenia di cibernetica considerava, dunque, lo studio dei processi riguardanti "la comunicazione e il controllo nell'animale e nella macchina". Wiener aveva derivato il termine dal greco antico *kybernetes* (κυβερνήτης indica il pilota di una nave), intendendo focalizzare l'attenzione sulla guida e sul controllo di uno o più insiemi di elementi in interazione, potendo, quest'ultima, riferirsi a scambi di materia, di energia o di informazioni, in comunicazione tra di loro e, pertanto, capaci di retroazioni, feedback, e informazioni in generale.

Il libro di Wiener, sebbene zeppo di formule e di concetti complessi come quello di entropia e di retroazione, ottenne un successo inaspettato, pur non essendo stato concepito per il grande pubblico, presumibilmente perché quegli studi sulla trasmissione e il controllo dei processi erano già percepiti da molti come un'interessante prospettiva precorritrice della contemporaneità e di discipline che sarebbero nate negli anni a venire, come l'intelligenza artificiale, la robotica e le neuroscienze.

Il padre della cibernetica, oltre ad aver influenzato letteratura e filmografia di fantascienza, ha determinato un nuovo approccio nel modo di rapportarsi alle macchine, proseguito fino ai giorni nostri, in cui tablet, smartphone e computer portatili, dispositivi indossabili, hanno trasformato la nostra quotidianità, modificando il nostro stesso modo di essere *homo sapiens*, amplificando sensazioni e percezioni, cambiando il rapporto tra individui, oltre che i rapporti Stato-cittadino, il mondo del lavoro e dell'economia. Dunque, un nuovo modello di società, in cui l'informazione svolge un ruolo strategico di fattore di sviluppo sociale ed economico, oltre che di crescita e di ricchezza culturale, condizionante l'efficienza dei sistemi e lo stesso sviluppo delle attività umane: la società dell'informazione che, con i suoi nuovi significati economici, sociali, politici e culturali, possa ulteriormente evolversi verso una società della conoscenza.

L'internet degli oggetti nella rivoluzione digitale

Dopo l'affermazione del World Wide Web negli anni novanta e del Mobile Internet dello scorso decennio, stiamo ora vivendo quella che viene generalmente considerata la terza fase della rivoluzione Internet, la c.d. "Internet of Things" (IoT), espressione usata inizialmente nei Laboratori del MIT di Boston, per riferirsi alla trasformazione delle tecnologie e dei dispositivi di identificazione elettronica che, partendo dal codice a barre,

si stavano all'epoca evolvendo nel mondo wireless con i c.d. Radio Frequency Identification devices (RFID), e in seguito ripresa in diversi articoli e simposi che ne prospettavano l'ampliamento della prospettiva e le applicazioni pratiche.

La svolta nella perimetrazione del concetto di IoT arrivò con una pubblicazione sull'argomento da parte della Strategy and Policy Unit dell'ITU (International Telecommunications Union), in particolare in una frase di Lara Srivastava: "*It's safe to say that technology today is more pervasive than we would ever have imagined possible 10 years ago. Similarly, 10 years from now things will continue in this general direction. That's what these new technologies are telling us*."

Un'ulteriore definizione, più precisa e declinata negli aspetti funzionali, è presente nel lavoro di H. Sundmaeker (Sundmaeker et al., 2010) secondo cui: "*The internet of Things links the objects of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time. These things should be able to exchange information and provide services through different means and from different places*".

Nel contesto dell'IoT una "cosa" o meglio, "un oggetto", si può descrivere come un elemento reale o fisico, digitale o virtuale, che esiste e si muove nello spazio e nel tempo ed è in grado di essere univocamente identificato all'interno della rete mondiale, dotato di capacità computazionale propria, oltre che, spesso, specializzato per svolgere precise funzioni secondo logiche predefinite. L'Internet degli oggetti collega il mondo reale con il mondo virtuale, consentendo in tal modo, sempre e ovunque sia disponibile una connessione, di interagire con chiunque e con qualunque sistema informatico. E' un mondo dove oggetti fisici e persone, nonché dati virtuali e ambienti, interagiscono tra loro nello spazio e nel tempo. Questi oggetti sono in grado di acquisire e scambiare informazioni attraverso mezzi eterogenei e da differenti luoghi geografici, generando complessivamente una grandissima quantità di dati, una vera e propria "data explosion".

I Big Data, ad esempio, trovano nell'IoT la più rilevante fonte di informazioni, dati preziosi che, per caratteristiche e quantità, consentono alle applicazioni di Data Mining e e Data Analitics di estrarre significati da grandi moli di informazioni aggregate. Temi applicativi e di ricerca relativi all'Intelligenza Artificiale, e aperti già da diversi decenni,

trovano dunque nuova linfa attraverso l'utilizzo di metodi come il Machine Learning e il più recente Deep Learning, proiettando, secondo gli Executive Senior intervistati nella rivista *Forbes*[1], il campo d'indagine sull'Intelligenza Artificiale, tra i temi più "caldi" del 2017, unitamente all'Internet of Things e alla Cyber-security. Quest'ultima, in particolare, nell'attuale società dell'informazione, globalmente interconnessa e che scambia dati in tempo reale, deve proteggere da vecchie e nuove insidie che minacciano la privacy e la difesa dei sistemi infrastrutturali e produttivi nazionali. La Cyber security, dunque, ha assunto un ruolo strategico ed è al vertice delle priorità politiche, sociali ed economiche contemporanee.

I Sistemi Cyber-Fisici

L'espressione "Cyber-physical systems" è generalmente attribuita a Radhakisan Baheti e Helen Gill per individuare una nuova generazione di sistemi che integrano capacità fisiche e computazionali e che possono interagire con gli esseri umani attraverso nuove e numerose modalità (Baheti and Gill in Samad and Annaswamy, 2011). Si definisce, pertanto, come sistema cyber-fisico, una struttura, o parte di essa, costituita da una componente hardware, tipicamente specializzata, e una componente software che definisce e controlla la funzione operativa del dispositivo (Lee and Seshia, 2017). I Sistemi Cyber-fisici, o CPS, sono sistemi intelligenti la cui abilità di interazione continua con il mondo fisico attraverso la capacità computazionale, la comunicazione e il controllo, ne espande notevolmente le potenzialità, configurandoli come un potente fattore abilitante per tutti i futuri sviluppi della tecnologia. I CPS hanno modificato radicalmente le modalità di interazione tra il mondo fisico e la sfera umana, in modo analogo a quelle in cui l'avvento di Internet ha trasformato il procedimento con cui gli individui interagiscono con l'informazione.

---

[1] "2017 Predictions for AI, Big Data, IoT, Cybersecurity, And Jobs from Senior Tech Executives", Forbes, 12 dicembre 2016. http://www.forbes.com/sites/gilpress/2016/12/12/2017-predictions-for-ai-big-data-iot-cybersecurity-and-jobs-from-senior-tech-executives/#2a7ee6ab62e9

La locuzione di sistema cyber-fisico si inserisce nel più diffuso lessico di Internet of Things, Industria 4.0, Machine Learning, Machine-to-Machine (M2M), Smart Grid, Smart Cities: terminologie che descrivono ambiti specifici di applicazione che hanno la caratteristica comune di connettere fisicamente e funzionalmente il mondo fisico reale con il mondo dematerializzato dell'informatica e del controllo di processo. I sistemi Cyber-fisici sono quindi una combinazione di capacità di calcolo e processi fisici; computer e reti embedded controllano processi fisici, solitamente con una struttura ad anello chiuso o di feedback, coerentemente con la logica cibernetica, in cui i processi fisici influenzano l'esito di elaborazioni e viceversa, in una logica bi-direzionale.

Dal punto di vista architetturale, un sistema di tipo Cyber-Fisico è un sistema in cui si integrano strettamente componenti elaborative ed elementi fisici. Esso rappresenta l'evoluzione ultima dei c.d. sistemi embedded, sistemi costituiti da una combinazione di hardware e software progettati per realizzare una funzione specifica, con cui condividono ancora buona parte dell'architettura hardware e software (Lee and Seshia, 2011).

A differenza dei classici sistemi embedded, già caratterizzati da una componente elaborativa che prevale sulla specializzazione dell'interfaccia fisica, i CPS si collocano ad un livello di astrazione più elevato e sono, tra l'altro, caratterizzati da una notevole capacità di interfacciamento tra la componente computazionale e il mondo fisico esterno, unitamente a grandi capacità di comunicazione con la rete globale.

La caratteristica distintiva di questi sistemi rispetto al variegato mondo informatico, e la prospettiva cui vanno osservati, è riassunta efficacemente da Rajkumar, Lee, Sha e Stankovic: "*As an intellectual challenge, CPS is about the intersection, not the union, of the physical and the cyber. It is not sufficient to separately understand the physical components and the computational components. We must instead understand their interaction*" (Rajkumar et al., 2010). Edward A. Lee [Lee, 2008] nel 2008 ha proposto una riflessione, in chiave informatica, sui Cyber-Physical Systems, comparando i CPS con i sistemi informativi tradizionali. Lee ha evidenziato che i CPS richiedono requisiti di affidabilità e sicurezza qualitativamente molto differenti da quelli generalmente garantiti da un sistema informatico di tipo "general purpose"; inoltre, i CPS sono, anche intuitivamente, molto diversi dalle componenti software object-oriented e dai linguaggi di programmazione attualmente utilizzati, che sono in grado di interfacciarsi con il livello

hardware sottostante ma non sono adeguati a garantire una sufficiente affidabilità e la sicurezza richiesta da un sistema cyber-fisico. I modelli standard, utilizzati per lo sviluppo del software object-oriented, non appaiono adeguati a raggiungere i requisiti di affidabilità e di sicurezza necessari all'interazione del sistema informatico con il mondo esterno, pertanto, secondo Lee, non sarà sufficiente migliorare la progettazione, i processi, e aumentare il livello di astrazione, o verificare progetti o architetture software basate sulle astrazioni attuali, ma per realizzare il pieno potenziale del CPS è necessario ripensare al modello architetturale dello sviluppo software che auspicabilmente dovrà contemplare la componente dinamica del sistema fisico e dello sviluppo software in modo unificato. L'enfasi è posta sulla modellazione, progettazione e analisi dei sistemi cyber-fisici, che integrano computing, networking e processi fisici (Lee, 2008; Lee, 2010).

In sintesi, un sistema cyber-fisico (CPS) è un sistema informatico in grado di interagire direttamente e dinamicamente con il mondo reale che le circonda ed è costituito da elementi hardware dotati ciascuno di capacità di elaborazione, e presenta capacità computazionale, di controllo e di comunicazione. Alla base del sistema, l'elemento base è, come visto in precedenza, un dispositivo di tipo "embedded".

I sistemi CPS rappresentano una vera e propria rivoluzione in ogni settore, dalle fabbriche intelligenti (la c.d. Industria 4.0) alla medicina, al settore automobilistico, al controllo di processo, risparmio energetico, sistemi di difesa, edifici intelligenti. Di particolare interesse per lo scopo del presente lavoro, sono le applicazioni dei sistemi cyber-fisici nel controllo delle Infrastrutture Critiche e nell'erogazione dei servizi pubblici strategici o essenziali poiché i Cyber-Physical Systems e i relativi sotto-sistemi (Internet of Things, SCADA, embedded systems, ecc.) sono ampiamente riconosciuti come importanti fattori abilitanti per applicazioni innovative che coinvolgono svariati settori dell'economia in tutto il mondo (NIST, 2016).

In conclusione, nella prospettiva legata ai servizi strategici per i cittadini, questi sistemi rappresentano sempre più il fondamento delle Infrastrutture Critiche, e costituiscono la base di emergenti e futuri servizi intelligenti che, ci si attende, miglioreranno la qualità della nostra vita.

Infrastrutture Critiche e servizi pubblici strategici

La prima definizione di Infrastruttura Critica, a livello europeo, è contenuta nella Comunicazione n.702/2004 del Consiglio Europeo, in materia di prevenzione di possibili attacchi terroristici, e comprende tutte "*Quelle risorse fisiche, servizi e installazioni, reti e risorse informatiche la cui degradazione avrebbe un serio impatto sulla sicurezza o il benessere economico degli Europei o sul funzionamento efficace dell'Unione Europea o dei Governi degli Stati Membri."* Le Infrastrutture Critiche individuate dalla Commissione includono impianti e reti energetiche, sistemi di comunicazione e di tecnologia dell'informazione, il settore finanziario, il sistema sanitario, la filiera alimentare, le reti idriche, i trasporti, la produzione, lo stoccaggio e il trasporto di sostanze pericolose (materiali chimici, biologici, radiologici e nucleari), reti di informazione, beni architettonici e naturali. La Comunicazione n.702 propone l'istituzione del Programma Europeo per la Protezione delle Infrastrutture Critiche *(European Programme for Critical Infrastructure Protection, EPCIP)* allo scopo di offrire una maggiore sicurezza per le infrastrutture critiche nell'Unione Europea. L'obiettivo dell'EPCIP è di "assicurare il funzionamento delle infrastrutture critiche europee" (EC/COM, 2004), per le quali il Consiglio europeo ha evidenziato gli effetti della natura transfrontaliera nel causare eventi a "cascata" che finiscano per coinvolgere infrastrutture critiche dei Paesi confinanti (EC/COM, 2006), procedendo a sviluppare i principi di governance specifici a livello europeo e a livello nazionale.

La Direttiva Europea 2008/114/CE, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione - al punto a) dell'art. 2 - definisce Infrastruttura critica "un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni";

Seppur non esaustiva, poiché focalizzata sui settori energia e trasporti, la Direttiva 2008/114/CE stabilisce che per la difesa e la protezione delle infrastrutture critiche sono necessarie e attese delle azioni da parte governativa, da parte delle aziende che le

gestiscono, ma soprattutto da parte dei singoli che agiscono all'interno di una cultura orientata alla sicurezza con una visione ampia sui sistemi oltre che sulle singole parti che concorrono alla realizzazione del sistema nel suo complesso.

Al punto b) dello stesso articolo, viene successivamente definita Infrastruttura Critica Europea (ECI): "un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture" (art. 2; Direttiva 2008/114/CE). Il nostro Paese ha recepito la direttiva 2008/114/CE attraverso il D.Lgs n. 61 dell'11 aprile 2011, che è entrato in vigore il 5 maggio 2011 a seguito della pubblicazione sulla Gazzetta Ufficiale (GU n. 102 del 4 maggio 2011).

All'art. 5 della Direttiva n.114, viene definita la procedura obbligatoria per i Paesi membri per l'implementazione dell'Operator Security Plan (OSP) che individua gli elementi della ECI e le soluzioni per la sicurezza già attive o di futura implementazione per la loro protezione. Ogni proprietario o Operatore di un'infrastruttura individuata come Infrastruttura critica europea dovrà necessariamente predisporre l'OSP (Piano di Sicurezza dell'Operatore). Viene definita altresì la metodologia da adottare per l'identificazione degli assets importanti, le procedure da seguire per condurre la risk analysis e l'identificazione, la selezione e la definizione delle priorità delle contro-misure da implementare. Infine, stabilisce che ogni Stato membro interagirà con la Commissione e con gli altri Stati membri attraverso un organismo nazionale competente per la protezione delle Infrastrutture Critiche. Ogni Stato membro è tenuto a condurre un'analisi e valutazione dei rischi e delle minacce riguardanti le ECI che insistono sul proprio territorio nazionale.

La ricerca nel campo delle infrastrutture critiche è rivolta a mantenere e sostenere il benessere pubblico, poiché è evidente che il funzionamento della società moderna dipende dalla qualità delle infrastrutture disponibili e che "*col tempo le infrastrutture sono diventate sempre più fondamentali per il funzionamento della società*", così "*come processi economici e sociali in larga misura si basano sui servizi forniti da tali sistemi*" (Thissen and Herder, 2003). Oltretutto i mutamenti sociali continuano a plasmare il significato di sistemi infrastrutturali, ampliandone i contenuti ben oltre i settori

dell'energia e dei trasporti, inizialmente considerati dalla normativa europea: telecomunicazioni, servizi bancari e finanziari, sistemi di approvvigionamento idrico, servizi di emergenza (tra cui soccorso sanitario, polizia, vigili del fuoco, protezione civile) e continuità di governo sono infrastrutture critiche che, per una società moderna come l'attuale, erogano servizi ritenuti strategici ed essenziali.

RISCHI E MINACCE NEL CYBER SPAZIO

Gli attacchi informatici

Con l'aumentare della complessità dei siti Web e lo sviluppo più rapido delle applicazioni, aumenta anche il rischio di attacchi potenziali. Hackers e cyber mercenari creano, distribuiscono e utilizzano sofisticati strumenti informatici per sottrarre o distruggere dati personali o aziendali, compromettere siti e interferire con le infrastrutture informatiche, pubbliche e private. I cyber attacchi sfruttano qualsiasi tipo di vulnerabilità, sia quelle presenti nei software o nei dispositivi, che dipendenti dalla persona che li utilizza o li gestisce.

Una miscela eterogenea di attori opera nel cyber space, e le attività illegali si dispiegano in diversi settori, come forme di vandalismo, attivismo, criminalità, terrorismo e conflitto, originando le seguenti principali tipologie di crimine informatico.

Il ***Cyber crime*** identifica tutte le attività illegali compiute nel cyber spazio, per interessi personali o a scopo di lucro, da parte di organizzazioni criminali o di singoli individui. Lo scopo primario è quello del raggiungimento di un profitto economico. Le attività illegali più conosciute sono le truffe telematiche, le frodi bancarie su Web o sulla rete mobile, e, fenomeno recente ma molto diffuso, il *ransomware* ovvero la richiesta di un riscatto per restituire all'utente l'accesso ai propri dati che hanno subito un processo di crittografia totale da parte del virus informatico, rendendo impossibile l'accesso e il recupero delle informazioni memorizzate da parte della vittima dell'attacco. Gli autori del ransomware contattano l'utente e, in cambio di denaro, forniscono il codice di sblocco e recupero dei propri dati.

Per ***Cyber attivismo*** si intende una nuova forma di resistenza "culturale e politica" portata avanti dalla comunità hacker. Questo tipo di attività è animata da motivi di natura socio-politica o per finalità di protesta su particolari e specifiche tematiche socialmente rilevanti. Gli strumenti di attacco più utilizzati, in questo caso, sono il *Distributed Denial of Service* (*DDoS*), la raccolta illecita di dati personali (mediante attacchi di tipo APT) e

diffusione di dati e di informazioni riservate (i c.d. *Data breach* e *Data leaks*).nn Appartiene al cyber attivismo anche l'attività di *defacing* ovvero l'intrusione non autorizzata nel sito web con modifica dei contenuti del sito.

Il ***Cyber spionaggio***, invece, riguarda generalmente operazioni di intelligence che hanno come scopo primario quello di guadagnare l'accesso a informazioni riservate, sensibili e strategiche. E' una forma di minaccia che si caratterizza per ampiezza e intensità variabili. Solitamente, precede le altre forme di cyber crime con intensità crescente e le accompagna sistematicamente, rendendo difficile stabilire una chiara distinzione tra queste categorie, e determinando, in ogni caso, danni finanziari o di reputazione – sia agli Stati colpiti che alle aziende - tali da causarne la potenziale esclusione dal mercato.
Tra le operazioni che conducono le Nazioni nel cyberspace, le attività di spionaggio occupano senza dubbio un posto di rilievo. Le attività più frequenti vanno dalla raccolta di informazioni aziendali segrete, alle intercettazioni di comunicazioni telefoniche o telematiche, comunicazioni, messaggi, social network, ecc., Lo spionaggio naturalmente non nasce con l'avvento del mondo cyber ma è una pratica a cui ricorrono tutti i governi, da sempre, poiché è evidente l'interesse di qualunque Stato di poter disporre in anticipo di informazioni riservate su altre nazioni. L'informazione è potere e lo spionaggio costituisce uno degli strumenti più efficaci per ottenere vantaggi politici, militari ed economici nei confronti di Paesi ostili o anche amici o alleati, in periodi di pace così come in tempo di guerra. Un Governo può arrivare a supportare o a non ostacolare attività illecite di cyber spionaggio nei confronti di industrie o aziende straniere, finalizzato alla sottrazione di segreti industriali o progetti tecnologicamente all'avanguardia e ciò allo scopo evidente di aumentare la competitività delle aziende nazionali a danno delle altre.

La ***cyber warfare*** è una vera guerra cibernetica e comprende tutte le attività ostili di cyber crime praticate da uno Stato nei confronti di un altro attraverso il cyber space. Appare, pertanto, evidente l'evoluzione che ha compiuto la minaccia cyber in questi ultimi anni, passando da tentativi imperfetti, condotti da una minoranza di esperti informatici, ad una forma coordinata di guerra tecnologica, supportata da Nazioni che la utilizzano come strumento strategico irrinunciabile per la competizione mondiale. Si realizza con il danneggiamento di sistemi informatici militari o industriali, di infrastrutture che

assicurano la fornitura di servizi essenziali tipo l'energia elettrica, gas, acqua, servizi di telecomunicazioni, ecc. La terminologia utilizzata riporta direttamente alla natura dell'attacco; infatti, distinguere tra cyber warfare e cyber crime significa richiamare automaticamente un diverso aspetto (militare o criminale), un differente obiettivo perseguito (vantaggi strategici o obiettivi monetari) e una diversa tipologia di agente (eserciti nazionali o organizzazioni criminali).

Devono infine menzionarsi le attività illegali rientranti nel ***cyber terrorismo*** che include alcuni dei concetti sopra esposti, ma che ha proprie caratteristiche e connotazioni. Infatti il terrorismo digitale ha alcuni importanti vantaggi rispetto al terrorismo "tradizionale" come l'anonimità, economicità e la distanza fisica dall'obiettivo, la cui ininfluenza, non può rappresentare un ostacolo al successo dell'attacco né un effetto deterrente per l'esecutore dell'attacco. Una chiara definizione di cyber-terrorismo è stata data dall'US National Infrastructure Protection Center (NIPC), come "*A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda*".

Le principali attività e le specifiche tecniche di attacco poste in essere dalle comunità criminali sono elencate nella seguente tabella:

Tipo di cyber minaccia	Descrizione
Virus	Malware che una volta attivato è in grado di replicarsi e infettare sistemi operativi, file e singoli documenti
Worm	Malware auto-replicabile in grado di auto-propagarsi e infettare tutti i sistemi connessi su una stessa rete
Phishing Spear-phishing	Malware contenuto in e-mail che sembrano provenire da soggetti conosciuti e che rubano password e informazioni finanziarie
Attacco brute force	Attacco capace di "craccare" le password generando ad altissima velocità tutte le possibili combinazioni di chiavi per aprire file protetti
Cross-site scripting (XSS)	Inclusione di codice html all'interno di una pagina web per effettuare operazioni malevoli quali prelievo di cookies privati
SQL injection	Tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input in modo che vengano eseguiti
Trojan	Malware impiegato per effettuare intercettazioni, rubare informazioni sensibili ed effettuare operazioni sui sistemi

Vulnerabilità 0 Day	Vulnerabilità di applicazioni non ancora divulgate o per le quali non è ancora stata distribuita una patch
Exploit	Esecuzione di codice malevolo che sfrutta una o più vulnerabilità con lo scopo di acquisire privilegi amministrativi
Keylogger	Strumento in grado di intercettare, in forma nascosta, le digitazioni effettuate sulla tastiera del dispositivo
DDoS	Attacco mirato a rendere indisponibile un servizio mediante un sovraccarico di richieste verso il sistema target
Spam	Comunicazioni indesiderate e ripetute da parte di mittenti sconosciuti usati anche per diffondere malware
APT (Advanced Persistent Threat)	Attacco di difficile identificazione finalizzato a guadagnare punti di accesso a una rete per un lungo periodo di tempo
Botnet	Rete di computer "zombie" infettati da un malware e controllati in via remota e nascosta da un attaccante

Si tratta di attività illecite poste in essere grazie all'utilizzo di software, suite specifiche, programmi costruiti ad hoc, che vengono reperiti nel *Dark Web*, dove è possibile acquistare o affittare, pacchetti di malware a prezzi accessibili, exploit zero-day, ma anche tutorial e consulenza on-line per l'attuazione degli attacchi (si pensi che nel 2013 il costo dei kit di exploit si aggirava tra i 450$ a settimana e i 1800 $ al mese; mentre il prezzo di attacchi DDos oscillava tra i 3 e i 5$ all'ora o, in alternativa, potevano essere acquistati al costo di 90-100$ al giorno, o di 400-600$ a settimana)[2].

Il c.d. Dark Web è quella specifica parte del *Deep Web* - quest'ultima è tutta quella fetta della rete mondiale non indicizzata dai motori di ricerca, contenente pagine web a contenuto dinamico, web software volutamente occultato, siti privati aziendali o configurati non rispettando gli standard, contenuti banditi dai motori perché illegali, ecc., che è stato stimato nel 99% del totale dei contenuti presenti sulla rete, ritenendo che il

[2] *The Underground Hacking Economy is Alive and Well*, di Elizabeth Clarke, https://www.secureworks.com/blog/the-underground-hacking-economy-is-alive-and-well

Surface Web, con contenuti accessibili a tutti, sia soltanto il restante 1%[3] - dove vi sono dati nascosti, irraggiungibili attraverso una normale connessione senza far uso di software specifici, in quanto giacenti su reti sovrapposte ad Internet e chiamate genericamente *Darknet*, come ad es. Tor, I2P, Freenet. Le Darknet vengono raggiunte attraverso software dedicati che fanno da collegamento tra la Internet e la Darknet e consentono agli utenti la navigazione anonima anche sulla Internet. All'interno della Darknet si è sviluppato un vero e proprio mercato: il *Black Market* dove si smerciano svariati tipi di prodotti illegali - quali droga, armi, banconote false, merce rubata, carte di credito, omicidi, accessi a conti bancari, identità, account vari, traffico di persone, organi, malware, servizi di hacking, ecc. - e dove hackers e crackers, anche non molto esperti, possono reperire ciò che è necessario per facilitare gli attacchi in base alle proprie necessità. Esso è governato dalle tradizionali leggi della domanda e dell'offerta, e la moneta usuale è il *bitcoin,* una criptovaluta che consente il possesso e il trasferimento anonimo delle monete in portafogli digitali. L'ultima tendenza del black market sono i servizi di hacking*,* ossia la vendita di servizi, piuttosto che di software: in sostanza viene aggiunto un supporto tecnico agli strumenti di hacking (interfacce semplificate, supporto tecnico per email o IRC) abbassando così la difficoltà di utilizzo degli strumenti offerti, e rendendo il crimine informatico accessibile anche a soggetti non particolarmente preparati in materia.

Gli attacchi elaborati dalle comunità criminali, facendo largo uso della darknet, possono essere raggruppati in alcune tipologie principali, il cui studio diventa l'elemento di partenza per determinare una ingegnerizzazione dei processi di Cyber Security, con un approccio *risk based*. Queste tipologie di crimini possono riguardare:

1) Sviluppo di tools, software e tecniche di attacco (es. Trojan, Virus, Tool di attacco, Vulnerabilità 0day, Exploit, Keylogger, ecc.)

---

[3] *The Deep Web you don't know about*, di Jose Pagliery, money.cnn.com/2014/03/10/technology/deep-web/index.html; *Entrepreneurs, Surface Web, Deep Web and Dark Web* di Joern Nielsen, http://entrepreneur-sme.asia/entrepreneurs-deep-web-dark-web/

Vengono usati sia per lo spionaggio che per il sabotaggio e gli attacchi veri e propri, e sono solitamente progettati per sfruttare vulnerabilità di funzionamento di programmi e sistemi digitali, talvolta non ancora scoperte dagli stessi produttori del software, oppure può trattarsi di virus capaci di sottrarre dati e manipolare o distruggere le informazioni contenute in server, database, e computer online; o, ancora, strumenti in grado di controllare pc e smartphone, anche bloccandone il funzionamento, sia dell'hardware che del software.

2) Fornitura di account o informazioni rubate (es. credenziali per accesso a vari servizi: bancari, VPN aziendali, Social, email, ecc.)

   Vengono utilizzati attacchi "brute force" per violare le password, codici crittografici e VPN a protezione dei sistemi informatici per usarli a proprio vantaggio; tecniche di phishing, attraverso le quali si riceve un'email da conoscenti ignari che invitano a cliccare sopra un link o un pdf che installa il virus, risalendo all'identità, alle risorse e ai conti online della vittima, per sostituirsi ad essa aggiungendo ogni volta nuovi dati al profilo che l'attaccante vuole utilizzare per poter operare al posto suo. Vi sono tecnologie di sorveglianza, come gli spyware, per intercettare le conversazioni di capi di governo e presidenti di organizzazioni economiche e finanziarie, oppure per il riconoscimento facciale, fino ai software che traducono conversazioni in testi scritti. Si tratta spesso di tecnologie dual-use, che possono essere usate per operazioni di polizia, ma anche per fini illeciti.

3) Fornitura di risorse di rete e di servizi (es. Botnet, Attacchi DDOS, diffusione di malware, CAPTCHA breaking, Training)

   Questi attacchi consistono nell'istallazione di programmi che rendono il sistema una sorta di "bot" (larva), o "zombie", controllabile a distanza dall'attaccante; possono essere operati attraverso reti di computer *zombie* controllabili in remoto da utenti illegittimi e senza che i proprietari ne siano a conoscenza; sostanzialmente si tratta di reti di computer create appositamente per concentrare sul bersaglio prescelto una serie di attacchi provenienti da ogni parte della rete con l'obiettivo di congestionare un sito o una applicazione Web in modo da non consentirne più l'accesso agli utenti legittimi, mediante l'esaurimento delle risorse

del bersaglio (ampiezza di banda, sistema operativo, potenza dei computer o dei server).

Evoluzione della cyber minaccia

La percezione delle minacce informatiche è piuttosto recente, ma esse sono, in realtà, presenti nel panorama mondiale già da due o tre decenni e, in questo lasso di tempo, si sono evolute e rafforzate.

Il worm che ha determinato una presa di coscienza a livello istituzionale dei rischi informatici e della necessità di politiche di cyber security, con l'istituzione del CERT (Computer Emergency Response Team), è stato diffuso in internet nel 1988, con il nome di Morris, come il suo creatore, Robert Tappan Morris, all'epoca studente al MIT. Morris voleva individuare il numero di computer presenti sulla rete, e non aveva scopi di hackeraggio, ma il suo programma che si copiava automaticamente su ogni macchina e inviava un messaggio a tutte le altre, finì per bloccare i computer dell'epoca, le cui risorse erano molto limitate[4].

