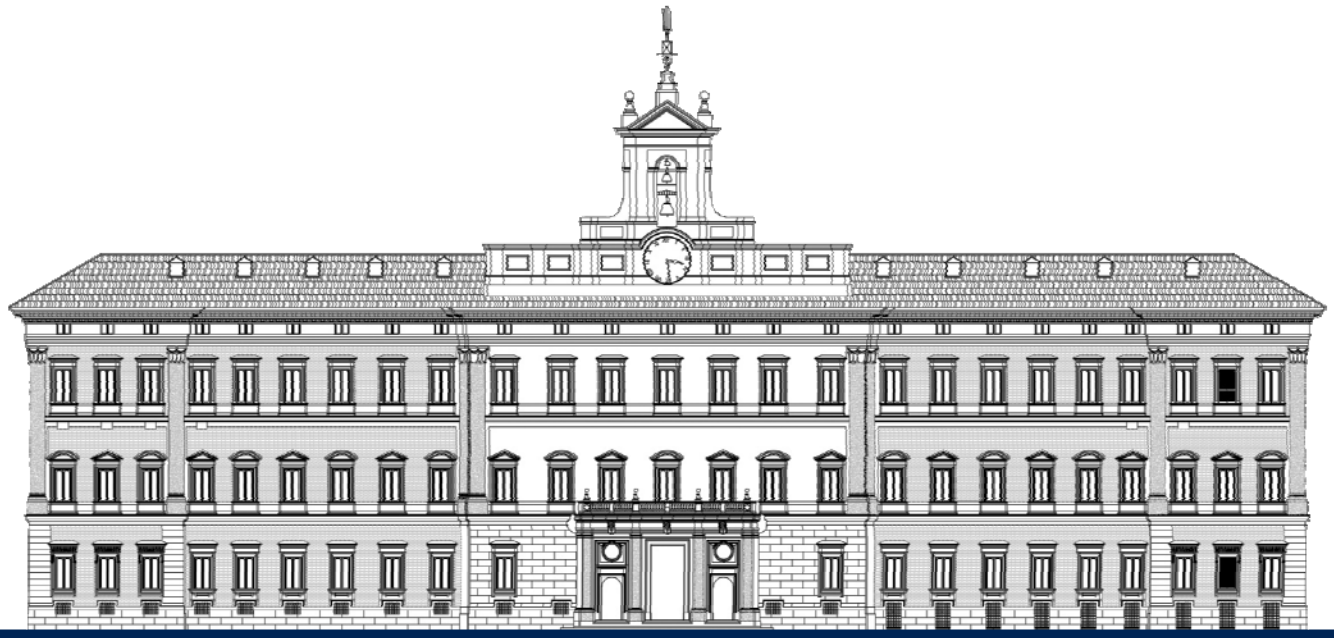
Camera dei deputati

XVIII LEGISLATURA

Documentazione e ricerche



Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa *cyber*

n. 83

24 settembre 2019

Camera dei deputati

XVIII LEGISLATURA

SERVIZIO STUDI

Documentazione e ricerche

Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa *cyber*

n. 83

24 settembre 2019

Il dossier è stato coordinato dal Servizio Studi - *Dipartimento Difesa*

Tel. 06 6760-4939 - st_difesa@camera.it - @CD_difesa

con la collaborazione dei seguenti Dipartimenti: Istituzioni, Giustizia, Trasporti, Attività produttive, Finanze e Affari comunitari

Hanno partecipato alla redazione del dossier i seguenti Servizi e Uffici:

Servizio Biblioteca
Tel. 06 6760-2278 – ✉ bib_segreteria@camera.it

Servizio Rapporti Internazionali
Tel. 06 066760-3948 – ✉ cdrin1@camera.it

Segreteria Generale - Ufficio Rapporti con l'Unione europea
Tel. 06 6760 2145 - ✉ cdrue@camera.it

***File**: DI0162.docx*

I N D I C E

PREMESSA

Il presenta *dossier* raccoglie materiale relativo alle principali tematiche che riguardano la difesa e la sicurezza dello spazio cibernetico, con particolare riferimento alle novità introdotte nell'ordinamento giuridico nazionale successivamente alla conclusione dell'indagine conoscitiva che su questi argomenti ha svolto nella passata legislatura la Commissione difesa della Camera dei deputati.

La prima parte del lavoro è pertanto dedicata all'analisi delle caratteristiche del dominio cibernetico e all'evoluzione della minaccia *cyber* nelle sue diverse tipologie malevole. In questa sezione viene, inoltre, illustrato il *framework* nazionale della sicurezza cibernetica. Sulla base dell'analisi dei documenti ufficiali e della normativa vigente si riporta l'architettura istituzionale preposta alla protezione cibernetica nazionale, specificando ruoli e competenze dei soggetti incaricati, nonché i meccanismi per la prevenzione dei rischi e per la gestione di crisi. Sono, inoltre, richiamate le principali disposizioni di contrasto della criminalità informatica.

Nella seconda e nella terza sezione si dà conto delle principali politiche nazionali ed europee volte a innalzare le capacità di protezione, reazione e risposta nei confronti della minaccia cibernetica in taluni ambiti strutturalmente interessati dall'evoluzione delle tecnologie dell'informazione e delle comunicazioni (*information, and communication technology*, ICT), mentre nell'ultima parte del *dossier* si ripotano le principali strategie nazionali e misure legislative in materia di *cybersecurity* adottate in Francia, Germania e Regno Unito.

In appendice è riportata una definizione esemplificativa di alcune espressioni utilizzate nel *dossier* o comunque connesse agli argomenti trattati.

Parte prima: Dominio digitale e *framework* nazionale della sicurezza cibernetica

CARATTERISTICHE DELLO SPAZIO CIBERNETICO E ANALISI DELLA MINACCIA *CYBER*

1. Il dominio cibernetico

Lo "spazio cibernetico" rappresenta un **nuovo dominio operativo** di natura artificiale, trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale), nel quale gli esseri umani, e nel prossimo futuro verosimilmente anche le intelligenze artificiali, possono agire e interagire a distanza.

Un dominio di **importanza strategica** per lo sviluppo economico, sociale e culturale dei diversi Paesi ma al contempo un nuovo "spazio virtuale" di competizione economica e geopolitica per l'ampiezza dei settori che ne sono coinvolti.

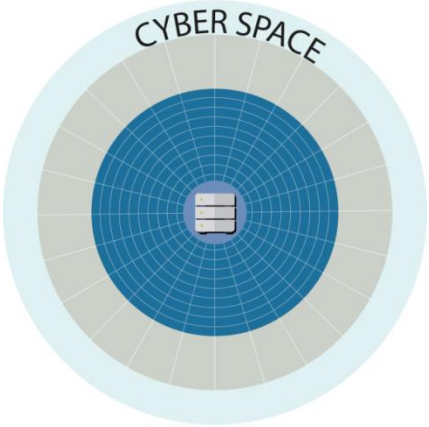
Grazie ai progressi delle tecnologie di comunicazione e l'impiego diffuso di dispositivi elettronici e di monitoraggio si intrecciano quotidianamente nello spazio cibernetico miliardi di interconnessioni, si scambiano conoscenze a livello globale e viene raccolto un gigantesco numero di dati e di informazioni compresi quelli di natura personale e sensibile (c.d. *big data).*

La dimensione cibernetica è pertanto generata dalla ramificatissima rete di infrastrutture materiali di collegamento e di comunicazione che, attraverso la tecnologia informatica, mettono in contatto tra loro un crescente numero di esseri umani e permettono loro di attivare e controllare da ubicazioni remote macchine e apparati in tutto il mondo.

Un ecosistema complesso nel cui ambito gli esperti della materia[1] sono soliti distinguere i seguenti tre livelli essenziali: : il livello fisico infrastrutturale, rappresentato dalle macchine (le architetture delle reti, i *computer*, i *router*...); il livello logico informativo rappresentato dal volume dei dati gestiti dalle macchine (*database*, *file*, ma anche *software* gestiti dalle macchine); il livello sociale cognitivo, ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei social network, gli indirizzi IP delle macchine).

2. Indeterminatezza, mutevolezza e vulnerabilità del dominio cibernetico

Da un punto di vista ambientale lo spazio cibernetico si presenta come un **ambiente virtuale,** privo di confini fisici nel senso tradizionale del termine, **uno spazio indefinito** nel cui ambito non esiste divisione tra pubblico e privato, tra la sfera militare e civile. "Un ambiente in cui pressoché **tutto è duale** e dove tutto può essere preso dalla parte civile e portato verso la parte militare: sistemi operativi, *off the shelf*, *storage*, una serie di software che comandano sistemi anche di comando e controllo di tipo militare"[2].



