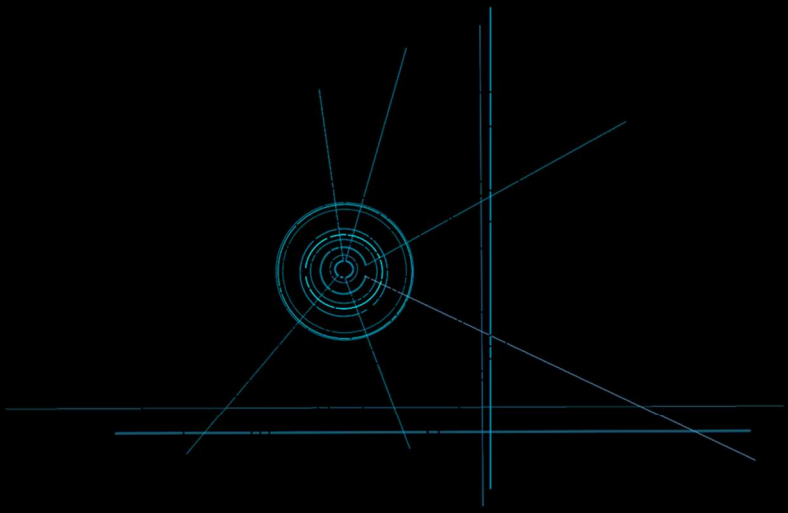
DAVIDE MANISCALCO
GIOVANNI GAMBINO

CYBER SPIONAGGIO AZIENDALE



SOCINT SOCIETÀ ITALIANA DI INTELLIGENCE

con la collaborazione
dell'INTELLIGENCE LAB DELL'UNIVERSITÀ DELLA CALABRIA

DAVIDE MANISCALCO
GIOVANNI GAMBINO

CYBER SPIONAGGIO AZIENDALE

Società Italiana di Intelligence
c/o Università della Calabria, Cubo 18-b, 7° piano via Pietro Bucci
87036 Arcavacata di Rende (CS) – Italia

https://www.socint.org

ISBN 979-12-80111-25-8

In collaborazione con IntelligenceLab dell'Università della Calabria

https://www.intelligencelab.org/

Design di copertina: Ing. Maria Abbate

INDICE

PROFILO DEGLI AUTORI

DAVIDE MANISCALCO è socio ordinario della Società Italiana di Intelligence (SOCINT). Avvocato cassazionista, ha assunto nel tempo anche ruoli di «alta direzione» in consolidati gruppi societari. Esperto di informatica giuridica e nuove tecnologie, è membro dello special team del Cyber security Research Center per la security fisica e logica delle infrastrutture critiche. Componente del gruppo informale «esperti digitali» presso la Commissione europea (Rappresentanza in Italia), è altresì Certified Business Continuity Professional, nonché Disaster Manager. Attualmente è Head Privacy Officer e Public Affairs presso Swascan -Tinexta Group.

GIOVANNI GAMBINO dopo aver completato gli studi in Giurisprudenza prosegue con un M.B.A. presso l'Università di Bologna ed un Master in Analisi Dati. Approfondisce il tema dell'Intelligence presso l'Università della Calabria conseguendo un Master di II livello. Ha conseguito un Data Science Advanced Specialization Program alla John Hopkins University. Presso la Venice International University ha studiato Europrogettazione. Si è specializzato nell'analisi dei network relazionali, compiendo studi su reti terroristiche e finanziarie. Ricercatore dell'IntelligenceLab dell'Università della Calabria, Senior Analyst del Centro Studi Analytica for Intelligence and Security Studies, segretario ed analista Società Italiana di Intelligence (SOCINT) per la regione Sicilia. Ha un diploma di sommelier.

ABSTRACT

Il 2020, secondo il Rapporto Clusit 2021, è stato caratterizzato da un record (negativo) di attacchi informatici. In particolare, si sono registrati, in Italia, n.1.871 attacchi gravi di dominio pubblico di cui n. 266 con finalità di spionaggio e sabotaggio[1].

È recente il clamore che l'attacco informatico posto in essere contro la Regione Lazio, il quale ha compromesso l'utilizzo di alcuni dei servizi ed applicazioni a disposizione dei cittadini, tra cui il sistema di prenotazione del vaccino contro il Covid-19, di cui a tutt'ora non appaiono ancora ben definiti i contorni della violazione.

Appare evidente che, il fenomeno "Covid-19" ha nei fatti accelerato la transizione digitale in ambito "smatworking" aprendo importanti risvolti in ambito sicurezza, ed i dati relativi alle violazioni informatiche messe in atto sono palesi e con incrementi più che significativi.

L'incremento delle violazioni è riconducibile anche ai nuovi assetti organizzativi adottati da aziende ed Istituzioni a seguito dell'emergenza COVID-19[2].

Al riguardo, come riportato nel Report "*Fraud in the Wake of COVID-19 Benchmarking Report*" redatto da ACFE[3] a dicembre 2020, dall'inizio della pandemia i professionisti che hanno risposto alla *survey* lanciata hanno registrato un incremento delle "*cyberfraud*[4]" pari al 85% a livello globale.

[1] "*Rapporto 2021 sulla Sicurezza ICT in Italia*"; CLUSIT; 2021

[2] Al riguardo, si precisa, che a seguito dei Decreti del Presidente del Consiglio dei Ministri (di seguito, "DPCM"), da marzo 2020 si sono susseguite misure restrittive atte a limitare i movimenti dei cittadini su tutto il territorio nazionale e a incentivare il "*remote working*". Tale circostanza ha portato ad una riorganizzazione di Aziende ed Istituzioni.

[3] Association of Certified Fraud Examiners

[4] L'ACFE include tra le "*cyberfraud*", a titolo esemplificativo e non esaustivo, le *business email* compromise, l'hacking, i ransomware e i malware.

Il presente paper analizza alcuni degli aspetti inerenti al fenomeno dello spionaggio aziendale effettuato mediante attacchi ai sistemi informatici (c.d. cyber spionaggio), nonché i relativi profili giuridici. Ulteriormente sono stati illustrati alcuni casi di cyber spionaggio che hanno coinvolto la società tedesca SolarWorld AG e Microsoft, nonché il caso di scuola del primo utilizzo del ransomware contro la centrale nucleare iraniana di Natanz.

PREMESSA

Lo scenario attuale in ambito sicurezza cibernetica è probabilmente il frutto derivante dall'unione di tre grandi direttrici: la digitalizzazione dei processi, la globalizzazione e la pandemia.

La digitalizzazione dei processi ha praticamente invaso tutti i settori umani, consentendo una migliore efficacia delle operazioni in ambito pubblico e privato.

Tale ottimizzazione è da inquadrare in ottica di globalizzazione, in quanto appare più che mai evidente che la digitalizzazione è da osservare in termini globali, essendo mutate le classiche basi geopolitiche, composte da limiti territoriali ben definiti.

I classici paradigmi relativi ai confini fisici tra stati in tale ottica sono stati sostanzialmente cancellati, in quanto internet ha di fatto creato un nuovo spazio operativo con caratteristiche geopolitiche.

Comunemente la geopolitica è definita come una disciplina che analizza le relazioni tra la geografia fisica, la geografia umana e l'azione politica. In questa ottica si andrà a sostituire geografia fisica con spazio digitale globale, ossia la rete internet.

Il contesto così delineato andrà a mutare, o forse accelerare, il fenomeno fin qui decritto, a causa della pandemia da COVID-19.

I vari lockdown attuati su scala internazionale dai vai governi hanno aumentato il ricorso a processi di remotizzazione

lavorativa, aumentando di fatto l'impiego delle infrastrutture cibernetiche onde assicurare la "business continuity" delle varie strutture produttive.
Probabilmente in molti contesti è stato anche migliorato il rapporto di produttività delle strutture.
Al classico schema terra, mare, cielo e spazio interstellare, lo spazio cibernetico è divenuto il quinto dominio, ed in tale dominio, di fatto in continua trasformazione, in termini di efficacia è considerato l'ambito preferibile ove implementare scenari di guerra, che qui assumono connotati di "cyberwarfare", anche in chiave asimmetrica delle operazioni di attacco.
Il fenomeno della digitalizzazione dei processi ormai interessa praticamente tutto, e questo tutto potrebbe essere oggetto di attacco cibernetico, ove quest'ultimo in linea teorica potrebbe compromettere le infrastrutture strategiche di una nazione, oppure di una singola azienda, nessuno pertanto è escluso.
Nel 2018 secondo il rapporto Clusit, "In Italia danni per 10 miliardi di euro, e la cifra è dieci volte superiore a quella degli attuali investimenti in sicurezza informatica, che arrivano oggi a sfiorare il miliardo di euro", mentre "a livello globale le perdite collegate agli attacchi informatici ammontano a 500 miliardi di dollari".

CAPITOLO 1
PERIMETRO DI INDAGINE E NORMATIVA

1. INTRODUZIONE ALLO SPIONAGGIO CYBER. IL RUOLO DEL VANTAGGIO COMPETITIVO.

In generale, lo spionaggio è il processo mediante il quale, un'organizzazione cerca di ottenere informazioni che non sono solitamente pubblicamente disponibili mediante l'utilizzo di risorse umane (agenti) o mezzi tecnici[5] (c.d. "*tradecrafting"*). In particolare, tra le informazioni target, oggetto di spionaggio, possiamo trovare segreti militari, segreti commerciali, segreti politici o l'identificazione di eventuali dissidenti (c.d. "*targeting dissidents*") [6].

L'*Economic Espionage Act* - atto normativo approvato nel 1996 dal Congresso degli Stati Uniti d'America - definisce lo spionaggio economico o industriale come l'attività volta a sottrarre con consapevolezza un segreto commerciale a vantaggio di un'altra organizzazione[7].

---

[5] https://www.cpni.gov.uk/espionage; "Espionage"; Center for the Protection of National Infrastructure.

[6] https://www.cpni.gov.uk/espionage; "Espionage"; Center for the Protection of National Infrastructure.

[7] *"(…) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly— ''(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;*

''(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; ''(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; ''(4) attempts to commit any offense described in paragraphs (1) through (3); or ''(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or

Si ritiene opportuno osservare il tema del segreto commerciale sotto una duplice veste, ossia quella inerente alla catena del valore in ottica vantaggio competitivo, e quella inerente alla normativa di settore in Italia. L'affermazione di un'impresa si può misurare, in termini di vantaggio competitivo, quando essa ha conquistato, in un determinato business una posizione di rilevanza, ed in tale vantaggio vi sono due elementi che lo consentono.
Il primo è riferibile al vantaggio di costo dato dalla capacità dell'impresa di fornire un prodotto o servizio analogo, ma con un costo di fornitura più basso.
Il secondo è il vantaggio di differenziazione, dato dalla capacità di offrire ai propri clienti un prodotto, oppure un servizio, differente da quello offerto dalla propria concorrenza, con la necessaria premessa che i propri clienti siano disposti a retribuire un differenziale di prezzo superiore al differenziale di mercato. Un concetto da evidenziare, nel procedimento logico che porta alla definizione del vantaggio competitivo è quello inerente alla catena del valore, in quanto nel famoso modello di relazioni sviluppato da McKinsey la prima attività è quella inerente all'area "Tecnologia, R&S". Appare evidente che tale tipo di attività non sarà presente in tutte le forme aziendali, ma in quelle ove vi è nella catena del valore la necessità di sviluppare beni o servizi.
Brevemente, l'area "Tecnologia e R&S" è riferibile a quella gamma di attività volte al miglioramento dei prodotti o processi aziendali. In tale area sono da includere anche le molteplici tecnologie a sostegno del prodotto finale, la ricerca di base, la

more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both. ''(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000. (…)" Economic Espionage Act degli Stati Uniti d'America del 1996.

progettazione del prodotto, gli studi sui media, la realizzazione delle apparecchiature di processo.
La protezione degli elementi inerenti al vantaggio competitivo pertanto saranno vitali per moltissime aziende, andando così a rappresentare quello che successivamente verrà denominato "segreto commerciale".