Agli inizi degli anni '90, gli hackers hanno cominciato a condurre i primi cyber attacchi in rete, in parallelo alla crescita dell'e-commerce. Il cyber crime comincia ad affermarsi sempre più, a volte favorito dall'inerzia dei governi nazionali. Nel decennio successivo diviene evidente la potenza dei virus informatici. Infatti, proprio nel 2000, il virus "The love bug" infetta circa 55 milioni di computer, diffondendosi dalle Filippine, dove era stato creato da due hackers, fino a Hong Kong e poi in Europa e negli Stati Uniti. Il virus, inviato tramite e-mail come allegato con la scritta "I Love You", una volta aperto, si auto-installava e inviava una copia della mail a tutti i contatti della rubrica dell'utilizzatore, oltre a sovrascrivere i file presenti nell'hard disk. Questo worm, ritenuto relativamente poco dannoso, ha causato danni stimati intorno ai 15 miliardi di dollari.

[4] Robert Morris, attualmente professore al MIT, presso il Computer Science and Artificial Intelligence Laboratory, dopo di questo episodio venne processato e condannato.

I malware successivi sono ancora più insidiosi: si pensi ai worm chiamati So Big, Bagle e My Doom; autoreplicanti, capaci di autoinviarsi ad altri utenti, ma anche in grado di impartire autonomamente comandi, oltre che di mettersi in rete tra di loro.

In seguito fanno il loro ingresso Storm Worm, un trojan horse che permette di controllare il computer infetto e aggiungerlo alla rete botnet Storm, e Zeus, un banking trojan capace di rubare informazioni di carattere bancario, come credenziali per accedere al conto corrente e dati della carta di credito. La botnet Storm è controllata dalla Russian Business Network- RBN, nota per ospitare affari equivoci e illegali, come materiale pedo-pornografico, spam, malware, phishing e ogni genere di attività criminale, ritenuta una delle principali organizzazioni criminali di cyber crime, oltre che provider per conduzione di cyber attacchi[5] e definita da VeriSign Inc., colosso della certificazione e della sicurezza, "the baddest of the bad", e che, sempre secondo Verisign, avrebbe offerto i propri servizi per rubare, solo nel 2006, 150 milioni di dollari da account bancari[6]. Symantec, altra azienda produttrice di software per la sicurezza, ritiene RBN il maggior provider del cybercrimine moderno[7].

Nell'ultimo decennio è, pertanto, evidente l'evoluzione delle cyber minacce e come i malware vengano utilizzati alla stregua di vere e proprie armi a disposizione delle maggiori potenze mondiali, come sintetizzato nella tabella sottostante, riassuntiva di alcuni dei principali attacchi informatici degli ultimi anni; non più tentativi imperfetti, condotti senza intenzioni malevole, ma metodi e strumenti di competizione tra Paesi, capaci di danneggiare le infrastrutture che garantiscono i servizi essenziali e, in genere, i sistemi informatici militari e industriali degli Stati.

---

[5] *Shadowy Russian Firm Seen as Conduit for Cybercrime*, Brian Krebs, washingtonpost.com, Staff Writer Saturday, October 13, 2007

[6] *A walk on the dark side,* The Economist, 30 agosto 2007, http://www.economist.com/node/9723768

[7] *White Paper: Symantec Enterprise Security - Symantec Report on Rogue Security Software*, ottobre 2009

Tipo di cyber-attack	Destinatari e conseguenze dell'attacco
Worm stuxnet	17 giugno 2010 – centrale nucleare di Natanz Primo importante attacco ai sistemi industriali di controllo (SCADA). 38.000 sistemi infetti (22.000 in Iran).
Data Breach	Agosto 2013 – Yahoo L'attacco Cyber compromette più di 1 miliardo di accounts. Pesanti effetti sul valore dell'azienda.
Data Breach	Settembre 2014 – JP Morgan &Chase Compromissione dei dati associati ad oltre 83Mln di Accounts.
Ransomware	24 novembre 2014 - Sony Costi di indagine e bonifica stimati intorno ai 15 Milioni di dollari.
Data Breach	Settembre 2015- Experian Experian T-mobile scopre l'hackeraggio dei dati di 15 milioni di clienti presenti sui propri server.
Trojan horse	23 dicembre 2015 – Black Energy Un Trojan apre sistemi SCADA e HMI e permette l'hackeraggio di centrali elettriche, privando di energia centinaia di migliaia di case per diverse ore.
APT	17 giugno 2016 – Mattel Danni per 3 milioni di dollari per l'email phishing dell'Amministratore Delegato della società emettendo un falso ordine di pagamento in Cina.
DDoS	Settembre 2016 - OVH.com Attacco massivo DDoS attraverso una rete di oltre 152.000 dispositivi IoT tra cui videocamere a circuito chiuso e registratori video personali.
DDoS	21 ottobre 2016 - Dyn DNS Molteplici attacchi Ddos all'infrastruttura online che associa nomi di dominio a indirizzi IP della rete mondiale (come Twitter, Amazon, Tumblr, Skype, Reddit, The New York Times, PayPal, Spotify e Netflix), basati su 10 Milioni di dispositivi IoT.
Botnet	29 novembre 2016 - Deutsche Telekom Gli Hacker aggiornano la botnet Mirai ed infettano i routers di Deutsche Telekom. Numerosi disservizi su circa 900.000 clienti per diverse ore.
Worm	31 dicembre 2016 - Burlington Electric Violata da hackers russi la rete elettrica dello stato del Vermont, senza causare interruzioni del servizio.

Impatto economico e geopolitico del crimine informatico

Il Global Economic Crime Survey 2016, uno studio periodico della PwC[8] su scala mondiale, evidenzia che l'incidenza della criminalità informatica esaminata dall'attività di indagine, nello scorso anno risulta nettamente superiore che in passato, posizionando il cyber crime dal 4° al 2° posto in classifica tra le forme di criminalità di tipo economico, andando dal 24% del 2014, al 32% del 2016. E' stata l'unica forma di criminalità ad aver registrato un aumento, mentre appaiono in lieve flessione illeciti più tradizionali, come l'appropriazione indebita, la corruzione, le frodi e il falso in bilancio. Sotto l'aspetto finanziario, le perdite conseguenti possono essere pesanti: una parte degli intervistati - circa 50 organizzazioni - ha dichiarato di aver subito danni per oltre 5 milioni di dollari; di questi, quasi un terzo, ha riportato perdite, causate da cyber attacchi, superiori ai 100 milioni di dollari.

Il report, "Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II" del giugno 2014, prodotto dal Center for Strategic and International Studies[9] e promosso dalla McAfee, una tra le aziende leader nel settore della sicurezza informatica, evidenzia che il cyber crime costa alle imprese circa 400 miliardi di dollari, che corrisponde a una perdita di 200mila posti di lavoro negli Stati Uniti e circa 150mila in Europa. Il costo più significativo prodotto dal cyber crime deriva dal danno causato alle imprese e alle economie nazionali. Secondo il report, il cyber crime danneggia mercati, competitività, innovazione e frena la ripresa e la crescita dell'economia globale.

---

[8] Global Economic Crime Survey 2016, http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

[9] CSIS - Center for Strategic & International Studies è un'organizzazione non profit di ricerca internazionale in tema di sicurezza e difesa localizzata a Washington DC (US), https://www.csis.org/

Il rapporto del CSIS stima che il crimine informatico sottrae una percentuale che oscilla tra il 15% e il 20% di tutto il valore creato da Internet.

Le tradizionali forme di autorità e di potere esercitate dagli Stati contemporanei non sono in grado di garantire il pieno controllo del cyber spazio poiché, per la natura stessa della rete, non vi sono limiti, confini o vincoli geografici nei cui ambiti esercitare la sovranità. I poteri - politico, legislativo, giudiziario, delle forze di polizia e militare - sono fortemente limitati e, in gran parte, incapaci di esercitare un controllo efficace del cyber spazio. Ma, poiché la capacità produttiva di un Paese e, nel complesso, la qualità di vita dei cittadini è sempre più collegata ai servizi erogati strettamente attraverso il mondo digitale internet, un'eventuale compromissione della funzionalità della rete e/o dei dispositivi fisici ad essa connessi, provoca inevitabilmente degli effetti negativi che potrebbero raggiungere livelli devastanti per il sistema Paese o per parte di esso.

E' evidente già da tempo che viviamo in un mondo digitalmente interconnesso dove si intrecciano e si sviluppano tutte le attività che interessano il genere umano, da quelle economiche e finanziarie a quelle politiche e sociali, dalle attività di intelligence a quelle illegali che possono provenire a partire da singoli individui fino a vere e proprie multinazionali del crimine. Non è errato sostenere che al giorno d'oggi un semplice personal computer può essere utilizzato come sistema d'arma e un'efficacia paragonabile a quella degli armamenti convenzionali. Un'organizzazione terroristica con personale militare e infrastrutture limitate può lanciare attacchi informatici da qualsiasi posizione nel mondo, e può causare danni massivi, sia che si tratti di infrastrutture, di finanza o della vita umana. James Lewis, del Center for Strategic and International Studies (US), definisce la minaccia di attacchi informatici nel XXI secolo come "a massive electronic Achilles' heel" (Lewis, 2002); immagine che, applicata ad uno scenario di rischio associato ad infrastrutture strategiche nazionali, fa risaltare immediatamente gli effetti rovinosi per l'economia di un Paese, oltre che per il benessere dei cittadini. Infatti, un attacco deliberato alle c.d. Infrastrutture Critiche Nazionali può certamente essere considerare un atto ostile e, di conseguenza, assumere una valenza di tipo militare. Non

a caso, nel vertice dell'8 e 9 luglio 2016, la stessa NATO, a Varsavia[10], ha dichiarato il cyberspazio come il quinto dominio sottoposto alla sua protezione militare, dopo la terra, il mare, l'aria e lo spazio; la Cyber Security è considerata "5th fighting dimension", ossia il quinto scenario di guerra vero e proprio, dove attacchi informatici possono assumere le connotazioni di un vero e proprio atto di guerra, e, secondo le "Rules of Engagement-ROE" della NATO, la risposta ad un atto ostile di tipo cyber può essere condotta, a determinate condizioni, con armi convenzionali in uno o più degli altri quattro domini: Aria, Terra, Mare e Spazio.

In ambito NATO si studia da tempo quella che viene definita la "Active Cyber Defense", ossia una misura proattiva finalizzata a rilevare o ottenere informazioni su un'intrusione informatica, un attacco informatico, o per determinare l'origine di un'operazione che prevede il lancio preventivo di un attacco di tipo cyber e di una contro-misura informatica contro la fonte della minaccia o dell'imminente atto ostile.

Ci sono molti dubbi però ad adottare una difesa "attiva", uno dei quali è rappresentato dalla difficoltà nel mondo cyber nel risalire agli effettivi mandanti degli attacchi.

Consapevoli della rilevanza del dominio del cyberspace, gli stati nazionali hanno creato strutture e dipartimenti ad hoc, dal *Cybercommand* negli Usa, all'*Enisa* europea, mentre Russia, Regno Unito e Cina hanno inglobato la guerra cibernetica nella loro intelligence militare. Non è un caso se il 2016 verrà ricordato come l'anno del conflitto nel cyber spazio tra le grandi potenze, un dominio nel quale il conflitto diplomatico e militare diventa conflitto digitale e la guerra cibernetica diventa globale. Basti pensare, ad esempio, ad un guasto su larga scala alle infrastrutture nazionali della rete elettrica: non funzionerebbero ospedali e fabbriche, sarebbero a rischio i servizi essenziali alla popolazione con potenziali effetti di panico e di blocco delle attività produttive; scenari che, potendo risalire con certezza al mandante, potrebbero indurre uno Stato a rispondere all'attacco cyber con un attacco militare tradizionale. Si pensi all'intrusione di hacker

[10] http://www.nato.int/cps/en/natohq/official_texts_133169.htm

russi nella rete elettrica del Vermont, ritenuta – come riportato dal Washington Post - una provocatoria dimostrazione di forza dopo le sanzioni americane contro gli hackeraggi russi ai danni di organizzazioni politiche che hanno interferito con la campagna presidenziale[11].

Per le ragioni descritte, l'escalation della tensione tra Russia e Usa si sta configurando come una situazione da guerra fredda. La cyber war è diventata un'opzione militare; la guerra cibernetica usa strumenti in grado di violare e mettere fuori uso sistemi informatici e va ad aggiungersi alle più classiche forme di spionaggio tecnologico. Le armi della cyber war permettono di conquistare un vantaggio tattico e strategico nei confronti degli avversari, sottraendo, manipolando e inquinando le loro informazioni oppure, come appena esposto, possono essere finalizzate al sabotaggio delle infrastrutture critiche e, in questo caso, sono strumenti che servono a colpire economie ed apparati militari e, allo stesso tempo, a disorientare e incutere paura tra la popolazione civile del Paese avversario. Alla luce dell'evidente pericolosità degli attacchi cyber, tutti i Governi si stanno impegnando nell'elaborazione di strategie di difesa informatica e, sovente, predispongono delle *linee guida* per sollecitare le strutture della PA e del mondo produttivo privato ad introdurre ed attivare al meglio le difese della cyber security.

Cyber crime e infrastrutture critiche nazionali

Nel 2010 si è registrato il primo clamoroso attacco cyber fisico a un impianto nucleare che, pur non strettamente classificabile come infrastruttura critica nazionale, è innegabilmente un impianto "sensibile" di una nazione sovrana. L'attacco è stato sferrato attraverso il malware Stuxnet, che ha messo fuori uso gran parte delle centrifughe, utilizzate per l'arricchimento dell'uranio per scopi bellici, installate all'interno

[11] https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.867753fceb02

dell'impianto nucleare iraniano di Natanz. Il successo di questo cyber attacco ha prodotto un notevole impatto poiché ha provocato un progressivo e importante deterioramento della capacità di produzione dell'uranio arricchito e il conseguente rallentamento del programma nucleare iraniano. Stuxnet è un worm specializzato negli attacchi ai sistemi di controllo SCADA (Supervisory Control And Data Acquisition) che l'impianto di Natanz utilizza per controllare gli impianti di arricchimento. Il worm, attraversando i sistemi di supervisione in ambiente Windows dove risiede il software di controllo della centrale, si è propagato ai livelli inferiori, avvicinandosi al livello fisico, fino a raggiungere i sistemi elettronici specializzati, i PLC (Programmable Logic Controllers), prodotti in questo caso da Siemens, che controllano e regolano fisicamente gli apparati e i processi produttivi. Sui PLC, che utilizzano un sistema operativo differente da Windows, Stuxnet si è autoinstallato ed ha assunto il controllo del sistema. In questo modo, modificando progressivamente i parametri di funzionamento delle centrifughe di arricchimento di uranio e, aumentandone progressivamente la velocità di rotazione, portandola a livelli molto più elevati rispetto alle specifiche previste dal costruttore, ne ha provocato il danneggiamento, continuando, però, ad inviare al sistema di controllo centrale dei parametri che continuavano a mostrare un apparente regolare funzionamento dell'infrastruttura in modo che il progressivo incremento di velocità non venisse rilevato né dai sistemi informatici di supervisione, né tantomeno dagli addetti al controllo e alla gestione dell'impianto.

Molto probabilmente, attraverso il cyber attacco Stuxnet si sono raggiunti risultati analoghi, se non superiori, a quelli che si sarebbero ottenuti con un attacco militare di tipo convenzionale. Va segnalato che si è trattato di un attacco estremamente raffinato e, osservandone il livello elevato di complessità, è evidente che si tratta di un'azione non alla portata di uno o più individui ma, al contrario, talmente elaborata da necessitare di conoscenze, competenze e disponibilità economiche di cui, probabilmente, solo uno Stato può disporre e che – come riportato dal New York Times – sarebbe infatti stato

programmato da Usa e Israele per sabotare le centrali in Iran e arrestarne i programmi nucleari[12].

Nell'agosto 2012, la rete di computer di una grande compagnia Saudita, la Saudi Aramco, è stata violata da un virus autoreplicante, chiamato Shamoon, che ha infettato circa 30.000 computer (Bronk et al., 2013). Nonostante le dimensioni e le ingenti risorse economiche di cui dispone, la società nazionale saudita ha lavorato intensamente quasi due settimane per recuperare la funzionalità informatica compromessa dall'attacco del virus. Specializzato nell'attacco di impianti petroliferi, Shamoon non interferisce nel controllo fisico degli impianti, ma opera una cancellazione indiscriminata dei dati presenti sulle memorie di massa dei computer colpiti dall'attacco. In seguito, è stato nuovamente utilizzato per attacchi all'agenzia di aviazione nazionale saudita. Secondo alcune fonti, l'attacco sarebbe stato sponsorizzato da uno stato straniero, presumibilmente l'Iran, già in passato collegato a Shamoon[13].

Va in ogni caso considerato, che sempre più frequentemente e in modo pervasivo i dispositivi fisici utilizzati per fornire gli ormai irrinunciabili servizi che accompagnano la nostra vita quotidiana sono controllati da sistemi informatici specializzati. Sistemi costituiti da sempre più numerosi oggetti dotati di capacità computazionale e software costantemente più complessi, distribuiti e interconnessi tra loro all'interno della rete globale. Ne sono esempio le connected-car, gli smartphones, le smart TV, tutta la galassia degli IoT, dai microsensori di inquinamento intelligenti, ai dispositivi indossabili.

Ed è proprio nelle caratteristiche intrinseche di questo tipo di sistema che si annidano delle insidie: infatti, l'interconnessione in rete e la presenza di un software che controlla i dispositivi fisici, costituisce il legame tra il mondo fisico e quello informatico e un

---

[12] http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?_r=0

[13]https://www.bloomberg.com/news/articles/2016-12-01/destructive-hacks-strike-saudi-arabia-posing-challenge-to-trump

‘hacker’ qualsiasi può riuscire ad ottenere il controllo del funzionamento dei dispositivi fisici del sistema e, di conseguenza, interferire nel loro regolare funzionamento. I cyber criminali possono colpire utilizzando a loro vantaggio la combinazione tra il numero significativo delle vulnerabilità e il sempre più frequente utilizzo dei dispositivi mobili per monitorare i sistemi di controllo industriali e colpire infrastrutture critiche. Ciò fa sì che un cyber-attack in grado di impattare su sistemi cyber-fisici sia potenzialmente realizzabile senza grandi mezzi o investimenti, e dunque alla portata di singoli individui. Il rischio è rappresentato dalla capacità dell’attacco informatico di produrre effetti concreti nel ‘mondo reale’, causando potenziali conseguenze su ambiente, economia, società o, in alcuni casi, mettendo in pericolo l’incolumità fisica di esseri umani.

Il primo cyber attacco a Infrastrutture Critiche è avvenuto nel 1982 ed ha colpito un gasdotto Trans-siberiano, provocando un'esplosione visibile dallo spazio (Miller e Rowe, 2012).

Negli Stati Uniti, nel 2003, un worm slammer è riuscito a penetrare nella rete di controllo dell'impianto nucleare di Davies-Besse in Ohio (Guan et al., 2011; Patel et al., 2005) e il virus di computer denominato “Sobig” è riuscito ad interferire con la rete ferroviaria e ad arrestare un treno in Florida (Miller e Rowe, 2012).

Sempre negli USA, nel 2006, un hacker ha penetrato il sistema di funzionamento di un impianto di depurazione a Harrisburg (Guan et al., 2011; Patel et al., 2005) e la centrale nucleare di Browns Ferry in Alabama (Nicholson et al., 2012).

Eclatante, ma certamente non unico, il caso dell’attacco alla rete elettrica in Ucraina operato attraverso il malware “BlackEnergy” subìto dalla compagnia elettrica dell’Ucraina nel dicembre 2015 e che, secondo quanto riportato dalla stampa del tempo, ha lasciato la metà delle abitazioni della regione di Ivano-Frankivsk (circa un milione e mezzo di persone) senza energia elettrica per ore a causa, per l’appunto, di BlackEnergy che ha assunto il controllo di diverse sottostazioni elettriche, disconnettendole dalla rete elettrica nazionale.

Tralasciando l’elencazione di ulteriori episodi della lunga sequenza di cyber attacchi subiti da Infrastrutture Critiche e tornando al contesto attuale, è evidente che queste infrastrutture nazionali che, si rammenta, costituiscono l’elemento fondamentale

nell'erogazione di servizi essenziali per la società odierna, hanno evidenziato in numerose occasioni la loro vulnerabilità agli attacchi cibernetici e i grossi rischi ad essi connessi.
Tutte le Infrastrutture Critiche sono controllate da sistemi cyber-fisici e operano sotto la supervisione e il controllo di sistemi ICT (Information and Communication Technologies). In effetti, le ICT sono diventate elementi essenziali nella nostra società perché offrono evidenti vantaggi nel miglioramento dell'efficienza, della riduzione dei costi e del miglioramento della qualità della vita e la maggior parte di queste strutture fisiche sono altamente interconnesse con altre infrastrutture nazionali (e anche internazionali) attraverso sistemi di comunicazione telematici (Alcaraz and Zeadally, 2013).
Tuttavia, questa nuova modalità di monitoraggio rende i sistemi controllo cyber fisici un elemento fortemente critico, a causa delle vulnerabilità informatica del sistema e per la sua sensibilità agli eventi avversi causati da guasti imprevisti o da attacchi intenzionali. Ciò significa anche che le Infrastrutture Critiche e i servizi essenziali che provvedono a fornire alla popolazione - ad esempio acqua, energia o trasporti - dipendono direttamente dal corretto funzionamento dei sistemi informatici di controllo e supervisione che sono parte integrante dei sistemi cyber-fisici che provvedono a gestire le reti fisiche preposte all'erogazione dei servizi ai cittadini. Si tratta dei c.d. "sistemi di controllo distribuito (DCS)" o "controllo di supervisione e sistemi di acquisizione dati (SCADA)", ed entrambi appartengono alla categoria dei Sistemi di controllo industriale (ICS); in particolare, i sistemi SCADA sono componenti fondamentali nelle Infrastrutture Critiche, e influenzano direttamente il livello di servizio di altre Infrastrutture Critiche interconnesse (Alcaraz et al., 2012). Gli SCADA sono costituiti da sistemi integrati hardware e software, dove una serie di processi di controllo risultano distribuiti su vaste aree geografiche e i dati di esercizio dell'infrastruttura sono generalmente centralizzati in un unico punto, il centro di controllo e di supervisione, collegato in rete; pertanto, risultano affetti dalle stesse vulnerabilità che caratterizzano le reti informatiche, in quanto esposti a minacce, di natura volontaria o involontaria, che si aggiungono ai difetti e alle vulnerabilità intrinseche alla tecnologia stessa, potendo facilmente determinare il degrado o, peggio, il blocco dei servizi erogati, causando il temuto effetto a cascata in tutta l'infrastruttura critica e anche tra le altre ad essa interconnesse (Rinaldi, 2004).

LA CYBER SECURITY

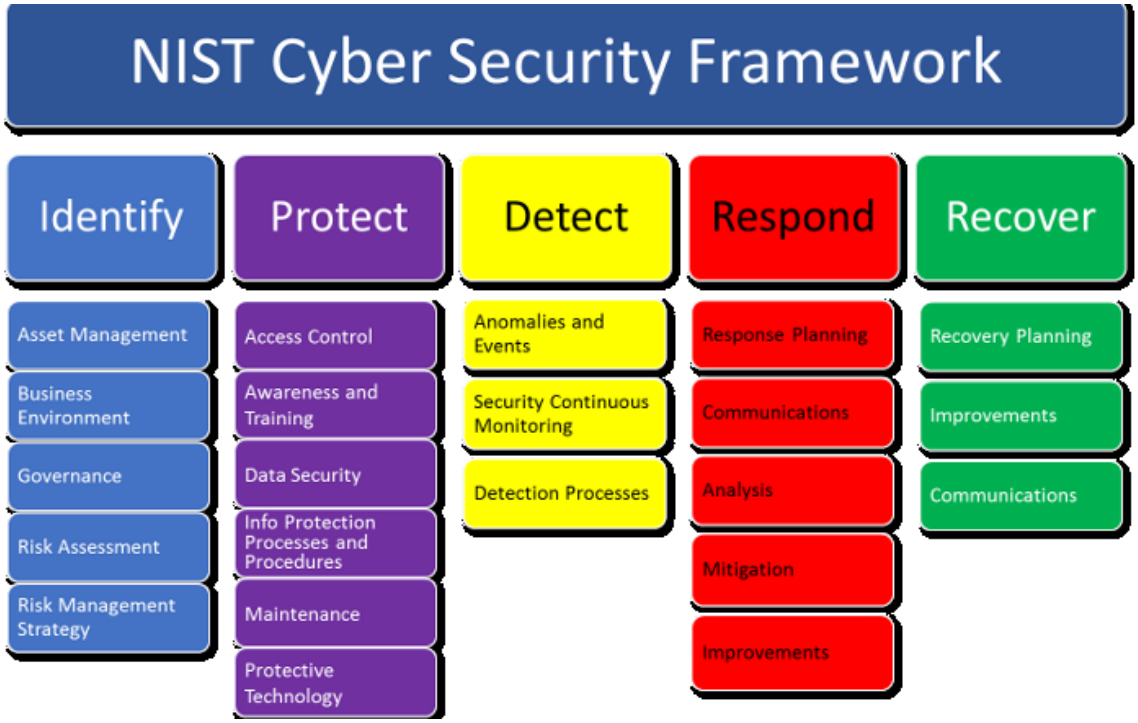
Sicurezza cibernetica: una priorità globale

Mai come in questo periodo sono saliti alla ribalta diversi casi di cyber crime, come quello ai danni di Sony, definito dal Presidente Obama come un attacco alla sovranità degli Stati Uniti, o alle intrusioni nella campagna presidenziale americana, o l'attacco alla rete elettrica ucraina con il malware "Black Energy" che ha disconnesso diverse sottostazioni elettriche della rete, fino ai recentissimi attacchi a siti istituzionali italiani. La crescita esponenziale delle minacce informatiche - dal terrorismo allo spionaggio, al crimine finanziario e oltre – nei confronti di cittadini, aziende e governi, da parte di complesse organizzazioni criminali, ha portato i Paesi di tutto il mondo ad intervenire sul tema della Cyber Security, ossia sul processo, globalmente inteso, che consente la protezione delle informazioni attraverso attività di prevenzione, rilevazione e risposta ad attacchi provenienti dal 'Cyberspazio'.

Il termine Cyber Security è spesso utilizzato in modo intercambiabile con l'espressione Information Security, ma, anche se vi sono oggettivamente molti elementi comuni, questi due concetti non sono sovrapponibili. La Cyber Security va ben oltre i confini della sicurezza informatica tradizionale e include non solo la protezione delle risorse informative, ma anche quella di altri ambiti, tra cui la protezione della persona, delle infrastrutture fisiche, degli assets economici, ecc. Inoltre, la Cyber Security ha come obiettivo principale la protezione dal danno realizzato da una minaccia informatica, oltre la semplice prevenzione dello stesso, con l'individuazione di procedure di identificazione, rilevazione e ripristino, come prevede il "Framework for Improving Critical Infrastructure Cybersecurity", pubblicato nel 2014 dallo statunitense National Institute of Standards and Technology (NIST- U.S. Department of Commerce) e destinato agli operatori delle Infrastrutture Critiche (NIST, 2014; NIST, 2017), in riscontro all'Executive Order n.13636 (EO) emesso dal Presidente degli Stati Uniti Obama nel marzo 2013 per supportare gli Operatori responsabili di servizi e Infrastrutture Critiche nell'implementazione e nella gestione della cyber security allo scopo di aumentare la resilienza e la resistenza agli attacchi cibernetici.

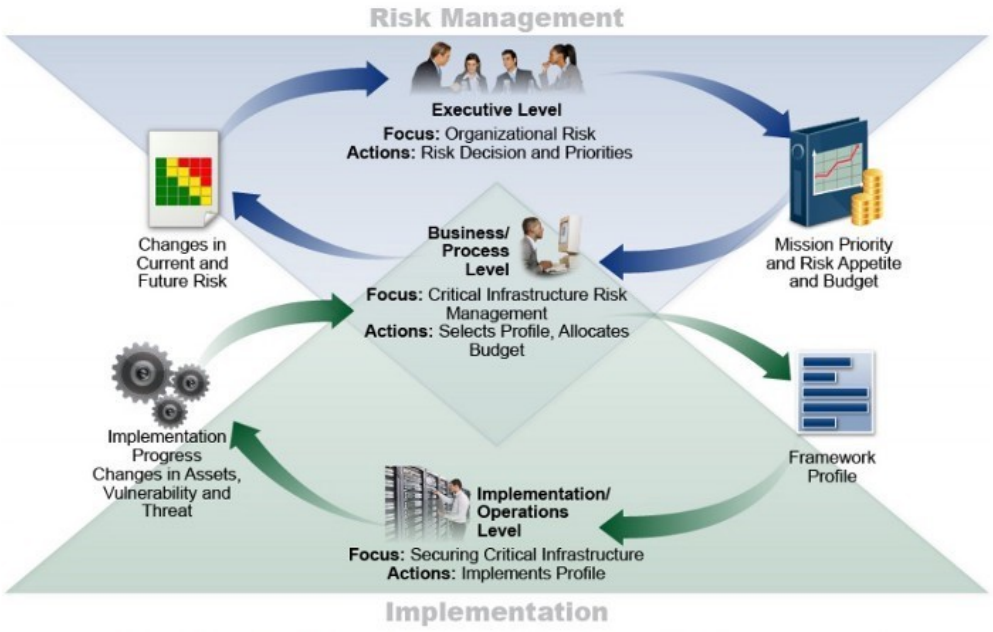
Il Framework, nella sua prima versione, prevede cinque funzioni – articolate in categorie e sottocategorie, relative a regole e controlli di sicurezza – che disegnano uno standard di Cyber Security finalizzato alla protezione di infrastrutture critiche, così delineato:

- *Identify* (sviluppare la comprensione organizzativa della gestione del rischio e della sicurezza informatica di sistemi, risorse, dati e funzionalità);
- *Protect* (sviluppare e implementare adeguate garanzie per assicurare la fornitura di servizi delle infrastrutture critiche);
- *Detect* (avviare e accrescere le attività opportune per rilevare tempestivamente il verificarsi di un'attività anomala e il suo potenziale impatto);
- *Respond* (sviluppare e attuare le opportune azioni, i processi e le procedure da eseguire per garantire una risposta tempestiva agli eventi di sicurezza informatica rilevati);
- *Recover* (sviluppare e implementare le attività idonee a mantenere piani di resilienza e capacità di ripristino di servizi che hanno perso valore, attraverso procedure di recupero).