In quanto dominio creato dall'uomo lo spazio cibernetico è, inoltre, in continua evoluzione e implementazione, in connessione con la rapidità e pressochè ininterrotta evoluzione delle tecnologie dell'informazione e della comunicazione *(information, and communication technology*, ICT) grazie alle quali vengono erogati in misura crescente servizi essenziali per la collettività e strategici per il Paese.

---

[1] Cfr.: Comitato parlamentare per la sicurezza della repubblica, *Relazione sulle procedure la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni*, XVII legislatura, Doc. XXXIV n. 7, pag. 17.

[2] Cfr.: Commissione Difesa della Camera dei deputati, seduta del 9 febbraio 2016, audizione del professore Roberto Baldoni nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico.

A questo proposito la dottrina che da tempo si occupa del tema della sicurezza cibernetica invita a riflettere sulla **vastità dei settori** che nelle moderne società **si avvalgono dei servizi digitali**.

Non esiste "un settore in questo momento – anche molto lontano, come l'agricoltura o altri – che non si poggi pesantemente sul *cyber space*"[3].

Servizi economici e finanziari, sistemi di comando e controllo militare, sistemi di fornitura di energia elettrica o acqua, l'assistenza sanitaria, le telecomunicazioni, dispositivi fisici con cui interagiamo giornalmente sono **controllati da sistemi informatici**.

Nello scenario di un futuro prossimo, osservano inoltre gli analisti, la diffusione di registri distribuiti in grado di registrare e gestire transazioni di vario tipo (*Blockchain*), di criptovalute (come *Bitcoin, LiteCoin, Ether e Ripple*), di sistemi di *Artificial Intelligence* (AI) e di *smart cities* (o città intelligenti) contribuirà ad un ulteriore ampliamento del dominio cibernetico e di conseguenza della superficie di attacco.

In allegato si riporta un approfondimento delle richiamate definizioni

In quanto dominio artificiale il dominio cibernetico presenta, delle "**vulnerabilità**" ovvero dei punti di debolezza attraverso i quali è possibile acquisire illegalmente dati e informazioni che "transitano" nello spazio cibernetico ovvero compromettere in tutto o in parte il funzionamento di servizi e sistemi digitali.

Le vulnerabilità del dominio cibernetico rappresentano pertanto il rovescio della medaglia del progresso tecnologico ed informatico.

Di difficile individuazione e classificazione tali "fratture" del sistema informatico possono dipendere sia da fattori tecnici congeniti al *software* applicativo, sia dal mancato o non corretto funzionamento dei sistemi di protezione.

Al riguardo, nel Documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, condotta dalla Commissione difesa della Camera dei Deputati nella XVII legislatura si analizzano le cause delle diverse vulnerabilità e al

[3] Cfr. Commissione Difesa della Camera dei deputati, seduta del 9 febbraio 2016, audizione del Prof. Baldoni,cit.

contempo si sottolinea l'esigenza di disporre di materiali tecnologicamente certificati più facilmente controllabili e monitorabili, con particolare riferimento alla fornitura di materiale militare[4].

Il Consiglio dei ministri, nella seduta del **19 settembre 2019**, ha approvato il decreto n.105 del 2019 (pubblicato nella Gazzetta Ufficiale del 21 settembre 2019) che introduce disposizioni urgenti in materia di **"perimetro"** di sicurezza nazionale cibernetica. Il decreto, come si legge nel comunicato, mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

Per un approfondimento si rinvia al relativo *dossier* .

3. Analisi della minaccia cibernetica

In tutti i principali contesti nazionali, europei ed internazionali nei quali si analizzano le principali sfide alla stabilità, alla sicurezza e alla crescita dei popoli la **minaccia cibernetica** viene da tempo considerata come una minaccia assai significativa, mutevole nei suoi tratti essenziali, **in continua evoluzione**, rapida nel bersaglio da aggredire e capace di produrre effetti a distanze non raggiungibili con gli ordinari strumenti di attacco.

[4] Più di recente, nell'ambito dell'indagine conoscitiva "sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5g ed alla gestione dei big data" in corso di svolgimento presso la Commissione Trasporti della Camera dei deputati, è stato osservato "l'incremento nell'uso di dispositivi e componenti di internet delle cose incrementerà e implementerà le potenziali vulnerabilità delle infrastrutture di rete, ciò soprattutto se i produttori e i fornitori di questi dispositivi e servizi privilegeranno l'abbattimento dei costi rispetto alle funzionalità di sicurezza e se non verrà posto il giusto accento alle misure di sicurezza cibernetica e al controllo della catena di approvvigionamento". Cfr. audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri, seduta del 7 maggio 2019.

Gli attacchi cibernetici possono, infatti, originare da qualsiasi punto della rete globale e per le loro peculiarità sono idonei a determinare rilevanti conseguenze sul funzionamento e l'integrità della rete informatica di un Paese.

Al riguardo viene di sovente ricordato che le operazioni nello spazio cibernetico si svolgono con una velocità di oltre 20.000 volte maggiore di quelle nello spazio fisico, di oltre 200.000 volte maggiore di quelle nell'aria, e di 10 milioni di volte maggiore di quelle in terra ed in mare"[5].

Se ne sottolinea, infine, il **carattere asimmetrico** in quanto i mezzi a disposizione del soggetto attaccante sono allo stato delle conoscenze attuali nettamente superiori alle capacità di difesa del soggetto attaccato.

La **difficile tracciabilità** degli attacchi rende inoltre estremamente complesse le attività preventive, investigative e di contrasto[6].

Con riguardo poi agli **effetti dell'aggressione** informatica in diversi documenti ufficiali pubblicati sia a livello nazionale che internazionale, si sottolinea la capacità degli attacchi cibernetici di produrre **danni** sulla società paragonabili a quelli di un conflitto combattuto **con armi convenzionali** e si sottolinea la necessità di predisporre capacità operative difensive al fine di preservare la sicurezza del "Sistema Paese" e di rafforzare la tenuta delle strutture politiche, economiche e sociali [7].

---

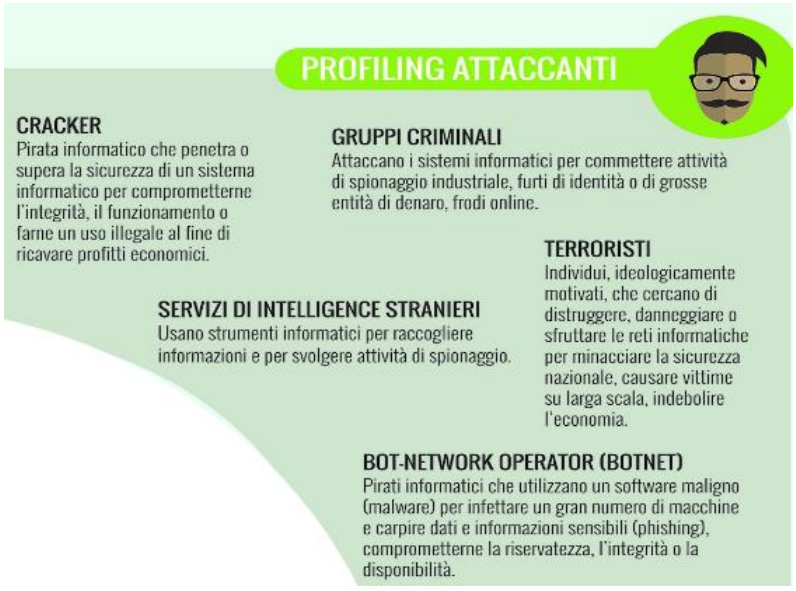
[5] Umberto Gori, *in Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali,* Informazioni della Difesa, supplemento al n.6/2014.

[6] A questo riguardo nella Relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza 2018, cit, p.6 dell'allegato, si osserva che sul fronte delle infrastrutture di attacco, è stato registrato il ricorso da parte di gruppi responsabili di azioni di *cyber-espionage* all'impiego di servizi IT commerciali (domini web, servizi di hosting, etc.), forniti da *provider* localizzati in diverse regioni geografiche, anche per rendere difficoltoso il processo di individuazione/ attribuzione.