2. SEGRETO COMMERCIALE

Fin qui è stata osservata la prospettiva del vantaggio economico del "segreto commerciale" in relazione alla catena del valore. Ora si osserverà ciò sotto il profilo normativo.
Il decreto legislativo del 10 febbraio 2005, n. 30 recante il Codice della proprietà industriale, coordinato ed aggiornato, da ultimo, con le modifiche apportate dal D.L. 119 maggio 2020, n. 34 e dal D.L. 11 marzo 2020, n. 16, convertito, con modificazioni, dalla L. 8 maggio 2020, n. 31, disciplina l'argomento relativo al "segreto commerciale".
Nel dettaglio, l'Art. 98 del Codice della proprietà industriale, definisce quale segreto commerciale tutte *"le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni siano "*segrete", *nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore*, che abbiano "un valore economico" in quanto segrete e che "siano sottoposte a misure da ritenersi ragionevolmente adeguate a mantenerle segrete".
Il comma 2 del predetto art. 98 in relazione alla tutela del segreto commerciale fa rientrare anche "*i dati relativi a prove o altri dati segreti, la cui elaborazione comporti un considerevole impegno ed alla cui presentazione sia subordinata l'autorizzazione*

*dell'immissione in commercio di prodotti chimici, farmaceutici o agricoli implicanti l'uso di nuove sostanze chimic*he".

Pertanto, in generale linea di principio, per segreto commerciale si farà riferimento a tutte quelle informazioni che assicurano al legittimo proprietario un vantaggio competitivo economicamente distintivo e che siano "teoricamente", e quindi nell'intento, mantenute segrete.

Nel dettaglio, lo spionaggio economico e scientifico-tecnologico insidia il capitale intellettuale di un'impresa, che costituisce l'*asset* aziendale di maggiore valore, in quanto un attacco spionistico, condotto da un'azienda concorrente o da un apparato d'intelligence straniero, sottrae *know how* all'azienda colpita, azzerando il posizionamento competitivo ed il possibile rendimento di investimenti coltivati da anni oltre ad esternalità negative che determinano impatti a volte distruttivi sul piano economico-sociale [8].

In particolare, nel 1996 il Congresso degli Stati Uniti d'America riconosceva l'importanza della protezione della proprietà intellettuale e dei segreti commerciali al fine di tutelare la sicurezza economica degli Stati Uniti. L'"*Economic Espionage Act*" contiene due disposizioni separate che criminalizzano il furto o l'appropriazione indebita di segreti commerciali. In particolare, la prima disposizione riguarda lo spionaggio economico straniero e richiede che il furto del segreto commerciale sia effettuato a vantaggio di un governo, di una strumentalità o di un agente straniero.

[8] "Information warfare 2011: la sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale"; U. Gori, L.S. Germani; Franco Angeli; 2012

Invece, la seconda disposizione rende criminale il più comune furto di segreti commerciali, indipendentemente da chi ne tragga vantaggio[9].

In Italia il novero di norme che vanno a definire il reato di spionaggio industriale, è ampio e frammentato, ma in tale contesto risulta di fondamentale importanza il ruolo dell'*intelligence*, il quale è stato (in parte) definito solo a seguito della Legge n.124 del 3 agosto 2007 (c.d. riforma dell'*intelligence* del 2007), la quale tra i compiti dell'Agenzia Informazioni e Sicurezza Esterna (di seguito, "AISE") e dell'Agenzia Informazioni e Sicurezza Interna (di seguito, "AISI") ha inserito anche "*(…) le attività di informazione per la sicurezza, che si svolgono* all'interno [o all'esterno] *del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia (…)"*[10].

In riferimento alla protezione degli interessi economici, scientifici e industriali, il Decreto Legge n.21 del 15 marzo 2012 (convertito con modificazioni dalla Legge n. 56 dell'11 maggio 2012), ha introdotto il concetto di "Golden Power" attribuendo dei poteri[11] esercitabili nel caso di "*minaccia di grave pregiudizio*" per gli interessi essenziali della difesa e della sicurezza nazionale, al fine di salvaguardare gli assetti proprietari delle imprese operanti in ambiti ritenuti strategici e di interesse nazionale. Successivamente, il Decreto Legge n.105 del 21 settembre 2019 ha ulteriormente ampliato il perimetro, inserendo il possibile pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti anche ai beni

---

[9] "*1122. INTRODUCTION TO THE ECONOMIC ESPIONAGE ACT*"; The United States Department of Justice Archives; giugno 2015.

[10] Legge 3 agosto 2007, n. 124

[11] I poteri esercitabili dal Governo sono sostanzialmente i seguenti: ***i)*** opposizione all'acquisto di partecipazioni; ***ii)*** veto all'adozione di delibere societarie; e ***iii)*** imposizione di specifiche prescrizioni e condizioni.

ed ai rapporti di rilevanza strategica per l'interesse nazionale nei settori individuati dall'articolo 4, paragrafo 1, del Regolamento (UE) n. 2019/452[12].

Ulteriormente, come si evince dalla "*Relazione sulla politica dell'informazione per la sicurezza 2019*", redatta dalla Presidenza del Consiglio dei Ministri - Sistema di Informazione per la Sicurezza della Repubblica, le agenzie d'*intelligence* italiane svolgono un'attività di promozione e diffusione della cultura della sicurezza non solo agli operatori strategici ma anche alle piccole e medie imprese, *"(...) ossatura del nostro tessuto produttivo, più vulnerabili alle iniziative di ingerenza e spionaggio da parte di attori ostili (...)*"[13].

In particolare, negli ultimi anni, l'attività di protezione svolta dalle agenzie d'intelligence è andata sempre più a consolidarsi sul versante della *cyber security*[14].

Appare evidente che il tema legato alla cyber security, e quindi anche al problema del cyber espionage, è legato al concetto di sicurezza cibernetica a 360 gradi, ed anche agli interlocutori privati ed istituzionali dei singoli sistemi paese.

Il nostro paese negli anni non ha avuto un chiaro interlocutore che si occupasse del monitoraggio e della prevenzione degli attacchi alla cyber security (rammentando che il rischio nullo di un eventuale attacco è praticamente zero).

Il nostro paese è corso ai ripari istituendo l'Agenzia per la cyber sicurezza nazionale (Acn), la quale avrà la funzione di

[12] Nel dettaglio: i) infrastrutture critiche; ii) tecnologie critiche e prodotti a duplice uso; iii) approvvigionamento di fattori produttivi critici; iv) accesso a informazioni sensibili; e v) libertà e pluralismo dei media.

[13] Relazione sulla politica dell'informazione per la sicurezza 2019; Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica; febbraio 2020

[14] Relazione sulla politica dell'informazione per la sicurezza 2019; Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica; febbraio 2020

salvaguardare le "funzioni essenziali dello Stato italiano da minacce informatiche e di sviluppare le capacità per prevenirle e combatterle". Essa andrà ad operare sotto la supervisione della Presidenza del Consiglio dei Ministri e dell'autorità delegata per la sicurezza della Repubblica, la quale quest'ultima assumerà anche con le funzioni di autorità nazionale in materia di cyber sicurezza.

Altra funzione, certamente non secondaria, sarà quella di contribuire al miglioramento della sicurezza delle tecnologie dell'informazione e della comunicazione delle pubbliche amministrazioni, con riferimento anche agli operatori dei servizi essenziali e dei fornitori di servizi digitali dello Stato, e inoltre, sarà il referente dei soggetti pubblici e privati della "cyber security", oltre che soggetto ispettivo in tale ambito.

In tale contesto di evidenti vulnerabilità informatiche, vi è la risalente attività di intrusione mirata alla acquisizione di informazioni, comunemente definita spionaggio.

Come tutte le attività di spionaggio, anche lo spionaggio industriale può essere posto in essere mediante l'utilizzo di diverse tecniche, dalle più tradizionali[15] a quelle che prevendono l'utilizzo di "*cyber attack"* al fine di accedere ai sistemi informatici della società *target* e in tale ultimo caso si parlerà di cyber spionaggio.

Lo spionaggio informatico è il prodotto di una robusta espansione a livello globale delle tecnologie informatiche, che di fatto sono presenti in quasi tutte le attività umane, appare evidente, pertanto, che vi sia necessità di adeguare, se non implementare, strategie di

[15] A titolo esemplificativo: *(i)* furto di documentazione societaria; *(ii)* infiltrazione di una "talpa" nell'organico della società target; *(iii)* intercettazioni telefoniche e/o ambientali; *(iv) dumpster diving*: ricerca nella spazzatura della società target di documentazione utile; *(v)* l'utilizzo della seduzione per venire a conoscenza d'informazioni sensibili; *(vi)* il reclutamento di una società privata d'intelligence; *(v)* falsi colloqui di lavoro finalizzati ad apprendere informazioni sensibili dai candidati; *(vi)* Open Sources Intelligence (OSINT).