Fonte: NIST Cybersecurity Framework – (pict. gfacr.org)

Il perseguimento degli obiettivi di sicurezza cibernetica – dall'integrità e responsabilità, fino alla riservatezza, disponibilità e garanzia dei dati – non può che partire dal processo di identificazione dei rischi e la stima delle probabilità di accadimento di una minaccia e del conseguente impatto sull'infrastruttura critica e sui servizi erogati. Il Risk Management, inteso come meccanismo volto ad identificare, controllare e mitigare i rischi del sistema, diventa l'elemento fondante della sicurezza generale dell'infrastruttura, comprendendo la previsione del pericolo, l'analisi costi-benefici, la selezione, implementazione e valutazione dei controlli, l'efficacia e l'efficienza delle azioni per la messa in sicurezza dell'infrastruttura, e l'impatto sulla missione dell'Impresa.



Fonte: NIST - Cybersecurity Framework, versione 1.0.

L'immagine rappresenta graficamente il flusso informativo e decisionale tra i diversi livelli di un'impresa: Executive, Business/Process e Implementation/Operations. Appare evidente che nel modello proposto dal NIST tutti i livelli dell'organizzazione sono coinvolti nel processo di implementazione e potenziamento della cyber security.

Quadro di riferimento

Mai come nel 2016, la Cyber Security è stata al centro dell'attenzione del legislatore europeo, che ha varato un pacchetto di riforme, che si aggiungono alle precedenti normative, il cui principale obiettivo consiste nel miglioramento della protezione delle infrastrutture critiche nell'UE, attraverso l'attuazione della legislazione europea in materia, a livello nazionale.

Con la Direttiva 2008/114/CE, la Commissione – nel definire l'Infrastruttura Critica come *"un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni"* - ha previsto una procedura per l'individuazione e la designazione delle infrastrutture critiche europee (ICE), ossia quelle specifiche infrastrutture, individuate all'interno di ogni Stato, per le quali, un malfunzionamento avrebbe conseguenze significative su almeno un altro Stato membro. Sono state date apposite istruzioni agli Stati membri, e sono state individuate misure dirette a facilitare l'attuazione dell'EPCIP *(European Programme for Critical Infrastructure Protection)*, fra cui un piano d'azione EPCIP, la rete informativa di allarme sulle infrastrutture critiche (CIWIN), il ricorso a gruppi di esperti in materia di protezione delle infrastrutture critiche a livello UE, procedure di scambio di informazioni sulla protezione di tali infrastrutture. La Direttiva, pur se riferita solo ai settori dell'Energia e dei Trasporti, sancisce, quale strumento cardine per la protezione delle Infrastrutture Critiche, l'approccio alla gestione del rischio con una analisi dei rischi basata sul modello classico minacce-vulnerabilità-impatto potenziale.

In questo contesto, il Regolamento n. 910 del 23 luglio 2014 (2014/910/UE), c.d. EIDAS (Electronic IDentification Authentication and Signature), ha stabilito uno standard comune in materia di transazioni elettroniche, sia nei processi aziendali che della Pubblica Amministrazione, intervenendo sui criteri che garantiscono l'identificazione delle controparti, il valore legale dei documenti e della relativa trasmissione, oltre che dei servizi digitali.

Sotto altra angolatura, lo scorso 4 maggio 2016 sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea i testi del Regolamento europeo in materia di protezione dei dati personali e della Direttiva n. 680/2016, che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Il Regolamento n.679/2016, General Data Protection Regulation, c.d. GDPR, sarà applicabile in via diretta a tutti gli Stati membri dal 25 maggio 2018, e sostituirà la Direttiva 95/46/EC, sulla protezione dei dati, avvicendando ai concetti di privacy, trattamento e protezione dei dati, quello globale di sicurezza informatica e di *data protection*. Scopo della norma è l'armonizzazione delle normative sulla protezione dei dati nell'Unione europea, facilitandone così l'osservanza da parte delle imprese extracomunitarie, stabilendo una severa disciplina di protezione dei dati, con rigide sanzioni che possono raggiungere il 4% del volume globale di affari.

Da ultimo, il 6 luglio 2016 è stata pubblicata la Direttiva n. 1148/2016, *Network and Information Security*, c.d. Direttiva NIS, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, che rappresenta l'ultimo avanzamento a livello normativo della legislazione europea in materia di sicurezza cibernetica. La Direttiva NIS impone agli Stati dell'UE obblighi in materia di Security Obligation, Risk Management e Incident Management. La direttiva prevede, per quegli Stati che non ne fossero ancora dotati, l'attuazione di una strategia nazionale che stabilisca obiettivi, politiche di governance e misure proattive. Dovrà essere aumentato il livello di cooperazione tra gli Stati membri, assicurando - attraverso la designazione di autorità competenti a livello nazionale per l'Information security, oltre che un CERT nazionale (Computer Emergency Response Team) in grado di gestire i rischi cyber e in particolare di rispondere in caso di incidenti gravi che coinvolgono le infrastrutture critiche del Paese - meccanismi di cooperazione identificati della Direttiva stessa, anche attraverso la creazione di un gruppo di collaborazione che faciliti i rapporti tra gli Stati, composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA (European Union for Network and Information Security Agency).

La Direttiva si rivolge agli operatori delle Infrastrutture Critiche, obbligando queste entità a dotarsi di misure di sicurezza appropriate per prevenire i rischi, garantire la sicurezza dei sistemi e delle reti, oltre che dei dati; ed infine a dimostrare la capacità di gestire le minacce, notificando all'autorità nazionale competente gli incidenti di sicurezza, sulla base di parametri che considerano il numero di utenti coinvolti, la durata dell'incidente e la sua diffusione geografica. Ciascuno Stato interno dovrà identificare le IC all'interno di ambiti strategici quali energia, trasporti, banche e sistema finanziario, salute, acqua ed infrastrutture digitali, secondo criteri parametrati alla dipendenza da sistemi informatici, alle ricadute su prestazioni di servizi essenziali, alla stessa importanza economico-sociale del servizio offerto. Anche i fornitori di servizi digitali, quali mercati on-line, motori di ricerca e servizi cloud, saranno tenuti, secondo la direttiva NIS, ad attuare misure di sicurezza appropriate e a notificare incidenti rilevanti, al pari degli operatori di servizi essenziali. Sono invece escluse dalla Direttiva le piccole e medie imprese.

La politica di sicurezza cibernetica in Italia

Il D. Lgs. 61/2011 ha recepito la Direttiva n.114 del 2008 ed ha specificato "le modalità di valutazione della sicurezza di tali infrastrutture e le relative prescrizioni minime di protezione dalle minacce di origine umana, accidentale e volontaria, tecnologica e dalle catastrofi naturali" (art. 1); ha istituito il Nucleo Interministeriale Situazione e Pianificazione (NISP) presso la Presidenza del Consiglio, composto da rappresentanti di vari ministeri; ha definito, per l'Italia, il Piano di Sicurezza per gli Operatori delle Infrastrutture Critiche Europee (PSO). Quest'ultimo deve contenere l'analisi dei rischi, delle vulnerabilità, delle minacce e del potenziale impatto nel caso di mancato funzionamento dell'infrastruttura. Al NISP sono affidate l'individuazione e la designazione delle ICE, la struttura responsabile (Segreteria per le IC, SIC) per le attività tecniche e scientifiche necessarie per le funzioni dello stesso Nucleo Interministeriale e per i rapporti con la Commissione e gli altri Stati Membri interessati dalle ICE che l'Italia intende designare.

Con il D.P.C.M. del 24 gennaio 2013, recante gli "indirizzi per la protezione cibernetica e la sicurezza informatica aziendale", l'Italia si è dotata del primo strumento legislativo per l'ordinamento della sicurezza cibernetica nazionale che ha riconosciuto la necessità di dotare la Nazione di una struttura per la protezione dalle minacce *cyber*, innovando rispetto al dettato normativo europeo precedente, attraverso una definizione più ampia di Infrastruttura Critica, riferita alla "…tutela dell'interesse nazionale relativamente alla infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica…"(art.1).

In attuazione del D.P.C.M. 24/01/2013, sono stati pubblicati due importanti documenti in tema di Sicurezza delle Informazioni: il "Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico" e il "Piano Nazionale per la Protezione Cibernetica e la sicurezza informatica". Il primo documento presenta la posizione strategica italiana per quanto attiene alla sicurezza del Cyberspace: individua le minaccia e le vulnerabilità per i sistemi e le reti di interesse nazionali, oltre che le linee d'azione e gli strumenti per potenziare e difendere il dominio cibernetico del Paese, stabilendo che la protezione dello spazio cibernetico è un processo, più che un fine, e introducendo il principio che occorrono misure proattive e reattive contro gli attacchi cyber.
Il Quadro Strategico individua 6 obiettivi strategici che riguardano: il miglioramento delle capacità operative e tecnologiche degli attori istituzionali impegnati nel contrasto alla minaccia cyber; il potenziamento della capacità di difesa delle Infrastrutture Critiche nazionali; l'incentivazione della cooperazione tra Istituzioni e imprese private; la promozione della cultura della sicurezza con un crescente coinvolgimento del mondo delle università e della ricerca; il rafforzamento della capacità di contrasto alla diffusione di attività e contenuti illegali online; il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica. Per conseguire tali obiettivi, sono stati individuati 11 indirizzi operativi, maggiormente delineati e dettagliati nel "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica" pubblicato contestualmente al Quadro Strategico, relativi al potenziamento delle capacità di intelligence, all'identificazione di una Autorità nazionale NIS (Network and Information Security) che cooperi con le altre autorità omologhe a livello internazionale. E' prevista la promozione della cultura di

cyber security, oltre che della formazione e addestramento di tutti gli attori coinvolti nell'impiego delle ICT, il rafforzamento della cooperazione internazionale, l'adeguamento normativo, anche con elaborazione ed adozione di norme tecniche, alla cooperazione con il "comparto" industriale e le PMI, l'attribuzione ai settori strategici della PA di risorse umane, finanziarie, tecnologiche e logistiche per il perseguimento degli obiettivi programmatici, e l'implementazione di un sistema integrato di Information Risk Management nazionale. Viene previsto anche di dare piena attuazione al CERT (Computer Emergency Response Team) Nazionale, individuato nell'ambito del Ministero dello Sviluppo Economico ai sensi dell'art. 16 bis del D.lgs. n. 259/2003, unitamente al CERT-PA. Il CERT nazionale deve essere sviluppato sulla base di un modello cooperativo pubblico-privato, collegando i CERT operanti sul territorio nazionale e interfacciandosi con il CERT europeo e i CERT di altri Stati. Il CERT-PA, evoluzione del CERT-SPC previsto dal D.P.C.M. del 01/04/2008, invece, è il punto di riferimento delle Pubbliche Amministrazioni e collabora con i suoi omologhi europei ed internazionali.

La direzione e l'organizzazione delle attività del CERT della Pubblica Amministrazione è assegnata all'AgID - Agenzia per l'Italia Digitale, istituita con Decreto-Legge n.83/2012, convertito in L.134/ 2012 – con funzioni e compiti di innovazione tecnologica e sviluppo della pubblica amministrazione, che, il 26/9/2016, ha pubblicato il documento delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni", in attuazione della corrispondente direttiva della Presidenza del Consiglio dei Ministri del 1 agosto 2015. Tali misure prevedono tre diversi livelli di attuazione e costituiscono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione. Il documento richiama espressamente i contenuti del "Framework Nazionale per la Cyber Security", realizzato dal CIS-Sapienza e dal Laboratorio Nazionale di Cyber Security, in collaborazione con diverse organizzazioni pubbliche e private, il quale, a sua volta, condivide l'impianto generale del "Framework for Improving Critical Infrastructure Cybersecurity" del NIST, inserendosi in un processo di standardizzazione e compliance tra soggetti pubblici e soggetti privati per la cyber security.

L'attuale quadro normativo dovrebbe essere revisionato a breve termine. E' stato deciso, infatti, nella riunione del Comitato Interministeriale per la Sicurezza della Repubblica, presieduto dal Presidente del Consiglio, tenutasi il 17 febbraio scorso[14], che verrà emanato un nuovo decreto, che sostituirà il D.P.C.M. 24 gennaio 2013, nelle more del recepimento della Direttiva Nis, e che dovrà prevedere una risposta coordinata di tutte le strutture competenti agli eventi cibernetici significativi, una forte interazione con l'AgID, il coinvolgimento del mondo accademico e della ricerca, oltre che la possibilità di avvalersi della collaborazione diffusa delle imprese di settore. La funzione direttiva e di coordinamento delle politiche di sicurezza cibernetica, con l'adozione di iniziative idonee a definire le necessarie linee d'azione verrà affidata al Dipartimento delle informazioni per la sicurezza - DIS[15], che verrà dunque rafforzato e posto in posizione strategica nel futuro programma nazionale di cyber security.

La protezione delle infrastrutture critiche nazionali

L'erogazione di servizi strategici attraverso le infrastrutture critiche nazionali è data per scontata ma, a causa delle interdipendenze tra le stesse, un'interruzione o un malfunzionamento nella fornitura di un servizio può causare interruzioni a catena che possono ripercuotersi anche sull'erogazione di altri servizi essenziali, con ripercussioni in settori che potrebbero sembrare apparentemente non correlati. La protezione delle Infrastrutture Critiche è quindi divenuta indispensabile per la rilevanza che rivestono nella vita quotidiana dei cittadini e dello Stato. La crescente consapevolezza della dipendenza delle infrastrutture critiche dalla tecnologia ICT rende particolarmente

[14] http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html

[15] Nato a seguito della Legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto ", pubblicata nella Gazzetta Ufficiale n. 187 del 13 agosto 2007, e relativa alla riforma dei servizi segreti italiani.

importante la sicurezza informatica dei relativi sistemi rispetto alle possibili minacce. I sistemi di controllo industriale maggiormente utilizzati sono i sistemi SCADA (Supervisory Control and Data Acquisition), che costituiscono il sistema di supervisione e controllo dei sistemi Cyber-fisici (CPS) e, tra l'altro, parte integrante delle infrastrutture critiche nazionali utilizzate per l'erogazione di servizi strategici (o essenziali) rappresentati dalla fornitura di energia elettrica, acqua, gas, assistenza sanitaria e tutti i servizi di telecomunicazioni.

Sono molte le componenti che spiegano la ragione di tanta attenzione: motivi politici, geopolitici, sociali e tecnici hanno portato in primo piano il tema della sicurezza cibernetica e la protezione di questi sistemi, che costituiscono parte integrante e fondamentale delle Infrastrutture Critiche Nazionali ed Europee, è diventata una priorità nell'Agenda politica nazionale ed europea. Dal punto di vista tecnico è utile evidenziare che in passato i sistemi di controllo e supervisione di processo venivano utilizzati prevalentemente in processi industriali e avevano caratteristiche tali da renderli praticamente immuni dalle minacce provenienti dal cyber spazio poiché, non essendo collegati in rete internet e utilizzando per lo più protocolli informatici per lo scambio dei dati che erano di tipo proprietario, risultavano più difficili da connettere digitalmente e/o da raggiungere fisicamente per potervisi collegare.

Queste infrastrutture nazionali hanno evidenziato in numerose occasioni la loro vulnerabilità agli attacchi cibernetici, non a caso, l'attenzione al fenomeno del cyber crime da parte dei Governi nazionali è sempre più elevata. Infatti, la vulnerabilità delle infrastrutture critiche e l'elevato rischio connesso si è manifestato chiaramente in recenti episodi di cyber-crime a danno di infrastrutture critiche, che oltretutto si verificano sempre con maggiore frequenza, che hanno mostrato che le e-mail, le transazioni bancarie, i video, le foto o qualsiasi altra informazione digitale che può essere trasmessa ed elaborata da una rete informatica rappresentano dei veicoli spesso inconsapevoli di malware utilizzati per sferrare i cyber attack.

Ritornando al tema delle Infrastrutture Critiche e dei Servizi Strategici, dunque quest'ultime hanno conquistato un ruolo centrale dovuto ad un numero sempre più ampio di attività quotidiane che ne fanno uso, configurandosi come una grande piattaforma trasversale e irrinunciabile, per l'erogazione di servizi essenziali in tutti settori pubblici o

privati, ma allo stesso modo in grado di provocare impatti devastanti in caso di blocco della rete dovuto a cause naturali (poco probabili) o a causa di attacchi di natura dolosa e intenzionale. Per quanto detto sopra, il tema della sicurezza e della qualità delle reti e dei sistemi informativi ha assunto una rilevanza molto elevata poiché il rischio di una avaria di sistema, avrebbe conseguenze immediate sulle comunicazioni, sulla produzione e distribuzione di energia elettrica o idrica, sui trasporti e sul sistema produttivo nazionale, con effetti che potrebbero estendersi sino a livello di sistemi di governo.

In ambito internazionale, negli ultimi anni sono emerse nuove minacce nel dominio cibernetico, la cui dinamica geopolitica globale risulta sempre più evidente: Stati e Governi si avvalgono di raffinati strumenti informatici, delle vere e proprie *Cyber-weapon*, allo scopo di imporre la propria egemonia politica, economica e militare. La "*Cybewarfare*" o il "*Cyber-terrorism*" sono dimensioni che ormai si affiancano al *cyber-crime* con caratteristiche tali da rappresentare un notevole potenziale offensivo, e i Sistemi Cyber-fisici, obiettivi considerati strategici in quanto elementi costitutivi di Infrastrutture Critiche Nazionali, sono bersagli primari. A rendere ancor più elevato il rischio, concorre l'aspetto non secondario che la maggior parte dei sistemi critici infrastrutturali non sono stati progettati tenendo in considerazione la sicurezza cibernetica poiché l'obiettivo principale era quello di garantire la maggiore continuità di servizio possibile.

In quest'arena globale, dunque, la cyber security nelle Infrastrutture Critiche è diventata una priorità nazionale e i Governi si sono da tempo attivati per sollecitare gli Operatori, siano essi soggetti pubblici o privati, per implementarla al massimo livello di efficacia possibile.

IL CYBER RISK MANAGEMENT

Risk management e Infrastrutture Critiche

La prima attività fondamentale da avviare per la protezione delle infrastrutture critiche è quella relativa all'implementazione di un modello di risk management di qualità: nel campo della sicurezza cibernetica, il risk management ne diventa parte integrante, adattandosi al contesto specifico e assumendo una forma più evoluta rispetto a quella tradizionalmente conosciuta.

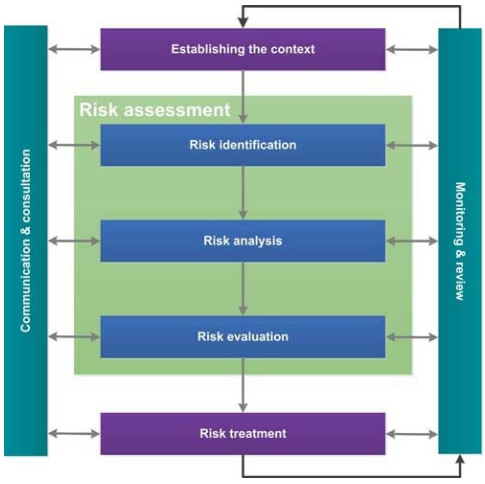
Un approccio risk-based applicato alla complessità della cyber security può offrire notevoli vantaggi, poiché un'adeguata stima del cyber risk consente di attivare un livello bilanciato di protezione e di contromisure informatiche in risposta ad eventuali cyber attack. Il bilanciamento è senza dubbio opportuno, poiché la cyber security non si implementa a costo zero ma, al contrario, presenta dei costi significativi che tendono oltretutto a crescere esponenzialmente all'aumentare del livello di sicurezza informatica che si è deciso di raggiungere.

Il risk management è dunque una delle principali attività da prevedere per definire un'adeguata protezione rispetto ad eventuali cyber attacchi, allo scopo di proteggere le infrastrutture critiche e i relativi servizi strategici erogati. La letteratura offre molti riscontri in tal senso ed è necessario considerare tutti i fattori chiave in grado di offrire un contributo per la corretta identificazione del reale livello di rischio a cui è soggetto un determinato sistema.

La definizione di "risk management" inteso come processo di gestione del rischio, è riportata nello standard internazionale ISO 31000:2009 "Risk management -- Principles and guidelines", aggiornato a dicembre 2016 (ISO, 2016) e nello standard ISO/IEC 27005:2011 "Information technology — Security techniques — Information security risk management" (seconda edizione) (ISO, 2011).

Il processo di Risk Management definito nello standard ISO31000 è rappresentato graficamente nella seguente figura:

(Fonte: AS/NZS ISO 31000:2009)



L'ISO 31000:2009 (ISO, 2009) è uno standard internazionale definito dalla International Organization for Standardization (ISO)[16] che fornisce i principi e le linee guida per una gestione efficace del rischio. Utilizza un approccio generico e può essere applicato a qualsiasi tipo di rischio, sia esso di tipo finanziario, naturale o tecnologico e applicato a qualsiasi organizzazione. Include raccomandazioni generali per costituire un risk management framework e per definire un risk management process e include termini e definizioni rilevanti per il tema, quali:

- ***Risk*** – "gli effetti dell'incertezza su obiettivi" (ISO, 2009, 2.1 def.) o, per meglio dire, gli effetti dell'incertezza sulla capacità di un'impresa di raggiungere i propri obiettivi;
- ***Risk management*** – "attività coordinata per dirigere e controllare un'organizzazione in materia di rischio" (ISO, 2009, 2.2 def.);
- ***Risk Assessment*** – è il "processo di identificazione dei rischi, analisi dei rischi e valutazione dei rischi" (*risk identification*, *risk analysis*, e *risk evaluation*) (ISO, 2009, 2.14 def.), dove l'identificazione dei rischi è il "processo di individuazione, riconoscimento e descrizione dei rischi" (ISO, 2009, 2.15 def.), l'analisi dei rischi è il "processo di comprendere la natura del rischio e per determinare il livello di rischio" (ISO, 2009, 2,21 def.) e la valutazione del rischio è il "processo di confronto dei risultati delle analisi dei rischi con criteri di rischio per determinare

[16] L'International Organization for Standard (ISO) è un'organizzazione internazionale senza scopo di lucro con sede a Ginevra e composta da 163 Paesi membri, sparsi in tutto il pianeta. http://www.iso.org

se il rischio e/o la sua magnitudine è accettabile o tollerabile"(ISO, 2009, 2.24 def.).

Gli approcci più comuni al risk assessment sono fondamentalmente di tre tipi: il primo è il c.d. *Approccio qualitativo* e la valutazione del rischio si basa su parametri definiti su una scala qualitativa esprimendone la magnitudo in termini non numerici; il secondo è il c.d. *Approccio quantitativo* che consiste nell'esprimere in valori numerici i risultati delle valutazioni effettuate; infine l'*Approccio semi-quantitativo è* costituito dalla combinazione di metodi qualitativi e quantitativi dove solitamente prima vengono individuati gli indicatori in maniera qualitativa, in seguito espressi in termini quantitativi, per essere successivamente utilizzati in calcoli di tipo numerico.

- ***Risk Treatment*** – è il processo di modifica del rischio a seguito di un intervento (ISO, 2009, 2.25 def.).

In tema di Risk management, a contorno e completamento dello standard ISO31000, l'International Standard Organization ha rilasciato ulteriori standard:

- ISO Guide 73:2009 Risk Management: Vocabulary.
- ISO 31004:2013 Guidance for implementation of ISO 31000.
- ISO 31010:2009 Risk assessment guide.

In sintesi, gli standard della famiglia ISO31000, inquadrano il *Risk Management* come un *processo strategico* finalizzato ad assumere decisioni consapevoli che tengano l'elemento *rischio* in debita considerazione.

La valutazione del rischio nel cyber spazio

Gli attacchi nel mondo cibernetico sfruttano le vulnerabilità di un sistema complesso che possono essere di natura tecnica, organizzativa, di processo, o anche in combinazione tra loro. Le vulnerabilità organizzative e di processo sono riconducibili in buona parte alla mancanza di misure di protezione informatica, come l'esercizio di buone pratiche di gestione o misure inadeguate di protezione anti-virus e anti-spam, che possano impedire a malware di penetrare il sistema e di provocare effetti dannosi sull'infrastruttura informatica e sui servizi da essa erogati; le vulnerabilità tecniche, invece, sono

riconducibili a falle di sicurezza del software applicativo o di sistema, nonché degli apparati di rete e di gestione di comunicazione dati.

Si rende necessario, pertanto, *individuare* e ridurre al massimo dette vulnerabilità, in particolare nel caso in cui si tratti di sistemi o reti di interesse nazionale, progettando un piano di prevenzione che faccia dell'analisi del rischio l'elemento fondamentale dai cui partire per mettere a punto un insieme di interventi da porre in essere per la gestione e la mitigazione del rischio cibernetico e per la definizione di una serie di misure di sicurezza fisica, logica e organizzativa.

Il *risk assessment* è, dunque, una fase fondamentale del più ampio risk management e può essere condotto utilizzando metodologie diverse. Nel mondo cyber l'approccio 'tradizionale' mostra chiari limiti, poiché l'evoluzione del rischio è estremamente rapida e mutevole rispetto a scenari più consolidati.

Rispetto alla sequenza lineare che caratterizza un tipico processo di risk management, l'approccio Cyber richiede costanti verifiche (feed-back) per riscontrare gli esiti degli interventi di cyber security implementati. L'elemento di svolta si è presentato nel febbraio 2014 quando il National Institute of Standards and Technology (NIST) ha presentato la prima versione del "Framework for Improving Critical Infrastructure Cybersecurity" (NIST, 2014), come descritto in precedenza nel presente lavoro, un framework nazionale non prescrittivo, messo a punto per proporre alle organizzazioni un approccio omogeneo ed efficace all'analisi del rischio per definire interventi di cyber security finalizzati a ridurre il rischio legato alle minacce provenienti dal cyber space. Il framework propone una metodologia sistematica facile da adottare per il cyber risk management e rappresenta un modello da applicare nella realtà organizzativa o industriale che aiuta a comprendere, identificare i rischi e proteggere i dati strategici e gli assets tecnologici e come rispondere e recuperare in caso di attacco dal cyber spazio.

In Italia il *Framework Nazionale per la Cyber Security* è stato prodotto dal CIS-Sapienza e il Laboratorio Nazionale di Cyber Security, in collaborazione con diverse organizzazioni pubbliche e private. Il *Framework Nazionale per la Cyber Security* e il *Cyber Security Report 2015* sono stati elaborati in chiave nazionale allo scopo di offrire alle organizzazioni e alle PMI un approccio omogeneo per affrontare la cyber security aumentando la resilienza delle imprese nei confronti della minaccia cyber. L'approccio

proposto nel framework italiano ricalca il *Framework for Improving Critical Infrastructure Cybersecurity* statunitense (NIST, 2014, NIST, 2017), ampliato e adattato al contesto italiano e propone un modello per incrementare il livello di cyber security orientato alla Piccola Media Impresa italiana, oltre che un pacchetto di raccomandazioni destinate al top management di grandi aziende e Operatori di infrastrutture critiche su come organizzare processi di cyber security risk management.

Ipotesi di ricerca e review della letteratura

Nel presente lavoro, si affronta in maniera sistematica il tema "caldo" della Cyber Security, un ambito che, come abbiamo visto, coinvolge governi nazionali, settori militari, servizi di informazione, il sistema economico e il mondo delle imprese nel suo complesso e, via via e a vario titolo e grado di interesse, ogni singolo cittadino del mondo. Questo scenario inedito è fortemente connotato da elevata incertezza, varietà e multilateralità delle minacce e, pertanto, si ritiene che l'applicazione sic et simpliciter delle tecniche "tradizionali" di valutazione del rischio, di derivazione aziendale o finanziaria, possa risultare inadeguata allo scopo, nonostante si rilevi che un certo grado di adattamento al nuovo scenario sia attualmente in corso.

L'analisi si concentra sulla ricerca di una sorta di "evoluzione adattativa" che sembra stia interessando il risk management nel contesto cyber, osservando lo "stato dell'arte" nel panorama accademico e scientifico mondiale nell'introduzione di nuovi e più evoluti metodi o modelli specifici per l'analisi e la valutazione del cyber risk.

Le ipotesi di ricerca che tracciano la direzione della presente indagine devono considerare che affrontare la valutazione del rischio cibernetico utilizzando le consuete tecniche di valutazione del rischio potrebbe non essere sufficiente a valutare adeguatamente il rischio e i danni derivanti da attività ostili e/o illegali di tipo informatico(**HP1**).

Inoltre, ipotizzando che l'analisi dello stato dell'arte della ricerca accademica in tema di rischio cibernetico evidenzi lo sviluppo di nuovi e specifici strumenti o l'evoluzione di altri già presenti, non è detto che gli stessi possano essere efficacemente impiegati in un contesto economico-organizzativo reale come quello di un'impresa (**HP2**).

Queste ipotesi rappresentano il punto di partenza dell'indagine scientifica che si intende effettuare.

Dal punto di vista metodologico si è scelto di affrontare la prima ipotesi (HP1) con un'analisi dell'avanzamento della ricerca nella letteratura scientifica e la seconda (HP2) con un caso di studio.

La prima ipotesi di ricerca si pone l'obiettivo di fornire una panoramica globale della letteratura scientifica attualmente disponibile in tema di valutazione del rischio nel contesto cibernetico; si analizzerà la produzione scientifica pubblicata nell'ultimo decennio utilizzando l'approccio metodologico della c.d. "**state-of-the-art review**".

State-of-the-art review

L'attività di ricerca è condotta attraverso una revisione della letteratura sulla base di quadro metodologico che individua una sequenza di procedure da realizzare secondo un protocollo predefinito. Attraverso questo processo di analisi, si intende identificare, valutare e interpretare tutti i lavori e le ricerche pubblicate che risultano rilevanti per l'argomento in questione, allo scopo di individuare i recenti progressi, quali dibattiti sono in corso e se emergono o meno lacune significative nella ricerca e, nel caso, trarne spunti sui quali indirizzare future attività di ricerca. Sui differenti approcci da adottare e su quali siano le metodologie più efficaci da adottare nelle review della letteratura, è in corso un significativo dibattito nella comunità scientifica. Tra i numerosi articoli che trattano l'argomento, il lavoro di analisi e classificazione svolto da M. J. Grant e A. Booth si caratterizza per una proposta di una classificazione molto dettagliata e applicabile a tutti i contesti di ricerca, incluso il presente; pertanto, si è deciso di adottare il modello della c.d. "*state-of-the-art review*", ricompresa nelle quattordici tipologie di review della letteratura (con relative metodologie) classificate nel loro lavoro (Grant and Booth, 2009).