[7] Ministero della Difesa, *Libro bianco per la sicurezza internazionale e la Difesa* 2015, punto 32 e 103; cfr. anche Documento conclusivo dell'indagine conoscitiva sulla difesa e sicurezza dello spazio cibernetico, cit.; in ambito internazionale, tra gli altri, cfr.: Conclusioni del vertice dai Capi di Stato e di Governo nel corso del summit di Varsavia8-9 luglio 2016 nel quale si è affermato che "Gli attacchi informatici rappresentano una sfida chiara alla sicurezza dell'Alleanza e potrebbe essere dannoso per le società moderne come un attacco convenzionale".

A livello nazionale da tempo le *Relazioni sulla politica dell'informazione per la sicurezza* trasmesse dal Governo (Presidenza del Consiglio dei ministri) al Parlamento ai sensi dell'articolo 38 della legge n. 124 del 2007[8] pongono particolare attenzione all'accresciuto livello di complessità e sofisticatezza della minaccia *cyber* e all'eterogeneità del profilo soggettivo dell'attaccante (cfr *box infra*).

Emerge, in proposito, una **variegata gamma** di attori che si muovono nel *cyber space* con finalità ed obiettivi diversi, tutti di difficilissima identificazione che vanno dall' *hacker* individuale che agisce a scopo di lucro, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici.[9]



Dal punto di vista della **pericolosità** si passa, quindi, dal **vandalismo cibernetico** alla vera e propria **guerra cibernetica**.

In futuro, osservano gli analisti, nuove tipologie di attacco saranno probabilmente elaborate anche in conseguenza del sempre più diffuso utilizzo dell'innovazione tecnologica dell'IOT (*internet of things* cfr. Appendice) in diversi ambiti domestici e lavorativi (dai televisori di ultima generazione a certi giocattoli per bambini, passando per le telecamere di sorveglianza attivabili da remoto).

In questi contesti, osservano gli esperti, sfruttando i richiamati dispositivi collegati in rete, sarà possibile a soggetti ostili acquisire illegalmente, con maggiore facilità rispetto agli attuali metodi intrusivi, informazioni riguardanti la vita privata e lavorativa della

[8] Cfr.: paragrafo successivo.
[9] Relazione 2015, p. 82.

vittima, ovvero prendere il controllo di dispositivi e macchinari altrui, dirottandone l'azione, visionare dati riservati (telefonici, di posta elettronica, etc.) oppure distruggere memorie o sequestrarle a scopo di ricatto (rendendole indisponibili al legittimo titolare)[10].

La tematica è di particolare interesse anche nel campo della Difesa dove l'evoluzione delle tecnologie dell'informazione ha da un lato permesso di velocizzare i processi decisionali ai vari livelli di comando grazie all'ausilio di sistemi informativi di comando e controllo automatizzati che permettono la memorizzazione e lo scambio di enormi quantità di dati ed informazioni in "tempo reale", dall'altro lato - sottolineano gli esperti - l'utilizzo di tali strumenti tecnologici ha tuttavia reso le Forze Armate particolarmente vulnerabili ai rischi afferenti alla sicurezza dei sistemi e delle informazioni ivi contenute provenienti da minacce interne ed esterne all'organizzazione militare.

Da qui la necessità, avvertita dai Paesi maggiormente evoluti sul piano militare di definire adeguate misure di difesa cibernetica rispetto a eventi di natura volontaria o accidentale che potrebbero compromettere o alterare dati e servizio fondamentali nell'ambito dell'organizzazione della Difesa.

4. Le relazioni presentate al Parlamento sulla politica dell'informazione per la sicurezza

Da diversi anni il tema della sicurezza cibernetica costituisce oggetto di analisi nell'ambito delle **Relazioni** sulla politica dell'informazione per la sicurezza, predisposte **dal Governo** (Presidenza del Consiglio dei ministri) e trasmesse **al Parlamento** ai sensi dell'articolo 38 della legge n. 124 del 2007, recante disposizioni **concernenti** il Sistema di informazione per **la** sicurezza della Repubblica e nuova disciplina del segreto.

Tale norma prevede, infatti, che entro il mese di febbraio di ogni anno il Governo trasmetta al Parlamento una relazione scritta, riferita all'anno precedente, sulla politica dell'informazione per la sicurezza e sui risultati ottenuti (comma 1). Alla relazione è allegato

[10] Rapporto Clusit 2019, p.199.

il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica (comma 1-*bis*)

In relazione a questo tema è possibile osservare come già nella Relazione sulla politica dell'informazione per la sicurezza relativa all'anno 2009 la *cybersecurity* veniva definita come "un fondamentale campo di sfida per l'intelligence (…) un fattore di rischio di prima grandezza, direttamente proporzionale al grado di sviluppo raggiunto dalle tecnologie dell'informazione".

A questa prima analisi hanno fatto seguito – nelle Relazioni presentate al Parlamento negli anni successivi – ulteriori riflessioni, che secondo un livello crescente di intensità hanno considerato la minaccia cibernetica come una "sfida crescente per le politiche di sicurezza degli Stati"[15], un obiettivo informativo prioritario dell'attività intelligence nazionale"[16], "la sfida più impegnativa per il sistema Paese". In particolare, proprio nella Relazione riferita all'anno 2012 che qualifica la minaccia cibernetica come "la sfida più impegnativa per il sistema Paese" tale valutazione viene motivata in considerazione "dei suoi peculiari tratti caratterizzanti che attengono tanto al dominio digitale nel quale viene condotta, quanto alla sua natura diffusa e transnazionale, quanto ancora agli effetti potenziali in grado di produrre ricadute peggiori di quelle ipotizzabili a seguito di attacchi convenzionali e di incidere sull'esercizio di libertà essenziali per il sistema democratico"[17].

Le Relazione riferite ad **anni più recenti** evidenziano a loro volta il costante *trend* di **crescita d**ei fenomeni di minaccia collegati con il ciberspazio in termini di **sofisticazione, pervasività e persistenza**, a fronte di un livello non sempre adeguato di consapevolezza in merito ai rischi e di potenziamento dei presidi di sicurezza.

Se nel 2015 i principali settori oggetto di attacchi *cyber* risultavano quelli delle telecomunicazioni, dell'aerospazio, dell'energia e della difesa, nel 2016 figurano ai primi posti il settore bancario – con il 17 per cento delle minacce a soggetti privati (+14 per cento rispetto al 2015) – nonché le Agenzie di stampa e le testate giornalistiche che, insieme alle associazioni industriali, si attestano sull'11 per cento.

I **soggetti pubblici** costituiscono la maggioranza delle **vittime** degli attacchi c*yber* con il 71 per cento degli attacchi, mentre si

attestano attorno al 27 per cento gli attacchi contro i soggetti privati. In entrambi i casi si registra un aumento pari, rispettivamente, al 2 per cento ed al 4 per cento. Un decremento del 6 per cento è stato viceversa osservato nell'ambito dei target non meglio identificati o diffusi (che costituiscono, complessivamente, il 2 per cento), solitamente oggetto di campagne hacktiviste.

Da ultimo, la Relazione riferita all'anno 2018 dà conto dell' **innalzamento della qualità e della complessità** di alcune tipologie di attacco. Sul fronte delle infrastrutture di attacco, si legge nella Relazione, i gruppi responsabili di azioni di *cyber-espionag*e hanno proseguito **nell'impiego di servizi IT** commerciali (domini web, servizi di hosting, etc.), forniti da *provider* localizzati in diverse regioni geografiche, anche per rendere difficoltoso il processo di individuazione attribuzione. Attenzione viene inoltre rivolta anche alla cd. minaccia ibrida, considerata quale impiego combinato di strumenti convenzionali e non, le cui traduzioni operative sono risultate (e saranno sempre più) amplificate grazie alla digitalizzazione che ha interessato ogni aspetto della vita sociale, arrivando ad esplicitarsi anche in operazioni di influenza/ingerenza poste in essere per condizionare il corretto svolgimento di fondamentali dinamiche dei processi democratici.

5. Le diverse tipologie di attacco

A seconda del diverso grado di **offensività** gli attacchi cibernetici vengono tradizionalmente ricondotti ad atti di *cyber* criminalità, *cyber spionaggio, cyber* terrorismo e *cyber* guerra [11].

In alcune analisi scientifiche è frequente il richiamo all'*Hacktivism* per indicare gli attacchi cyber motivati ideologicamente.