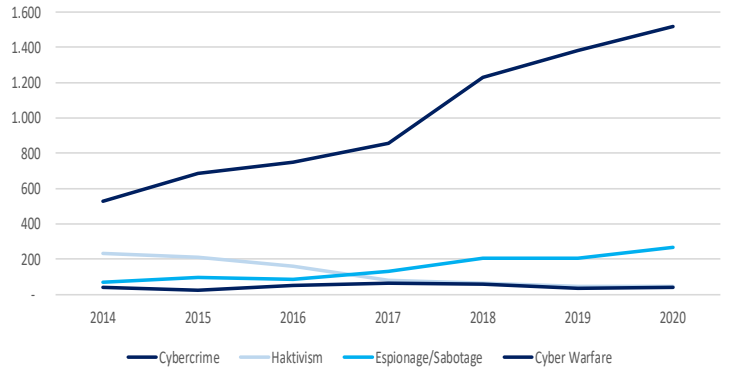
sicurezza nazionale da parte degli Stati, ponendo l'accento anche verso la sfera prettamente economica della sicurezza informatica, considerando che nell'era della globalizzazione e delle sempre più presenti tecnologie di "information and communication technologies" la componente squisitamente economica è di naturale importanza, se non predominanza.
In relazione a quanto detto, considerato l'elevato grado di complessità che i sistemi informatici ed economici hanno raggiunto nell'odierno panorama, è e sarà sempre più difficile e complesso porre in essere le necessarie attività di contrasto allo spionaggio informatico, ovviamente senza tralasciare la componente "umana" della questione "cyber espionage", perché spesso l'anello debole della catena non è la "vulnerabilità informatica" ad essere la serratura da aprire, è molto più semplicemente l'uomo.
In tutto ciò, non è assolutamente trascurabile il fine ultimo del "cyber espionage", ossia quello inerente al mero interesse economico a monte delle varie attività intrusive, senza scomodare a forza "misteriosi e segreti" scontri tra Stati, considerato che i profitti dello spionaggio economico e scientifico-tecnologico sono spesso elevati.
Il Cyber spionaggio può essere molto più conveniente rispetto ai tradizionali metodi di spionaggio per differenti motivi, tra cui: *(i)* tendenzialmente è più economico rispetto ai sistemi tradizionali; *(ii)* la sua natura remota permette all'organizzazione spia un elevato livello di negabilità circa la paternità dell'operazione; *(iii)* il volume dei dati trafugabili è potenzialmente immenso; e *(iv)* un attacco cyber non richiede il dislocamento di personale in prossimità dell'organizzazione *target*[16]. Andando ad analizzare nel dettaglio gli attacchi informatici subiti e dichiarati da operatori

[16] https://www.cpni.gov.uk/espionage;"Espionage"; Center for the Protection of National Infrastructure.

italiani, come si evince dal "Rapporto 2021 sulla Sicurezza ICT in Italia" redatto dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT), nel 2020 in Italia sono stati registrati e dichiarati n. 1.871 attacchi informatici (il 12% in più rispetto al 2019 e il 114% in più rispetto al 2014)[17].
In particolare, nella tabella di seguito riportata ci fornisce evidenza della distribuzione degli attacchi per tipologia dal 2014 al 2020.

Distribuzione degli attacchi per tipologia dal 2014 al 2019
Fonte dei dati: Rapporto 2021 sulla Sicurezza ICT in Italia - CLUIST

Tipologia	2014	2015	2016	2017	2018	2019	2020	2014- 2020
Cybercrime	526	684	751	857	1.232	1.383	1.517	**6.950**
Haktivism	236	209	161	79	61	48	47	**841**
Espionage/Sabotage	69	96	88	129	203	204	266	**1.055**
Cyber Warfare	42	23	50	62	56	35	41	**309**
Totale	**873**	**1.012**	**1.050**	**1.127**	**1.552**	**1.670**	**1.871**	**9.155**



Ad integrazione e commento della tabella soprariportata è bene precisare che, le organizzazioni generalmente tendono a non segnalare eventi di spionaggio commerciali di cui sono state vittima al fine di evitare eventuali azioni da parte degli azionisti e

[17] "*Rapporto 2020 sulla Sicurezza ICT in Italia*"; CLUIST; 2020

pertanto molti CEO, Consigli d'Amministrazione e responsabili della sicurezza ritengono che sia meglio *"(...) imparare in silenzio dai propri errori (...)*"[18].

3. OBBLIGO DI SEGNALAZIONE: PROFILI NORMATIVI.

In tale contesto generale di escalation in termini di "data breach", nel 2016 l'Unione Europea ha approvato una Direttiva comunitaria per la sicurezza delle reti e dell'informazione, nota come Direttiva NIS (Network and Information Security), che fissa i requisiti minimi relativi alla sicurezza informatica per gli operatori dei servizi essenziali e dei servizi digitali.

La direttiva NIS del 2016 è stata fatto oggetto da parte della Commissione Europea di una proposta di revisione. Tale proposta mostra con estrema chiarezza quanto sia ritenuta importante per le istituzioni europee la materia riguardante la cyber security. Le novità introdotte riguardano l'estensione di determinati obblighi in materia anche nei confronti di soggetti operanti in settori ad oggi non coperti dalla Direttiva NIS, tra i quali il settore del ciclo dei rifiuti, aerospaziale, della produzione e consegna di alimenti, della produzione e distribuzione di prodotti chimici, dei servizi postali, della produzione di dispositivi medici, apparecchiature elettroniche e della pubblica amministrazione.

Una nota di particolare merito riguarda l'aspetto inerente all'apertura di una procedura di infrazione da parte della Commissione Europea a carico di alcuni Stati Membri che non hanno ancora attuato a pieno la Direttiva NIS.

La tendenza "all'occultamento" di un "data breach" da parte delle vittime a livello normativo non è più consentita, infatti, soprattutto

[18] "Economic Espionage: How to Protect Your Clients' Trade Secrets"; Robert Tie; Fraud Magazine; 2008

su impulso delle istituzioni comunitarie, le intrusioni informatiche sono state fatte oggetto di apposita regolamentazione, rendendo l'omessa segnalazione un illecito.
La normativa di riferimento in ambito europeo è stata attivata onde favorire, se non imporre, strumenti che garantiscano un ambiente, in termini di sicurezza informatica, il più performante possibile contro le minacce cibernetiche. Gli strumenti normativi più importanti sono la citata Direttiva Nis, introdotta nell' ordinamento italiano con il Decreto Legislativo 18 maggio 2018 n. 65, oltre il D.p.c.m. 131/2020, il quale disciplina il "Perimetro nazionale di sicurezza cibernetica", volto alla attuazione della direttiva NIS.
La normativa è diretta ai soggetti determinati dalla Direttiva, ossia gli "operatori di servizi essenziali" ed i "fornitori di servizi digitali".
Gli "operatori di servizi essenziali" sono i gestori di quelle reti riferite a sanità, energia, trasporti, sistemi bancari e finanziari, distribuzione di acqua potabile, nonché i sistemi di telecomunicazione.
I fornitori di servizi digitali svolgono un ruolo fondamentale in considerazione della loro struttura servente in relazione a sistemi di e-commerce, cloud computing, oppure al "semplice" motore di ricerca. Il Perimetro nazionale di sicurezza cibernetica determina gli attori pubblici e privati che svolgono compiti essenziali per la sicurezza nazionale. Appare evidente che il fine della normativa è quello inerente al mantenimento della stabilità "delle funzioni e dei servizi essenziali" (art. 2 D.p.c.m. 131/2020) delle attività da parte di tutti gli attori operanti nell'ambito delle infrastrutture strategiche nazionali.
Gli operatori individuati dalla normativa introdotta dal Perimetro, pubblici (art. 3 D.p.c.m. 131/2020) o privati che siano, avranno

l'obbligo giuridico[19] , al verificarsi di uno degli incidenti elencati, aventi impatto in particolare su beni ICT (information & communication technology) - i soggetti inclusi nel perimetro sono tenuti a procedere alla notifica al CSIRT italiano (Computer security incident response team) presso il DIS, tramite appositi canali di comunicazione entro 6 ore o entro 1 ora in base alla tipologia di incidente.

L'omessa notifica dell'incidente informatico, ex art. 21 comma 3 del D. Lgs. 65/2018 (attuazione direttiva NIS) dispone che, Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti, ai sensi dell'articolo 12, comma 5, è soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

In linea di massima, la violazione dell'omessa notifica in relazione all'incidente informatico, ivi incluso un "data breach", a livello sanzionatorio si avrà un illecito di natura amministrativa, e solamente nelle ipotesi residuali, si avranno sanzioni di natura penale, e nel caso di enti o persone giuridiche si farà riferimento al d.lgs. 231/2001, come ad esempio il fornire false informazioni se rivolte alla Presidenza del Consiglio dei Ministri, oppure al Ministero dello sviluppo economico, qualora vi sia attività ispettiva e/o di vigilanza.

Sotto il profilo squisitamente normativo il "data breach" in relazione alla violazione dei dati personali è regolamentato dal GDPR, il quale stabilisce che "una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare

[19] Schema di decreto del Presidente del Consiglio dei ministri recante regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto legge 21 settembre 2019, n. 105, convertito, con modificazioni, della legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.
http://documenti.camera.it/leg18/dossier/pdf/AC0457.pdf?_1621541784842

danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione[20], pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena si viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Relativamente alla sanzione pecuniaria in caso di violazione della comunicazione, in conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 (o 20 000 000) di Euro, o per le imprese, fino al 2 (o 4) % del fatturato mondiale totale annuo dell'esercizio precedente (in taluni casi specifici ed a secondo del tipo di violazione).

[20] La pseudonimizzazione viene così definita come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4(5), GDPR).

Relativamente a quei soggetti che non sono inclusi all'interno del Perimetro e della direttiva NIS, si andranno ad applicare le disposizioni in tema di privacy (GDPR).

4. ASPETTO ECONOMICO DELLO SPIONAGGIO INFORMATICO.

L'avvento dell'informatica e della connessione digitale globale ha aperto porte ad azioni di sottrazione di informazioni riservate fino a pochi anni or sono inimmaginabili. Appare evidente che i soggetti colpiti da spionaggio, o attacco cyber, oltre a sostenere un costo economico direttamente riconducibile all'azione criminosa, subiscono non indifferenti conseguenze sotto il profilo prettamente produttivo e di reputazione.

Il furto delle informazioni riservate sotto il profilo economico ha un duplice impatto. Il primo è relativo a tutte quelle attività riferibili al processo prettamente tecnico, che vanno dalla rilevazione delle modalità di intrusione fino al ripristino e successiva messa in sicurezza del "perimetro cyber" del soggetto colpito. Tutte queste attività hanno con estrema evidenza un costo, alcune volte non indifferente.

Ulteriormente, vi sono quei costi che si mostrano sul medio e lungo periodo, e riguardano soprattutto la sottrazione in termini di competitività, patrimonio "immateriale" come ad esempio tutto quello che potrebbe essere relativo a progetti oppure brevetti frutto di quelle attività di R&S derivati spesso da ingenti costi (ad esempio in ambito farmaceutico o software, oppure prettamente industriale).

Assolutamente da non minimizzare il possibile danno di immagine, in quanto la reputazione pubblica del soggetto colpito potrebbe essere duramente colpita.

Dal punto di vista economico, come riportato nel documento "*The Scale of impact of industrial espionage and theft of trade secrets through cyber*" pubblicato dalla Commissione Europea nel 2018, *l'European Center for International Political Economy* (di seguito, "*ECIPE*") stimava per il 2018 una perdita economica a seguito del furto di segreti commerciali mediante *cyber attack*, a livello europeo, pari a Euro 60 miliardi e a una perdita di 289 mila posti di lavoro[21].

Nel dettaglio, l'ECIPE ha precisato che una quantificazione circa l'impatto negativo derivante dal furto di segreti commerciali mediante attività di cyber spionaggio è molto difficile per molteplici ragioni, come ad esempio la mancanza di consapevolezza o di essere stati vittima di un attacco informatico o del furto di un segreto commerciale (c.d. "*lack of awarness*") e la mancanza di un'adeguata valutazione dei segreti commerciali detenuti da parte dell'organizzazione stessa[22].

Per completezza, si precisa che, sulla base di taluni *feedback* ricevuti dall'ECIPE da organizzazioni vittime di attività di cyber spionaggio con furto di segreti commerciali, l'impatto diretto derivante da tale furto ammonterebbe solo per il 10% ad un incremento dei costi mentre, per il restante 90% dipenderebbe da impatti indiretti a lungo termine come la perdita di conoscenza, di vantaggio competitivo e perdita di posti di lavoro[23].