La State-of-the-art review, tende ad individuare i lavori di ricerca più rilevanti in uno specifico settore, riguardanti un determinato argomento, allo scopo di costruire un chiaro quadro di sintesi su filoni di ricerca attuali ed emergenti, sulle priorità della ricerca e sulla presenza o meno di lavori c.d. "di frontiera".

Produrre una State-of-the-art review di qualità, consente di individuare nella letteratura corrente quali sono i lavori di ricerca che rappresentano una discontinuità con i precedenti o una significativa evoluzione nel settore, e ciò risulta in linea con gli obiettivi di analisi del presente lavoro che, si rammenta, è focalizzato sulla ricerca di una componente 'evolutiva' che interessi gli strumenti per la valutazione del rischio nell'era cibernetica e dello stato dell'arte nel panorama accademico e scientifico mondiale, oltre che l'introduzione di nuovi e più evoluti strumenti per l'analisi del Cyber Risk.

Metodologia:

Si intende affrontare la review della letteratura adottando un approccio rigoroso, molto simile a quello seguito dalla più rigida Systematic Literature Review, che prevede che le varie fasi del processo di review siano condotte in modo rigoroso, trasparente e replicable (CRD, 2001). Pertanto, nella presente state-of-the-art review si adottano i medesimi principi: rigore, trasparenza e replicabilità; il processo di review seguirà una precisa sequenza di attività e sarà documentato nel suo svolgimento in modo sufficientemente dettagliato da consentirne la replicabilità. Dal punto di vista strettamente metodologico la state-of-the art review si differenzia dalla review sistematica per non doversi necessariamente attenere ad una valutazione di qualità di tipo formale e, naturalmente, per la facoltà di poter restringere il campo di analisi al solo "stato dell'arte" della ricerca accademica.

L'adozione di un approccio rigoroso aumenta l'affidabilità dei risultati della review rispetto ad altri modelli di indagine non supportati da rigore metodologico (Mays et al., 2001). La presente attività di review, pertanto, si articolerà seguendo una precisa sequenza:

1. individuare gli studi e gli articoli più rilevanti in tema di cyber risk assessment in Infrastutture Critiche;
2. definire la domanda di ricerca;
3. selezionare le basi dati da utilizzare per la ricerca degli articoli;
4. definire i criteri di selezione degli articoli (le chiavi e le modalità di ricerca sui database);
5. definire e applicare i criteri di inclusione ed esclusione degli articoli pubblicati;

6. analizzare e fornire una breve sintesi dei contenuti dei lavori considerati più rilevanti;
7. classificare gli articoli selezionati;
8. considerazioni finali.

Fase 1: prima ricognizione

Partendo dall'ipotesi di ricerca definita in precedenza (HP1), si è effettuata una prima ricerca tra le riviste accademiche sul tema del Cyber Security Risk Management, con l'obiettivo di definire il perimetro di ricerca e di individuare la terminologia comunemente utilizzata allo scopo di definire le parole chiave da utilizzare nel processo di ricerca degli articoli accademici all'interno dei database. La prima ricerca è stata effettuata utilizzando l'opzione "ricerca "globale" e utilizzando la keyword di ricerca generica "cyber security" per la ricerca degli articoli nei database. Il sistema informativo della biblioteca di Ateneo ha effettuato la ricerca completa sul catalogo informatico e ha prodotto un elenco di ben 18921 articoli, dei quali 10966 pubblicati su riviste peer-reviewed. In successive ricerche, alla keyword principale, si sono aggiunti altri termini più specifici, seppur generici, come "risk", "assessment" o "SCADA", e ciò ha ridotto significativamente il numero di pubblicazioni individuate e aumentato la pertinenza degli articoli all'argomento oggetto della presente indagine. L'attività di selezione e di lettura sommaria degli abstract ritenuti attinenti all'argomento trattato, ha evidenziato l'uso ricorsivo di numerosi vocaboli. Tra questi, si selezioneranno successivamente le keyword da utilizzare per l'estrazione degli articoli dai database.

Fase 2: definizione della research question

A valle dell'attività di ricognizione dei contributi scientifici nell'ambito del cyber risk, osservato nella prospettiva delineata dall'ipotesi di ricerca, si procede alla definizione della domanda di ricerca che si definisce, rimodulando l'ipotesi di ricerca (HP1), come segue:

*"**Q1** - L'eterogeneità e la multilateralità delle minacce nel cyber-space richiede nuovi strumenti per la valutazione del rischio?"*

Si tratta di una domanda di ricerca volutamente ampia e aperta, poiché nella fase iniziale della selezione degli articoli accademici deve poter raccogliere contributi che potrebbero risultare apparentemente distanti rispetto al mainstream di settore.
Analogamente, si procede alla definizione della seconda domanda di ricerca che si definisce, rimodulando l'ipotesi di ricerca (HP2), come segue:

*"**Q2** - in un contesto economico-organizzativo reale e complesso come quello di una grande Impresa, nuovi e specifici strumenti o l'evoluzione di altri già presenti, rivenienti dal mondo della ricerca, sono direttamente ed efficacemente impiegati?"*

A questa seconda domanda di ricerca si risponderà più avanti, con uno studio di caso.

Fase 3: selezione dei database

I contributi sono stati selezionati accedendo ai database disponibili on-line, attraverso l'accesso riservato, nella rete intranet dell'Università degli studi di Salerno.
Le attività di ricerca "operativa" della literature review inizia con la definizione delle fonti informative da utilizzare per l'attività di estrazione della letteratura presente sull'argomento in questione.

Fonti informative utilizzate per la ricerca degli articoli della literature review:

Fonte	Tipo	URL Internet
ISI Web of Knowledge	Database	http://www.isiknowledge.com/
Wiley Online Library	Database	http://onlinelibrary.wiley.com/
IEEE Xplore	Database	http://www.ieexplore.ieee.org/
SpringerLink	Database	http://link.springer.com/
ScienceDirect (Elsevier e-journal)	Database	http://www.sciencedirect.com/
Scopus	Database	https://www.scopus.com/home.uri
Emerald Insight	Database	http://www.emeraldinsight.com/
The ACM Digital Library	Database	http://portal.acm.org/

Per completezza di esposizione, si segnala che l'accesso di Ateneo a Web of Science comprende l'accesso ai motori di indicizzazione Science Citation Index Expanded, Social Science Citation Index, Arts and Humanities Citation Index, Conference Proceedings

Citation Index-SCIENCE (CPCI-S), Conference Proceedings Citation Index-SOCIAL SCIENCE & HUMANITIES (CPCI-SSH), che si vanno ad aggiungere ad altri motori di ricerca come JCR–Journal Citation Reports o come Human Resources Abstracts (EBSCO).

Fase 4: criteri di selezione

Definite le basi dati da utilizzare per la ricerca degli articoli scientifici presenti in letteratura, si procede con la definizione dei criteri generali da applicare nella ricerca informatica dei contributi scientifici presenti in letteratura.

I criteri generali da utilizzare per le query sui database sono così definiti:

- la finestra temporale di ricerca degli articoli è limitata agli ultimi 10 anni (dal 01/01/2007 al 31/12/2016);
- la ricerca è circoscritta alle sole riviste scientifiche presenti nei database selezionati. Non è presa in considerazione la c.d. Grey literature, books, technical reports, articoli pubblicati su riviste non accademiche;
- sono presi in considerazione esclusivamente articoli sottoposti a peer review;
- per la ricerca degli articoli all'interno delle basi dati si utilizzano chiavi di ricerca (keyword) multiple, predisponendo "query" composte da più parole chiave concatenate tra loro con logica di tipo booleano.

Definiti i criteri generali di ricerca, si procede con la definizione dei termini da utilizzare nella ricerca degli articoli all'interno delle basi dati selezionate.

Processo di ricerca ed estrazione degli articoli

La prima attività di selezione operata è relativa alla finestra temporale presa in considerazione, fissata dal 1 gennaio 2007 al 31 dicembre 2016, per un intervallo temporale totale di anni 10. In questo caso la "ricerca globale" utilizzando la keyword generica "***cyber security***" ha individuato **7888** articoli pubblicati su riviste peer-reviewed (12615 articoli totali).

Il passo successivo consiste nell'escludere tutti gli articoli che non ricadono nelle Subject Area attinenti o connesse al contesto Cyber, considerate nelle varie declinazioni: crime, security, protection, smard grid, terrorism, ecc. Operativamente si selezionano le subject

area di interesse e, mantenendo invariati i parametri di selezione impostati nella ricerca precedente, si effettua nuovamente la ricerca nei database. Il risultato della query, espresso in termini quantitativi, è riportato nella seguente tabella:

Subject Area ricerca con keyword '***cyber security***'	**Numero di articoli complessivi risultanti dalla ricerca**	**Riviste Peer reviewed**	**Percentuale articoli non soggetti a peer-review**
Computer Crime	73	62	15,07%
Computer Information Security	584	569	2,57%
Computer security	410	331	19,27%
Cyber Security	414	264	**36,23**%
Cybersecurity	0	0	-
Cyber terrorism	136	123	9,56%
Information security	218	143	**34,40**%
Information warfare	24	14	**41,67**%
Information Technology	377	306	18,83%
Internet security	123	110	10,57%
Management	148	135	8,78%
Network security	530	444	16,23%
Risk assessment	0	0	-
Risk Management	0	0	-
Security & protection	459	457	0,44%
Security Management	651	624	4,15%
Smart Grid	269	192	28,62%
Terrorism	151	126	16,56%
Totale	**4567**	**3900**	14,60%

La tabella riporta il risultato della ricerca effettuata applicando i criteri di selezione stabiliti, integrati da una seconda scrematura effettuata limitando la selezione alle sole subject area ritenute rilevanti. Il processo di selezione ha restituito 4567 articoli presenti su riviste accademiche, dei quali **3900** risultano pubblicati su journal peer reviewed. Il processo di selezione continua con l'eliminazione dei duplicati, poiché uno stesso lavoro può ricadere in più subject area, rischiando di venir considerato più di una volta nel totale

numerico. Al termine del processo di selezione utilizzando la parola chiave *cyber security*, risultano selezionati ben **2165** articoli pubblicati su riviste peer reviewed.

La seconda attività di selezione operata è relativa alla stessa finestra temporale già presa in considerazione, utilizzando la keyword generica "***cyber risk***"; la ricerca ha individuato 6109 articoli pubblicati su journal peer-reviewed (8093 articoli in totale).

Anche in questo caso il passo successivo consiste nell'escludere tutti gli articoli che non ricadono nelle Subject Area attinenti o connesse al contesto Cyber, nelle varie declinazioni: crime, security, protection, smard grid, terrorism, ecc.

Il risultato della query, espresso in termini quantitativi, è riportato nella seguente tabella:

Subject Area ricerca con keyword '***cyber risk***'	**Numero di articoli complessivi risultanti dalla ricerca**	**Riviste Peer-reviewed**	**Percentuale articoli non soggetti a peer-review**
Computer Crimes	42	37	11,90%
Computer Information Security	299	293	2,01%
Computer security	200	171	14,50%
Cyber Security	136	94	**30,88**%
Cybersecurity	70	55	21,43%
Cyber terrorism	0	0	-
Information security	136	96	29,41%
Information warfare	0	0	-
Information Technology	237	215	9,28%
Internet security	0	0	-
Management	116	108	6,90%
Network security	254	224	11,81%
Risk Assessment	135	117	13,33%
Risk Management	169	145	14,20%
Security & protection	0	0	-
Security Management	380	364	4,21%
Smart Grid	0	0	-
Terrorism	0	0	-
Totale	**2174**	**1919**	**11,73**%

La ricerca complessiva per 'cyber risk', effettuata contemporaneamente in tutti i topic individuati, ha individuato **1919** pubblicazioni su riviste peer reviewed (2174 articoli in totale). Il processo di selezione continua con l'eliminazione dei duplicati, poiché uno stesso articolo può ricadere in più subject area e contabilizzato più di una volta nel calcolo del totale numerico. Al termine del processo di selezione con la parola chiave *cyber risk*, risultano selezionati **1112** articoli pubblicati su riviste peer reviewed.

La comparazione dei risultati delle due ricerche, effettuata attraverso una verifica sui titoli degli articoli visualizzati, evidenzia che gran parte degli stessi compaiono in entrambe le ricerche e che sono presenti un ridotto ma significativo numero articoli che compaiono in una sola ricerca e non nell'altra. Non si è effettuata la verifica numerica puntuale degli stessi, in quanto non necessaria allo scopo, poiché risulta evidente che la ricerca effettuata unendo al termine "cyber" entrambe le parole "security" e "risk" restituisce un elenco di articoli che, seppur inferiori in termini numerici rispetto all'iniziale ricerca con la parola chiave "cyber security", risultano essere maggiormente attinenti al tema trattato nel presente lavoro, operando un'ulteriore selezione tematica degli articoli scientifici individuati nei database.

Chiave di ricerca primaria	**Numero di articoli selezionati nei cataloghi on-line**
cyber security	*2165*
cyber risk	*1112*
cyber security risk	**1903**

La chiave primaria di ricerca che si utilizzerà sarà: "***cyber security risk***".

Step 5: Selezione e analisi degli articoli

Definita la chiave di ricerca primaria che, si rammenta, ha prodotto un elenco di oltre millenovecento articoli, si rende necessario restringere ulteriormente l'ambito di ricerca individuando la composizione ottimale della chiave di ricerca secondaria e, successivamente, effettuare la ricerca finale nei database indicando gli argomenti (topic) da utilizzare per affinare definitivamente la selezione informatica dei paper.

La prima fase della definizione della chiave secondaria segue è simile a quella effettuata per la definizione della chiave di ricerca primaria. Si sono effettuate delle ricerche sui database aggiungendo alla chiave di ricerca primaria alcuni termini generalmente

utilizzati nel linguaggio di settore, osservandone i risultati e valutandoli come potenziali elementi costituenti la chiave secondaria di ricerca. I termini considerati sono i seguenti: assessment, management, framework, algorithm, SCADA, analysis, model, methods, evaluation, critical infrastructure. Alcuni termini sono sinonimi o presentano risultati simili nella ricerca informatica: presentano questa caratteristica i termini evaluation, assessment e analysis, oppure model, methods, framework o algorithm.

Al termine di questa fase di valutazione, la chiave secondaria che meglio individua la letteratura necessaria è definita come "***assessment critical infrastructure methods***".

I topic selezionati per l'affinamento della ricerca sulla base di dati sono: Telecommunications Systems & Internet Communications, Security Management, Security and Protection (Ci), Security, Risk Management, Risk Assessment, Risk, Network Security, Internet, Information Security, Experimental/Theoretical, Cyber Security, Computer Information Security.

Nella tabella seguente si riporta il riepilogo dei risultati dell'attività di ricerca informatica sui database descritta nel presente paragrafo:

Chiave composta di ricerca: *(chiave primaria AND chiave secondaria)* ***cyber security risk*** AND ***assessment critical infrastructure method***
1) Numero di articoli selezionati utilizzando la chiave di ricerca composta (primaria + secondaria): **525**
2) Esito finale della selezione: articoli filtrati per appartenenza ai topic selezionati per la ricerca: **248**

L'esito finale delle operazioni di ricerca e selezione informatica degli articoli scientifici si conclude con un gruppo costituito da duecentoquarantotto articoli. Le ulteriori selezioni non verranno effettuate automaticamente da un sistema informatico ma verranno praticate dallo scrivente dopo aver definito alcuni criteri di selezione ai quali sarà necessario attenersi.

Criteri di inclusione e criteri di esclusione

Con la state-of-the-art review, si intende individuare i modelli, le metodologie, gli algoritmi o altri strumenti per l'analisi, valutazione e gestione del rischio applicato o applicabile al contesto cibernetico delle Infrastrutture Critiche Nazionali e ai relativi

servizi strategici da esse erogati, che rappresentino la frontiera ultima o quantomeno una novità nel cyber risk management. Partendo dai 248 articoli selezionati elettronicamente, si procederà alla prima scrematura analizzando ogni singolo titolo degli articoli selezionati, contrassegnando quelli che, rispondendo alle caratteristiche sopra definite, si prestano alla successiva e più approfondita valutazione in funzione dei seguenti **criteri di inclusione**:

- i contenuti degli articoli ritenuti idonei per la state-of-the-art review devono contenere una *proposta* di un ***nuovo modello***, un ***framework***, un ***approccio innovativo*** oppure evidenziare *aspetti inediti* relativi a profili o dinamiche di rischio per le ***Infrastrutture Critiche*** o per i sottosistemi ***cyber-fisici*** che le compongono;

o di esclusione:

- sono da escludere articoli che si concentrano su aspetti o elementi eccessivamente tecnici o di dettaglio e non forniscono un quadro sufficientemente ampio sotto l'aspetto architetturale o organizzativo dello specifico lavoro di ricerca proposto.

Questa prima analisi ha ridotto a **78** gli articoli da analizzare rispetto ai 248 iniziali. La fase successiva prevede l'analisi degli abstract dei singoli articoli e, se l'articolo viene ritenuto rispondente al focus del presenta lavoro di indagine, verrà salvato su memoria non volatile, sotto forma di file. I contributi scientifici che avranno superato questa fase selettiva, verranno interessati dalla successiva e approfondita analisi dei contenuti proposti.

Al termine del processo di ricerca dei contributi scientifici da utilizzare per la state-of-the-art review in tema di cyber security risk management nelle infrastrutture critiche, risultano selezionati un totale di **39 articoli**, tutti pubblicati su riviste internazionali soggette a peer review. Nella tabella seguente si riporta il riepilogo dei risultati dell'attività di selezione:

Criterio di discriminazione degli articoli	Numero di articoli trovati nei cataloghi on-line
Selezionati per titolo (1° selezione)	**78**
Selezionati per abstract (2° selezione)	**39**

Si procede, dunque all'analisi e all'elaborazione di ogni singolo articolo nelle modalità descritte nel prosieguo del presente lavoro.

Review della letteratura

1. *A Comprehensive Network Security Risk Model for Process Control Networks* (Henry and Haimes, 2009): gli autori presentano un modello quantitativo di risk assessment di tipo probabilistico definito Network Security Risk Model (NSRM), un modello e una metodologia che combinano i preesistenti modelli hierarchical holographic modeling (HHM), access level and barrier diagram (ALBD) e fault tree (FT), partendo dall'identificazione delle metriche del rischio fino a costruire nel sistema uno scenario di attacco informatico allo scopo di calcolarne le probabilità di successo. Il modello prevede il calcolo del rischio prima e dopo aver implementato strumenti di cyber security nel sistema e, successivamente, analizza la differenza tra i risultati e il costo di implementazione della soluzione di cyber security. Questi dati consentono l'individuazione del livello ottimale di sicurezza e del dimensionamento del budget di spesa per cyber security. Non è specificato nell'articolo come sono stimate le probabilità di un evento informatico ostile ma si evidenzia che le stesse seguono la distribuzione di Poisson. Pur mostrando dei limiti, peraltro ben evidenziati dagli autori, il modello NSRM sembra costituire un significativo avanzamento rispetto ai modelli di network security comunemente utilizzati nella valutazione dell'efficacia delle misure al livello di sistemi (informativi, scada, infrastrutturali) di risk management.

2. *Cybersecurity for Critical Infrastructures: Attack and Defense Modeling* (Ten et al., 2010): in questo articolo gli autori presentano un modello di risk assessment di tipo quantitativo su base probabilistica, applicato ai sistemi SCADA, articolato in quattro fasi (Real-time monitoring, Anomaly detection, Impact analysis e Mitigation strategies) integrato con una metodologia per l'analisi dell'impact analysis sviluppata dagli autori, basata su diagrammi di tipo attack-trees applicati

a infrastrutture di trasporto e distribuzione dell'energia elettrica per valutare il sistema, lo scenario e le vulnerabilità allo scopo di individuare le componenti del sistema più vulnerabili che hanno maggiore probabilità di essere colpite da un attacco di tipo cyber.

3. *Hierarchical, model-based risk management of critical infrastructures* (Baiardi et al., 2009): gli autori propongono una strategia di risk management che utilizza una sequenza gerarchica, basata su modelli, per descrivere le interdipendenze tra le componenti di una Infrastruttura Critica. Anche in questo caso l'approccio proposto è di tipo quantitativo e utilizza gli Hypergraph (generalizzazione della teoria matematica dei grafi) per modellare le interdipendenze del sistema per stimare le probabilità di un attacco e di estromettere dal modello di analisi del rischio tutti gli elementi caratterizzati da bassa probabilità di attacco. La probabilità di un attacco è influenzata dalla complessità delle azioni e delle risorse necessarie per compierlo e nella valutazione il modello tiene conto dei dati storici degli attacchi informatici subiti dal sistema.

4. *Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems* (Ye et al,. 2015): gli autori presentano un nuovo modello di valutazione delle vulnerabilità in tema di cyber security, caratterizzato da un'analisi delle potenziali conseguenze che un cyber attacco può provocare nel mondo fisico. La fase successiva prevede la modellazione del processo di attacco utilizzando la Teoria dei Giochi e la relazione tra le diverse tipologie di vulnerabilità è analizzata con il supporto di matrici di adiacenza o matrice di connessione (una particolare struttura dati comunemente utilizzata nella rappresentazione dei grafi); l'articolo si conclude con uno specifico studio di caso.

5. *Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements* (Patel et al., 2008): con questo paper gli autori propongono un nuovo approccio per la valutazione della vulnerabilità dell'organizzazione rispetto a violazioni della sicurezza nelle infrastrutture

informatiche. Anche se gli autori hanno evidenziato che, fino ad allora, gran parte della ricerca scientifica è stata realizzata utilizzando un approccio di tipo qualitativo a fronte di una scarsa presenza di letteratura scientifica su approcci di tipo numerico per quantificare il rischio sicurezza delle informazioni. Con questo articolo, pertanto, propongono un metodo per quantificare il rischio esprimendolo in valore numerico, come "grado di cyber security" e per far ciò presentano due indici, l'indice di minaccia-impatto e l'indice di cyber-vulnerabilità, basati sugli alberi di vulnerabilità (vulnerability trees). Un aspetto degno di nota è che utilizzando detti indici, il management può fissare il livello di rafforzamento ottimale di cyber security da implementare, disponendo di elementi per definire il budget di spesa per l'implementazione del livello di cyber security definito e, in conclusione viene presentata la sperimentazione del modello effettuata su un sistema SCADA.

6. *Risk assessment framework for power control systems with PMU-based intrusion response system* (Yan et al., 2015): l'articolo propone un Framework da utilizzare per l'analisi del rischio nelle Infrastrutture Critiche per l'energia elettrica, con l'obiettivo di aumentarne la resilienza nei confronti dei cyber attack. Il framework utilizza due strumenti combinati tra loro: il metodo di valutazione "fuzzy", impiegato per individuare le vulnerabilità del sistema, e l'attack graph, per identificare possibili intrusioni che possono verificarsi e, infine, viene adottato l'indice CLEs (conditional Lyapunov exponents), molto utilizzato in studi sulla sincronizzazione di sistemi caotici, per stimare la stabilità dei sistemi infrastrutturali elettrici.

7. *A cyber-resilient architecture for critical security services* (Kreutz et al., 2016): in questo lavoro gli autori propongono il progetto di un'architettura funzionale finalizzato ad aumentare la resilienza delle infrastrutture critiche che provvedono all'erogazione di servizi strategici. Il modello è applicato strattamente ad aspetti di tipo tecnologico e si concentra sui servizi di *Identity provider* e di Autenticazione, Autorizzazione e Accounting (AAA). Allo scopo, gli autori

hanno sviluppato due algoritmi basati rispettivamente sui protocolli standard OpenID e RADIUS. Gli algoritmi sono stati testati su due distinti prototipi e valutati con il modello *attack trees* per testarne i punti di forza e di debolezza. Pur raggiungendo l'obiettivo dell'aumento del grado di resilienza, l'applicazione dell'innovazione è limitata ad uno specifico settore del sistema informatico che controlla e gestisce l'erogazione dei c.d. servizi critici.

8. *A fault diagnosis system for interdependent critical infrastructures based on HMMs* (Ntalampiras et al,. 2015): gli autori propongono un framework basato su modelli probabilistici per analizzare gli effetti di attacchi cibernetici a Infrastrutture Critiche interdipendenti. Il lavoro proposto si basa sull'analisi delle relazioni tra flussi di dati provenienti da due nodi di rete utilizzando il c.d. "Hidden Markov Model" o HHM applicato a dei "training scenario" configurati su sistemi SCADA per simulare le condizioni fisiche presenti nelle infrastrutture critiche. Questo modello è in grado di fornire significative informazioni agli Operatori per l'analisi delle vulnerabilità delle loro infrastrutture critiche.

9. *A Method for Revealing and Addressing Security Vulnerabilities in Cyber-Physical Systems by Modeling Malicious Agent Interactions with Formal Verification* (Wardell e al., 2016): in questo articolo viene presentato un nuovo metodo per l'identificazione delle vulnerabilità in tema di cyber security applicata a sistemi cyber-fisici, utilizzando modelli di "malicious agent interactions" associati ai modelli matematici di modellazione di controllo dei sistemi per produrre simulazioni e condurre dei test.

10. *A multidimensional approach to information security risk management using FMEA and fuzzy theory* (Silva et al., 2014): viene presentato un approccio al security risk management basato sul modello Failure Mode and EffectsAnalysis (FMEA) e sulla fuzzy theory, quest'ultima in grado di elaborare informazioni inaccurate utilizzando strumenti matematici. Il framework analizza cinque dimensioni della sicurezza informatica: access to information and systems,

communication security, infrastructure, security management and secure information systems development. Un modello di cyber security risk management è stato definito e applicato in un laboratorio universitario. I test sono stati eseguiti coinvolgendo un gruppo accademico di ricerca rilevando un incremento del livello di cyber security in due delle cinque dimensioni considerate: Communication security e infrastructure. Il modello è in grado di fornire informazioni significative sulle vulnerabilità nei sistemi critici in termini qualitativi.

11. *A probabilistic relational model for security risk analysis* (Sommerstad et al., 2010): nel lavoro proposto, gli autori ricorrono a numerosi modelli PRM (Probabilistic Relational Model) per valutare il livello di sicurezza in un'architettura informatica che integrano con un pacchetto di astrazioni "PRM-classes" che specificano come gli attributi dello stato degli oggetti dipendono dallo stato degli altri attributi presenti in un modello architetturale. Questo gruppo di "abstract classes" vengono utilizzate per creare dei modelli relazionali probabilistici (PRM) per la valutazione del rischio informatico a supporto delle decisioni del management o del Decisore pubblico poiché il concetto di rischio restituito dal modello, definito come il prodotto tra la perdita finanziaria e la probabilità di un incidente provocato da un attacco informatico, rappresenta un elemento importante per il processo decisionale (Ryan and Ryan, 2006; Tsiakis and Stephanides, 2005).

12. *A three-stage analysis of IDS for critical infrastructures* (Cazorla et al., 2015): questo articolo utilizza un approccio di tipo qualitativo e l'aspetto della sicurezza di una Infrastruttura Critica è trattato nella più ampia accezione. Gli autori evidenziano la stretta interconnessione esistente tra il livello fisico e quello informatico e la forte interrelazione che si configura tra le varie infrastrutture critiche. Il framework NFR (non-functional requirements), descritto in Chung et al. (2000), è utilizzato unitamente alle metriche (approccio quantitativo). Il framework è utilizzato per modellare obiettivi qualitativi process-oriented, dividendoli in requisiti non funzionali e tecniche di satisficing per conseguire dei

c.d. “soft-goals” ovvero risultati "senza una rigida definizione e/o parametri che prevedono solo due stati, si/no o vero/falso, poiché i framework NFRs sono soggettivi, relativi e interdipendenti. Il modello proposto è applicato ai sistemi SCADA ed ai c.d. CCS o “sistemi dei sistemi”, come parti di Infrastrutture Critiche, ed è in grado di fornire delle metriche riferite a diversi aspetti tecnologici del sistema.

13. *A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness* (Karabacak et al., 2016): questo articolo propone l’utilizzo di un “maturity model” per misurare i livelli di protezione di Infrastrutture Critiche Nazionali. Lo sviluppo del modello è strutturato in due fasi: la prima analizza i dati relativi ai progetti di nazionali di cyber security utilizzando la c.d. “grounded theory” per estrarre le cause primarie della vulnerabilità delle infrastrutture critiche alle minacce cibernetiche; la seconda fase definisce i criteri di maturità, sottoponendo le cause primarie ad un gruppo di esperti intervistati in un sondaggio di Delphi. I risultati ottenuti con il modello di maturità, basati sulle indagini effettuate, vengono applicati per valutare gli sforzi di protezione delle infrastrutture critiche in Turchia, dimostrando che il maturity model risulta utile per valutare il livello di cyber security implementato in una Infrastrutture Critica Nazionale.

14. *Awareness and reaction strategies for critical infrastructure protection* (Cazorla et al., 2015): gli autori propongono un framework metodologico in grado di determinare gli elementi essenziali presenti nel IDPRS (Intrusion Detection, Prevention and Response Systems) di una Infrastruttura Critica, valutando ogni singolo sub-componente in termini di adeguatezza al contesto critico al quale viene applicato. Una review della letteratura ha permesso agli autori la composizione di modello tassonomico per l’IDPRS che contiene i principali elementi e la caratteristiche desiderabili per la protezione dei Sistemi Critici.

15. *Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET* (Shin et al., 2016): in questo studio viene presentato un modello di Cyber Security Risk evaluation per Sistemi Critici basato su modelli "*Bayesian network"* (BN) e "*event trees"* (ET). Gli autori propongono una metodologia per costruire un modello per la cyber security risk evaluation applicata ai sistemi informatici e di comunicazione di un impianto nucleare. I risultati analitici ottenuti dal modello BN sono utilizzati nel modello probabilistico ET allo scopo di ottenere un'approfondita comprensione del cyber security risk.

16. *Development of a cyber security risk model using Bayesian networks* (Shin et al., 2014): in questo lavoro viene proposto un modello di risk assessment per la cyber security, basato sul "Bayesian network", impiegato per la valutazione integrata della sicurezza informatica su impianti nucleari. Il modello proposto consente la valutazione degli aspetti della cyber security, sia procedurali che tecnici, rispettivamente con linee guida e architetture di sistema valutate con il modello di analisi "activity-quality" sviluppato per valutare come persone od organizzazioni sono "compliance" con le linee guida definite dal Regolatore in tema di cyber security. Analogamente gli autori hanno creato un modello di analisi dell'architettura per valutare la presenza di vulnerabilità e le misure di mitigazione dei loro effetti sulla sicurezza cibernetica. I due modelli sono stati successivamente integrati in un singolo modello, denominato "the cyber security risk model", in modo che la cyber security venga valutata da una prospettiva sia procedurale che tecnica allo stesso tempo.