[11] La classificazione che segue è stata per la prima volta rappresentata a livello parlamentare nell'ambito della *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico,* Doc.XXXIV, n. 4, approvato dal Comitato parlamentare per la sicurezza della repubblica in data 7 luglio 2010. Nel richiamato documento viene fatto riferimento ai seguenti profili soggettivi: *Bot-network operator*, gruppi criminali, servizi di intelligence stranieri, hacker, insider, *phisher, spammers*, autori di *spyware/malware*, terroristi.

Ciascuna delle richiamate fattispecie presenta al suo interno molteplici sfaccettature, così come un'operazione malevola complessa nello spazio cibernetico può essere il risultato di una pluralità di azioni intrusive di natura diversa.

Lo **spionaggio cibernetico** di frequente precede le altre forme di minaccia con intensità crescente e le accompagna nella loro evoluzione. In tale ambito non sempre è possibile riconoscere una chiara distinzione tra queste categorie.

Al di là delle singole peculiarità caratteristica comune di tutte le tipologie di attacchi criminali è la difficile individuazione degli autori degli atti ostili, la loro provenienza geografica e, talvolta, la stessa finalità dell'attacco *cyber*.

6. La Cyber war e la minaccia cibernetica militare

La cosiddetta "**guerra cibernetica**" rappresenta la più grave forma di attacco informatico perpetrato da uno Stato nei confronti di un altro Stato per uno qualsiasi degli scopi tradizionalmente perseguiti con il ricorso alla guerra e allo strumento militare.

Quando l'attacco è portato attraverso lo spazio cibernetico, si parla di "guerra cibernetica" (*cyber-warfare*) e correlativamente di "**difesa cibernetica**" (*cyber-defence*), intesa come l'insieme della **dottrina, dell'organizzazione** e delle attività atte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti tramite lo spazio cibernetico.

La letteratura scientifica che si occupa di questo argomento è solita far risalire **all'attacco all'Estonia del 2007** il primo caso di *cyber war*. Per alcuni giorni i siti istituzionali e di comunicazione

dell'Estonia, uno dei paesi al mondo maggiormente informatizzato, sono stati messi fuori uso a seguito di alcuni attacchi cibernetici[12].

Come si vedrà più diffusamente nel successivo paragrafo è questo il **primo caso** in cui uno Stato membro della NATO ha richiesto l'applicabilità **dell'articolo 5 del Trattato istitutivo** dell'Alleanza Atlantica, a seguito di un **attacco di natura cibernetica** alle proprie strutture digitali.

La guerra e la difesa cibernetica tra Stati sono ad oggi, "a parte alcune avvisaglie, uno scenario soltanto possibile", pur tuttavia un numero crescente di analisi strategiche individua nello spazio cibernetico un nuovo fondamentale campo di battaglia e di competizione geopolitica dell'umanità[13].

In tali analisi è infatti ricorrente l' affermazione secondo la quale "le prossime guerre tra gli Stati non saranno certamente condotte soltanto con i tradizionali strumenti di offesa e di difesa via terra, mare e aria, ma saranno accompagnate e probabilmente iniziate – e in qualche caso vinte - con attacchi perpetrati attraverso lo spazio cibernetico" [14].

Come evidenziato anche nel citato Documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, gli attacchi cibernetici più sofisticati non solo sono potenzialmente in grado di danneggiare o paralizzare il funzionamento di gangli vitali dell'apparato statale e la fornitura di servizi essenziali ai cittadini, ma possono avere anche effetti potenzialmente distruttivi (soprattutto in prospettiva) se impiegati per indurre il malfunzionamento delle infrastrutture critiche (ad esempio centrali elettriche, nucleari, dighe, torri di controllo

[12] Per un'analisi di questa problematica e dei relativi orientamenti dottrinali si rinvia al resoconto stenografico della seduta del 16 febbraio 2016 della IV Commissione Difesa della Camera dei deputati nel corso della quale si è svolta l'audizione del professor Stefano Silvestri, *past president* e membro del comitato direttivo dell'Istituto affari internazionali (IAI). Si veda, altresì, resoconto stenografico della seduta del 28 aprile 2016 nel corso della quale si è svolta l'audizione dell'avvocato Stefano Mele, specializzato in Diritto delle tecnologie, *privacy* e sicurezza delle informazioni, consulente in materia di *cyber-security*, *cyberintelligence*, *cyber-terrorism* e *cyberwarfare*.

[13] Cfr. Programma dell' indagine conoscitiva sulla difesa e sicurezza dello spazio cibernetico, cit.;

[14] Cfr. Libro bianco per la difesa e la sicurezza internazionale 2015 cit.

aeroportuali, sistemi di navigazione aerea e di trasporto civile, sistemi di comando e controllo militari, nonché fabbriche altamente automatizzate, che impieghino robot interconnessi, etc.) generando danni materiali ingenti e la potenziale perdita di vite umane.

In un contesto di *cyber war* la minaccia cibernetica può dunque manifestarsi sotto **diverse forme**. In alcuni casi potrebbe, ad esempio determinare **un'errata percezione** da parte dei comandanti della situazione operativa tale da influire in maniera viziata sugli schermi di comando e controllo dei propri assetti; in altri, la minaccia cibernetica potrebbe consistere in **un'intrusione nei sistemi di comando e controllo** finalizzata non solo allo spionaggio, ma anche al **sabotaggio** e al malfunzionamento degli stessi con effetti distruttivi analoghi a quelli condotti con armi convenzionali.

7. Alcune problematiche connesse alla cyber war

In relazione al tema della c*yber war* una delle principali questioni affrontate in ambito accademico e politico internazionale ha riguardato le **misure di legittima difesa** che potrebbero essere attivate dagli Stati nel caso di attacco *cyber* prolungato e generalizzato alle proprie infrastrutture critiche, con particolare riferimento all'azionabilità dei meccanismi di difesa collettiva di cui all'articolo 5 del Trattato istitutivo dell'Alleanza Atlantica, richiamato anche dall'articolo 51 della Carta delle Nazioni unite

Ai sensi dell'articolo 5 del Trattato Nord-atlantico, fatto a Washington il 4 aprile 1949 e ratificato dall'Italia con la legge 1° agosto 1949, n. 465 Le Parti convengono che un attacco armato contro una o più di esse, in Europa o nell'America settentrionale, costituirà un attacco verso tutte, e di conseguenza convengono che se tale attacco dovesse verificarsi, ognuna di esse, nell'esercizio del diritto di legittima difesa individuale o collettiva riconosciuto dall'art.51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti così attaccate, intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'impiego della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale. Qualsiasi attacco armato siffatto, e tutte le misure prese in conseguenza di esso, verrà immediatamente segnalato al Consiglio di Sicurezza. Tali misure dovranno essere sospese non appena il Consiglio di Sicurezza avrà adottato le disposizioni necessarie per ristabilire e mantenere la pace e la sicurezza internazionali

In occasione della prima richiesta di attivazione di tale disposizione, risalente al richiamato "caso Estone", **la Nato** osservò come l'Estonia, sebbene fortemente danneggiata dagli attacchi *cyber,* non avesse comunque subito vittime o distruzioni fisiche alle infrastrutture critiche, ma unicamente il blocco dei sistemi informatici e pertanto, **non ravvisando l'estremo dell'aggressione** "contro l'integrità territoriale di uno Stato", così come definita dallo Statuto dell'Onu, **non ha dato seguito** alla richiesta **di attivazione dell'articolo 5**[15].

Il CCDCOE, istituito successivamente agli attacchi dell'aprile 2007 ed inizialmente formato da Estonia, Lettonia, Lituania, Germania, Italia, Spagna e Slovacchia, ha come scopo l'analisi e la condivisione delle informazioni all'interno del Patto Atlantico, sui temi della cyberwar. Nell'ambito del CCDOE un apposito gruppo di studio ha elaborato il Tallinn Manual on the International Law Applicable to Cyber Warfare , considerato come uno dei più importanti documenti di riferimento giuridico sulla cyber war.

Va peraltro rilevato che successivamente a questo episodio la NATO ha prestato particolare attenzione al tema della difesa cibernetica non solo dando vita già nel 2008 al **Tallin NATO *Cooperative Cyber defence***, centro d'eccellenza per la ricerca, l'analisi e la condivisione delle informazioni all'interno del Patto Atlantico sui temi della *cyber war*, ma soprattutto modificando negli anni successivi la propria politica di difesa cibernetica.