Nel dettaglio, le organizzazioni coinvolte nell'indagine statistica svolta dal ECIPE, hanno precisato che la gestione della crisi a seguito di un attacco informatico genera dei costi solitamente compresi tra i 50 e 200 milioni di euro e il 70% delle

[21] "The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber"; European Commission; 2018

[22] "The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber"; European Commission; 2018

[23] "The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber"; European Commission; 2018

organizzazioni considera rilevante l'impatto delle perdite economiche e reputazionali generate dal furto di segreti commerciali.
In aggiunta, si evidenzia, come gli impatti economici sono proporzionati al valore delle informazioni e dei dati rubati pertanto, la perdita di informazioni o dati di valore significativo può avere un effetto diretto sulla redditività dell'organizzazione andando, tra le altre, a influenzare negativamente il prezzo di mercato delle azioni (nel caso di società quotata) e in casi più gravi può portare anche al fallimento della società[24].

5. PROFILI GIURIDICI

Come già rappresentato nella sezione introduttiva, In Italia il novero di norme che vanno a definire il reato di spionaggio industriale è sicuramente più ampio e frammentato in particolare, bisogna innanzitutto differenziare la condotta, ai fini di spionaggio, perpetrata da un soggetto interno all'Azienda o Ente (c.d. spionaggio interno) da quella di un soggetto esterno (c.d. spionaggio esterno).
A titolo di premessa e prima di entrare nel vivo della trattazione, si evidenzia che solo recentemente, con Sentenza della Suprema Corte di Cassazione del 10 aprile 2020, i dati informatici (*files*) sono stati qualificati, per la prima volta, "*(…) cose mobili ai sensi della legge penale (…)*"[25], in quanto sino a questo momento il

[24] "The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber"; European Commission; 2018
[25] Nel dettaglio, la Sentenza della Suprema Corte di Cassazione n. 11959 del 10 aprile 2020, sancisce che: "(…) i dati informatici (files) sono qualificabili cose mobili ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la sottrazione da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer "formattato" (…)".

“furto di dati” era punito esclusivamente quando era realizzato il furto del supporto contenente gli stessi (cartaceo o informatico).
Pertanto, se in precedenza qualcuno effettuava la copia di un documento senza l’autorizzazione del legittimo titolare, che quindi non perde la disponibilità del *file* illegittimamente copiato, ovvero, casi nei quali ci si appropri del contenuto del documento (per esempio copiandolo ed incollandolo su un nuovo *file*) senza neppure creare una copia del medesimo, in tutte queste ipotesi, si rientra in quelle che la Suprema Corte etichetta come mera *"presa di conoscenza"* non sanzionabile ai sensi degli articoli 624 e 646 c.p., rispettivamente furto e appropriazione indebita.

5.1 SPIONAGGIO INTERNO

Per la legge italiana, lo spionaggio industriale costituisce reato punibile a querela della persona offesa, secondo quanto disposto dagli art. 622 e 623 del codice penale. L’art. 622 c.p. regola la fattispecie della “rivelazione di segreto professionale”, messa in atto da chiunque sia a conoscenza, anche lecitamente, di un segreto inerente al proprio lavoro, ma senza giusta causa (quindi, illecitamente) lo distrae dal suo ambito di riservatezza, diffondendolo. L’art. 623 c.p. descrive poi l’ipotesi di “rivelazione di segreto scientifico e industriale”, riferendosi al c.d. “know-how”, ovvero il patrimonio di conoscenze di un’impresa: una risorsa strategica che, con l’attività di spionaggio, viene illecitamente sottratta per essere riferita a soggetti esterni all’azienda titolare. In entrambe le fattispecie, l’elemento caratterizzante è la condotta: la rivelazione del segreto professionale o industriale deve essere finalizzata a realizzare un profitto proprio o altrui, arrecando per questo un danno all’impresa a cui il segreto viene sottratto.

È di tutta evidenza che, perché possa essere dichiarata la colpevolezza di chi ha violato il segreto, bisognerà che vengano fornite le prove di essa e che tali prove siano valide in giudizio. A questo provvedono le investigazioni e le indagini di controspionaggio industriale, condotte secondo criteri professionali da addetti con competenze specifiche.
L'articolo 615-quater, introdotto dalla legge n° 547/93, intitolato "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", dice: "chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all´accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5164 euro".

5.2 SPIONAGGIO ESTERNO

La principale novità del nuovo art. 623 c.p. consiste proprio nella estensione della tutela del patrimonio immateriale dell'azienda, affiancando alla tutela delle *"notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche"* anche quella dei "*segreti commerciali*"[26]; il bene giuridico tutelato dalla nuova formulazione normativa è da individuarsi, pertanto, nel c.d. segreto *scientifico-commerciale* che, simmetricamente a quello disciplinato in ambito civilistico, rappresenta una speciale figura

[26]L'ampia formula descrittiva del segreto commerciale prevista dalla norma incriminatrice induce, ora, a ritenere che entrambe le figure distinte del segreto scientifico-industriale (metodi di lavorazione, macchinari utilizzati, prodotti realizzati) e del segreto scientifico-commerciale (contratti in corsa, organizzazione della produzione, della distribuzione, della pubblicità) siano comprese nell'area di tutela assicurata dalla disposizione.

del segreto professionale, e che si compone dei tre elementi costitutivi del requisito della segretezza, del valore economico e della protezione[27].

L'ultima novità consiste nella previsione dell'aggravante, prevista dal nuovo terzo comma, che interviene quando il fatto è *"commesso tramite qualsiasi strumento informatico"*: tale ampia formulazione porta a suppore una sua applicazione generalizzata in quanto, attualmente, appare difficile ipotizzare una condotta di acquisizione, divulgazione ed uso di segreti commerciali commessa interamente senza l'uso di alcun strumento informatico[28].

Da un confronto tra l'art. 646 c.p., così come interpretato dalla Suprema Corte nella sentenza precedentemente menzionata, e l'art. 623 c.p., le due norme, pur presentando una parziale sovrapponibilità, mantengono zone di intervento distinte.

Le differenze sono da ricondurre all'oggetto materiale del reato (cosa mobile dotata di una fisicità *vs* segreto scientifico o commerciale) e alla condotta (appropriazione *vs* divulgazione o

[27] Per quanto attiene il primo requisito, la segretezza, pur se la sussistenza del medesimo non può essere rimessa alla esclusiva valutazione dell'imprenditore o di altro beneficiario, dovendo pur sempre scaturire da oggettive ragioni giustificatrici del divieto di conoscenza da parte dei terzi, tuttavia, la presenza di procedure di gestione di tali informazioni nonché di specifiche clausole contrattuali di confidenzialità appare un utile strumento al fine di rafforzare tale carattere di segretezza. Il valore economico, in linea con il dettato di cui all'art. 98 c.p.i., non fa riferimento ad una quotazione di mercato quanto, piuttosto, a un oggettivo quanto concreto vantaggio per il suo utilizzatore esclusivo rispetto alla concorrenza, idoneo ad assicurare o addirittura accrescere la posizione di mercato. Per quanto concerne l'elemento costitutivo della protezione, assicurando il precetto la tutela penale soltanto al titolare del diritto al segreto che possa dimostrare di avere positivamente assolto ad un onere di diligenza nella protezione dei dati da altrui intrusioni, è di preminente importanza che tali protezioni siano state correttamente individuate e predisposte correttamente. Cfr. GALLI, *Il Nuovo Diritto del know-how e dei segreti commerciali Prima lettura sistematica delle novità introdotte dal D.Lgs. 11 Maggio 2018*, n. 63 ss.

[28] Cass. Pen. 18 maggio 2001, n. 25008.

utilizzo). Le due fattispecie, peraltro, potrebbero concorrere: si pensi se, in un caso come quello analizzato nella sentenza, i *files* illecitamente appresi dall'*ex* dipendente contengano segreti scientifici o commerciali e gli stessi siano successivamente rivelati o utilizzati (per esempio) nell'ambito della nuova società presso la quale il medesimo viene assunto, al fine di conseguire un profitto (per il dipendente e/o per il nuovo datore di lavoro).

Nel sistema di tutele così delineato vi è un grande assente. Né il reato di appropriazione indebita né il reato di rivelazione di segreti scientifici o commerciali son inclusi nel catalogo dei reati presupposto di cui al d. lgs. 231/2001. Una assenza, soprattutto quella dell'art. 623 c.p., che non può che suscitare profonde critiche se si consideri che, nell'attuale contesto economico, non è certamente situazione residuale che un furto di informazioni aziendali (*rectius* di segreti scientifici o commerciali) sia commesso nell'interesse o a vantaggio di una impresa la quale potrà beneficiarne (in termini di sviluppo di nuovi prodotti, di identificazione di nuovi potenziali clienti, ecc.)7.

Tale vuoto normativo può, tuttavia, essere parzialmente compensato dalla possibilità di ricondurre condotte di appropriazione di informazioni (anche riguardanti segreti) a talune fattispecie rilevanti per la responsabilità degli enti,

Non può peraltro sfuggire che, con le modifiche operate dalla l. n. 179/2017 in tema di *whistleblowing*, è stato necessario un coordinamento tra la tutela dei soggetti segnalanti e le altre disposizioni poste a presidio della non circolazione di informazioni che è interesse delle aziende mantenere riservate, fra le quali figurano i segreti commerciali. Il legislatore ha risolto tale possibile contrasto configurando nelle ipotesi di segnalazione effettuata "*nelle forme e nei limiti previsti nel comma 2-bis*", il riconoscimento del perseguimento dell'interesse all'integrità dell'ente, costituendo la "*giusta causa*" di rivelazione di notizie

coperte formalmente dall'obbligo di segreto. In tal modo, le norme che sanzionano la rivelazione dei segreti vedranno un restringimento della loro area di operatività non potendosi incriminare quali *"rivelazioni illecite"* le segnalazioni effettuate per il tramite del canale predisposto dal modello 231. In merito, si è osservato come, in considerazione della operatività limitata della giusta causa, ancorata ai soli casi delle segnalazioni effettuate correttamente ai sensi della normativa 231, occorre domandarsi quali conseguenze discendano qualora le segnalazioni, una volta effettuate, si rivelino *"improprie"*. In tal caso, la segnalazione sarà potenzialmente in grado di arrecare un danno ai beni giuridici tutelati dalle norme di cui agli artt. 622 e 623 c.p. e quindi giustificare l'operatività delle due fattispecie incriminatrici, quali la corruzione tra privati o l'accesso abusivo a sistemi informatici (inserite nel decalogo dei reati presupposto 2318).

Per quanto concerne l'accesso abusivo ad un sistema informatico o telematico, questo può essere considerato un reato che fornisce una tutela anticipata rispetto a condotte infedeli quali il furto di dati o la rivelazione di segreti: tale reato, infatti, punisce il semplice accesso abusivo ad un sistema informatico altrui protetto da misure di sicurezza – quale, per esempio, un *server* condiviso aziendale – precedentemente (ed indipendentemente) da qualsiasi atto concreto lesivo del patrimonio informativo aziendale.

Di particolare interesse appaiono le definizioni di sistema informatico e di abusività dell'accesso.