17. *From old to new: Assessing cybersecurity risks for an evolving smart grid* (Langer et al., 2016): questo recente lavoro propone un metodo pratico di risk assessment che coinvolge due flussi di attività: un'analisi diretta a livello dei sistemi implementati, l'altra portata a livello concettuale con lo scopo di comprendere i profili di rischio in una Smart Grid senza disporre di una implementazione nel sistema cyber-fisico. Questo doppio approccio consente di analizzare il rischio nel

breve e medio termine in termini architetturali della Smart Grid individuando in modo chiaro gli elementi informativi per comprendere i Cyber Security Risk.

18. *Identification of safety and security critical systems and activities* (Aven, 2008): partendo dall'assunto che un sistema o un'attività è critica se la vulnerabilità e il rischio sono alti, Aven suggerisce un approccio alternativo per identificare i Sistemi Critici e valutare il rischio, proponendo di integrare, all'interno del concetto classico di rischio, elementi come l'incertezza, il valore atteso, oltre che a considerare prospettive di rischio alternative da inserire in modelli già esistenti, aprendosi ad un contesto più ampio, dove le incertezze e le possibili sorprese sono considerate una parte importante del quadro complessivo di rischio. Integrando nel modello le dimensioni incertezza e probabilità relative al verificarsi degli eventi ostili, consente di gestire il rischio informatico, fornendo elementi razionali per il processo decisionale del management in tema di investimenti in materia di cyber security.

19. *Integrating cyber attacks within fault trees* (Nai Fovino et al., 2009): gli autori presentano un nuovo metodo per la valutazione quantitativa del cyber risk in sistemi complessi, combinando la *fault-tree analysis*, tradizionalmente impiegata nell'analisi di affidabilità, con la *attack-tree analysis*, recentemente introdotta, utilizzata per lo studio di schemi di attacco ostili. L'impiego combinato dei due modelli, supporta le decisioni del management in tema di investimenti finanziari in cyber security resi necessari dall'introduzione delle moderne tecnologie ICT nei sistemi di controllo delle infrastrutture critiche. L'approccio proposto permette di considerare che l'interazione di attacchi informatici intenzionali agisce con errori casuali. Vengono fornite le definizioni formali di fault-tree e attack tree e viene presentato un modello matematico per il calcolo delle probabilità di guasto del sistema nel suo complesso.

20. *Model for comprehensive approach to security management* (Kralik et al., 2016): viene proposto un modello integrato e complesso di sicurezza informatica, il c.d.

"*complex integrated security model*". Si tratta di un modello integrato di security management system, sviluppato in una prospettiva struttural-organizzativa, che si basa su alcuni punti:

- classificazione delle responsabilità per la sicurezza fino al livello del top management della società;
- ripartizione delle responsabilità per la sicurezza e garantire il suo sostegno;
- introduzione di regole di approvazione e controllo per garantire l'efficacia del sistema integrato di sicurezza gestione;
- creazione di una nuova unità organizzativa, il dipartimento di sicurezza informatica.

Il modello rende possibile l'interazione tra i singoli settori di sicurezza così come la gestione dei rischi sulla base di indicatori per ridurre l'impatto di eventuali minacce a un livello accettabile, consente l'ottimizzazione degli investimenti in cyber security.

21. *Security risk assessment: Applying the concepts of fuzzy logic (Bajpai et al., 2009):* In un precedente articolo, gli autori hanno presentato il modello denominato "Security Risk Factor Table" (SRFT) dove, per la valutazione del rischio, venivano considerati fattori quali posizione, proprietà, visibilità dei vari impianti dislocati all'interno del perimetro di un complesso industriale nel settore chimico. In questo lavoro, gli stessi, propongono un'evoluzione del precedente modello SRFT per adattarlo al tema cyber, introducendo i concetti della fuzzy-logic. Nel modello SRFT modificato, due Fuzzy Linguistic Scales (three-point and four-point) sono concepite sulla base di numeri fuzzy trapezoidali. La soggettività dei diversi esperti coinvolti nel precedente SRFT modello è affrontata mappando i loro punteggi sulla scala fuzzy di nuova concezione, infine, il punteggio (score) fuzzy così ottenuto è "de-fuzzyzzato" applicando dei fattori di correzione, ottenendo i risultati finali.

22. *Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?* (Zio and Aven, 2011): Zio e Aven presentano un framework di analisi sviluppato per rappresentare e trattare l'incertezza nelle valutazioni del rischio e delle vulnerabilità nelle Infrastrutture Critiche e nello specifico nelle Smart Grid per la produzione e distribuzione dell'energia elettrica. Rispetto ad approcci probabilistici "puri" gli autori propongono qualche metodo alternativo di rappresentazione dell'incertezza e ne suggeriscono le linee guida per l'applicazione in contesti reali, a supporto delle decisioni.

23. *Vulnerability analysis of interdependent infrastructure systems: A methodological framework* (Wang et al., 2011): questo lavoro prende come esempio l'Infrastruttura idrica ed elettrica di una grande città cinese e sviluppa un quadro per l'analisi della vulnerabilità dei sistemi infrastrutturali interdipendenti. Sono introdotte alcune strategie di progettazione, basate su distanza, grado di interfaccia e coefficiente di clustering. Due tipi di vulnerabilità - vulnerabilità a lungo termine e vulnerabilità concentrata - sono illustrate e analizzate e, infine, viene proposto un metodo per classificare i componenti critici in infrastrutture interdipendenti, finalizzato alla protezione dei sistemi critici, che risulta molto utile per l'analisi di vulnerabilità di sistemi interdipendenti a supporto delle decisioni sulla progettazione dell'infrastruttura e sui relativi investimenti per aumentarne il grado di protezione.

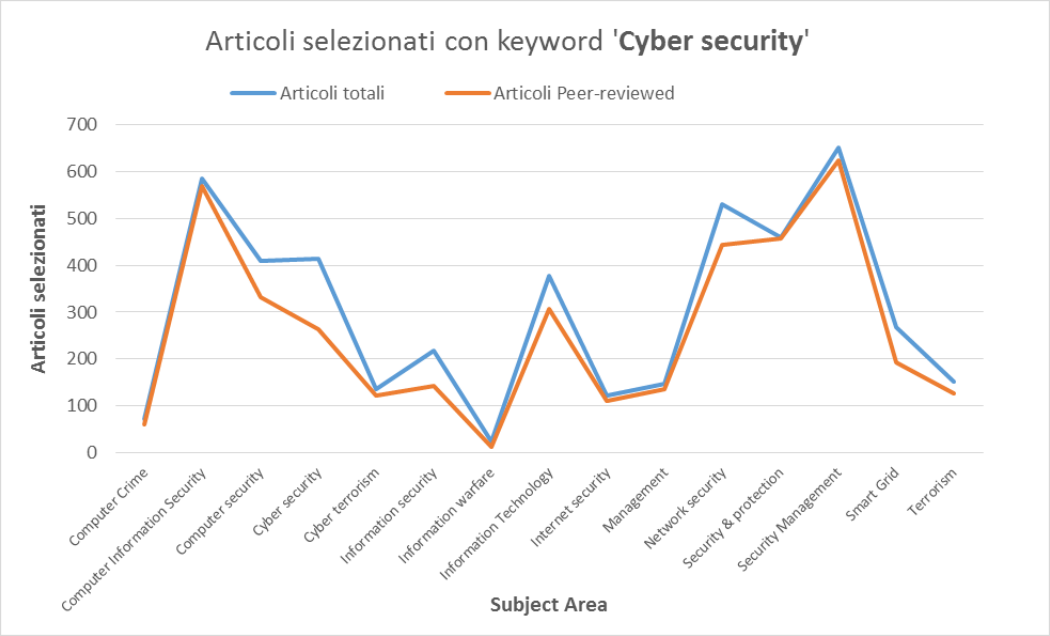
L'analisi approfondita degli articoli selezionati ha ulteriormente ristretto il numero dei contributi inclusi nella State-of-the-art review, dai 39 selezionati con l'analisi dell'abstract ai **23** articoli finali.

Risultati della ricerca

Analisi della prima fase della ricerca informatica sul database

Si osservano alcune caratteristiche e proprietà emerse dal processo di ricerca ed estrazione dei contributi selezionati dai database di Ateneo considerando che la prima ricerca sui database, effettuata con le keyword *cyber security* e *cyber risk*, è stata effettuata in due passaggi consecutivi; prima ricercando gli articoli in funzione della keyword su tutti i mezzi di diffusione scientifica come Journals e proceedings di convegni, soggetti o meno a peer-review, libri e gray literature e successivamente applicando la restrizione ai soli articoli pubblicati su journal internazionali soggetti a peer-review.

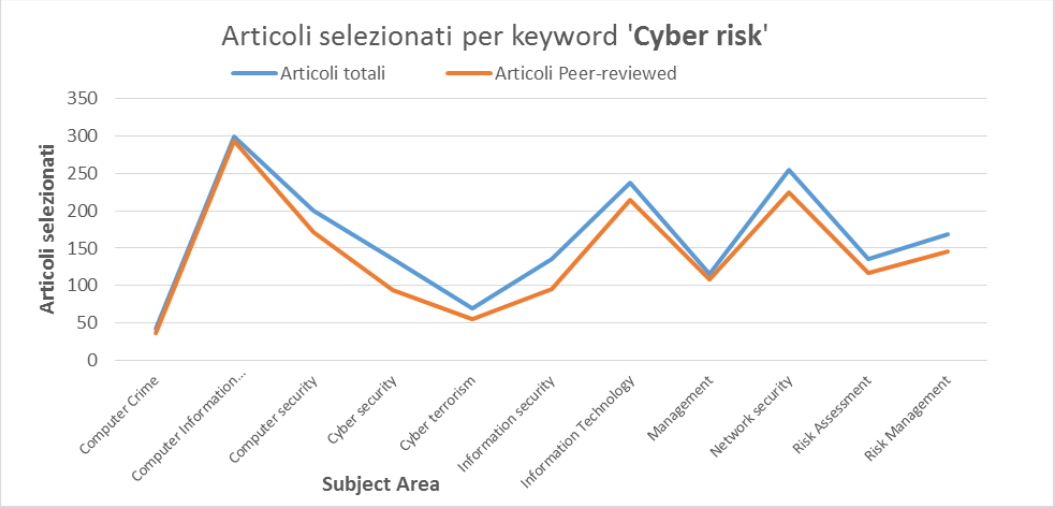
Articoli selezionati per parole chiave "cyber security"



Gli articoli esclusi dalla prima selezione rappresentano il 14,6% del totale (667 esclusi su 4567). Si possono notare da subito alcuni elementi interessanti osservando gli scostamenti per singola *subject area*, poiché l'ampiezza tra le pubblicazioni peer-reviewed e quelle non sottoposte a review, sono molto variabili: si passa dallo 0,44% nella subject area *Security & protection* al 41,67% della subject area *Information warfare*, ponendo in evidenza che, nel primo caso, la quasi totalità degli articoli (457 su 459) sono stati sottoposti a valutazione secondo le regole della revisione paritaria e pertanto dispongono

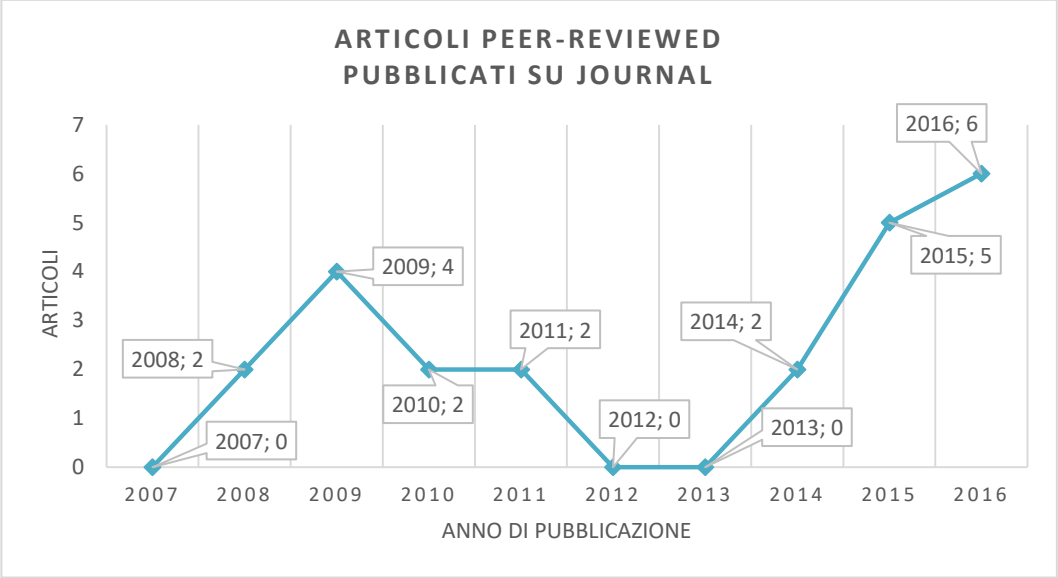
del carattere di ***oggettività*** necessario per il riconoscimento della dignità di pubblicazione nella letteratura scientifica peer-reviewed. Nel secondo caso, al contrario, oltre il 40% degli articoli risultano pubblicati in atti di convegni, raccolte tematiche, libri o comunque nella c.d. Gray literature, non sottoposti a review, ma rappresentano, in ogni caso, contributi significativi al dibattito in corso. Una chiave di lettura che spieghi differenze così significative tra differenti subject area, senza alcuna pretesa scientificità, potrebbe trovarsi nelle caratteristiche intrinseche dell'argomento trattato e nella vivacità del dibattito in corso poiché gli articoli, non dovendo sottostare ai vincoli della peer-review, consentono maggiore libertà agli autori/relatori di proporre valutazioni soggettive, nuove prospettive di ricerca o differenti paradigmi interpretativi, una sorta di indice di "vivacità" del dibattito in corso nella subject area presa in considerazione.

Articoli selezionati per parole chiave "cyber risk"



La ricerca è stata ripetuta utilizzando la keyword *cyber risk* e si sono ottenuti dati che, seppur differenti nei valori e nella distribuzione, sostanzialmente confermano le considerazioni fatte nel caso esposto in precedenza. In questo caso, gli articoli esclusi dalla prima selezione rappresentano l'11,73% del totale (255 esclusi su 2174) e gli scostamenti per singola subject area, appaiono meno marcati: si passa dallo 2,01% nella subject area *Computer Information Security* al 30,88% della subject area *Cyber security*.

Analisi della distribuzione tra journal degli articoli selezionati per la review:



L'intervallo temporale definito per la ricerca dei contributi scientifici va dal primo gennaio del 2007 al 31 dicembre 2016. Riportando graficamente la suddivisione del numero di articoli pubblicati per anno, appaiono subito evidenti alcune particolarità:

- nel 2007, 2012 e 2013 non si sono individuate pubblicazioni rispondenti ai criteri di selezione stabiliti nella presente ricerca;
- vi è un significativo picco nell'anno 2009;
- dal 2014 in poi il numero di pubblicazioni è in costante e significativa crescita.

Nel periodo che va dal 2008 al 2010, i papers selezionati propongono framework e algoritmi tipici delle discipline matematiche, informatiche e ingegneristiche. Dal 2014 al 2016, dopo il fermo del 2011 e del 2012, le pubblicazioni selezionate mostrano un interesse della comunità scientifica all'approccio metodologico alla cyber security, in aggiunta all'evoluzione di strumenti di analisi e valutazione del rischio cibernetico nelle applicazioni in sistemi cyber-fisici e nelle infrastrutture critiche. Si ritiene ragionevole ipotizzare che un significativo stimolo alla ricerca, assumendo una prospettiva più ampia in tema di cyber security, possa provenire dalla pubblicazione del marzo 2014 del Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2014).

Elenco degli articoli selezionati per la State-of-the-art review:

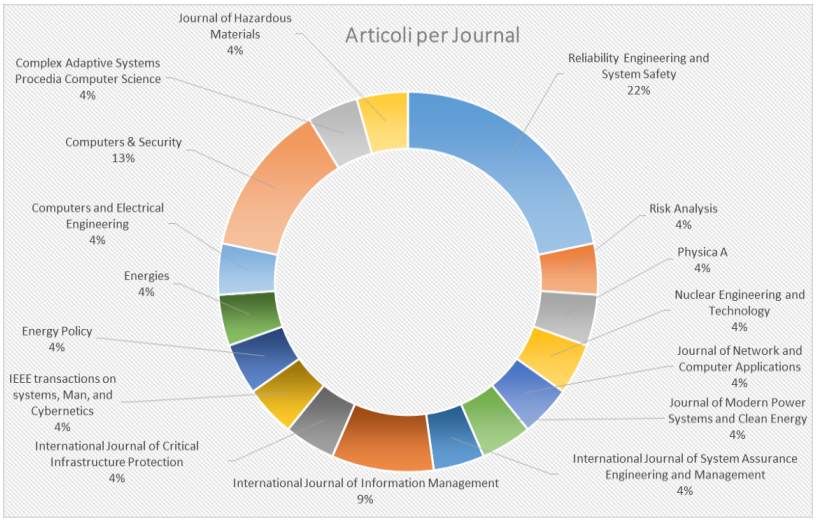
Titolo	Autori	Anno	Journal	Settore	Approccio	Modello
Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements	Patel et al.	**2008**	International Journal of Information Management	Information management	Quantitativo probabilistico	Vulnerability trees, indice di cyber vulnerabilità
Identification of safety and security critical systems and activities	Aven	**2008**	Reliability Engineering and System Safety	Ingegneria	Quantitativo probabilistico	Incertezza e valore atteso in modelli esistenti
A Comprehensive Network Security Risk Model for Process	Henry and Haimes	**2009**	Risk Analysis	Mathematical Methods	Quantitativo probabilistico	Network Security Risk Model (NSRM)
Hierarchical, model-based risk management of critical infrastructures	Baiardi et al.	**2009**	Reliability Engineering and System Safety	Ingegneria	Quantitativo probabilistico	Hypergraph theory
Integrating cyber-attacks within fault trees	Nai Fovino et al.	**2009**	Reliability Engineering and System Safety	Ingegneria	Quantitativo probabilistico	Fault trees analysis
Security risk assessment: Applying the concepts of fuzzy logic	Bajpai et al.	**2009**	Journal of Hazardous Materials	Risk assessment - ambiente	Algoritmi soft computing	Fuzzy logic
Cybersecurity for Critical Infrastructures Attack and Defense Modeling	Ten et al.	**2010**	IEEE transactions on systems, Man, and Cybernetics	Ingegneria	Quantitativo probabilistico	Impact analysis attack-trees
A probabilistic relational model for security risk analysis	Sommerstad et al.	**2010**	Computers & Security	IT Security & IT Audit	Quantitativo probabilistico	Modelli Relazionali Probabilistici
Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?	Zio and Aven	**2011**	Energy Policy	Energia	Framework probabilistico	Incertezza valutata in contesti reali
Vulnerability analysis of interdependent infrastructure systems: A methodological framework	Wang et al.	**2011**	Physica A	Statistical mechanics	Framework di analisi delle vulnerabilità	Strategie parametriche di progettazione
A multidimensional approach to information security risk management using FMEA and fuzzy theory	Silva et al.	**2014**	International Journal of Information Management	Information management	Algoritmi soft computing	Failure Mode Effect Analysis e Fuzzy theory
Development of a cyber security risk model using Bayesian networks	Shin et al.	**2014**	Reliability Engineering and System Safety	Ingegneria	Framework tecnico e procedurale	Bayesan Networks e analisi activity-quality
A three-stage analysis of IDS for critical infrastructures	Cazorla et al.	**2015**	Computers & Security	IT Security & IT Audit	Qualitativo	Non Functional Requirements
Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems	Ye et al.	**2015**	Energies	Ingegneria	Quantitativo probabilistico	Teoria dei giochi, matrici di adiacenza
Risk assessment framework for power control systems with PMU-based intrusion response system	Yan et al.	**2015**	Journal of Modern Power Systems and Clean Energy	Ingegneria	Algoritmi soft computing	Fuzzy theory, attack graph, indice CLEs
A fault diagnosis system for interdependent critical infrastructures based on HMMs	Ntalampiras et al,	**2015**	Reliability Engineering and System Safety	Ingegneria	Quantitativo probabilistico	HMMs Hidden Markov Model
Awareness and reaction strategies for critical infrastructure protection	Cazorla et al.	**2015**	Computers and Electrical Engineering	IT / Ingegneria	Framework metodologico	Modello tassonomico
A cyber-resilient architecture for critical security services	Kreutz et al.	**2016**	Journal of Network and Computer Applications	IT	Quantitativo probabilistico	Attack-trees
A Method for Revealing and Addressing Security Vulnerabilities in Cyber-Physical Systems by Modeling Malicious Agent Interactions with Formal Verification	Wardell e al.	**2016**	Complex Adaptive Systems Procedia Computer Science	IT / Ingegneria	Framework metodologico	Malicius Agent Interactions, Modellazione matematica
A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness	Karabacak et al.	**2016**	International Journal of Critical Infrastructure Protection	Ingegneria	Qualitativo	Grounded Theory e Maturity model
Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET	Shin et al.	**2016**	Nuclear Engineering and Technology	Ingegneria	Framework metodologico	Bayesan Networks e Event Trees
From old to new- Assessing cybersecurity risks for an evolving smart grid	Langer et al.	**2016**	Computers & Security	IT Security & IT Audit	Metodo pratico per la Risk analysis	Analisi architetturale e simulazioni
Model for comprehensive approach to security management	Kralik et al.	**2016**	International Journal of System Assurance Engineering and Management	Ingegneria applicata	Framework stuttural - organizzativo	Complex integrated security model

Articoli per Istituzione e area di appartenenza dell'Autore principale

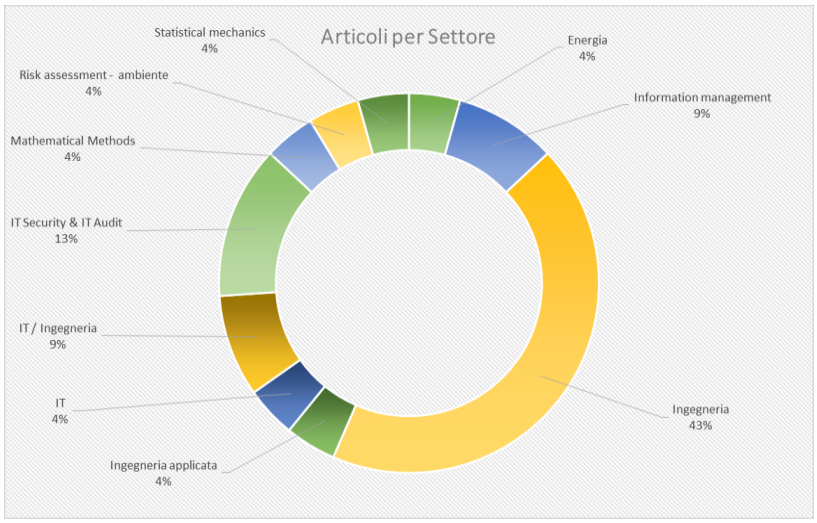
Autore principale	Anno	Afferènza Autore principale	Area
Aven	2008	SEROS - Centre for Risk Management and Societal Safety University of Stavanger, Norway	Social Science
Patel	2008	Department of Information Science and Systems, Graves School of Business and Management, Morgan State University, Baltimore, MD 21251, USA	Information Science
Bajpai	2009	Department of Chemical Engineering, National Institute of Technology, Jalandhar, India	Engineering
Baiardi	2009	Dipartimento di Informatica - Università di Pisa	Information Science
Nai Fovino	2009	European Commission, Joint Research Center, Institute for the Protection and Security of the Citizen, Ispra (VA), Italy	Government
Henry	2009	Johns Hopkins University Applied Physics Laboratory, Laurel, MD (US)	Engineering
Ten	2010	School of Electrical, Electronic and Mechanical Engineering, University College Dublin	Engineering
Sommerstad	2010	Royal Institute of Technology (KTH), Industrial information & control systems, Stockholm, Sweden	Information Science
Wang	2011	Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, 430074, PR China	Engineering
Zio	2011	Ecole Centrale Paris–Supelec, Paris, France and Politecnico di Milano, Italy.	Engineering
Silva	2014	Costa School of Engineering, Centre for Technology and Geosciences, Department of Production Engineering, Universidade Federal de Pernambuco, Recife, Brazil	Engineering
Shin	2014	Department of Nuclear Engineering, Kyung Hee University, Republic of Korea	Engineering
Yan	2015	Market Engineering, MISO Electric, Carmel, IN 46032, USA	Engineering
Cazorla	2015	Computer Science Department, University of Malaga, Spain	Information Science
Cazorla	2015	Computer Science Department, University of Malaga, Spain	Information Science
Ye	2015	College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China	Engineering
Ntalampiras	2015	European Commission, +Joint Research Center, Institute for the Protection and Security of the Citizen, Ispra (VA), Italy	Government
Kralik	2016	Faculty of Applied Informatics, Tomas Bata University Zlin, Czech Republic	Information Science
Shin	2016	Department of Nuclear Engineering, Kyung Hee University, Republic of Korea	Engineering
Wardell	2016	Air Force Institute of Technology, 2950 Hobson Way, Dayton OH (US)	Engineering
Langer	2016	Digital Safety and Security Department, Austrian Institute of Technology, Vienna, Austria	Engineering
Karabacak	2016	Graduate School of Informatics, Middle East Technical University, 06800 Cankaya, Ankara, Turkey	Information Science
Kreutz	2016	SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg	Information Science

Articoli pubblicati per Journal

La valutazione dei risultati della review inizia osservando la distribuzione degli articoli sui vari journal, rilevando che il 22% dei contributi selezionati sono stati pubblicati su *Reliability Engineering and System Safety*; seguito da *Computer & Security* al 13% e, al terzo posto, *International Journal of Information Management*. Deve notarsi che la quasi totalità delle riviste sono accumunate da una forte vocazione tecnologica e ingegneristica e l'unica che si occupa di management, seppur specifico per sistemi informativi, rappresenta il 9% del totale.



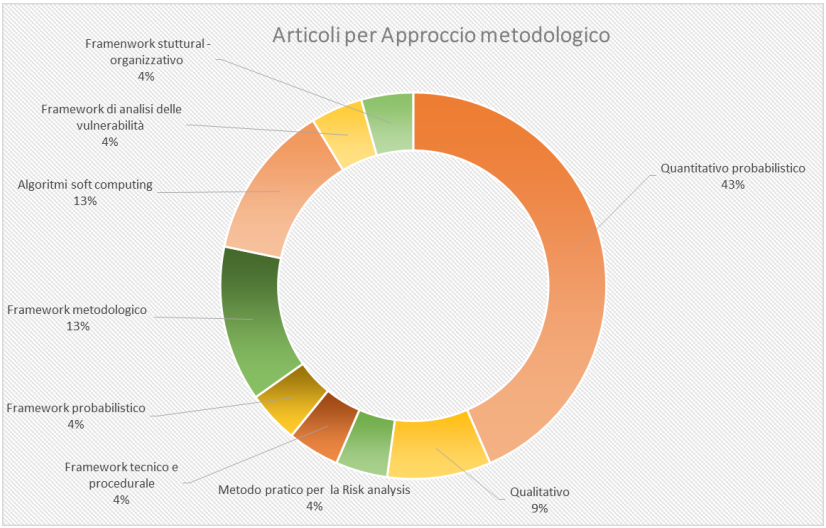
Articoli per settore:



La distribuzione per settore degli articoli vede in testa l'area ingegneristica, complessivamente al 47%, seguita da quella informatica, al 26%. L'aspetto di management è trattato nel 9% dei paper analizzati.

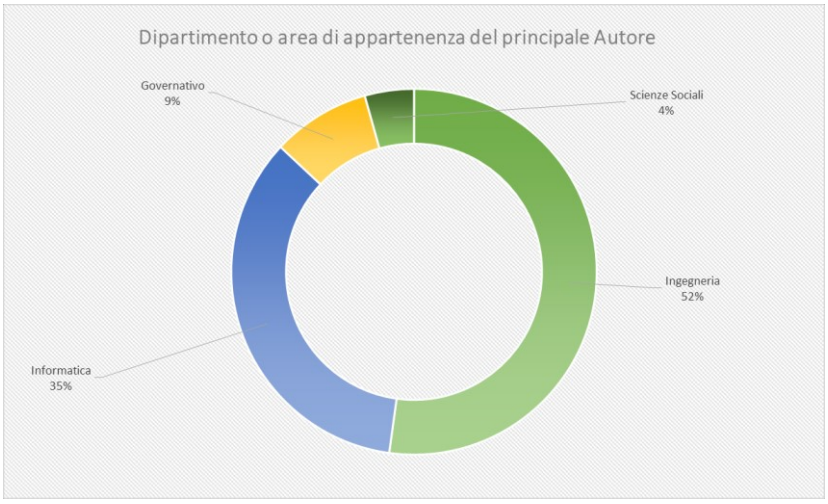
Articoli per approccio metodologico:

L'approccio metodologico più frequente, tra i paper selezionati, è risultato quello *quantitativo di matrice probabilistica*, riscontrato nel 43% del paper analizzati, seguiti dai framework metodologici che si attestano, nel complesso, al 30% circa. Approcci e algoritmi di tipo euristico, come la fuzzy logic, rappresentano il 13% del totale.



Aree di afferenza dei corresponding author:

Le aree di ingegneria (52%), e informatica (35%), da sole, assorbono quasi nove corresponding author su dieci; seguono al 9% i due autori afferenti al settore pubblico seppur riconducibili, per contenuti, all'area ingegneristica e, infine, una sola rappresentante di un Dipartimento di Scienze Sociali di un'università norvegese.



Considerazioni sulla review

La state-of-the-art review ha fornito un quadro attendibile sullo stato dell'arte dell'avanzamento della ricerca nel campo Cyber Security Risk Management. E' emerso un crescente interesse e una discreta vivacità della ricerca nel settore, riconducibili quasi esclusivamente a ricercatori afferenti al settore ingegneristico o informatico. In buona parte sono stati proposti modelli o algoritmi che rappresentano un'evoluzione di modelli preesistenti ma adattati o fatti evolvere per essere impiegati nel campo della cyber security delle infrastrutture critiche.