Nel corso del **vertice NATO** del 4-5 settembre 2014 in **Galles** i Capi di Stato e di Governo dei Paesi membri dell'Alleanza Atlantica hanno chiarito che la difesa cibernetica fa parte del compito

[15] Su questo tema cfr. resoconto stenografico della seduta del 16 febbraio 2016 della IV Commissione difesa della Camera dei deputati nel corso della quale si è svolta l'audizione del Prof Silvestri, *past president* IAI. "Il problema primo e principale è la capacità di attribuire l'attacco a un nemico preciso. Finora è molto difficile. L'attacco condotto a suo tempo contro l'Estonia è stato da questo Paese attribuito alla Russia, ma in realtà non si sa se a un gruppo di hacker russi o a un ente ufficiale russo. Il secondo è arrivato dal Brasile. Se, dunque, l'Estonia avesse voluto intervenire per bloccare l'attacco, sarebbe dovuta intervenire contro il Brasile a quel punto, non contro la Russia. La questione è rimasta aperta persino per l'attacco condotto recentemente contro la Sony in America, che si dice sia stato condotto dalla Corea del Nord. Non si sa se si tratti della Corea del Nord, della Cina o di qualcun altro".

principale della NATO di difesa collettiva ed hanno affermato che l'eventuale attivazione dell'articolo 5 in seguito ad un attacco cibernetico verrà decisa caso per caso.

Nel successivo vertice di **Varsavia** del luglio 2016 "Gli attacchi informatici" sono stati considerati come "una sfida chiara alla sicurezza dell'Alleanza e (…) un pericolo per la società moderna, al pari di un attacco convenzionale". Nel comunicato ufficiale rilasciato alla chiusura del vertice si sottolinea in particolare come la NATO continuerà ad implementare la propria politica di cyber defence "con l'intento di rafforzare le capacità dell'Alleanza, beneficiando di tecnologie all'avanguardia".

Il Summit di **Bruxelles** dell'11 luglio 2018 ha segnato un ulteriore, importante rafforzamento delle capacità cibernetiche della Nato. Il Summit ha infatti stabilito la nascita di un *Cyber Operations Center* con l'obiettivo coordinare le operazioni degli alleati nel dominio cibernetico.

In ambito dottrinario la questione relativa alla possibilità di definire un attacco cibernetico come un atto di guerra regolato dalle relative norme del diritto internazionale viene reputata possibile nella misura in cui l'intensità e gli effetti dell'aggressione informatica, inserita in un contesto di conflittualità tra Stati, siano paragonabili a quelli di un attacco armato.

Da un punto di vista pratico ed operativo resta però ferma la problematica di fondo relativa **all'estrema difficoltà**, allo stato delle conoscenze tecniche e scientifiche di qualificare un determinato attacco *cyber* come **un attacco di *cyber war***.

Come precedentemente osservato le caratteristiche del *cyber space* ed in particolar modo **l'assenza di confini e limiti** spaziali incidono fortemente sulla **possibilità di individuare** con certezza **l'autore di un attacco cibernetico**, *conditio sine qua non* per l'avvio di qualsiasi azione di legittima difesa ai sensi delle norme del diritto internazionale.

Si evince in tale difficoltà di attribuzione una delle principali differenze rispetto ai conflitti che hanno luogo nei tradizionali domini nell'ambito dei quali risulta astrattamente agevole

l'identificazione dell'autore dell'attacco e l'individuazione del punto d'origine delle manovre.

Viceversa la **pervasività del *cyberspazio***, la difficoltà di alzare barriere al suo interno e la possibilità di operare in modo anonimo rendono **difficoltoso l'accertamento dei reali effetti** prodotti da un'azione di tipo informatico, condizione anch'essa essenziale per qualificare un attacco cibernetico come atto di conflittualità e per valutare la proporzionalità delle eventuali misure di risposte.

8. Cyber crime, cyber espionage e cyber terrorismo

Nella categoria del ***cyber-crime*** vengono generalmente ricompresi gli atti ostili posti in essere da organizzazioni criminali nazionali o transnazionali che sfruttano la dimensione cibernetica per compiere reati quali la truffa, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali.

La tecnica più utilizzata dal *cybercrime* è il ***malware***.

Nel corso del 2018 secondo quanto riportato nel Rapporto Clusit 2019 gli attacchi gravi globali basati sui *malware* sono stati 585 (68% del totale), per una crescita del 31,2%, e continuano a trovarsi al primo posto per il secondo anno di fila.

In tale Rapporto al primo posto come singoli *malware* importanti vengono registrati i ***ransomware*** (23%), *malware* diffuso sotto forma di allegato di posta elettronica apparentemente lecito e inoffensivo, che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione, seguiti dai ***cryptominer*** (23%, cfr. appendice).

Un'altra tecnica che ha mostrato una crescita sopra la media è stata il ***Phishing*** (+56,9%) ovvero un attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (*user-id*, *password*, numeri di carte di credito, PIN, etc.) con l'invio di false *e-mail* generiche a un gran numero di indirizzi. Le *e-mail* sono formulate in modo tale da convincere i destinatari ad aprire un allegato o ad accedere a siti web creati ad hoc dall'attaccante. Il *phisher* utilizza i dati raccolti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Scendendo fra metodologie che sono state riscontrate in numeri più contenuti di attacchi, troviamo in crescita le *Multiple Techniques*

/APT (+55,6%), 0-Day (+66,7%) e *Phone Hacking* (9, +200%, cfr. Appendice). Cresce anche l'*Account Cracking* (+7,7%), mentre resta stabile la tecnica DDoS, ovvero attacchi lanciati da un gran numero di sistemi compromessi ed infetti (*botnet*), volti a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi.

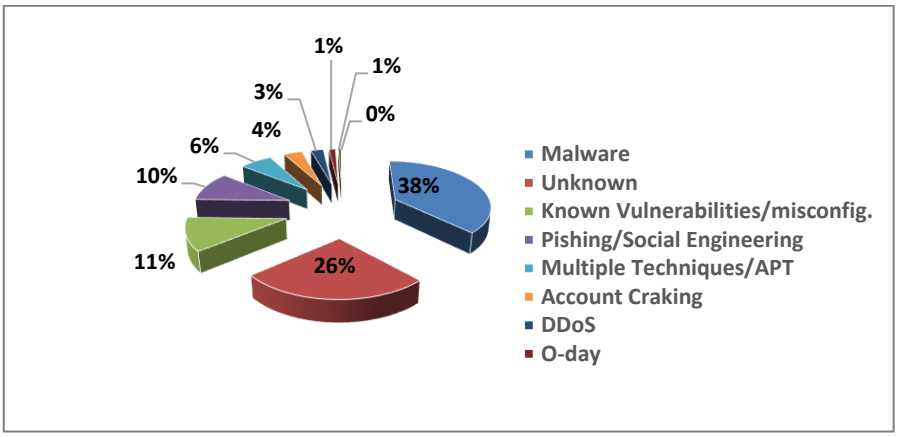
Diminuiscono in maniera considerevole gli attacchi SQL *Injection* (-85,7% cfr. Appendice), tecnica mirata a colpire applicazioni *web* che si appoggiano su *database* programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in input e l'inserimento di codice malevolo all'interno delle *query*. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

I grafici che seguono illustrano la distribuzione delle diverse tipologia di attacco nel periodo 2014 - 2018 e la percentuale di attacchi per tipologie di malware utilizzato 2017/2018.

Distribuzione delle tecniche di attacco (2014-2018)
Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi– Rapporto Clusit 2019

Tecniche di attacco	*2014*	*2015*	*2016*	*2017*	*2018*
Malwere	127	106	229	446	585
Unknown	199	232	338	277	408
Known Vulnerabilities/misconfig	195	184	136	127	177
Pishing/Social Engineering	4	6	76	102	160
MultipleTechniques/APT	60	104	59	63	98
Account craking	86	91	46	52	56
DDoS	81	101	115	38	38
O-day	8	3	13	12	20
Phone Hacking	3	1	3	3	9
SQL Injection	110	184	35	7	1

Percentuale di attacchi per tipologie di malware utilizzato nel periodo 2017/2018.
Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi – Rapporti Clusit 2019



A sua volta la categoria *cyber espionage* ricomprende le attività volte a sfruttare le potenzialità della rete per sottrarre segreti industriali o istituzionali a fini di concorrenza sleale (se consumati nel mercato dei brevetti civili) o di superiorità strategica (nel caso di sottrazione di disegni e apparecchiature militari o *dual-use*).