Le Sezioni Unite, dirimendo un contrasto giurisprudenziale circa il *locus commissi delicti* in casi di accessi abusivi effettuati da postazioni remote, nel concludere che "*il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615 ter c.p., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente*", fornivano importanti indicazioni sulla nozione di

sistema informatico; si osservava come *"un dispositivo elettronico assurge al rango di sistema informatico o telematico se si caratterizza per l'installazione di un software che ne sovrintende il funzionamento, per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati oggetto di trattamento"*, facendo rientrare nell'ambito della protezione offerta dall'art. 615 *ter* c.p., *"anche i sistemi di trattamento delle informazioni che sfruttano l'architettura di rete denominata client - server, nella quale un computer o terminale (il client) si connette tramite rete ad un elaboratore centrale (il server) per la condivisione di risorse o di informazioni, che possono essere rese disponibili a distanza anche ad altri utenti*"[29].

Una ulteriore opzione attiene alla possibilità che condotte riconducibili ai reati di appropriazione indebita (di *file*), o di rivelazione o utilizzo di segreti scientifici o commerciali, si configurino quali reati fine di una associazione per delinquere. Il discorso appare molto simile a quanto avvenuto nell'ambito dei delitti tributari prima che questi venissero inseriti nei reati presupposto della responsabilità degli enti. Prima del c.d. *"decreto fiscale"* – d.l. 26 ottobre 2019 n. 124 la giurisprudenza di legittimità prevedeva, seppur in via indiretta, la possibilità di confisca di beni della persona giuridica, quale profitto dei reati fiscali (reati fine) compiuti dall'associazione per delinquere (reato presupposto). Si veda anche sul punto Cass. 14 ottobre 2015, n. 46162.

Nel ricondurre i sistemi di tipo "*client – server"* alla nozione di sistema informatico, la Suprema Corte mostrava esplicitamente di riconoscere lo sviluppo di una nuova *"dimensione aterritoriale"*, incrementata dalla diffusione di dispositivi mobili e dalla

[29] Cass. Pen. 26 marzo 2015, n. 17325, in Riv. Pen., 2015, 521.

tecnologia del *cloud computing "che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate alle quali è possibile accedere da qualunque parte del globo"*[30].
Di conseguenza, in presenza di una banca dati *"ubiquitaria, circolare o diffusa sul territorio, nonché contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso"*, la Suprema Corte riteneva arbitrario scomporre i singoli componenti dell'architettura di rete: *server* e *client* sono parte integrante di un complesso meccanismo *"strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del client"*[31].
Si è osservato come tale ultima pronuncia abbia avallato una concezione di sistema informatico caratterizzato da *"una dimensione – o almeno una capacità di dimensione – illimitata, e una profondità spaziale che perde ogni connotazione fisica per diventare virtuale rimanendo però assolutamente reale, distribuita intorno alla banca dati centrale lungo raggi indefinibili che la rendono sostanzialmente ubiquitaria, circolare, diffusa"*[32].
Tale processo di dematerializzazione appare ancora più evidente nella recente giurisprudenza di legittimità, che riteneva integrativo del reato di cui all'art. 615 *ter* c.p. l'accesso all'altrui casella di posta elettronica *"trattandosi di uno spazio di memoria, protetto da una password personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio",* sottolineando come *"l'accesso a questo spazio di*

[30] Cass. Pen. 26 marzo 2015, n. 17325, cit.
[31] Cass. Pen. 26 marzo 2015, n. 17325, cit. Negli stessi termini anche Cass. 22 luglio 2015 n. 37343; Cass. Pen. 20 gennaio 2016, n. 12951.
[32] SCIUBA, Osservazioni a Cass. Pen., 26 marzo 2015, sez. UU, n. 17325, in Cass. Pen., 2015, 3507 s.

memoria concreta un accesso a sistema informatico, giacché la casella è una porzione della complessa apparecchiatura – fisica e astratta – destinata alla memorizzazione delle informazioni, quando questa porzione di memoria sia protetta, in modo tale da rivelare la chiara volontà dell'utente di farne uno spazio a sé riservato, con la conseguenza che ogni accesso abusivo allo stesso concreta l'elemento materiale del fatto"[33].

A differenza del reato di appropriazione indebita – fattispecie delittuosa inserita già nell'originario assetto codicistico ancorata al concetto di *"cosa"* – il reato di cui all'art. 615 *ter* c.p., prevedendo quale oggetto materiale un *"sistema informatico"*, si presta con maggiore facilità ad adattarsi alla nuova realtà dematerializzata: se è vero che i sistemi informatici dell'epoca dell'introduzione del reato (1993) e le relative modalità di utilizzo degli stessi sono incredibilmente mutati nel corso degli ultimi trent'anni, la locuzione *"sistema informatico"* pare potersi quasi integralmente adattare all'attuale contesto tecnologico, non prestando il fianco a sostanziali vuoti di tutela.

Passando al concetto di abusività, anch'esso presenta una accezione piuttosto lata, ove un accesso abusivo può ricorrere in caso di originaria mancanza di autorizzazione o di sua successiva revoca[34], ma altresì quando, alla luce dei principi espressi dalle

[33] Cass. Pen. 2 maggio 2019, n. 18284

[34] Cass. Pen. 25 ottobre 2018, n. 48895, secondo la quale "La preposizione ad una branca o un settore autonomo dell'impresa del dipendente con qualifica dirigenziale non implica necessariamente l'accesso indiscriminato a tutte le informazioni in possesso dell'imprenditore preponente, perché una compartimentazione dell'accesso informativo è pienamente compatibile, sul piano logico e giuridico, con il carattere settoriale della preposizione. Ne consegue che risponde di accesso abusivo a sistema informatico il dirigente che non provi di avere accesso illimitato ai dati del datore e superi i limiti della suddetta compartimentazione".

Sezioni Unite dalle note sentenze *"Casani"*[35], e *"Savarese"*[36], l'agente "*violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema*" ovvero "*ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito*".

Con riferimento a tale ultima situazione, la Suprema Corte, con la recente sentenza della Quinta Sezione della Suprema Corte n. 18284 del 2 maggio 2019, qualificava come accesso abusivo la condotta di *"accesso, mediante abusivo utilizzo della password"* ad una casella di posta elettronica, della lettura della corrispondenza privata e della modifica apportata alle credenziali d'accesso rendendo, in tal modo, inaccessibile la casella da parte del titolare. In tale arresto, la Suprema Corte estendeva per la prima volta i principi enunciati nella sentenza *"Savarese"* anche al settore privato – *"nella parte in cui vengono in rilievo i doveri di fedeltà e lealtà del dipendente che connotano indubbiamente anche il rapporto di lavoro privatistico"* – qualificando come illecito e abusivo qualsiasi comportamento del dipendente che si ponga in contrasto con i suddetti doveri manifestandosi in tal modo la *"ontologica incompatibilità"* dell'accesso al sistema

[35] Cass. Pen. Sez. Un., 27 ottobre 2011, n. 4694: "Integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema".

[36] Cass. Pen. Sez. Un., 18 maggio 2017, n. 41210: "Integra il delitto previsto dall'art. 615-ter comma 2 n. 1 c.p. la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un servizio informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita".

informatico, connaturata ad un utilizzo dello stesso estraneo alla *ratio* del conferimento del relativo potere.
Nel caso in cui il *"furto"* e la successiva rivelazione dell'informazione/segreto da parte di un esponente aziendale, sia esso apicale o subordinato, si manifestino quale diretta conseguenza di una precedente promessa o ricezione di denaro o di altra utilità, tale condotta potrebbe rilevare in termini di violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà di cui alla fattispecie della corruzione tra privati, disciplinata dall'art. 2635 c.c.
In merito, se gli obblighi inerenti all'ufficio disciplinati dall'art. 2635 c.c. sono quelli rilevabili da precetti civilistici che regolano e disciplinano i singoli doveri dei soggetti qualificati, in tale categoria andrebbero inseriti tutti quegli gli obblighi di portata ampia e generica (a patto che trovino concretizzazione in una fonte scritta o in negozi giuridici ed atti formali) assumendo quindi rilevanza le violazioni di qualunque obbligo finalizzato ad assicurare la tutela degli interessi patrimoniali della società, inclusi quelli derivanti da beni immateriali quali informazioni rilevanti e/o segrete. Peraltro, a norma del terzo comma, alla responsabilità del dipendente *"infedele"*, si andrebbe ad aggiungere quella del corruttore.
In entrambe le ipotesi sopra descritte, quindi, qualora il reato venisse commesso nell'interesse o a vantaggio di una persona giuridica – il nuovo datore di lavoro per esempio –, quest'ultimo potrebbe essere chiamato a rispondere per gli illeciti di cui agli articoli 24 *bis* comma 1 (reati informatici) e 25 *ter* comma 1 lett. s-*bis*) (reati societari) del d. lgs. 231/2001. A tal fine, sarà sempre necessario che il reato presupposto sia commesso in concorso dal dipendente che si appropri delle informazioni/*file* aziendali (il quale, al momento del fatto, sarà ancora formalmente legato alla società vittima del reato) con un esponente della società

beneficiaria, quale istigatore del reato di accesso abusivo ovvero quale corruttore[37].

[37] AMATI, Infedeltà a seguito di dazione o promessa di utilità, in ROSSI (a cura di), Reati societari, Torino, 2005, 441.

CAPITOLO 2
CASE STUDY E LA RILEVANZA PER IL SETTORE DELLE PMI

1. IL CASO SOLARWORLD AG

Il rapporto Clusit 2020 (relativo all'anno 2019) evidenziava come *"Nell'anno appena passato si è consolidata una discontinuità, si è oltrepassato un punto di non ritorno, tale per cui ormai ci troviamo a vivere ed operare in una dimensione differente, in una nuova epoca, in un "altro mondo",* del quale ancora non conosciamo bene la geografia, gli abitanti, le regole e le minacce".
La SolarWorld AG era un'azienda tedesca quotata sul mercato DAX, la quale operava nella produzione e nella commercializzazione di prodotti per il mercato fotovoltaico.
Tra maggio e settembre 2012, nel medesimo periodo in cui la controllata americana, SolarWorld America, stava affrontando un contenzioso per *dumping*[38] contro dei produttori cinesi, la medesima fu vittima di un attacco informatico finalizzato alla sottrazione di alcuni dati sensibili, tra cui segreti commerciali, detenuti sui server della società[39].
Nel 2014, i Pubblici Ministeri federali hanno incriminato per violazione di sistemi informatici della SolarWorld America e di altre società, molte delle quali coinvolte in *trade disputes* con la Cina[40], cinque cittadini cinesi, ufficiali dell'Unità 61398 del terzo

[38] *"(…) Il dumping è una forma di concorrenza sleale poiché i prodotti vengono venduti ad un prezzo che non rispecchia in modo accurato il costo di produzione (…)*". Fonte: "*Che cos'è il dumping? Definizione e impatto*"; Parlamento Europeo; 2018.
[39] "*The Cost of Malicious Cyber Activity to the U.S. Economy*"; The Council of Economic Advisers; Executive Office of the President of the United States; febbraio 2018
[40] "*Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying*"; Diane Cardwell; The New York Times; 2014

dipartimento dell'Esercito Popolare di Liberazione cinese – unità specializzata in *cyberwar*[41].