Tuttavia, sono stati proposti modelli e algoritmi avanzati, riconducibili a raffinati modelli teorici come la *Teoria dei Giochi* (von Neumann and Morgenstern, 1944; Nash, 1950, 1953) o la *Fuzzy logic* (Zadeh, 1968, 1978; Wang and Sun, 2012), introducendo nella Risk Analisys elementi caratteristici dell'*approccio euristico* (Bakr et al., 2012; Aven, 2004, 2012), più adatto alle condizioni di elevata incertezza e di carenza di informazioni storicizzate del mondo Cyber, rispetto a quelli utilizzati nei metodi di risk analysis in contesti più tradizionali.

Gli articoli che propongono modelli organizzativi (Shin et al, 2016; Kralik et al., 2016) sono stati pubblicati solo negli ultimi anni osservati e sono tutt'altro che numerosi. Si è altresì rilevato che anche i contributi che trattano il tema del cyber risk management da una prospettiva metodologica (Zio and Aven, 2011; Wang et al., 2011; Cazorla et al., 2015; Wardell et al., 2016), sono stati pubblicati su riviste di area tecnico-scientifica e, inaspettatamente, si registra la totale assenza di articoli pubblicati su riviste di management o di area aziendale e oltretutto, come rilevabile in tabella, la quasi totalità degli Autori principali dei 23 articoli sottoposti alla State-of-the-art review, afferiscono a dipartimenti universitari di Ingegneria, Informatica o comunque di area tecnico-scientifica. In conclusione, pubblicazioni scientifiche di ricerca e analisi nell'ambito della valutazione del cyber risk nelle Infrastrutture Critiche Nazionali nella prospettiva di Management, al momento appare assente, nonostante il "Framework for Improving Critical Infrastructure Cybersecurity – NIST", significativo elemento di stimolo in questa direzione, sia stato pubblicato da quasi tre anni.

CASO DI STUDIO: CYBER SECURITY NEL GRUPPO ENEL

Il Gruppo ENEL: caso di studio ottimale

L'analisi dello stato dell'arte nel campo della ricerca accademica sul tema del rischio cibernetico deve essere testata nel contesto reale; pertanto, alla seconda domanda di ricerca, come già prospettata in precedenza, si intende rispondere con un caso di studio, analizzando la raffinata implementazione del framework per la cyber security operata da una grande azienda multinazionale, il Gruppo ENEL.

Il lavoro di ricerca e di analisi del caso di studio, che si è articolato in varie fasi e a differenti livelli di dettaglio, è stato effettuato grazie alla possibilità di accedere a numerose informazioni pubblicate dal gruppo, ed alla opportunità di interagire con interlocutori privilegiati.

ENEL, il cui acronimo significava originariamente Ente Nazionale per l'energia ELettrica, istituita come ente pubblico a fine 1962, venne trasformata nel 1992 in società per azioni e nel 1999, in seguito alla liberalizzazione del mercato dell'energia elettrica in Italia, venne privatizzata.

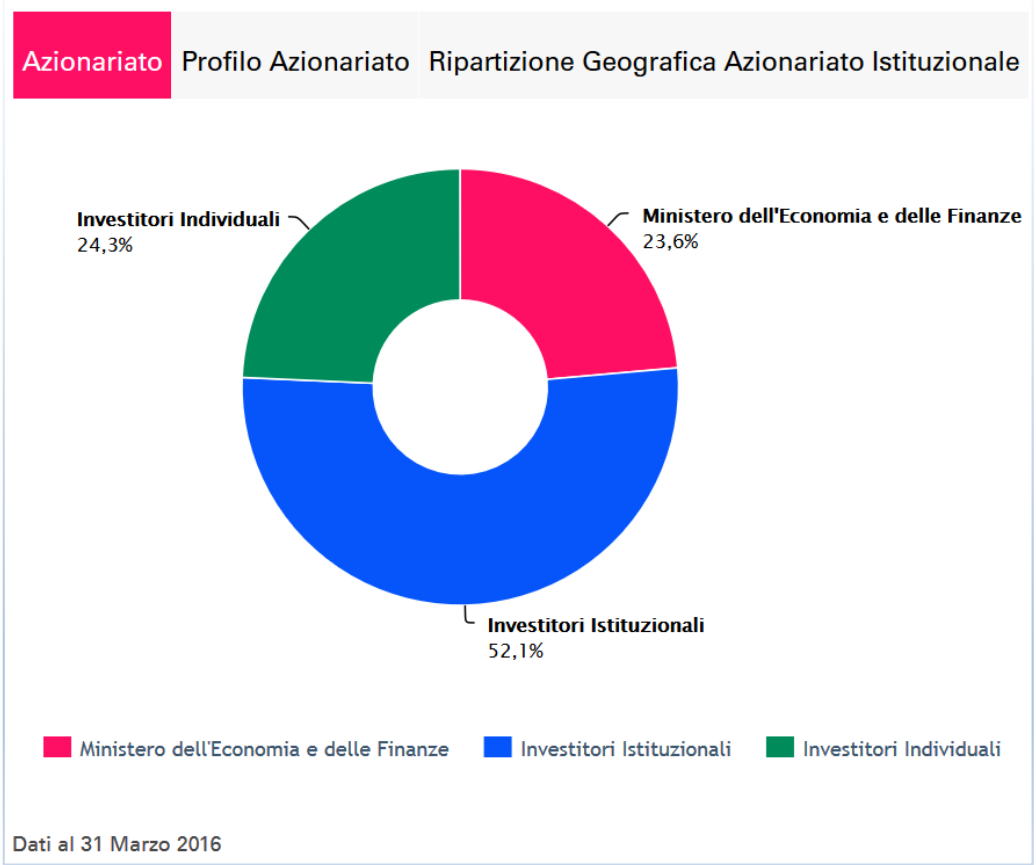
La società è quotata nell'indice FTSE MIB della Borsa di Milano, ed in altre piazze internazionali, attraverso proprie controllate, quali ad esempio la borsa di New York con la latinoamericana Enel Américas (che riunisce le compagnie operanti in Argentina, Brasile, Colombia e Perù), Enel Chile ed Enel Generación Chile.

Lo Stato italiano, tramite il Ministero dell'Economia e delle Finanze, è il principale azionista di Enel S.p.A. e detiene il 23,6% del capitale sociale. In virtù dello sviluppo internazionale della società e della sua crescente redditività, insieme a una forte politica ambientale e della sostenibilità, nonché all'adozione delle migliori pratiche in materia di trasparenza e di corporate governance, gli azionisti di Enel includono fondi di

investimento nazionali e internazionali, compagnie assicurative, fondi pensione ed etici, oltre ad un milione di piccoli risparmiatori[17].

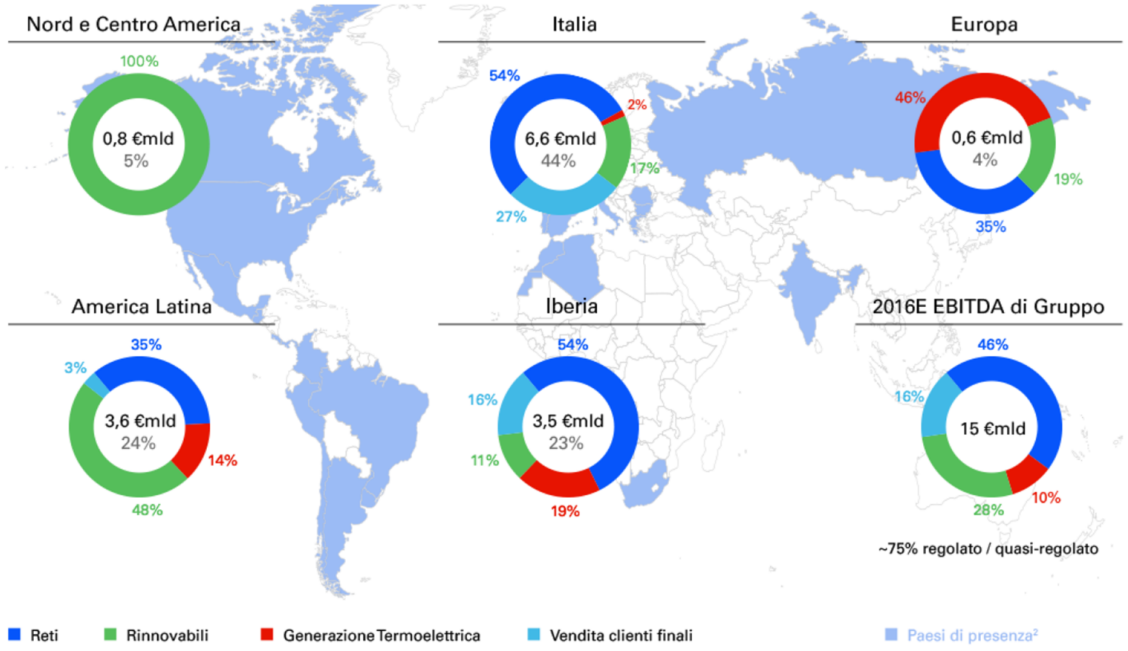
ENEL è dunque oggi un operatore globale, di ragguardevole dimensione, tra le prime 60 aziende al mondo per fatturato, ed è la più grande utility integrata d'Europa in termini di capitalizzazione.

E' presente in oltre 30 paesi nel mondo in 4 continenti, con società di generazione, vendita e distribuzione di energia elettrica. In Europa ha una presenza molto articolata, prioritariamente in Italia e Spagna, ed è inoltre uno dei maggiori operatori energetici delle Americhe.



[17] fonte: https://www.enel.com/it/investors1/a201609-azionisti.html

Distribuzione geografica EBITDA



La società ha una capacità di generazione netta installata di oltre 90 GW, producendo poco meno della metà completamente da fonti di energia pulita. Mantiene in esercizio 1,9 milioni di km di reti, serve oltre 61 milioni di clienti e gestisce i consumi attraverso oltre 40 milioni di smart meter[18].

Il gruppo vanta la costante presenza nei principali indici di sostenibilità quali il Dow Jones Sustainability Index (DJSI World), FTSE4Good, CDP, STOXX Global ESG Leaders Index, gli indici ECPI, e più specificamente gli indici ECPI Global Renewable Energy

[18] fonte: https://www.enel.it/it/azienda/a201610-azienda-globale.html

Equity, ECPI Global Megatrend Equity, ECPI Euro ESG Equity ed ECPI World ESG Equity[19].

Il trend di crescita della popolazione mondiale vede il passaggio da 7 a 8 miliardi di abitanti nei prossimi dieci anni, così come è in aumento la crescita dell'aspettativa di vita e si osserva un progressivo spostamento della popolazione verso le città e le economie emergenti assumono un ruolo sempre più rilevante nel panorama internazionale.

La domanda energetica globale è destinata a crescere, in uno scenario di risorse naturali sempre più limitate e con la necessità di contrastare il cambiamento climatico in atto.

I tradizionali paradigmi stanno, dunque, cambiando rapidamente con opportunità enormi offerte dalle nuove tecnologie. Il ruolo e le responsabilità delle aziende devono restare al passo con questi cambiamenti.

L'azienda, nel proprio bilancio di sostenibilità (che include peraltro una sezione dedicata alla resilienza del gruppo rispetto al rischio Cyber) assume impegni importanti per la sostenibilità a lungo termine del proprio operato nel rispetto delle generazioni future. Espone un approccio strategico definito "Open Power", volendo in tal modo intendere il profondo intento a rispondere alle nuove sfide dello scenario energetico, tecnologico e sociale, globale facendo leva su due driver principali: sostenibilità, innovazione, creazione di valore condiviso.

Un impegno riconosciuto anche a livello internazionale, al punto che l'azienda si è classificata al quinto posto, unica italiana e unica tra le utilities, al ranking del *Fortune Global* tra le *50 aziende che contribuiscono a cambiare il mondo*. [20]

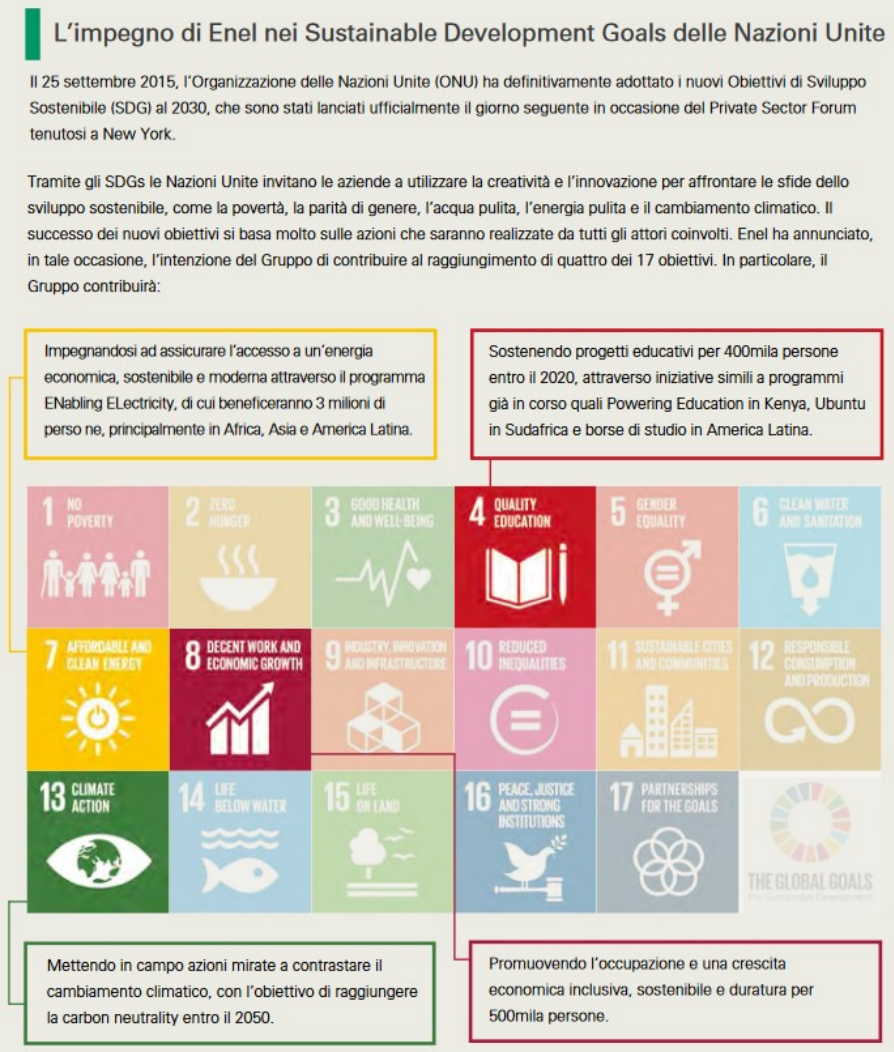
---

[19]https://www.enel.com/it/investors1/a201608-indici-di-sostenibilita.html; https://www.enel.com/it/media/press/d201702-enel-confermata-linclusione-negli-indici-di-sostenibilit-ecpi-.html

[20]https://www.enel.com/it/media/press/d201702-enel-confermata-linclusione-negli-indici-di-sostenibilit-ecpi-.html

Il *'mindset'* di operatore globale responsabile è chiaramente riscontrabile nelle linee strategiche descritte nel piano industriale[21] presentato a Londra lo scorso 22 novembre 2016

Il nuovo piano, tra l'altro, introduce il fattore della digitalizzazione come pilastro fondamentale della strategia di sviluppo[22].



Nel periodo 2017-2019 il gruppo prevede investimenti a tale titolo per 4,7 Miliardi di Euro destinati a digitalizzare gli asset industriali, l'operatività e i processi del Gruppo e potenziare la connettività, con l'obiettivo di generare un incremento

[21]http://strategy2016.enel.com/

[22]https://www.enel.it/it/media/news/d201611-digitalizzazione-e-qualit-la-nuova-dimensione-dellenergia.html

cumulato dell'EBITDA[23] per 1,6 miliardi di euro[24].

Nuove sfide, unite ad un preesistente installato tecnologico imponente, costruito in decenni di costante evoluzione di impianti e sistemi, vanno a determinare dunque uno scenario tecnologico e organizzativo estremamente complesso.

Un contesto, quello dell'ICT del gruppo Enel, attraversato negli ultimi due anni da una trasformazione, di dimensione e profondità senza precedenti su scala globale, orientata verso l'adozione paradigmi di funzionamento più moderni ed efficienti. Una metamorfosi che ha interessato sia il parco applicativi, razionalizzandoli, sia la gestione delle 'Operations' di data centers, oggi Cloud based, ed informatica distribuita. Una revisione dei processi di sviluppo applicativo resi più agili ed orientati al servizio end-to-end ai processi di business.

Sono massicciamente presenti tecnologie in continua evoluzione (cloud, mobile, app, web, Wi-Fi, IoT, etc…) e sono diverse migliaia i sistemi interconnessi: sistemi informativi gestionali (IT) e sistemi di controllo industriali (OT) sviluppati a livello centrale e locale. L'enorme quantità di dati elaborati ogni giorno richiede necessariamente una ferrea organizzazione e un'estrema chiarezza dei flussi di lavoro anche e soprattutto sotto il profilo della cyber security.

---

[23] Ebitda -Earnings Before Interest, Taxes, Depreciation and Amortization, è un indicatore di redditività un'azienda basato solo sulla sua gestione caratteristica ed esprime il vero risultato del business dell'azienda.

[24]https://www.enel.com/content/dam/enel-common/press/it/1666492-1_PDF-1.pdf; http://strategy2016.enel.com/files/Enel_Group_2016_Capital_Markets_Day.pdf

L'habitat di una multinazionale: Complessità tecnologica e normative in continua evoluzione

La gestione di un così articolato ecosistema tecnologico è accompagnato da ulteriori sfide ed opportunità.

Forte è l'attenzione del gruppo al tema dell'innovazione, che è perseguita mediante un processo 'attivo' di ricerca aperto a contributi esterni catturando opportunità a supporto del continuo sviluppo di nuovi progetti, nuove aree di business, nuovi impianti e sistemi industriali.

Operare su scala mondiale richiede di adeguarsi a prescrizioni derivanti da normative e leggi nazionali ed internazionali in continua evoluzione.

Le strategie di posizionamento sul mercato, che prevedono anche una gestione attiva del portafoglio, con conseguenti acquisizioni di nuove società, determina la necessità di poter integrare efficacemente i relativi sistemi informatici e modelli organizzativi rendendoli "compliant" con gli standard di cyber security del Gruppo nel rispetto delle normative globali.

Il tema della sicurezza informatica e della standardizzazione dei processi di sicurezza è dunque per Enel un tema costantemente all'ordine del giorno.

Un approccio innovativo nel panorama internazionale

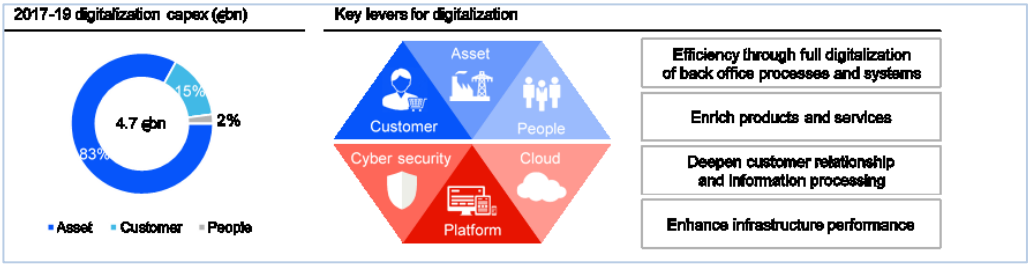
Focalizzando l'analisi sul processo di gestione del rischio Cyber, emerge sin da subito la presenza di caratteristiche innovative.

Torniamo ad osservare quanto descritto nel documento che accompagna la presentazione dello Strategic Plan 2017-2019, del 22 novembre 2016:

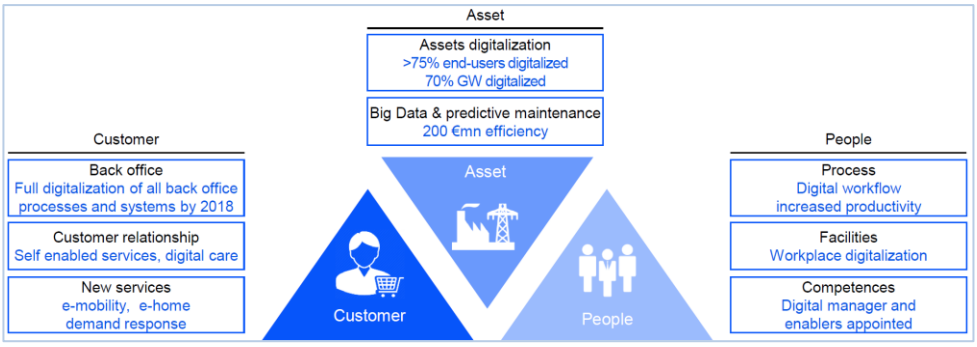
Al presente studio non è sfuggita la lucidità con la quale, contestualmente al lancio della sfida della digitalizzazione, è stata identificata, esposta e chiaramente indirizzata la gestione della minaccia Cyber.

La Cyber Security è stata, infatti, espressamente indicata tra le componenti fondamentali necessarie a sostenere la strategia di digitalizzazione, al fianco del Cloud e dell'uso di piattaforme applicative modulari.

Investimenti in Digitalizzazione pianificati dal gruppo Enel nel triennio 2017-19 [25]

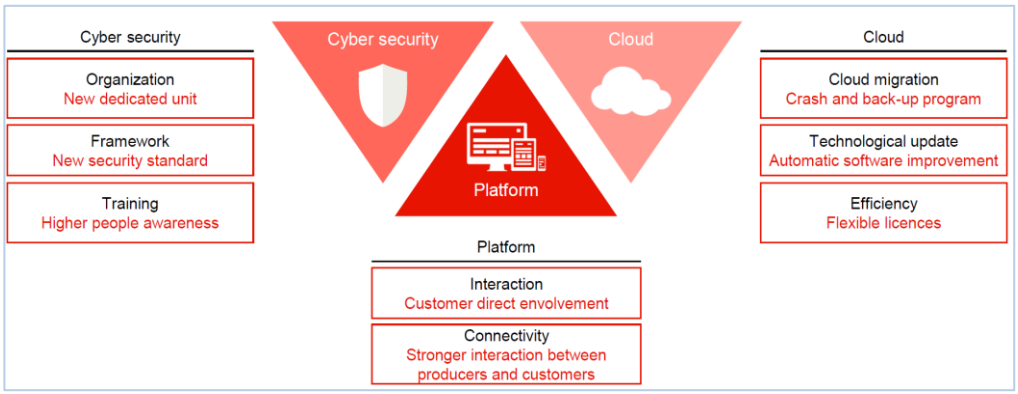


Aree di intervento

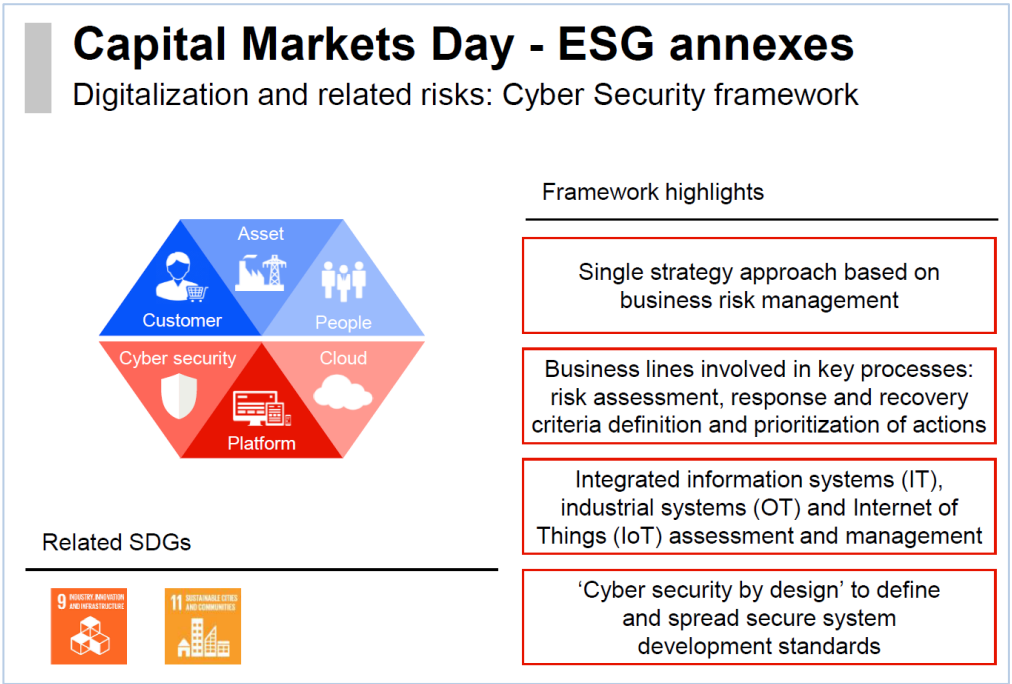


[25] http://strategy2016.enel.com/files/Enel_Group_2016_Capital_Markets_Day.pdf

Colonne portanti della digitalizzazione



Focus sulla Cyber Security, elementi chiave del nuovo framework



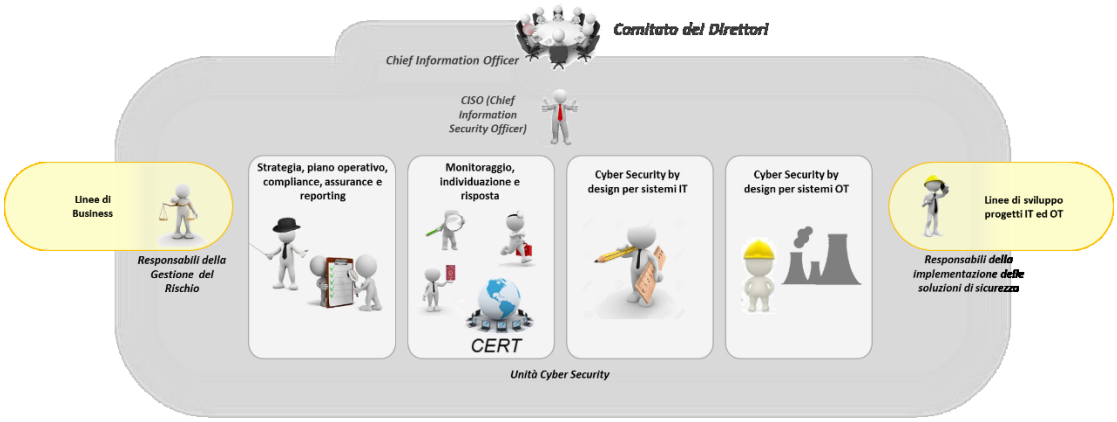
Il nuovo framework della Cyber Security intende quindi indirizzare lo sviluppo e la gestione del ciclo di vita dei progetti con un modello di sicurezza by design, che tenga conto del contesto normativo e delle tecnologie in uso, ma che soprattutto sia bilanciato da un'appropriata valutazione del rischio informatico che consenta di adottare per i progetti IT ed OT le protezioni più adeguate in relazione al danno che i processi di business potrebbero subire in caso di attacco.

Osservando il modello di funzionamento della Cyber Security nel gruppo Enel si sono individuate delle caratteristiche decisamente innovative che non trovano precedenti nel confronto con organizzazioni di analoghe dimensioni, ove persistono modelli di gestione più tradizionali, ovvero:

Gli elementi chiave identificati sono:

- Una *Strategia Risk Based* con il coinvolgimento costante delle Business Lines, mediante assetti organizzativi forti, nelle fasi chiave: analisi del rischio, definizione di criteri «response e recovery» e definizione delle priorità delle azioni da intraprendere;
- l'adozione del principio della *Security by Design*;
- un governo realmente olistico dell'intera superficie di esposizione aziendale ai rischi Cyber mediante gestione integrata di sistemi informatici gestionali (IT), dei sistemi industriali (OT), dell'Internet delle cose (IoT);
- l'integrazione dell'ingegneria delle soluzioni Cyber con le aree di sviluppo applicativo.

Di seguito la struttura organizzativa adottata dal gruppo:



Responsabili della valutazione del rischio (Risk Managers):

E' l'elemento di connessione con ciascuna delle Business Line in modo che la Cyber Security venga vissuta stabilmente all'interno del Business.

E' una risorsa full-time incaricata dell'analisi dei rischi Cyber. Mantiene un legame organizzativo stabile alle aree di business di appartenenza, pur rispondendo contemporaneamente anche al CISO (doppio riporto gerarchico). La particolarità della Risk Based strategy ENEL, come già detto, è infatti la costante presenza delle aree di business all'interno della funzione di Cyber Security con un assetto organizzativo di piena integrazione, così realizzato.

Ma non solo, a questa figura viene chiesto di operare in maniera evoluta per fronteggiare le insidie e le particolarità del rischio cyber, e ciò implica una certa dose di *pensiero laterale.*

Ha la seguente missione:

- Nella fase di Risk assessment:
  - Individuare all'interno della propria area di business di appartenenza (risk assessment standard – Ivi, pagina 43) rischi e minacce che vengono successivamente valutate collegialmente, con la regia del CISO, con una prospettiva di gruppo (approccio olistico) partendo dal presupposto che l'azienda ha una *superficie di esposizione* unica, che prescinde da perimetri organizzativi o geografici.
  - Integrare le analisi classiche basate sul venir meno di un'erogazione/produzione di un servizio con la valutazione del rischio eventualmente rappresentato da un'infrastruttura che va a comportarsi in modo improprio (es. erogando energia quando non dovrebbe). Ciò perché un attacco Cyber può determinare non solo, ovviamente, un'indisponibilità dell'asset, ma anche un suo funzionamento fuori specifiche, che è oggettivamente il maggiore dei rischi possibili.
- Assicura che gli indirizzi strategici ed il piano operativo della Cyber Security siano coerenti con i livelli attesi di copertura dei rischi di sicurezza informatica specifici della propria linea di business.
- Predispone che la propria Linea di business preveda il budget necessario a realizzare gli interventi adeguati per la cyber security.
- Partecipa attivamente alla definizione della Strategia della Sicurezza Informatica considerando i driver provenienti dall'area di business (evoluzione dei mercati, tipologie di frode, etc…)
- Definisce le priorità di intervento pianificando le attività di Cyber Security in funzione del corrispondente rischio di business.

Responsabili dell'implementazione delle soluzioni di sicurezza (Response Managers))

Garantisce l'integrazione tra la Cyber Security e le unità responsabili di sviluppo e gestione delle applicazioni e dei sistemi di automazione (IT, OT e IoT). Anch'egli a livello organizzativo, risponde sia al CISO, sia al Responsabile dell'Unità di cui fa parte, incaricata di sviluppare applicazioni e sistemi per una precisa linea di business (Distribuzione, Mercato, Produzione, etc.).