A questo riguardo le più recenti relazioni al Parlamento sulla politica dell'informazione per la sicurezza manifestano

preoccupazione per la rilevanza del fenomeno e per la pericolosità degli attacchi di *cyber* spionaggio.

Lo spionaggio digitale viene infatti considerato come la minaccia più insidiosa per le sue elevate capacità di rimodulazione rispetto alle misure difensive adottate per ridurre la superfice d'attacco.

Con particolare riferimento agli attacchi registrati nell'anno 2018 nella Relazione al Parlamento riferita a tale anno si rende noto che lo sforzo più significativo posto in essere dal Comparto ha riguardato il contrasto a campagne di spionaggio digitale, "gran parte delle quali verosimilmente riconducibili a gruppi ostili strutturati, contigui ad apparati governativi o che da questi ultimi hanno ricevuto linee di indirizzo strategico e supporto finanziario"[16].

A livello dottrinario si sottolineano, invece, gli effetti particolarmente offensivi di attacchi di spionaggio digitale nel settore dell'aerospazio e della difesa, finalizzati all'acquisizione di segreti industriali e militari[17].

La tematica riveste particolare rilievo in relazione allo sviluppo dei noti velivoli multiruolo senza pilota rispetto ai quali gli esperti sottolineano come non possano escludersi a priori possibili attacchi volti a penetrare e riconfigurare i relativi sistemi di comando e controllo sfruttando le vulnerabilità del complesso sistema di navigazione satellitare degli UAV[18].

La categoria del *cyber terrorism* abbraccia, infine, la molteplicità delle azioni informatiche poste in essere dalle organizzazioni del terrorismo a fini di propaganda, denigrazione o affiliazione e, nei casi estremi, per mettere fuori uso, attraverso l'utilizzo della rete o dei controlli telematici, i gangli di trasmissione critica delle strutture o dei processi che attengono la sicurezza nazionale.

---

[16] Relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza 2018 cit, p. 6 dell'Appendice.

[17] Per un approfondimento di questo tema si veda l'audizione del Professor Silvestri, *past president* e membro del comitato direttivo dell'Istituto affari internazionali, svolta nel corso della seduta della Commissione difesa della Camera dei deputati del 16 febbraio 2016.

[18] Cfr. M. Nones e A. Marrone, La trasformazione delle Forze armate: il programma Forza Nec, edizione nuova cultura, 2010, p. 49; T. De Zan, A. Marrone, *Il programma Forza NEC, Forze armate e innovazione tecnologica*, 2015.

A questo riguardo sebbene la Relazione annuale riferita all'anno 2015 sottolinei come "fino ad oggi non si siano manifestate azioni terroristiche finalizzate a distruggere o sabotare infrastrutture ICT di rilevanza strategica", pur tuttavia il richiamato documento ritiene ragionevole ipotizzare che, nel futuro, "tali obiettivi possano effettivamente rientrare negli indirizzi strategici del cd. Jihad globale, aggiungendo, quindi, una nuova dimensione alla minaccia terroristica".

In tal senso anche nel più volte richiamato Documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, nel quale si afferma che anche l'utilizzo dello spazio cibernetico da parte di organizzazioni terroristiche è una possibile minaccia alla sicurezza nazionale, *in primis* per lo sfruttamento della rete a fini di propaganda, addestramento, autofinanziamento e pianificazione. La capacità di questi gruppi di rappresentare un pericolo reale alle infrastrutture critiche resta più limitata, si legge nel Documento, ma destinata a crescere nel medio-lungo termine, anche a causa dell'aumento della loro competenza tecnica".

9. Dati statistici sui principali attacchi Cyber

Secondo quanto riportato nel Rapporto Clusit 2019,il 2018 è stato "l'anno peggiore di sempre in termini di evoluzione delle minacce cyber e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo, evidenziando un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti mai registrato in precedenza".

Nell'ultimo biennio, documenta il Rapporto Clusit 2019, il tasso di crescita del numero di **attacchi gravi** è **aumentato di 10 volte** rispetto al precedente.

Al riguardo si osserva, infatti, che, mentre nell'arco del biennio 2017-2018 il numero di attacchi gravi è cresciuto del 37,7%, **la crescita** registrata nel biennio 2015-2016 **è stata del 3,8%.**

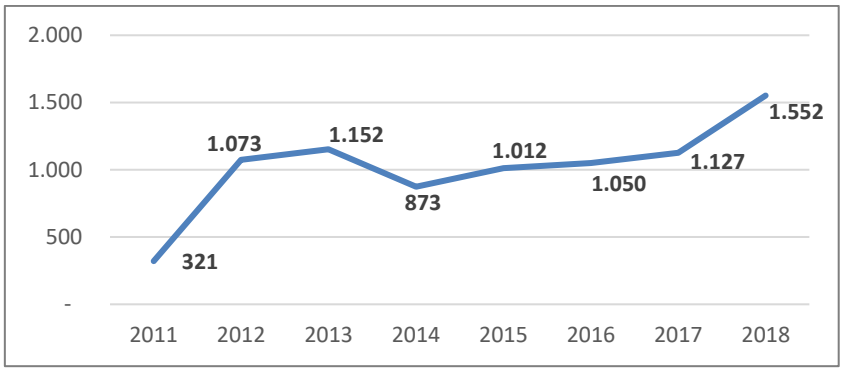
Il seguente grafico mostra il ***trend*** degli attacchi gravi rilevati a livello globale (Italia compresa) tra il 2011 ed il 2018 riportati nei

Rapporti Clusit del 2017, 2018 e 2019 e relativi al settore privato e pubblico.

Per quanto concerne l'anno 2018 la base dati è composta da un totale di 8471 attacchi noti.

Numero di attacchi gravi rilevati per anno (2011-2018).

Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi, Camera dei Deputati – Rapporti Clusit 2017-2019



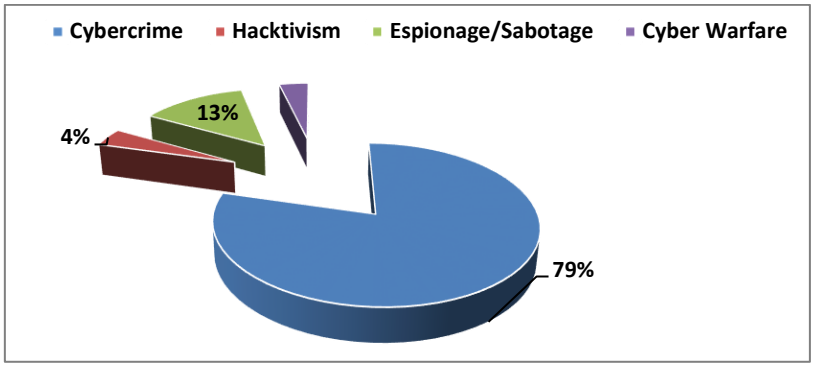
Gli attacchi registrati sono stati catalogati per tipologia: *Cybercrime, Hacktivism, Espionage/Sabotage, Cyber warfare* (cfr. *supra*).

In termini assoluti, nel 2018 le categorie *Cybercrime* e *Cyber Espionage* fanno registrare il numero di attacchi più elevato degli ultimi 8 anni.

Nel 2018 sono aumentati (+43,8%) rispetto al 2017, gli attacchi gravi compiuti per finalità di *Cybercrime* (che ha come obiettivo l'arricchimento economico), così come quelli riferibili ad attività di *Cyber Espionage* (+57,4%).

Tipologia e distribuzione degli attaccanti 2018

Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi, Camera dei Deputati – Rapporti Clusit 2019



Rispetto al passato, precisa il Rapporto risulta più difficile distinguere nettamente tra *Cyber Espionage* e *Information Warfare*: Sommando gli attacchi di entrambe le categorie, nel 2018 si assiste a un aumento del 35,6% rispetto all'anno precedente (259 contro 191).

I grafici che seguono riportano il numero di attacchi per tipologie di attacco nel periodo 2011 2018.