Nel dettaglio, come si evince dall'i*ndictment* n. 14-118 di maggio 2014, il Sig. Wen Xinyu[42] mediante l'utilizzo di un *malware* denominato "*ugls.exe*" si era infiltrato nella rete informatica della SolarWorld sottraendo segreti commerciali appartenenti alla SolarWorld America. L'attacco sarebbe consistito in circa 13 intrusioni che avrebbero portato alla sottrazione di migliaia di *e-mail* e *file* appartenenti a sette *executive* della società. I dati sottratti riguardavano informazioni finanziarie, sulla capacità produttiva, sui costi, sull'andamento del business e sulle strategie da adottare in relazione al "*trade dispute"* in atto (Stati Uniti contro Wang Dong 2014) [43].

Nel particolare, grazie alla documentazione sottratta, i concorrenti cinesi potevano[44]:

- valutare lo stato di salute finanziario della società al fine di comprendere il grado di sopportazione di un eventuale situazione di tensione finanziaria;
- replicare dei prodotti mediante l'analisi dei dati sulla produzione non sostenendo alcun costo di ricerca;
- comprendere le marginalità di SolarWorld e modificare i prezzi al fine di rendere SolarWorld meno competitiva;
- conoscere le informazioni circa il trade dispute in atto al fine di porre in essere una strategia difensiva adeguata.

[41] "Cyber Security: Espionage and Social Networking"; SSA Elvis Chan; Federal Bureau of Investigations; 2015

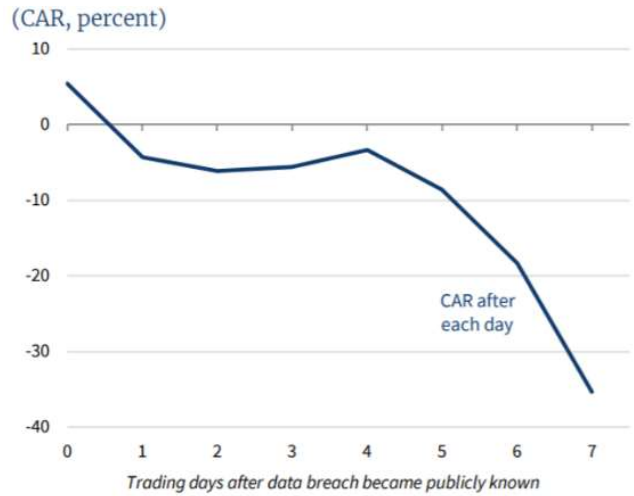
[42] Meglio conosciuto anche come: Wen Xin Yu, WinXYHappy, Win_XY e Lao Wen.

[43] "*The Cost of Malicious Cyber Activity to the U.S. Economy*"; The Council of Economic Advisers; Executive Office of the President of the United States; febbraio 2018

[44] "*The Cost of Malicious Cyber Activity to the U.S. Economy*"; The Council of Economic Advisers; Executive Office of the President of the United States; febbraio 2018

L'impatto derivante dall'attacco informatico in parola è stato devastante, la società ha registrato una perdita di valore pari al 35% del suo valore di mercato (Euro 178 milioni)[45].
Nel grafico di seguito riportato si evidenzia il *Cumulative Abnormal Return*[46] dal giorno zero, giorno in cui è stata data comunicazione al mercato del *data breach,* ai 7 giorni successivi.

Cumulative Abnormal Return* dopo che la società aveva reso pubblica la notizia circa il *data breach



Fonte: "The Cost of Malicious Cyber Activity to the U.S. Economy"; The Council of Economic Advisers; Executive Office of the President of the United States

[45] "*The Cost of Malicious Cyber Activity to the U.S. Economy*"; The Council of Economic Advisers; Executive Office of the President of the United States; febbraio 2018
[46] Il *Cumulative Abnormal Return* (CAR) è la somma delle differenze tra il rendimento atteso su un titolo (rischio sistematico moltiplicato per il rendimento di mercato realizzato) e il rendimento effettivo. Fonte: Nasdaq.com

A maggio 2017, SolarWorld AG ha presentato istanza di fallimento e la SolarWorld America, la controllata americana, è stata messa in vendita al fine di coprire le passività generate dalla capogruppo.
Successivamente, la società SolarWorld AG veniva acquisita dalla società SolarWorld Industries GmbH, la quale nel 2018 ha dichiarato fallimento[47].

2. IL CASO MICROSOFT EXCHANGE

In data 20 febbraio 2021, è stata resa nota una vulnerabilità molto grave su sistemi *Microsoft Exchange* (di seguito "*MS Exchange*") - uno dei software più diffusi al mondo per la gestione delle caselle email aziendali e dei calendari – codificata come "*CVE-2020-0688 | Microsoft Exchange Validation Key Remote Code Execution Vulnerability*", grazie al quale, tra gennaio e marzo, sono stati condotti degli attacchi informatici (secondo quanto riportato nel documento "*New nation-state cyberattacks*"[48]) da parte di un gruppo di *cyber criminali* denominato Hanfium.
In particolare, si tratterebbe di un gruppo di *hacker* cinesi attivo nell'attività di cyber spionaggio e con interessi in *target* operanti nei settori della ricerca, della difesa e dell'industria nonché in organizzazioni politiche e non governative. In relazione a tale gruppo, Tom Burt, vicepresidente corporate di Microsoft e responsabile del settore *Customer Security & Trust di Microsoft*, ha affermato che "*Si tratta di un attore* [ndr, Hanfium] *altamente qualificato con capacità ricercate*" [49].

---

[47] "*The Cost of Malicious Cyber Activity to the U.S. Economy*"; The Council of Economic Advisers; Executive Office of the President of the United States; febbraio 2018
[48]https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/
[49]https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Nel dettaglio, gli attacchi ai server di *MS Exchange* sarebbero stati prima focalizzati ai server presenti sul territorio USA e successivamente si sarebbero estesi in Europa e nel resto del mondo.

Al riguardo, anche Jake Sullivan, consigliere per la sicurezza nazionale del presidente statunitense Joe Biden, ha dichiarato che la Casa Bianca sta "*monitorando attentamente*" la patch di emergenza rilasciata dal colosso di Redmond per rispondere alle vulnerabilità emerse nei software Exchange Server e segnala "*potenziali compromissioni di think tank statunitensi e aziende cruciali per l'industria della difesa*"[50].

In Europa è stato rilevato che un numero crescente di installazioni di *MS Exchange* è stato oggetto di attacchi che hanno comportato impatti dannosi e, solamente in Italia, potrebbero essere interessate migliaia di aziende che si affidano al *software* di Microsoft. Al riguardo, si stima che sul territorio Italiano ci siano n.3.700 server di MS Exchange vulnerabili contro i n. 20.000 degli Stati Uniti d'America[51]. Tali numeri sono da considerarsi in aumento, in quanto nel frattempo, molti altri gruppi APT[52] e attori delle minacce stanno utilizzando le vulnerabilità per esfiltrare dati e diffondere *malware* in tutto il mondo.

Tra le varie vittime europee coinvolte, c'è l'Autorità Bancaria Europea (di seguito, "*EBA*"), che in data in data 7 marzo 2021, ha comunicato di essere stata vittima di un attacco informatico sui *server* Microsoft Exchange a seguito di talune e meglio descritte nel prosieguo vulnerabilità *zero-day*[53]. Al contempo, l'EBA ha dichiarato che l'incidente non ha pregiudicato la riservatezza dei

[50] https://twitter.com/JakeSullivan46/status/1367660450855477256

[51] https://www.cybersecurity360.it/nuove-minacce/vulnerabilita-in-microsoft-exchange-server-ecco-le-soluzioni-di-mitigazione/

[52] Gli *Advanced Persistent Threat* sono una tipologia di attacchi mirati e persistenti.

[53] https://www.eba.europa.eu/cyber-attack-european-banking-authority

sistemi e dei dati dell'Autorità Bancaria[54] e al riguardo, si precisa, che EU *Cyber Crises Liaison Organisation Network* (*CyCLONe*) e la rete dei CSIRT stanno monitorando la situazione.

Sebbene l'obiettivo degli attacchi fosse inizialmente l'esfiltrazione di informazioni (*records*), gli aggressori sembrano tuttavia sfruttare le vulnerabilità di *Microsoft Exchange*[55]*e* anche per installare *ransomware*[56], al fine di ottenere profitti e al riguardo, si osserva, che sono stati segnalati diversi casi di sistemi infettati dal *ransomware* noto come "*DearCry*".

Successivamente, Microsoft identificava le seguenti e ulteriori n.4 vulnerabilità *zero-day*[57] [58]

- CVE-2021-26855, una vulnerabilità SSRF (*server-side request forgery*) in Microsoft Exchange che potrebbe essere sfruttata da un utente malintenzionato per l'autenticazione come server Exchange inviando richieste HTTP arbitrarie;
- CVE-2021-26857, un problema di de-serializzazione non sicuro che risiede nel servizio di messaggistica unificata. Questo difetto consente a un utente malintenzionato con autorizzazione amministrativa di eseguire codice come SYSTEM, il livello di privilegio più elevato, sul server *Exchange*;

---

[54] https://www.eba.europa.eu/cyber-attack-european-banking-authority-update-3

[55] Sulla base delle ricostruzioni effettuate da Microsoft, per compiere la violazione, i cyber criminali hanno sfruttato la vulnerabilità per accedere tramite una connessione da remoto attraverso la porta 443, inviando delle richieste http eseguendo un'autenticazione come Exchange Server.

[56] "(…) *Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access (…)*" McAfee Definition - https://www.mcafee.com/enterprise/it-it/security-awareness/ransomware.html#:~:text=Ransomware%20is%20malware%20that%20employs,then%20demanded%20to%20provide%20access.

[57] Per vulnerabilità *zero-day* è una qualunque vulnerabilità di un software non nota ai suoi sviluppatori o da essi conosciuta ma non gestita.

[58] https://github.com/microsoft/CSS-Exchange/tree/main/Security

- CVE-2021-26858 e CVE-2021-27065, che consentono entrambi agli utenti autenticati di scrivere arbitrariamente file su *Exchange Server*.

Segnatamente, le vulnerabilità rilevate, se sfruttate, permetterebbero di *(i)* ottenere il controllo del sistema Exchange con privilegi di *administrator; (ii)* eseguire il codice malevolo (*Ransomware*); *(iii)* accedere alle *mailbox* e alle *Active Directory*. Tali vulnerabilità possono essere sfruttate sulle versioni del *software* Exchange Server 2010, Exchange Server 2013, Exchange Server 2016 ed Exchange Server 2019, ossia tutte le versioni in commercio del software ad eccezione di Exchange Online[59] ed in aggiunta, sui server in cui:

1. *Microsoft Exchange Client Access Role* è attivo, se è attiva la funzionalità di accesso all'interfaccia Web della posta elettronica: Outlook Web Access (OWA);
2. L'attaccante dispone di una Login valida, presenza di email compromesse nel *darkweb*, *deep web* e web.