Questo attore ha una rilevanza fondamentale nel garantire la sicurezza informatica nelle applicazioni e nei sistemi già in esercizio o da realizzare.

In particolare, deve assicurare:

- La corretta attuazione delle misure di sicurezza in conformità con le linee guida e prescrizioni tecniche di sicurezza informatica;
- il supporto al processo di Response della Cyber Security;
- la definizione, pianificazione e implementazione delle attività di rimedio conseguenti ai risultati delle attività svolte sistematicamente da Assurance (penetration test, vulnerability assessment, ethical hacking);
- la partecipazione alle attività di progettazione dell'unità di Ingegneria della Cyber Security nella definizione dei nuovi standard o delle nuove soluzioni di sicurezza.

Funzioni core dell'unità Cyber security:

Non meno importanti sono ovviamente le aree operative demandate a garantire il funzionamento organico dell'unità.

Qui in sintesi:

Una prima area garantisce che venga presidiato:

- Il processo di definizione della strategia di Cyber security del gruppo;
- l'ordinata emissione e aggiornamento delle policy, procedure, line guida e processi inerenti la C.S., monitorando la compliance alla normativa globale;
- l'erogazione dei processi di Assurance (Attività di Vulnerability Assessment e Penetration Test attraverso Hacking Etico sulle proprie infrastrutture);
- la gestione delle campagne di formazione ed educazione al rischio Cyber (Education, Training & Awareness).

Una seconda area garantisce che venga presidiato:

- L'erogazione h24 dei servizi di detection, monitoraggio e gestione degli eventi di sicurezza (incident management);
- la gestione del costituendo CERT del gruppo;
- la gestione il servizio di digital identity management.

Infine, altre due aree, una per l'ambito IT (Information Technology) l'altra per l'ambito OT (Operation Technology), sono incaricate di:

- Propagare le pratiche di sviluppo sicuro guidando l'adozione del paradigma di Security by design;
- Guidare l'ingegneria della Sicurezza Informatica, identificando soluzioni e best practice di gruppo e stabilendo prescrizioni tecniche vincolanti.

I due ambiti IT e OT, evolvono costantemente e le relative tecnologie procedono intersecandosi frequentemente ma mantenendo consistenti specificità e differenti priorità. L'ambito IT è infatti caratterizzato dal primario obiettivo di proteggere la riservatezza delle informazioni, mentre l'ambito OT ha come obiettivo primario garantire la disponibilità degli impianti.

Anche i contesti fisici in cui operano i sistemi e le architetture sono molto diverse, ne consegue che le soluzioni da identificare e realizzare, al netto delle componenti comuni, richiedono competenze e tecnologie specifiche.
L'armonizzazione di IT e OT è dunque fondamentale al fine di poter raggiungere un alto grado di sicurezza. L'esistenza di due aree di specializzazione risponde a questa necessità.

Awareness, l'importanza del fattore umano:

Un'efficace gestione del rischio non può prescindere dal proteggere uno degli elementi più vulnerabili: l'uomo.
L'awareness è un elemento fondamentale è necessario dare alle persone informazioni e strumenti per essere attenti e coscienti del rischi. L'obiettivo è che gli utenti imparino ad interagire con la tecnologia, senza introdurre ingiustificati timori, ma pienamente coscienti dei pericoli derivanti da un uso troppo disinvolto.
Sotto il profilo della cyber security ogni persona che lavora o collabora all'interno del gruppo deve quindi conoscere le corrette pratiche di gestione. Per questo Enel ha attivato diverse campagne di sensibilizzazione sul tema della sicurezza, veicolate a tutti i livelli organizzativi ed utilizzando linguaggi e temi comprensibili a ciascun ambito aziendale.

Il CERT

La strategia di Cyber Security di Enel prevede la costituzione di un Computer Emergency Response Team (CERT) per una più efficace prevenzione e risposta ai possibili incidenti di sicurezza su sistemi IT ed OT. Il CERT di Enel avrà un ruolo attivo all'interno della comunità Internazionale della Cyber Security, promuovendo l'info-sharing che è alla base stessa del paradigma di collaborazione pubblico-privato. Sarà accreditato nei principali paesi nel mondo in cui è presente un CERT nazionale istituzionale.

Innovazione

Il gruppo è naturalmente un rilevante utilizzatore di soluzioni tecnologiche di primaria qualità reperibili sul mercato. La strategia di Cyber Security di Enel però, prevede anche

una ricerca attiva di soluzioni innovative, anche ancora in fase di sviluppo, purché siano adatte ad essere 'scalate' sulla dimensione della stessa.
Collaborando strettamente con la Funzione Innovation del gruppo, l'unità di Cyber Security effettua un sistematico scouting delle proposte emergenti nel mondo delle Start-Up anche mediante l'organizzazione di competizioni (Hackathon) aprendo ai vincitori opportunità di test in campo reale delle soluzioni, con l'obiettivo di sperimentare soluzioni fortemente innovative che includono le più recenti tecnologie di Machine Learning e Big-Data Analytics.

Definizione del Cyber Security Framework

Si è provveduto ad analizzare i principali processi di funzionamento allo scopo di riscontrate la rispondenza al framework preso a riferimento.
Si incontra quanto di seguito sintetizzato.

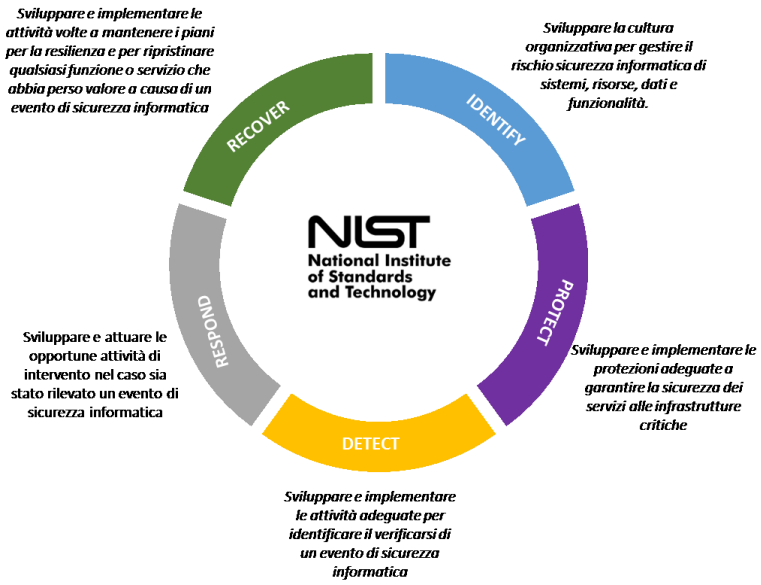
Obiettivi:

- Definire una strategia di sicurezza Informatica basata su una corrispondente valutazione del rischio calato sui processi di business;
- Realizzare un modello di protezione delle applicazioni e sistemi a supporto dei processi di business basato sulla "cyber security by design", che consenta di progettare I requisiti di sicurezza a partire dalle fasi iniziali del progetto e di manutenerle per tutto il ciclo di vita del progetto stesso, ottimizzando i costi;
- Attivare un processo di miglioramento continuo di sistemi gestionali ed industriali che consenta di mantenere, nel tempo, un adeguato livello di sicurezza coerente con il livello di rischio tollerato e con la continua evoluzione delle minacce.

Punti chiave

- **Forte coinvolgimento del Top Management** tramite il **CIO**[26] per indirizzare, realizzare e rispettare la strategia di sicurezza Informatica;
- **Indirizzo Globale della cyber security,** guidata dal **CISO**[27] con l'ausilio delle Aree di Business, definendo in modo adeguato le priorità delle iniziative e misurando gli investimenti necessari in proporzione al rischio coperto ed in relazione alle diverse tecnologie (sistemi IT ed OT).
- **Verifica del livello di protezione** di sistemi IT ed OT utilizzati dalle diverse Aree di business per individuare ed adottare i miglioramenti necessari a proteggerli in modo adeguato rispetto al rischio dei corrispondenti processi di business supportati.

Mappatura del Framework ENEL sullo standard NIST

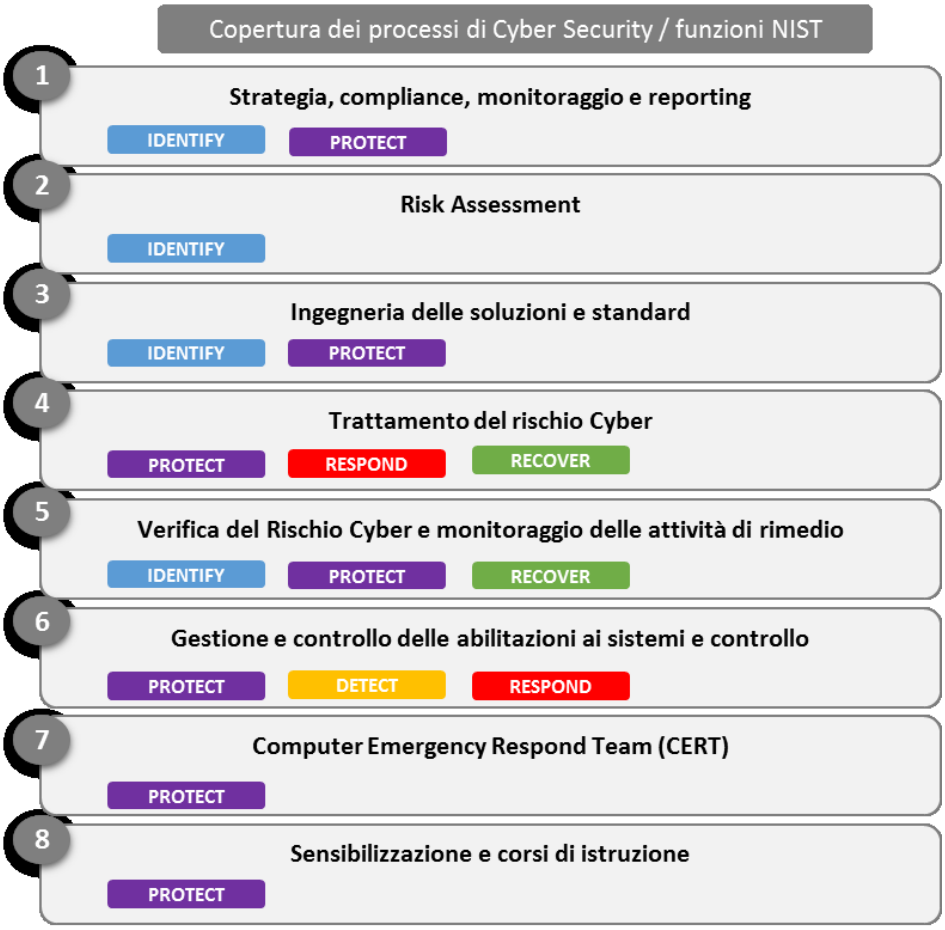


[26] Chief Information Officer

[27] Chief Information Security Officer

Il Cyber Security Framework ENEL è stato sviluppato in modo da declinare un set di processi operativi chiaramente riconducibili alle funzioni del framework NIST[28] preso a modello.

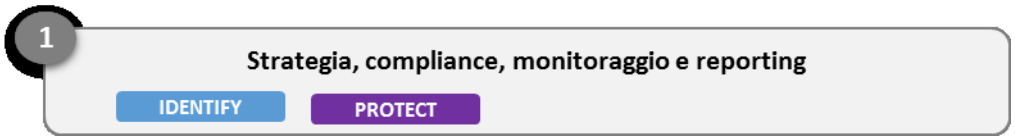
La rappresentazione della struttura è riportata di seguito:



Analizzando specificatamente le fasi e i flussi di processo, occorre previamente osservare che le azioni indicate sono state anche, contestualmente, attribuite ai diversi attori attraverso una matrice di assegnazione di responsabilità RACI (Responsible, Accountable, Consulted, Informed). L'esistenza di tale matrice è fatto assai rilevante ai

[28] Si veda sull'argomento, il paragrafo "Sicurezza cibernetica: una priorità globale", al capitolo su "La Cyber Security".

fini del presente studio in quanto essa è un elemento di grande sostegno all'effettività ed integrità dei processi descritti. Tuttavia, la sua articolazione è stata qui omessa, a favore di una maggiore leggibilità, in quanto il suo contenuto è univocamente contestualizzato alla specifica realtà aziendale.



Strategia, compliance, monitoraggio e reporting	
Definizione e approvazione del piano strategico (1/5)	
Input da esiti attività anno precedente:	• Risk Assessment; • Analisi Assurance; • Piano strategico / piano operativo; • Evidenze dal CERT; • Solution scouting; • Evoluzione dei mercati; • Evoluzione del Business; • Evoluzione delle tecnologie; • Indirizzi strategici del Gruppo; • Evoluzione delle tipologie di attacco informatico.
Azioni:	• Definizione piano strategico; • Condivisione; • Approvazione.
Output:	• Piano strategico approvato (globale, per area di business, per Paese, per sistemi IT ed OT).

Strategia, compliance, monitoraggio e reporting	
Definizione e approvazione del piano operativo (2/5)	
Input:	• Piano strategico.
Azioni:	• Definizione delle iniziative di Cyber Security necessarie. • Definizione dei KPI e KRI necessari alla supervisione delle iniziative pianificate. • Condivisione. • Approvazione.
Output:	• Piano operativo approvato (globale, per area di business e per sistemi IT ed OT) • KPI e KRI (globali, per area di business, per Paese, per sistemi IT ed OT)

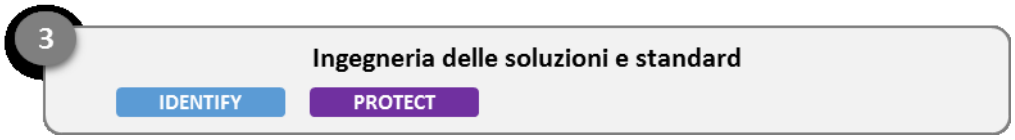
Strategia, compliance, monitoraggio e reporting	
Implementazione del piano operativo (3/5)	
Input:	• Piano operativo • KPI e KRI
Azioni:	• Definizione dei piani di attività necessarie a realizzare il Piano operativo. Programmazione dei progetti e attività a piano in termini di risorse (umane, economiche, tecnologiche) e tempi. • Condivisione. • Approvazione.
Output:	• Piani di attività e progetti di Cyber Security (globali, per area di business, per Paese, per sistemi IT ed OT)

Strategia, compliance, monitoraggio e reporting	
Monitoraggio del piano operativo e Reporting (4/5)	
Input:	• Stato avanzamento di Piani di attività e progetti di Cyber Security
Azioni:	• Monitoraggio del piano operativo; • Valutazione dei KPI e dei KRI; • Valutazione eventuali modifiche, ritardi; • Predisposizione reportistica executive e operativa;
Output (globali, per area di business, per Paese, sistemi IT ed OT):	• Reporting executive ed operativo con KPI e KRI del Piano operativo e dei relativi piani di attività e progetti. • Evidenziazione esiti KPI e KRI • Evidenziazione eventuali ripianificazioni o cambiamenti • Eventuale intervento sul piano strategico in caso di eventi eccezionali.

Strategia, compliance, monitoraggio e reporting	
Definizione policies e procedure (5/5)	
Input:	• Leggi e normative • Esigenze aziendali Globali o Locali • Rapporti con Enti Esterni;
Azioni:	• Definizione delle politiche di sicurezza informatica in linea con Leggi e Normative vigenti nei Paesi; • Definizione delle politiche di sicurezza informatica in linea con esigenze di processo e aziendali;
Output:	• Policy e procedure (globali, per area di business, per Paese, per sistemi IT ed OT).

Risk Assessment	
Definizione e pianificazione Risk Assessment (1/2)	
Input da anno precedente:	• Risk Analisis / BIA eseguite; • Mappa dei processi di Business; • Mappa delle applicazioni IT; • Mappa delle applicazioni OT; • Mappa dei Processi / Sistemi IT ed OT; • Risk Assessment; • Rischi e minacce emergenti; • Esiti di attività di Audit; • Esiti attività di Assurance; • Evidenze dal CERT
Azioni:	• Collazione, analisi e correlazione degli input • Definizione del piano di attività; • Condivisione e approvazione.
Output:	• Risk Assessment fase 1 (aggiornato sulla base degli input anno precedente); • Piano di attività (Lista ad integrazione delle «Risk Analysis» già eseguite, conseguente a variazioni intercorse, ad introduzione di nuovi sistemi, ad integrazione di Risk Analysis non ancora eseguite, a variazioni di perimetro, a nuove leggi, etc…).

Risk Assessment	
Esecuzione Risk Assessment (2/2)	
Input:	• Risk Assessment fase 1; • Piano di attività (Lista ad integrazione delle «Risk Analysis» già eseguite, conseguente a variazioni intercorse, ad introduzione di nuovi sistemi, ad integrazione di Risk Analysis non ancora eseguite, a variazioni di perimetro, a nuove leggi, etc…).
Azioni:	• Esecuzione delle Risk Analisis di sistemi e applicazioni; • Aggregazione degli esiti delle Risk Analisis a rappresentazione del rischio per processo; • Rappresentazione degli esiti • Condivisione e approvazione risultati.
Output:	• Risk Assessment «target» rappresentante il rischio per processi e applicazioni / sistemi (globale, per area di business, per Paese, per sistemi IT ed OT)



Ingegneria delle soluzioni e standard	
Predisposizione Linee Guida e prescrizioni tecniche; scouting tecnologie e soluzioni (1/2)	
Input:	• Nuove tecnologie; • Standard internazionali; • Normative di riferimento; • Progetti innovativi; • Nuovi scenari. • Partecipazione a convegni • Valutazione coinvolgimento «Sturt Up» • Valutazione richieste / casi d'uso provenienti dalle linee di Business • Partecipazione a comitati di normazione;
Azioni:	• Predisposizione Linee Guida e prescrizioni tecniche; • Partecipazione a progetti innovativi; • Analisi di particolari soluzioni o esigenze di Business non indirizzate dalle Linee Guida o Prescrizioni tecniche esistenti. • Partecipazione ad organismi internazionali di normalizzazione o gruppi di esperti al fine di tenere il passo con i tempi anticipando ed indirizzando standard e normative internazionali in base alle esigenze dell'azienda.
Output:	• Emissione Linee Guida e Prescrizioni Tecniche; • Partecipazione attiva all'emissione di standard internazionali. • Definizione soluzioni ad hoc per esigenze particolari derivanti da casi d'uso e nuove esigenze di business, nuovi progetti.

Ingegneria delle soluzioni e standard	
Implementazione delle soluzioni Cyber Security nei progetti (2/2)	
Input:	• Nuovi progetti • Varianti di progetti esistenti • Progetti strategici
Azioni:	• Esecuzione o revisione della Risk Analysis a cura dei Responsabili della gestione del rischio. • Per i progetti rilevanti (strategici) e per i progetti le cui soluzioni di sicurezza non sono ancora normate diretto coinvolgimento dell'ingegneria della Cyber Security a partire dalla Risk Analisys. • Per i progetti già normati dalle linee guida coinvolgimento dei Responsabili delle soluzioni di sicurezza che garantiscono, a partire dalla Risk Analisys, che l'implementazione sia in linea con gli Standard di Sicurezza e le Guide Line definite dall'ingegneria della Cyber Security.
Output:	• Definizione delle soluzioni di sicurezza secondo il criterio della security by design (sicurezza pensata fin dall'inizio delle attività di progettazione del nuovo sistema o della modifica

Trattamento del rischio Cyber	
Definizione trattamento delle vulnerabilità e carenze (1/3)	
Input:	• Vulnerabilità rilevate e il livello relativo di gravità (applicative, infrastrutturali, TLC); • Carenze nelle misure di sicurezza messe in atto
Azioni:	• Analisi possibili soluzioni • Definizione piano di rimedio • Condivisione • Approvazione
Output:	• Piani di rimedio approvati (globale, per area di business, per Paese, per sistemi IT ed OT)

Trattamento del rischio Cyber	
Implementazione delle risoluzioni (2/3)	
Input:	• Piani di rimedio approvati (globale, per area di business, per Paese, per sistemi IT ed OT)
Azioni:	• Esecuzione attività di rimedio
Output:	• Lista delle attività di rimedio completate (globale, per area di business, per Paese, per sistemi IT ed OT).

Trattamento del rischio Cyber	
Piani di risoluzione e monitoraggio (3/3)	
Input:	• Lista delle attività di rimedio completate (globale, per area di business, per Paese, per sistemi IT ed OT).
Azioni:	• Aggiornamento dei piani di rimedio approvati e calcolo dei relativi KPI - KRI
Output:	• Redazione di Report executive e operativi per la valutazione e rappresentazione coerente dei risultati e la pianificazione di eventuali retroazioni (azioni di recupero), con evidenziazione KPI e KRI.

Verifica del Rischio Cyber e monitoraggio delle attività di rimedio	
Definizione del piano di Assurance (1/3)	
Input:	• Risk Assessment; • Attività Assurance precedenti; • Piano strategico / piano operativo; • Evidenze dal CERT; • Indirizzi dal Business • Evoluzione delle tipologie di attacco informatico.
Azioni:	• Definizione piano di Ethical Hacking • Condivisione • Approvazione
Output:	• Piano di Assurance (globale, per area di business, per Paese, per sistemi IT ed OT) (Penetration Test, Ethical Hacking, Malware Analysis, compliance verification, risk analysis, overview of disaster recovery and business continuity plans etc.)

Verifica del Rischio Cyber e monitoraggio delle attività di rimedio	
Esecuzione del piano di Assurance (2/3)	
Input:	• Piano di Assurance
Azioni:	• Esecuzione attività di verifica sui sistemi IT ed OT a piano ed individuazione delle carenze. • Analisi delle possibili attività di rimedio ed approvazione.
Output:	• Vulnerabilità rilevate e il livello relativo di gravità (applicative, infrastrutturali, TLC); • Carenze nelle misure di sicurezza messe in atto;

Verifica del Rischio Cyber e monitoraggio delle attività di rimedio	
Monitoraggio del piano di Assurance (3/3)	
Input:	• Vulnerabilità / carenze rilevate • Piani di rimedio approvati.
Azioni:	• Verifica della copertura vulnerabilità / carenze e relativi piani di rimedio approvati. • Calcolo dei KPI / KRI • Verifica delle attività di rimedio completate (a campione o completa).
Output:	• Report executive e operativi rappresentanti la situazione; • Escalation nel caso di carenze nella copertura dei piani di rimedio e nelle misure di sicurezza messe in atto; • Pianificazione follow up per la verifica puntuale di situazioni particolari

Gestione delle abilitazioni ai sistemi e controllo	
Gestione dell'infrastruttura (1/3)	
Input:	• Infrastruttura di Identity Access Management
Azioni:	• Valutare evoluzioni dell'infrastruttura al fine di gestire correttamente tutte le identità nella Società • Supervisione delle identità IT / OT / IoT per autenticazione / autorizzazione implementazioni di soluzioni.
Output:	• Report delle carenze ed evoluzioni possibili

Gestione delle abilitazioni ai sistemi e controllo	
Ciclo di vita degli accessi logici (2/3)	
Input:	• Report delle carenze ed evoluzioni possibili
Azioni:	• Valutazione e pianificazione dei miglioramenti in relazione alle priorità ed esigenze delle linee di business (ad esempio applicazioni ICFR Relevant, etc.) • Definizione / aggiornamento delle politiche di sicurezza e dei principi SOD.
Output:	• Pianificazione attività di miglioramento condivise.

Gestione delle abilitazioni ai sistemi e controllo	
Gestione degli accessi logici - controllo e reporting (3/3)	
Input:	• Estrazioni periodiche o su richiesta di utenti e ruoli da sistemi e applicazioni
Azioni:	• Verifica ID utente e Ruoli assegnati con le corrispondenti prescrizioni delle politiche di sicurezza. • Verifica con incrocio dati tra ID utente con evidenziazione incongruenze tra reale e stato teorico degli User ID gestiti a sistema.
Output:	• Pianificazione eventuali attività di bonifica

Computer Emergency Respond Team (CERT)	
CERT soluzioni e setup dei servizi (1/3)	
Input:	• Infrastruttura CERT (Consolle di monitoraggio, IDS, IPS, Firewall, Sonde, etc…)
Azioni:	• Supervisione della realizzazione e valorizzazione di soluzioni e servizi di sicurezza informatica per il monitoraggio e la risposta ad attacchi Cyber sui sistemi IT, OT, sui dispositivi utente e le TLC; • Set Up, in linea con gli indirizzi strategici, della rete e delle infrastrutture di sicurezza per il rilevamento e la risposta degli ambienti IT e OT, in collaborazione con le Unità di Business pertinenti. • Monitoraggio e valutazione dei "prodotti" per la protezione dei sistemi IT e OT (ad esempio firewall, sistemi di intrusion detection / prevention, web, contenuti di sicurezza elettronica di filtraggio) e per la protezione degli End Point (ad esempio antivirus, protezione comportamentale, firewall personale)
Output:	• Risultati delle valutazioni con eventuali azioni di rimedio finalizzate ad un costante miglioramento dei servizi offerti, al passo con l'evoluzione degli attacchi.

Computer Emergency Respond Team (CERT)	
CERT Monitoraggio e risposta ad attacchi (2/3)	
Input:	• Eventi da infrastruttura CERT (Consolle di monitoraggio, IDS, IPS, Firewall, Sonde, etc..
Azioni:	• Monitoraggio costante per individuazione anomalie ed eventuali risposte, al fine di assicurare consentendo la gestione di servizi nel pieno rispetto di livelli di sicurezza richiesti. • Vulnerability Assessment periodici. • Attacchi DDoS mitigazione. • Security patch supervisione.
Output:	• Monitoraggio costante per individuazione anomalie ed eventuali risposte, al fine di assicurare consentendo la gestione di servizi nel pieno rispetto di livelli di sicurezza richiesti. • Vulnerability Assessment periodici. • Attacchi DDoS mitigazione. • Security patch supervisione.

Computer Emergency Respond Team (CERT)
CERT Reporting (3/3)

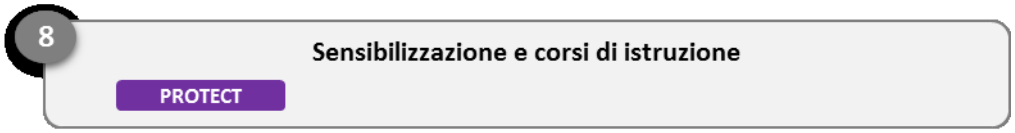
Input:	• Monitoraggio costante per individuazione anomalie ed eventuali risposte, al fine di assicurare consentendo la gestione di servizi nel pieno rispetto di livelli di sicurezza richiesti. • Vulnerability Assessment periodici. • Attacchi DDoS mitigazione. • Security patch supervisione.
Azioni:	• Monitoraggio costante per individuazione anomalie ed eventuali risposte, al fine di assicurare consentendo la gestione di servizi nel pieno rispetto di livelli di sicurezza richiesti. • Vulnerability Assessment periodici. • Attacchi DDoS mitigazione. • Security patch supervisione.
Output:	• Monitoraggio costante per individuazione anomalie ed eventuali risposte, al fine di assicurare consentendo la gestione di servizi nel pieno rispetto di livelli di sicurezza richiesti. • Vulnerability Assessment periodici. • Attacchi DDoS mitigazione. • Security patch supervisione.

La costituzione di un CERT[29], o dell'equivalente CSIRT[30], consente di gestire efficacemente le prime risposte alle minacce informatiche o eventi di sicurezza e a condividere rapidamente informazioni con vari attori - interni ed esterni all'Impresa, oltre che istituzionali - circa le minacce correnti, attuando l'information sharing (ENISA, 2015)[31], allo scopo di contribuire ad una resilienza sistemica globale dell'Azienda e di tutto il sistema Paese (Baldoni e Montanari, 2016).

[29] Sui CERT, nazionali ed europei, e sul CERT-PA, si rinvia al paragrafo su "La politica di sicurezza cibernetica in Italia", nel capitolo su "La cyber security".

[30] CSIRT - Computer Security and Incident Response Team

[31] https://www.enisa.europa.eu/publications/cybersecurity-information-sharing/at_download/fullReport



Sensibilizzazione e corsi di istruzione	
Istruzione e sensibilizzazione definizione piani (1/3)	
Input:	• Evidenze provenienti dal CERT, evoluzione delle tipologie di attacco, eventi di attacco più comuni. • Piano Strategico e piano operativo. • Evidenze provenienti dalle attività di Assurance.
Azioni:	• Definizione e condivisione dei piani di sensibilizzazione e di istruzione realizzati ad hoc in relazione al target dei discenti.
Output:	• Piani di sensibilizzazione e istruzione approvati.

Sensibilizzazione e corsi di istruzione	
Istruzione e sensibilizzazione pianificazione progettazione ed esecuzione piani (2/3)	
Input:	• Piani di sensibilizzazione e istruzione approvati.
Azioni:	• Definizione di un piano dettagliato deli corsi di istruzione e delle attività di sensibilizzazione (programmazione tempo, i canali di comunicazione più efficaci per massimizzare l'appello del messaggio, l'utilizzo dei mezzi di comunicazione, logistica, etc.); • Sviluppo di consapevolezza e di materiale di formazione, appropriato e tempestivo per il pubblico previsto.
Output:	• Esecuzione dei corsi e delle attività di sensibilizzazione • Monitoraggio dei KPIs e dello stato di avanzamento delle attività.

Sensibilizzazione e corsi di istruzione	
Iniziative non pianificate – risposte mirate (3/3)	
Input:	• Pianificazione tempestiva delle risposte a nuovi rischi, violazioni della sicurezza poco note, minacce e incidenti occorsi.
Azioni:	• Definizione dell'iniziativa necessaria in termini di target di riferimento e contenuti di comunicazione; • Definizione del canale migliore comunicazione idoneo a supportare l'iniziativa.
Output:	• Esecuzione dell'iniziativa e monitoraggio del livello di recepimento ottenuto (KPIs) e dello stato di avanzamento delle attività

Considerazioni sul caso di studio

L'osservazione del caso di studio fornisce alcuni interessanti spunti di riflessione in quanto, ancorché fosse atteso incontrare una adeguata maturità, anche tecnologica, sul tema da parte di un operatore di questo tipo, sorprendentemente le caratteristiche che appaiono particolarmente innovative sono di tipo organizzativo, più che tecnologico.

Nei grandi gruppi, i perimetri organizzativi producono barriere a volte invalicabili che rendono difficoltoso il cambiamento della struttura (Beckhard, 1969; Touhill, 2015). Ciò diventa ancora più critico per aziende con rilevanti asset industriali, nelle quali una mancata gestione integrata della sicurezza IT e OT può determinare una grande ed ingovernabile esposizione al rischio cibernetico. Nel caso di studio, invece, emerge in maniera evidente l'impegno e la determinazione del vertice aziendale per istituire una gestione realmente 'olistica' del rischio Cyber.