Distribuzione degli attacanti per tipologia (2011-2018)

Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi, Camera dei Deputati - Rapporti Clusit 2017-2019

Attaccanti per tipologia	*2011*	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*
Cybercrime	170	633	609	526	684	751	857	1.232
Hackyivism	114	368	451	236	209	161	79	61
Espionage/Sabotage	23	29	67	69	96	88	129	203
Cyber Warfare	14	43	25	42	23	50	62	56
TOTALE	321	1.073	1.152	873	1.012	1.050	1.127	1.552

Con riferimento ai **settori oggetto di attacchi** quello Governativo registra, rispetto al 2017, un aumento del 40,8%; il settore sanitario, quello finanziario e delle infrastrutture un aumento, rispettivamente del 98,8%; del 33,3% e del 42.5%.

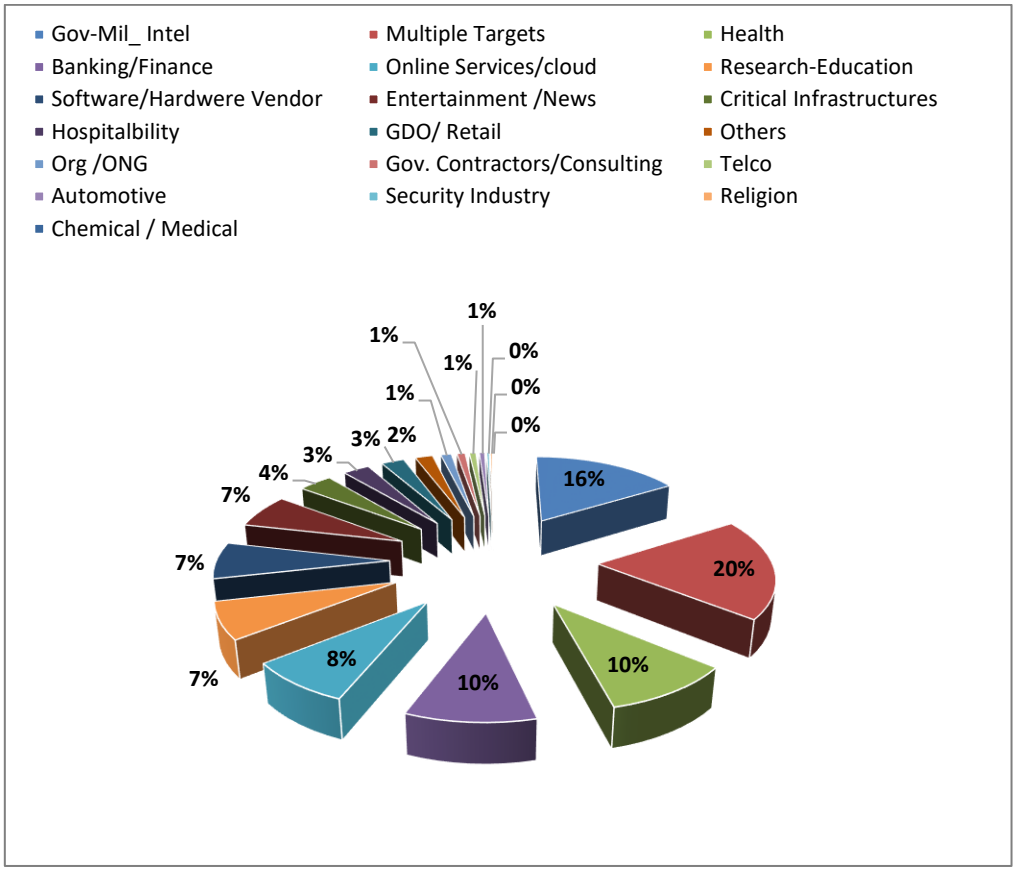
Numero di attacchi nei diversi (2014-2018)

Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi, Camera dei Deputati – Rapporti Clusit 2019

Vittime per tipologia	*2014*	*2015*	*2016*	*2017*	*2018*	*2018/2017*
Gov-Mil_ Intel	213	223	220	179	252	40,8%
Multiple Targets	-	-	49	222	304	36,9%
Health	32	36	73	80	159	98,8%
Banking/Finance	50	64	105	117	156	33,3%
Online Services/cloud	103	187	179	95	129	35,8%
Research-Education	54	82	55	71	110	54,9%
Software/Hardwere Vendor	44	55	56	68	109	60,3%
Entertainment /News	77	138	131	115	102	-11,3%
Critical Infrastructures	13	33	38	40	57	42,5%
Hospitalbility	-	39	33	34	45	32,4%
GDO/ Retail	20	17	29	24	39	62,5%
Others	172	51	38	40	30	-25%
Org /ONG	47	46	13	8	18	125%
Gov. Contractors/Consulting	13	8	7	6	14	133,3%
Telco	18	18	14	13	11	-15,4%
Automotive	3	5	4	4	9	125%
Security Industry	2	3	0	11	4	-63,6%
Religion	7	5	6	0	3	
Chemical / Medical	5	2	0	0	1	
TOTALE/ MEDIA VARIAZIONI	873	1.012	1.050	1.127	1.552	

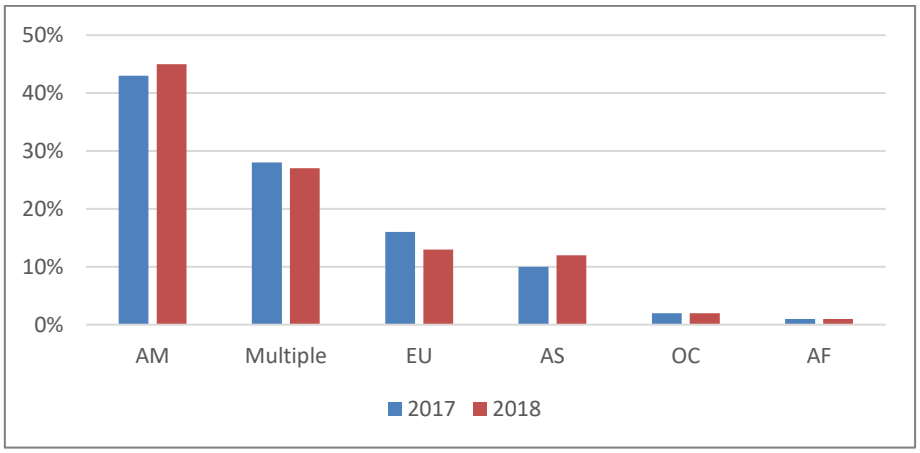
Percentuale di attacchi nei diversi settori 2018

Fonte: Elaborazione dati a cura del dipartimento Difesa, Servizio Studi, Camera dei Deputati – Rapporti Clusit 2019



Con riferimento, infine, all'**area geografica** di appartenenza nel 2018 aumentano le vittime di area americana (dal 43% al 45%), mentre, gli attacchi noti verso realtà basate in Europa sembrano addirittura diminuire (dal 16% al 13%) e aumentano quelli rilevati contro organizzazioni asiatiche (dal 10% al 12%). Percentualmente rimangono sostanzialmente invariati gli attacchi gravi verso bersagli multipli distribuiti globalmente (categoria "Multiple"), dall'28% del 2017al 27% del 2018.

Appartenenza geografica delle vittime per area geografica 2017-2018.
Fonte: Elaborazione dati – Rapporti Clusit 2019



L'ARCHITETTURA STRATEGICA NAZIONALE PER LA SICUREZZA E LA DIFESA CIBERNETICA

1. Premessa

Nel corso degli ultimi anni sono stati adottati una serie di provvedimenti normativi volti a definire l'architettura strategica nazionale per la sicurezza cibernetica al fine di potenziare progressivamente le capacità di difesa cibernetica del Paese.

Nello specifico, **nel 2013**, con il cd. "decreto Monti" (DPCM 24 gennaio 2013), l'Italia ha provveduto a definire le molteplici competenze di settore tra i diversi attori istituzionali delineando la *governance* nazionale in materia di *cyber security*.

Il 17 **febbraio 2017** è stato adottato il Decreto del Presidente del Consiglio dei Ministri recante la Direttiva in materia protezione cibernetica e sicurezza informatica nazionali" (cd."Decreto Gentiloni") che ha interamente sostituito il precedente decreto del 2013 introducendo importanti innovazioni volte, in particolare, ad assicurare un maggiore coordinamento tra le diverse strutture istituzionali previste nel nuovo quadro strategico.