Il 2 marzo 2021, Microsoft ha iniziato il rilascio diversi aggiornamenti di sicurezza per Microsoft Exchange Server per affrontare le vulnerabilità utilizzate negli attacchi in corso[60].

3. DA STUXNET AI RAMSOMWARE 2.0: È ANCHE UNA QUESTIONE DI SPIONAGGIO.

L'evoluzione delle attività di intrusione sotto il profilo prettamente cyber negli anni hanno subito radicali trasformazioni, sostanzialmente derivanti dalle ampie capacità dei cyber criminali i quali, sono andati letteralmente a "caccia" di numerose falle

[59] https://csirt.gov.it/contenuti/sfruttate-vulnerabilita-0-day-su-exchange-server-al01-210303-csirt-ita

[60] "*Situational Report on Microsoft Exchange Vulnerabilities*"; ENISA; 2021

informatiche, e non solo, che possano loro consentire di avere un qualche tipo di vantaggio.
La "cyber warfare" è divenuta negli ultimi anni una costante che va a rendere con estrema evidenza un significativo terreno di battaglia la quarta dimensione, spesso definita quale "spazio cibernetico", sia sotto il profilo dello scontro tra attori istituzionali, ed ovviamente, come si è avuto modo di osservare, anche tra privati.
Il paradigma dei conflitti sta velocemente mutando, infatti l'impiego delle risorse in ambito informatico sarà chiaramente più contenuto rispetto ad uno sforzo militare. Fino ad oggi lo scontro cyber avrebbe potuto rappresentare il conflitto di tipo "non convenzionale". Nel prossimo futuro potrebbe rappresentare il conflitto convenzionale.
L'antesignano di tale mutamento di scenario potrebbe rappresentare l'utilizzo del celebre virus informatico "Stuxnet" da parte dei soggetti coinvolti per colpire la centrale nucleare di Natanz in Iran nel 2009.
Stuxnet è un attacco informatico di tipo "zero day", in quanto lo sviluppatore del sistema informatico vittima non è a conoscenza della vulnerabilità, ed esso ne ha utilizzate contemporaneamente ben cinque. Si utilizza il termine "zero day" in quanto gli attaccanti e gli attaccati hanno "zero giorni" per sfruttare il bug o per risolverlo, in quanto ci potrebbe essere, in determinati casi, la corsa alla vendita o all'acquisto della falla di sicurezza nel mercato illegale.
Tutto il percorso che ha portato all'attacco informatico è stato frutto di una geniale strategia che ha portato gli attaccanti ad infettare delle macchine disconnesse dal web.
E questo è un aspetto centrale della vicenda.
Nello specifico, l'obiettivo finale di "Stuxnet" era quello di provocare la distruzione delle centrifughe della centrale nucleare

target, rendendo di fatto impossibile l'arricchimento del materiale fissile. Il virus apparentemente è stato inoculato all'interno del perimetro informatico della centrale di Natanz tramite una chiavetta USB (questo aspetto non è certo ma probabile).

Una volta riconosciuto l'hardware bersaglio, ossia le centrifughe con componentistica Siemens (si attivava operativamente solo in presenza di componentistica di questa azienda in quanto utilizzata nella centrale di Natanz), Stuxnet fu in grado di variare la velocità di funzionamento delle centrifughe, danneggiandole. Altro aspetto determinante nella vicenda, fu quello di ingegnare il mancato report delle anomalie agli operatori in servizio, rendendoli di fatto all'oscuro della problematica in atto.

Il caso Stuxnet ha avuto quasi certamente dei tramiti per il raggiungimento dell'obiettivo finale, ossia alcune aziende iraniane che avevano rapporti di servizio con la centrale di Natanz. Questo aspetto ci mostra quanto è necessario che tutta la catena dei soggetti coinvolti in un determinato "eco-sistema" siano assolutamente coscienti ed informati in relazione ai rischi delle intrusioni informatiche, in quanto come abbiamo visto, a cascata è "colpibile" anche un obiettivo formalmente disconnesso della rete, ma che nei fatti, tratti un classico sistema di plug in di dispositivi hardware consentono di arrivare al target finale. La questione è di non poco conto.

Gli addetti ai lavori hanno constatato quanto sia stato produttivo Stuxnet, in quanto esso riuscì ad infettare numerosissimi dispositivi su scala globale.

Non appare errato affermare che questo virus informatico abbia rappresentato l'inizio delle battaglie con armi di tipo cibernetico.

L'evoluzione degli attacchi informatici ha portato gli attori informatici ad utilizzare altre tipologie di attacco, molto differenti per tipo e target, rispetto a quanto visto con "Stuxnet".

La nuova frontiera, in rapida evoluzione, è data dagli ormai famosi ransomware (in inglese ransome si riferisce al riscatto). Essi sono strumenti in grado di rendere inaccessibili i file ed i dati dei dispositivi infettati criptandoli, e qui gli autori richiedono la corresponsione di un riscatto (solitamente in bitcoin) per ripristinare le funzionalità.
Di fatto si vanni a sequestrare i file" tramite una cifratura fino a quando non verrà pagato il "riscatto".
Il vettore più comune per inoculare al target il ransomware è la classica mail di phishing, ove il destinatario tramite il link allegato viene indirizzato verso un sito web, spesso fedele riproduzione di un altro, sul quale viene richiesto di scaricare ed aprire il software malevolo.
In tali contesti vi è troppo spesso una reale carenza di attenzione di ciò che si sta per compiere.
In altri casi vi sono altri vettori di inoculazione che derivano da altre vulnerabilità. Altro aspetto da tenere conto nella propagazione del virus informatico è quello inerente al social engeneering, ove tramite tecniche, alcune volte elementari, si carpiscono informazioni rilevanti per la condotta di attacco. Altre tecniche appaiono ancor più semplice, come quella del "classico" smarrimento di una chiavetta USB con all'interno il software malevolo (tale tecnica è denominata baiting e sfrutta la curiosità umana); colui che andrà a rinvenire la predetta andrà a curiosare inserendola nel dispositivo che verrà infettato. Altre tecniche prevedono la creazione di siti che andranno a causare un download con software dannoso, oppure l'utilizzo di appositi "crack" con cui si andrà a bypassare la chiave di attivazione di software costosi (ad es. Office o prodotti Adobe), andando a causare un prezzo/costo molto alto.

L'evoluzione del classico ransomware rappresenta una è una sfida tutta diversa, soprattutto se si possiedono dati riservati e questi vengono esfiltrati.
Le prime versioni dei ransomware si limitavano a crittografare la macchina bersaglio, ora l'evoluzione 2.0 ha un antefatto alla tipica richiesta di pagamento: l'esfiltrazione dei dati che andranno a rappresentare una nuova minaccia estorsiva nei confronti del bersaglio qualora non si proceda al pagamento. In ambito cyber espionage questo è un cambiamento di paradigma, in quanto sovente le aziende che non cedono al ricatto avranno il serio problema di subire anche la possibile divulgazione di dati sensibili, soprattutto nel dark web. Appare questo un problema ulteriore di non poco conto. Il ransomware "Maze" è stato uno dei primi che di fatto si è evoluto in 2.0, infatti egli andava a raggirare la eventuale disponibilità di una copia di backup anche se la vittima ne fosse stata in possesso, in considerazione della pubblica evidenza di un "data breach" oltre che di eventuali sanzioni in relazione alla normativa GDPR.
Tale tipo di attacco informatico è quello che tipicamente mira alla remunerazione economica, infatti il trend è ampiamente in crescita, come confermato dal rapporto Clusit del 2021 nel quale viene specificato che i ransomware nell'anno 2018 rappresentavano il 23% di tutti i malware, nel 2019 sono diventati quasi la metà (46%) e nel 2020 sono arrivati al 67%, andando a rappresentare più di un terzo di tutti gli attacchi malevoli.
In riferimento agli Stati più colpiti, secondo il rapporto "Unit 42 Ransomware Threat Report 2021" di Palo Alto Networks e di The Crypsis Group, la nazione vittima di maggiori attacchi con ransomware nel 2020 è stata rappresentata dagli Stati Uniti, con l'Italia che si posiziona al quarto posto in Europa, dopo Germania, Regno Unito e Francia.

Si è già visto come alcuni ransomware sfruttino le vulnerabilità, infatti uno dei più famosi è stato WannaCry, il quale nella prima metà del 2017 andò a sfruttare la citata vulnerabilità di Exchange Server per consegnare il codice dopo aver compromesso i server.
Alcuni casi eclatanti di doppia estorsione con ransomware 2.0 (maze) sono quelli con vittima Enel, Campari e Allied Universal.
La minaccia data da tali attacchi informatici è notevole, e chiaramente è importante anche ai fini di spionaggio industriale, anche se in fase iniziale il tutto parte da una semplice "estorsione".

4. LE PMI E LA SICUREZZA INFORMATICA

I grandi player aziendali ed amministrativi sostanzialmente si stanno uniformando alle prescrizioni richieste dalla normativa. Sarebbe opportuno andare a verificare lo stato dell'arte assunto dalle PMI in relazione all'adozione di strumenti utili a contrastare le minacce derivanti dagli attacchi alla cybersecurity, anche in ottica di prevenzione dello spionaggio informatico.
Relativamente al contesto italiano appare utile rammentare che, in riferimento ad alcuni parametri forniti dalla Commissione europea in termini di dipendenti, fatturato ed attivo di bilancio, le piccole e medie imprese in Italia sono 148.531.
Orbene, in relazione a quest'ultimo dato notiamo che 123.495 sono piccole imprese, e 25.036 sono medie aziende. In termini prettamente occupazionali notiamo che esse occupano più di 4 milioni di lavoratori, di cui più di 2 milioni sono impiegati in piccole aziende, e 1.9 milioni in aziende di media grandezza. Il dato numerico in relazione al business, in termini economici, ci riferisce che tali aziende hanno prodotto un giro d'affari di circa 886 miliardi di euro.
Quanto riportato fa ampiamente comprendere l'importanza in termini strutturali delle PMI sotto il profilo sia della sicurezza

prettamente cyber di tali tipi di aziende, ma anche in un contesto più ampio in termini di sistema paese.
La ricerca condotta, sotto il profilo dei dati disponibili in termini di adozione di adeguate misure volte ad evitare dei "data breach", ha mostrato una sostanziale carenza di un adeguato campione informativo che possa consentire una valida analisi. Le indagini svolte da vari operatori del settore sono abbastanza limitate per fornire dati effettivamente utili ad inquadrare il panorama oggetto di indagine. Gli studi osservati (rapporto Clusit, EY) riferiscono di indagini a campione, svolte prettamente nei confronti di aziende di medie e grandi dimensioni, escludendo quindi l'ampia platea di piccole imprese.
Spesso le aziende di piccole dimensioni fanno parte di un più ampio indotto, ove un "data breach" potrebbe rappresentare un cavallo di troia nei confronti di realtà più grandi, e quindi più appetibili in ottica di attacco alla sicurezza.
Secondo una indagine svolta da Capterra è stato osservato che il 37% delle Pmi italiane è a rischio attacchi informatici. Il sondaggio, effettuato su un campione di oltre 500 impiegati in piccole e medie imprese, mostra "una situazione preoccupante in merito all'adozione di best practice di sicurezza informatica aziendale basiche ed essenziali".
Stando ai dati, solo il 21% dei dipendenti accede al server aziendale attraverso una VPN, appena il 26% ha installato un antivirus, il 37% è stato vittima di phishing, mentre il 22% non ha mai ricevuto alcuna formazione in materia di sicurezza informatica.
Appare importante sottolineare che, in numerosi casi le violazioni alla sicurezza informatica sono andate in porto non tanto per la capacità degli attaccanti, quanto per la scarsa padronanza dell'argomento da parte dei dipendenti.