Nel corso dello studio di caso, si è dunque rilevata un'inedita configurazione gerarchico-funzionale poiché, nell'azienda esaminata, lo schema di management della cyber security è trasversale rispetto alla struttura organizzativa aziendale, integrandosi in diversi punti della stessa, configurando dei "doppi riporti" gerarchico-funzionali in capo ad alcune figure incaricate dell'analisi del Cyber Risk, operanti all'interno delle Business Lines, che rappresentano l'elemento di connessione con l'Unità apicale di Cyber Security del Gruppo.

Si tratta di una struttura organizzativa che mostra evidenti elementi di originalità, non agevolmente inquadrabili sotto il profilo teorico in un'unica Teoria del Management, ma che si presta semmai ad un'analisi multi-prospettica, potendosi individuare alcuni elementi caratteristici della *System Theory* (von Bertalanffy, 1934; Beers, 1959, 1966; Johnson, 1964) rappresentati, in primo luogo, dall'approccio *olistico* al tema del Cyber Risk Management, o della prospettiva dinamico-evolutiva della *Learning Organization* (Argyris and Schön, 1978; Argyris, 1982) per il carattere ricorsivo di alcuni processi della Strategia Risk Based o, infine, dal *Business Process Reengineering* BPM (Hammer and Champy, 1993) per l'insieme delle azioni tecniche e organizzative poste in essere dal

Management del Gruppo ENEL per ottenere il livello ottimale di Cyber Security con la massima efficienza e al minimo costo.

Nell'analisi effettuata, si è altresì verificato che il livello di coinvolgimento delle aree di business nella gestione quotidiana del rischio cyber è davvero ragguardevole. Tale scelta ha evidenti effetti positivi sull'intera catena del valore (Porter, 1985), in tutte le fasi chiave dei processi cyber, mettendo in condizione coloro i quali lavorano alla realizzazione di applicazioni e sistemi, di identificare le soluzioni tecniche ottimali, realizzando una concreta '*Security by design*' (Casola et al., 2016; Schoknecht et al., 2016) ed anche coloro i quali monitorano gli eventi di sicurezza, in condizione di fare scelte più corrette durante le operazioni di contrasto.

Si prenda ad esempio la metodologia di *Business Impact Analisys* (BIA) (Radeschütz, 2015), da tempo usata nel Gruppo, che è stata aggiornata per recepire i benefici dell'accresciuta profondità di analisi oggi possibile. Oltre a permettere una valutazione più rispettosa delle già descritte specificità dei contesti IT e OT, il nuovo modello consente l'identificazione di punti di intervento a livello funzionale, sia nei processi che, conseguentemente, negli applicativi, in passato non rintracciabili, consentendo di generare soluzioni *'intrinsecamente'* molto più sicure rispetto alle minacce provenienti dal cyber spazio.

E' tuttavia evidente che il solo assetto organizzativo non è sufficiente a contrastare il rischio cibernetico. Quello Cyber è un ambito tecnologico nel quale occorre che gli strumenti messi in campo siano aggiornati ed efficienti. Anche su questo fronte si è riscontrato un sistematico processo di ricerca di soluzioni innovative, ad esempio con sperimentazione avanzata di tecnologie di identificazione delle anomalie di traffico dati, basate su recentissime tecniche di *machine learning* (Alpaydin, 2004, Carbonell et al., 1983).

CONSIDERAZIONI FINALI E SVILUPPI FUTURI

Nonostante vi sia un grande fermento intorno a temi come Industrie 4.0, Internet degli Oggetti, Intelligenza Artificiale, Cloud, Machine/Deep Learning, ecc. la ricerca accademica appare in ritardo rispetto alle esigenze contingenti del mondo industriale, del settore pubblico e della società civile in genere. La review della letteratura sul tema del Cyber Security Risk Management per le Infrastrutture Critiche ha evidenziato che le pubblicazioni sul tema provengono da autori di area tecnico-scientifica e, al contrario, vi è una totale assenza di contributi rinvenienti da indagini condotte da studiosi di estrazione economico-organizzativa, o di management, o comunque afferenti all'Area delle Scienze Sociali o Aziendali. Un aspetto, quest'ultimo, alquanto rilevante poiché, come riportato nel presente lavoro, il tema della sicurezza informatica coinvolge tutti i settori della società: la Pubblica Amministrazione, il sistema produttivo, la sicurezza e i servizi essenziali per il cittadino, la sicurezza nazionale; in sintesi, il sistema Paese nel suo complesso, con tutte le implicazioni di natura economica, sociale e geopolitica che ne conseguono.

Gli esiti dell'indagine relativi alla prima domanda di ricerca ("Q1 - *L'eterogeneità e la multilateralità delle minacce nel cyber-space richiede nuovi strumenti per la valutazione del rischio?")* hanno permesso di riscontrare l'effettivo sviluppo di nuovi e più adatti modelli o algoritmi specializzati per la cyber risk analisys, anche se le soluzioni proposte risultano molto orientate agli aspetti tecnologici e informatici della questione ed è improbabile che da sole possano rappresentare una risposta adeguata in tema di Cyber Security Risk Management.

L'indagine empirica relativa alla seconda domanda di ricerca *("Q2 - in un contesto economico-organizzativo reale e complesso come quello di una grande Impresa, nuovi e specifici strumenti o l'evoluzione di altri già presenti, rivenienti dal mondo della ricerca, sono direttamente ed efficacemente impiegati?"*), rappresentata dal caso di studio del Gruppo ENEL, ha evidenziato che non è possibile considerare "direttamente ed efficacemente" applicabili all'interno del contesto aziendale gli algoritmi e i framework delle soluzioni presentate nei lavori scientifici selezionati.

Oltretutto nell'impostazione del Cyber Risk Management in ENEL, gli elementi più innovativi sono stati introdotti all'interno del modello organizzativo e nelle modalità di coinvolgimento del management e dei soggetti operanti nelle Aree di Business, definendo procedure, prassi e logiche di sicurezza che permeano tutti i livelli dell'organizzazione e del management, relegando le soluzioni squisitamente tecnologiche ai processi operativi.
Sotto il profilo tecnologico, ENEL sta sperimentando soluzioni avanzate nel campo dei Big Data, degli Analytics e del Machine Learning, a supporto delle funzioni di identificazione delle minacce cibernetiche e non si esclude che algoritmi "evoluti", come quelli rintracciati con la state-of-the-art review effettuata, possano essere implementati nell'attività di Risk Assessment aziendale e contribuire ad innalzare il livello di *cyber resilience* (Goldman et al., 2011; Arghandeh et al., 2011; Jason, 2015) dell'Azienda nel suo complesso.
In effetti, non sono stati individuati modelli scientifici di tipo aziendale, che affrontino il Cyber Risk Management delle Infrastrutture Critiche, ad esclusione della letteratura di Area Tecnico-Scientifica, relativa ad aspetti specificamente tecnologici o, comunque, con modelli semplificati di natura meramente operativa. Questo mostra un significativo 'gap' della ricerca che rende ancor più evidente quanto ampi siano gli spazi di indagine che si prospettano in connessione con il tema trattato e che sarebbe opportuno approfondire.
Nel dettaglio, occorrerebbe elaborare un framework per la valutazione del cyber risk, sviluppato nella prospettiva aziendalistica, in grado di fornire la stima del rischio cibernetico con parametri economici e finanziari, a supporto delle decisioni del management aziendale. Andrebbero sviluppati modelli di management di tipo adattivo capaci di aumentare la resilienza dell'Impresa rispetto al Cyber Risk e, possibilmente, da sperimentare in campo.
Inoltre, occorrerebbe analizzare, su una scala più ridotta, ma al contempo più variegata, la realtà delle piccole e medie imprese, definendo i modelli applicabili alla specifica realtà delle PMI, con un approccio di tipo olistico, che, come nel caso di studio esaminato, è già risultato efficace nelle grandi aziende.

BIBLIOGRAFIA

Alcaraz, C. and Zeadally, S., (2013). Critical Control System Protection in the 21st Century: Threats and Solutions, in IEEE Computer, vol. 46, num. 10, pp. 74-83, ISSN: 0018-9162.

Alpaydin, E., (2004). Introduction to Machine Learning, The MIT Press, Cambridge MA, ISBN 0-262-01211-1

Amantini, A., Choraś, M., D'Antonio, S. et al., (2012). The human role in tools for improving robustness and resilience of critical infrastructures, Cognition Technology & Work. 14: 143. doi:10.1007/s10111-010-0171-2

Arghandeh, R., von Meier, A., Mehrmanesh, L., Mili, L., (2016). On the definition of cyber-physical resilience in power systems, Renewable and Sustainable Energy Reviews, Vol. 58, Pag. 1060–1069. http://dx.doi.org/10.1016/j.rser.2015.12.193

Argyris, C., (1982). Organizational learning and management information systems, ACM SIGMIS Database, Vol. 13 Issue 2-3, Winter-Spring, Pages 3-11, ACM New York, NY, USA. Doi:10.1145/1017692.1017693

Argyris, C., Schön D. A., (1978). Organizational Learning: A Theory of Action Perspective, Addison Wesley, Reading, MA

Ashok, A., Hahn, A., Govindarasu, M. (2014). Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment, Journal of Advanced Research, Vol. 5, Issue 4, 481-489, ISSN 2090-1232, http://dx.doi.org/10.1016/j.jare.2013.12.005.

Aven, T., (2004). Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective, Book, ISBN: 9780471495482, Online ISBN: 9780470871249. Wiley Online Library, DOI: 10.1002/0470871245

Aven, T., (2009). Identification of safety and security critical systems and activities, Reliability Engineering & System Safety, Vol. 94, Issue 2, 404-411, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2008.04.001

Aven, T., (2012). Foundations of Risk Analysis, Second Edition, Book, ISBN: 9781119966975 Online ISBN: 9781119945482. Wiley Online Library
DOI: 10.1002/9781119945482

Baheti, R., Gill, H., in T. Samad, T., Annaswamy, A.M., (2011). The Impact of Control Technology, IEEE Control System Society, New York, NY (US).
http://ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02CyberphysicalSystems.pdf

Baiardi, F., Telmon, C., Sgandurra, D., (2009). Hierarchical, model-based risk management of critical infrastructures, Reliability Engineering & System Safety, Vol. 94, Issue 9, 1403-1415, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2009.02.001.

Bajpai, S., Sachdeva, A., Gupta, J.P., (2010). Security risk assessment: Applying the concepts of fuzzy logic, Journal of Hazardous Materials, Vol. 173, Issues 1–3, 258-264, ISSN 0304-3894, http://dx.doi.org/10.1016/j.jhazmat.2009.08.0

Bakr, A. F., El Hagla K., Nayer A., Rawash A., (2012). Heuristic approach for risk assessment modeling: EPCCM application (Engineer Procure Construct Contract Management), Alexandria Engineering Journal, Vol. 51, Issue 4, 305–323 http://dx.doi.org/10.1016/j.aej.2012.09.001

Baldoni R., Montanari, L., (2016). 2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security, CIS-Sapienza e Laboratorio Nazionale di Cybersecurity http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf
ISBN: 9788894137316

Beckhard, R., (1969). Organization Development: Strategies and Models, Addison-Wesley Publishing Company, Reading, Mass. 01867.

Beers, S., (1959). Cybernetics and Management, English University Press. 214pp, John Wiley & Sons Ltd, Baffins Lane, Chichester, West Sussex PO19 1UD, England

Beers, S., (1966). Decision and Control: The Meaning of Operational Research and Management Cybernetics, Book, 568pp, John Wiley & Sons Ltd, Baffins Lane, Chichester, West Sussex PO19 1UD, England.

Betz, D.J. and Stevens, T., (2011). Cyberspace and the state: towards a strategy for cyber-power (Abingdon: Routledge/International Institute for Strategic Studies, 2011), p. 112. Si veda anche Libicki, M.C., (2007). Conquest in cyberspace: national security and information warfare, New York: Cambridge University Press.

Carbonell, J. G., Michalsky, R. S., Mitchell, (1983). An overview of machine learning, Machine Learning, Springer-Verlag, Berlin Heidelberg.

Casola, V., De Benedictis, A., Rak, M., Rios, E., (2016). Security-by-design in Clouds: A Security-SLA Driven Methodology to Build Secure Cloud Applications, Procedia Computer Science, Volume 97, 2016, Pages 53-62, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2016.08.280.

Cazorla, L., Alcaraz, C., Lopez, J., (2015). A three-stage analysis of IDS for critical infrastructures, Computers & Security, Vol. 55, 235-250, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2015.07.005.

Cazorla, L., Alcaraz, C., Lopez, J., (2015). Awareness and reaction strategies for critical infrastructure protection, Computers & Electrical Engineering, Vol. 47, 299-317, ISSN 0045-7906, http://dx.doi.org/10.1016/j.compeleceng.2015.08.010.

Cooper H, Hedges L, (1994). *The Handbook of Research Synthesis*. New York: Russell Sage Foundation.

Christopher Bronk & Eneken Tikk-Ringas (2013), *The Cyber Attack on Saudi Aramco*, Survival, 55:2, 81-96, 2013. DOI: 10.1080/00396338.2013.784468

Centre for Reviews and Dissemination (CRD) (2001). Undertaking systematic reviews of research on effectiveness: CRD's guidance for those carrying out or commissioning reviews, CRD Report 4 (2nd ed.). York: NHS Centre for Reviews and Dissemination, University of York.

Commission of the European Communities, (2004). Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the Fight against Terrorism, COM (2004) 702 Final, Brussels, Belgium eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:NOT, 2004.

Commission on the European Communities, (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM (2006) 786 Final, Brussels, Belgium. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Cowley, J.A., Greitzer, F.L., Woods, B., (2015). Effect of network infrastructure factors on information system risk judgments, Computers & Security, Vol. 52, 142-158, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2015.04.011

Dean C. Wardell, Robert F. Mills, Gilbert L. Peterson, Mark E. Oxley, (2016). A Method for Revealing and Addressing Security Vulnerabilities in Cyber-physical Systems by Modeling Malicious Agent Interactions with Formal Verification, Procedia Computer Science, Vol. 95, 24-31, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2016.09.289.

DiMase, D., Collier, Z.A., Heffner, K. et al., (2015). Systems engineering framework for cyber physical security and resilience, Environment Systems and Decisions 35: 291. doi:10.1007/s10669-015-9540-y

El-Gayar, O.F., Fritz, B.D., (2010). A web-based multi-perspective decision support system for information security planning, Decision Support Systems, Vol. 50, Issue 1, 43-54, ISSN 0167-9236, http://dx.doi.org/10.1016/j.dss.2010.07.001

ENISA, (2015). Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, European Union Agency for Network and Information Security (ENISA), ISBN 978-92-9204-131-1, doi:10.2824/43639

Farwell J.P., R.Rohozinski, R., (2011). Stuxnet and the Future of Cyber War" in Survival, Survival, vol.53 issue 1, 2011, http://dx.doi.org/10.1080/00396338.2011.555586

Fovino, I.N., Guidi, L., Masera, M., Stefanini, A., (2011). Cyber security assessment of a power plant, Electric Power Systems Research, Vol. 81, Issue 2, 518-526, ISSN 0378-7796, http://dx.doi.org/10.1016/j.epsr.2010.10.012.

Goldman, H., McQuaid, R., Picciotto, J., (2011). Cyber resilience for mission assurance 2011 IEEE International Conference on Technologies for Homeland Security (HST)

Pages: 236 - 241, DOI: 10.1109/THS.2011.6107877

Guariniello, C., DeLaurentis, D., (2014). Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis, Procedia Computer Science, Vol. 28, 720-727, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2014.03.086.

Grant, M. J. and Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health Information & Libraries Journal, 26: 91–108. doi:10.1111/j.1471-1842.2009.00848.x.

Henry, M. H. and Haimes, Y. Y. (2009). A Comprehensive Network Security Risk Model for Process Control Networks. Risk Analysis, 29: 223–248. doi:10.1111/j.1539-6924.2008.01151.x

Hummer, M., Champy, J., (1993). Reengineering the Corporation: Manifesto for Business Revolution. Business Horizons, 1993, Vol.36(5), pp.90-91, ISSN: 0007-6813; DOI: 10.1016/S0007-6813(05)80064-3

Humphreys, E., (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, Vol. 13, Issue 4, 247-255, ISSN 1363-4127, http://dx.doi.org/10.1016/j.istr.2008.10.010.

Jason, F., (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. Journal of business continuity & emergency planning, Vol.9 (2), 185-95. ISSN: 1749-9216 ; PMID: 26642176 Version:1

Johnson, P., Ullberg, J., Buschle, M. et al., (2014). An architecture modeling framework for probabilistic prediction. Information Systems and e-Business Management 12: 595. doi:10.1007/s10257-014-0241-8

Johnson, R. A., Kast F. E., Rosenzweig J. E., (1964). Systems Theory and Management, Management Science, Vol. 10, No. 2, pp. 367-384, US. Published by INFORMS URL: http://www.jstor.org/stable/2627306

Karabacak, B., Yildirim, S.O., Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness, International Journal of Critical Infrastructure Protection, Vol. 15, 47-59, ISSN 1874-5482, http://dx.doi.org/10.1016/j.ijcip.2016.10.001.

Kralik, L., Senkerik, R. & Jasek, R. (2016). Model for comprehensive approach to security management, International Journal of System Assurance Engineering and Management (2016) 7: 129. doi:10.1007/s13198-016-0420-8.

Kreutz, D., Malichevskyy, O., Feitosa, E., Cunha, H., Righi, R.R., de Macedo, D. D.J. (2016). A cyber-resilient architecture for critical security services, Journal of Network and Computer Applications, Vol. 63, 173-189, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2015.09.014.

Langer, L., Skopik, F., Smith, P., Kammerstetter, M., (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid, Computers & Security, Vol. 62, 165-176, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2016.07.008.

Lavrova, D., Pechenkin, A. & Gluhov, V., (2015). Applying correlation analysis methods to control flow violation detection in the internet of things, Automatic Control and Computer Sciences 49: 735. doi:10.3103/S0146411615080283

Liu, T., Sun, Y., Liu, T., Gui, Y., Zhao, Y., Wang, D., Shen, C., (2015). Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for Smart Grid attack detection, Future Generation Computer Systems, Vol. 49, 94-103, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2014.10.002.

Lee E. A. and Seshia, S. A., (2011). Introduction to Embedded Systems, A Cyber-Physical Systems Approach, http://LeeSeshia.org, ISBN 978-0-557-70857-4.

Lee, E. A. (2008). CPS Foundations in *"Proc. Of the 47th Design Automation Conference* (DAC), ACM, 737,742, 2010. Published in Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on 5-7 May, 2008, pp. 363-369, Orlando, FL. doi 10.1109/ISORC.2008.1.

Lee, E. A. (2006). Cyber-Physical Systems - Are Computing Foundations Adequate?, Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, Austin, Texas.

Lee, E.A., (2008). Cyber Physical Systems: Design Challenges, 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), pp. 363-369. doi:10.1109/ISORC.2008.25.

Lee, E. A. and Seshia, S. A., (2017). Introduction to Embedded Systems, A Cyber-Physical Systems Approach, Second Edition. MIT Press, ISBN 978-0-262-53381-2.

Lewis, J. (2002). *Assessing the risks of cyberterrorism, cyber war, and other cyber threats*. Washington, DC: Center for Strategic and International Studies.

Mays, N., Roberts, E., & Popay, J. (2001). Synthesising research evidence. In N. Fulop, P. Allen, A. Clarke, & N. Black (Eds.), Studying the organisation and delivery of health services: Research methods. London: Routledge.

McQueen, M. A., Boyer, W. F., Flynn M. A. and Beitel, G. A. (2006). Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006, pp. 226-226. doi: 10.1109/HICSS.2006.405

Miller B. and Rowe, D., (2012). A survey of SCADA and critical infrastructure incidents, Proceedings of the First Annual Conference on Research in Information Technology, pp.51–56.

Nai Fovino, I., Masera, M., De Cian, A., (2009). Integrating cyber attacks within fault trees, Reliability Engineering & System Safety, Vol. 94, Issue 9, 1394-1402, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2009.02.020.

Nash, J. F. (1950). The Bargaining Problem, Econometrica Vol.18, Issue 2, 155-182, The, Econometric Society, New York University, Department of Economics, New York, NY.

Nash, J. F. (1953). Two-Person Cooperative Games, Econometrica Vol.21, Issue 1, 128-140, The, Econometric Society, New York University, Department of Economics, New York, NY.

Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H., (2012). SCADA security in the light of Cyber-Warfare, Computers & Security, Vol. 31, Issue 4, 418-436, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2012.02.009.

NIST, (2014). Framework for Improving Critical Infrastructure Cybersecurity" Version 1.0, National Institute of Standards and Technology, Gaithersburg, MD (US).

NIST, (2017). Framework for Improving Critical Infrastructure Cybersecurity" Version 1.1, National Institute of Standards and Technology, Gaithersburg, MD (US).

NIST CPS Public Working Group, (2016). Framework for Cyber-Physical Systems, National Institute of Standards and Technology, Gaithersburg, MD (US).

Ntalampiras, S., Soupionis, Y., Giannopoulos, G., (2015). A fault diagnosis system for interdependent critical infrastructures based on HMMs, Reliability Engineering & System Safety, Vol. 138, 73-81, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2015.01.024.

Okoli, C., (2015). A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems, 37(43), pp.879–910. Available at: http://aisel.aisnet.org/cais/vol37/iss1/43

Ouyang, M., (2014). Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering & System Safety, Vol. 121, 43-60, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2013.06.040

Patel, S.C., Graham, J.H., Ralston, P., (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements, International Journal of Information Management, Vol. 28, Issue 6, 483-491, ISSN 0268-4012, http://dx.doi.org/10.1016/j.ijinfomgt.2008.01.009.

Petticrew, M., Roberts H., (2006). Systematic Reviews in the Social Sciences: A practical guide, Oxford: Blackwell Publishing.

Porter, E., (1985). Competitive Advantage: Creating & Sustaining Superior Performance, The Free Press, New York NY, Book, ISBN: 0-02-925090-0.

Radeschütz, S., Schwarz, H., & Niedermann, F., (2015). Business impact analysis—a framework for a comprehensive analysis and optimization of business processes, Computer Science, Research and Development, Vol. 30, Issue 2. 69 - 86. doi:10.1007/s00450-013-0247-3

Rajkumar, R., Lee, I., Sha, L., J. Stankovic, J., (2010). Cyber-physical systems: the next computing revolution. In Proceedings of the 47th Design Automation Conference (DAC '10). ACM, New York, NY, USA, 731-736.

Ryan, J. J., Daniel J. Ryan, D. J. (2006). Expected benefits of information security investments, Computers & Security, Vol. 25, Issue 8, Pag. 579-588, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2006.08.001.

Rinaldi, S., (2004) Modeling and simulating critical infrastructures and their interdependencies in: Proceedings of the 37th annual Hawaii international conference on System sciences, IEEE (2004), p. 8.

Rok Bojanc, R., Jerman-Blažič, B., (2008). An economic modelling approach to information security risk management, International Journal of Information Management, Vol. 28, Issue 5, 413-422, ISSN 0268-4012, http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.002.

Schoknecht, A., Schiefer, G., Citak, M., Oberweis, A., (2016). Security-by-Design in der Cloud-Anwendungsentwicklung, HMD Praxis der Wirtschaftsinformatik, ISSN: 1436-3011 (Print), 2198-2775 (Online), 53:688–697, Springer Fachmedien Wiesbaden. 2016. DOI 10.1365/s40702-016-0258-1

Shin, J., Son, H,. Khalil ur, R., Heo, G., (2016). Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET, Nuclear Engineering and Technology, Available online ISSN 1738-5733, http://dx.doi.org/10.1016/j.net.2016.11.004

Shin, J., Son, H,. Khalil ur, R., Heo, G., (2015). Development of a cyber security risk model using Bayesian networks, Reliability Engineering & System Safety, Vol. 134, 208-217, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2014.10.006.

Silva, M.M., Henriques de Gusmão, A.P., (2014). Thiago Poleto, Lúcio Camara e Silva, Ana Paula Cabral Seixas Costa, A multidimensional approach to information security risk management using FMEA and fuzzy theory, International Journal of Information Management, Vol. 34, Issue 6, 733-740, ISSN 0268-4012, http://dx.doi.org/10.1016/j.ijinfomgt.2014.07.005.

Singh, S., Jeong, Y., Park, J.H., (2016). A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications, Vol. 75, 200-222, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.09.002.

Sommestad,T. , Ekstedt, M. , Johnson, P., (2010). A probabilistic relational model for security risk analysis. Computers & Security, Vol. 29, Issue 6, 659–679.

Sundmaeker, H., Guillemin, P., Friess, P., Woelffl, S., (2010). Visions and challenges for realising the internet of things. Cluster of European Research Projects on the Internet-of-Things (CERP-IoT).

Touhill, G. J. and Touhill, C. J. (2014) Change Management, in Cybersecurity for Executives: A Practical Guide, John Wiley & Sons, Inc., Hoboken, NJ. doi: 10.1002/9781118908785.ch6

Ten, C. W., Manimaran G. and Liu, C. C., (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling, in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, July 2010. doi: 10.1109/TSMCA.2010.2048028

Thissen, W., Herder P., (2003). Critical Infrastructures: State of the Art in Research and Application, Kluwer Academic Publishers, Norwell, Massachusetts

Tsiakis, T., Stephanides, G., (2005). The economic approach of information security, Computers & Security, Vol. 24, Issue 2, Pag. 105-108, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2005.02.001

Von Bertanlaffy, L., (1968) General System Theory: Foundations, Development, Applications, George Braziller lnc., One Park Avenue, New York, N.Y. 10016

von Neumann J. and Morgenstern O., (1944). Theory of Games and Economic Behaviour. Princeton University Press, Princeton, NJ (US).

Wiener, N., (1948). Cybernetics: Or Control and Communication in the Animal and the Machine. Librairie Hermann & Cie, Paris, and MIT Press.Cambridge, MA.

Wiener, N., (1968). La Cibernetica - Controllo e Comunicazione nell'animale e nella macchina (traduzione in italiano), Il Saggiatore, Milano.

Wang, S., Hong, L., Chen, X., (2012). Vulnerability analysis of interdependent infrastructure systems: A methodological framework, Physica A: Statistical Mechanics and its Applications, Vol. 391, Issue 11, 3323-3335, ISSN 0378-4371, http://dx.doi.org/10.1016/j.physa.2011.12.043.

Wang, S., Hong, L., Ouyang, M., Zhang, J., Chen, X., (2013). Vulnerability analysis of interdependent infrastructure systems under edge attack strategies, Safety Science, Vol. 51, Issue 1, 328-337, ISSN 0925-7535, http://dx.doi.org/10.1016/j.ssci.2012.07.003.

Wang J., Sun Y., (2012). The Intuitionistic Fuzzy Sets on Evaluation of Risks in Projects of Energy Management Contract, Systems Engineering Procedia, Vol. 3, 30-35, Elsevier. https://doi.org/10.1016/j.sepro.2011.11.004

Wang, W., Lu, Z., (2013). Cyber security in the Smart Grid: Survey and challenges, Computer Networks, Vol. 57, Issue 5, 1344-1371, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2012.12.017.

Kröger, W., (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, Reliability Engineering & System Safety, Vol. 93, Issue 12, 1781-1787, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2008.03.005.

Yan, J., Govindarasu, M., Liu, C.C. et al., (2015). Risk assessment framework for power control systems with PMU-based intrusion response system, Journal of Modern Power Systems and Clean Energy, 9/2015, Vol.3, pp.321-331. doi:10.1007/s40565-015-0145-8

Ye X, Zhao J, Zhang Y, Wen F. (2015). Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems. Energies; 8(6):5266-5286.

Zadeh, L. A., (1968). Probability measures of fuzzy events, Journal of Mathematical Analysis and Applications (Elsevier), 23, pp. 421-427.

Zadeh, L. A., (1978). Fuzzy Sets as a basis for a Theory of Possibility, Fuzzy Sets and Systems 1, pp. 3-28, North-Holland Publishing Company (Elsevier), Amsterdam, (NL).

Zio, E., (2016). Challenges in the vulnerability and risk analysis of critical infrastructures, Reliability Engineering & System Safety, Vol. 152, 137-150, ISSN 0951-8320, http://dx.doi.org/10.1016/j.ress.2016.02.009.

Zio, E., Aven, T., (2011). Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?, Energy Policy, Vol. 39, Issue 10, 6308-6320, ISSN 0301-4215, http://dx.doi.org/10.1016/j.enpol.2011.07.030.

ACRONIMI

AI	Artificial Intelligence
BIA	Business Impact Analisys
CCD-CoE	Cooperative Cyber Defence-Centre of Excellence
CDMA	Cyber Defence Management Authority (NATO)
CERT	Computer Emergency Response Teams.
CIIs	Critical Information Infrastructures (infrastrutture critiche informatizzate)
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
COPASIR	Comitato Parlamentare per la Sicurezza della Repubblica
CPS	Cyber-Physical Systems
CSIRT	Computer Security and Incident Response Teams
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerability Scoring System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DIS	Dipartimento per l'Informazione e la Sicurezza
EECTF	European Electronic Crime Task Force
EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
EP3R	Partnership Europea Pubblico-Privata per la Resilienza
EPCIP	European Programme for Critical Infrastructure Protection
ESCAPE	Electronically Secure Collaboration Application Platform for Experts
FIRST	Forum of Incident Response and Security Teams
FT	Fault Tree

GCA	Global Cyber-security Agenda
GRC	Global Response Center
HMM	Hierarchical Holographic Modeling
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IMPACT	International Multilateral Partnership Against Cyber Threats
IPS	Intrusion Prevention Systems
ISCOM	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Ministero dello Sviluppo Economico).
ISRM	Information Security Risk Management
IT	Information Technology
ITU	International Telecommunication Union
JRC-IPSC	Joint Research Centre - Institute for the Protection and Security of the Citizen (UE)
NATO	North Atlantic Treaty
NIS	Network and Information Security (UE)
NIST	National Institute of Standards and Technology (US)
NSRM	Network Security Risk Model
OT	Operational Technology
PIC	Protezione Infrastrutture Critiche
PSA	Probabilistic Safety Assessment
RA	Risk Analisys
RMF	Risk Management Framework
R&S	Ricerca e sviluppo
SCADA	Supervisory Control and Data Acquisition
TIC	Tecnologie dell'informazione e della comunicazione