Uno studio condotto da Almaviva tramite la piattaforma Cyber intelligence Joshua rileva che delle 500 top PMI analizzate solamente il 10% non presenta vulnerabilità. Benché il campione sia riferito ad una determinata categoria di imprese, un quadro a tinte fosche si potrebbe già ben intravedere all'orizzonte in relazione al campione dimensionale più piccolo delle PMI.
Gli organi di stampa spesso portano a conoscenza l'opinione pubblica che le violazioni informatiche siano compiute soltanto ai danni di grandi aziende. Tale divulgazione ha probabilmente alimentato l'intendimento che le PMI non siano fatte oggetto di attacchi informatici.
Purtroppo spesso tali tipi di imprese non diffondono informazioni in merito alle violazioni informatiche subite, e sfortunatamente, vi è anche il problema delle violazioni non individuate.
Altro aspetto estremamente importante è quello inerente alla logica di supply chain, infatti potrebbe accadere che, in ottica di cyber threat intelligence, un "data breach" potrebbe avere origine proprio da una PMI come "backdoor" verso l'obiettivo finale, ove sostanzialmente l'attaccante ha utilizzato l'anello debole della catena (la PMI) per accedere al sistema aziendale più esteso, e più importante, di cui era fornitore.
In tale cotesto per tali aziende vi potrebbe essere il doppio problema dell'aver subito l'attacco informatico e di aver perso il cliente o fornitore.
Una delle principali incertezze in relazione alla sicurezza informatica delle PMI potrebbe essere quella inerente alla percezione di tale problematica.
Quest'ultima dovrebbe essere considerata quale processo volto al radicare la solidità aziendale, quindi creazione di valore, e non come un semplice costo da sostenere. Già è stato evidenziato come il fenomeno della digitalizzazione dei processi in relazione anche alla globalizzazione, offre delle notevoli possibilità di sviluppo per

le imprese, ma dall'altra vi è necessità di predisporre adeguate "best practice" in relazione alla sicurezza informatica, in quanto il sistema di sicurezza andrà a tutelare le relazioni con clienti e fornitori, inoltre consentirà di mantenere la produttività in quanto si eviteranno interruzioni della catena produttiva di valore.
Il costo economico dei data breach è da considerare sotto una duplice dimensione.
Infatti, contemporaneamente vi è il problema del danno relativo all'impatto sulla reputazione, al costo in termini di tempo ed energie impiegate onde porre rimedio all'attacco informatico subito, alle possibili controversie di natura giudiziaria con chiunque subisca un danno materiale o immateriale causato da una violazione dati (possibilità data dall'art. 82 del GDPR).
Ulteriormente, come già si è osservato, l'art. 83 del GDPR prevede che le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente e quelle di maggiore gravità, e fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
Altro aspetto, e certamente non secondario, è quello inerente al sistema ransomware e relativo riscatto.
Il problema è certamente importante da definire e contenere, in quanto sembrerebbe, secondo un articolo del Corriere della Sera, che le aziende che abbiano ceduto al ricatto siano il 25%, dati certamente allarmanti in ottica di comprensione globale del fenomeno e della sua importanza.
Appare evidente che i costi legati alle violazioni della sicurezza informatica hanno ampio corollario, ed in tale ottica sarà assolutamente necessario intraprendere un percorso di

sensibilizzazione da parte delle PMI in relazione alla cyber security.
In tale contesto potrebbe giocare un ruolo importante la certificazione ISO 27001, la quale fa riferimento allo standard internazionale riferito alla gestione della sicurezza delle informazioni. Nello specifico è un insieme di best practices inerenti alle misure di gestione della sicurezza.
Qualche accenno in riferimento all'implementazione della normativa europea in Italia.
Preliminarmente sarebbe opportuno adottare a livello europeo un regolamento, e non una direttiva (NIS), onde evitare frammentazioni in termini di adozioni di strumenti di cyber security in ambito UE.
L'adozione degli "input" forniti dalla direttiva in ambito cyber security sono stati a macchia di leopardo, e pertanto, un regolamento "self executed" ben ideato certamente consentirebbe una architettura generale ben definita tra i paesi membri UE.
L'attuale quadro generale in ambito sicurezza informatica da parte delle PMI italiane presenta sostanzialmente molte ombre e pochissime luci.
Si è evidenziato come esse rappresentano il centro nevralgico della struttura produttiva italiana, pertanto in tale contesto sarebbe più che mai opportuno, e finanche urgente, andare a predisporre un sistema condiviso di "best practice" da parte di tali aziende.
La pregnante necessità di adozione di responsabilità per le PMI potrebbe consentire di limitare gli impatti delle violazioni di sicurezza informatica in ottica "sistema paese" sotto più profili, tra cui la "business continuity", il segreto industriale e la sicurezza dati in senso stretto.
In relazione a quanto evidenziato in merito alla scarsa sensibilità al tema sarebbe opportuno mettere a "sistema" le risorse presenti sul territorio onde innescare quel processo informativo in primis,

e successivamente in termini di adozione, di tutte quelle attività volte al miglioramento della conoscenza in tale ambito.
L'aspetto sostanziale da far comprendere al deputato amministratore delle PMI è quello inerente al cambio di visione.
Esso dovrà essere messo in grado di comprendere che i costi legati all'implementazione delle dovute "best practice" in ambito sicurezza informatica devono essere inquadrati sotto il profilo dell'investimento in ottica futura, e non come un mero costo di gestione. Il discrimine potrebbe essere proprio questo, in quanto l'adozione di adeguati sistemi di difesa potrebbe certamente consentire la "messa in sicurezza" delle attività digitali le quali, ormai non sono più confinate al mero quinto dominio, ma sostanzialmente a quasi tutte le attività aziendali.
Altro aspetto assolutamente necessario in ottica cyber security è quella inerente allo stato della domanda in prodotti ICT/OT delle PMI italiane. Termini quali industria 4.0 hanno avuto di recente un grande impatto, ma tale discussione dovrà essere analizzata anche sotto la carenza, praticamente generale, di adeguati sistemi di sicurezza dei sistemi OT, in quanto proprio questi ultimi di fatto rappresentano l'insieme hardware e software per monitorare e controllare processi fisici, dispositivi e infrastrutture. Appare quanto mai evidente l'importanza cruciale di tali sistemi, in considerazione della crescente importanza dei sistemi di video sorveglianza (una nota trasmissione televisiva ha mostrato che alcuni sistemi di video sorveglianza forniti da aziende estere, e installati presso importanti enti governativi, avevano un traffico dati verso l'esterno di sospetta natura). Anche qui vi sono rilevanti profili di potenziale spionaggio, non solo di tipo industriale, ma anche governativo.
Il budget medio delle PMI allocato in information security, dai dati disponibili, risulta essere praticamente irrisorio. Potrebbe pertanto essere quanto mai fondamentale incoraggiare gli amministratori

all'adozione di sistemi cyber security tramite incentivi fiscali, anche sotto il profilo della mera divulgazione della tematica.
A fronte di una domanda praticamente assente di sicurezza informatica delle PMI, l'offerta di prodotti ICT/OT è molto frammentata e data sostanzialmente, eccetto un player di medie dimensioni in Italia, da piccole realtà, e pertanto, potrebbe avere senso creare uno standard condiviso dopo aver condotto una adeguata campagna divulgativa verso le PMI, considerata la bassa conoscenza in primis della problematica, e successivamente del mercato di riferimento.
Quindi sarebbe opportuno, quale secondo step, standardizzare la domanda, in funzione di stimolo ed orientarla per creare un più efficace matching con l'offerta di mercato.

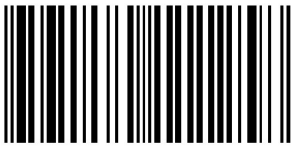
5. CONCLUSIONI

Il futuro non si aspetta: il futuro si prepara.
In tale modo Mario Caligiuri[61], nello studio predisposto dalla "Cyber Threat Intelligence e Cyber Warfare" della Società Italiana di Intelligence, relativo alla nuova Agenzia per la Cybersecurity Nazionale esprime in modo preciso l'importanza di pianificare ciò che verrà.
Ed appare evidente che il nostro futuro avrà fondamenta digitali, le quali senza ombra di dubbio dovranno essere protette.
I temi trattati nel presente paper mostrano con estrema evidenza che lo spionaggio aziendale ed industriale si è evoluto verso un "naturale" cyber spionaggio, logica conseguenza della globalizzazione digitale che la nostra società sta vivendo.

[61] Presidente della Società Italiana di Intelligence (SOCINT), Direttore del Master in Intelligence dell'Università della Calabria.

L'impatto delle attività di compromissione dell'integrità dei sistemi informatici nel contesto italiano sono davanti gli occhi di tutti, appare pertanto irrinunciabile rendere (quanto meno) affidabile l'intera filiera digitale del nostro sistema.
La protezione delle infrastrutture informatiche non si risolve *sic et simpliciter* con l'adozione di sistemi affidabili, ma si necessita anche di adeguati impianti normativi che possano consentire la protezione degli ambienti informatici contro furti di segreti commerciali i quali, come abbiamo visto, hanno enormi ricadute economiche.
I vari case study hanno mostrato che la "fantasia" degli attaccanti spesso supera l'immaginazione, e pertanto, servono professionisti del settore che diffondano la cultura della sicurezza informatica, andando a curare gli interessi di quei settori, che purtroppo distrattamente sembrano essere non abbastanza tutelati, come il contesto delle PMI in Italia.
Lo spionaggio digitale è effettivamente un fenomeno da sottoporre all'attenzione con estrema ed imprescindibile necessità.
Alcuni anni or sono è divenuta di dominio pubblico l'inchiesta "eye pyramid", agli atti portata a compimento dai fratelli Occhionero, i quali nel 2018 sono stati condannati a pene certamente non trascurabili. Non è qui la sede opportuna per dibattere la vicenda giudiziaria ed informatica soprattutto, ma alcune ombre pare ci siano, e non di poco conto. Allo stato attuale il procedimento penale è definito con sentenza di condanna primo grado, in quanto la Procura di Roma ha sostenuto (ed il giudice fino ad ora ha dato conferma alle accuse) che i due fratelli Occhionero abbiano perpetrato attività volte al cyber spionaggio, nei confronti anche di politici, enti istituzionali, grandi aziende, in particolare per accesso abusivo a sistemi informatici e intercettazione illecita di comunicazioni informatiche (due su nomi di rilievo su tutti, Matteo Renzi e Mario Draghi). Appare

evidente quanto siano essenziali le adozioni di tutte quelle misure necessarie, soprattutto in relazione agli ambiti istituzionali ed anche a riguardo di tutti quei attori definibili strategici e/o di interesse nazionale.



9791280111258