Nel **maggio 2018** con il D.Lgs. 65/2018 di recepimento della Direttiva 2016/1148 (c.d. "Direttiva NIS") sono stati delineati ulteriori interventi di rafforzamento del sistema di sicurezza cibernetica del Paese. Dal 2018 trova, inoltre, applicazione il **decreto legislativo n. 101** adottato per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 (noto come "GDPR" *General Data Protection Regulation*) che impone a chi custodisce e tratta dati personali (soggetti pubblici e privati) l'adozione di standard di sicurezza più elevati rispetto al passato. A sua volta il **Regolamento** (UE) **2019/881** del Parlamento Europeo e del Consiglio del 17 aprile 2019 *Cybersecurity Act* introduce una certificazione europea della sicurezza cibernetica di *hardware* e *software* trasponendo in campo informatico gli stringenti *standard* già applicati alla sicurezza fisica dei beni prodotti nella UE. Responsabile delle certificazioni è l'Agenzia europea per la sicurezza delle reti e dell'informazione (*European Network and Information Security Agency*, ENISA).

Da ultimo il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il decreto n.105 del 2019 (pubblicato nella Gazzetta Ufficiale del 21 settembre 2019) che introduce disposizioni urgenti in materia di "**perimetro**" di sicurezza nazionale cibernetica.

Al riguardo, si ricorda che il **19 luglio 2019** il Consiglio dei ministri aveva approvato il disegno di legge sul "**perimetro di sicurezza nazionale cibernetica**" (A.S. 1448).

Inoltre in data 11 luglio 2019 era stato approvato dal Consiglio dei Ministri il decreto legge n. 64 del 2019 (**non convertito in legge**) **sull'estensione del Golden Power** per garantire la sicurezza delle nuove infrastrutture di telecomunicazione con particolare riferimento a quelle 5G[19].

Completano, infine, l'impianto normativo e regolamentare una serie di ulteriori disposizioni normative adottate in ambito nazionale che hanno riguardato profili specifici del tema della sicurezza cibernetica con particolare riferimento alle modalità di contrasto al fenomeno *cyber crime* e alle relative attività di *intelligence* (cfr. successivo capitolo " Il contrasto della criminalità informatica e la tutela dei diritti).

Nei successivi paragrafi è riportata una breve descrizione dei principali provvedimenti normativi che delineano l'architettura strategica nazionale in materia di sicurezza cibernetica con particolare riferimento alle competenze assegnate in tale ambito ai principali attori istituzionali.

2. Evoluzione della normativa nazionale in materia di sicurezza cibernetica

Nel gennaio del 2013, anche sulla base di analoghe iniziative intraprese a livello europeo ed internazionale, il Governo ha adottato il DPCM del 24 gennaio del 2013 (c.d. "**decreto Monti**"), che, fino all'entrata in vigore del successivo DPCM del 17 febbraio 2017 (c.d. "**decreto Gentiloni**"), ha definito l'architettura

[19] Sulla "sanatoria degli effetti" del richiamato decreto legge n. 64 del 2019 si veda l'articolo 1 del ddl di conversione del decreto legge n. 75 del 2019 (A.C. 2107).

istituzionale "deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali".

Nel dicembre del medesimo anno, in attuazione di un'espressa disposizione contenuta nel DPCM del 2013, sono stati approvati il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* e il *Piano nazionale per la protezione cibernetica*. Nell'insieme questi documenti individuano, per la prima volta in maniera organica a livello nazionale, i compiti affidati a ciascuna componente istituzionale con competenze nel settore della sicurezza e della difesa cibernetica ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.

Nello specifico il DPCM del 2013 individuava nella Presidenza del Consiglio dei Ministri il vertice dell'architettura nazionale in materia di sicurezza cibernetica. Presso l'Ufficio del Consigliere Militare (UCM) veniva incardinato il Nucleo per la Sicurezza Cibernetica (NSC), in funzione di prevenzione, preparazione, risposta e ripristino rispetto ad eventuali situazioni di crisi cibernetica. Venivano quindi istituiti un **CERT nazionale** all'interno del Ministero dello Sviluppo economico e un **CERT della Pubblica amministrazione** all'interno dell'Agenzia per l'Italia digitale (AgID).

Nel febbraio 2017 il Governo ha emanato una nuova direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale (D.P.C.M 17 febbraio 2017, c.d. "**decreto Gentiloni**") che ha interamente **sostituito** la precedente direttiva del 2013.

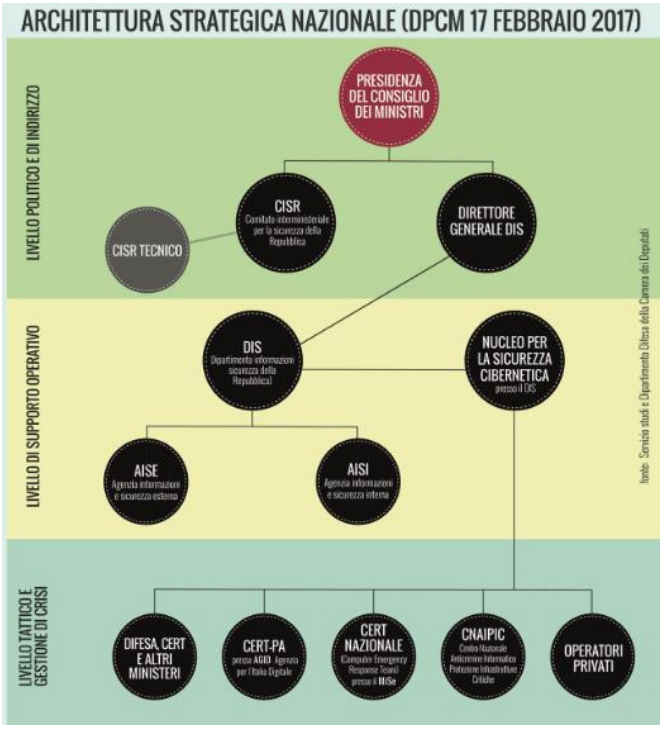
Al decreto è seguita l'emanazione, nel marzo 2017 di un nuova edizione del *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica.*

Nel nuovo assetto strategico delineato con il Decreto del 2017 al Presidente del Consiglio dei ministri viene espressamente affidata l'alta direzione e la responsabilità della politica generale del Governo **anche nel campo della sicurezza dello spazio cibernetico**. In tale funzione, come si vedrà più diffusamente in seguito, egli

provvede al coordinamento delle politiche dell'informazione per la sicurezza cibernetica, impartisce le direttive e, sentito il CISR, emana le disposizioni necessarie per l'organizzazione e il funzionamento del Sistema di sicurezza cibernetica.

Al centro della *governance* per la *cybersecurity* il decreto pone il **Sistema di informazione per la sicurezza della Repubblica** (cfr. *infra*) con particolare riferimento al **Dipartimento Informazioni per la Sicurezza** (DIS) nel cui ambito viene collocato il **Nucleo Sicurezza Cibernetica** (traferito dall'UCM).

L'analisi dei singoli organismi che compongono il Sistema di informazione per la sicurezza della Repubblica con particolare riferimento ai relativi poteri in ambito di sicurezza cibernetica è contenuta nel successivo paragrafo 4.



In base alla nuova architettura strategica il **Nucleo è** l'organismo intergovernativo che svolge funzioni di gestione delle crisi cibernetiche e di raccordo tra le diverse componenti dell'architettura istituzionale.

Il Nucleo **riferisce direttamente al direttore generale del DIS** per la successiva informazione al Presidente del Consiglio dei ministri e al Comitato interministeriale per la sicurezza della Repubblica (CISR).

Con il decreto del 2017 **il vice direttore del DIS**, oltre ad avere incarico di coordinamento interministeriale, **presiede il NSC** che è composto anche dal consigliere militare e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli

affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale.

Spetta, inoltre, al **direttore generale del DIS** il compito di definire le necessarie linee di azione per innalzare i livelli di sicurezza dei sistemi e delle reti, con particolare riferimento all'individuazione dei più adeguati e **avanzati supporti tecnologici**. Per la realizzazione di tali iniziative, "è previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore".

Il Nucleo della sicurezza cibernetica, su iniziativa del DIS, ha promosso l'avvio di un **gruppo di lavoro** chiamato a individuare possibili soluzioni tecnico-amministrative per garantire un approvvigionamento di beni e servizi informatici, caratterizzato da maggiori garanzie di sicurezza sotto il profilo cibernetico per la pubblica amministrazione. Le attività del gruppo di lavoro si sono concluse con l'elaborazione di un **testo unico di buone prassi e prescrizioni**, sotto forma di linee guida obbligatorie dell'AGID (Agenzia per l'Italia digitale), pubblicate sul relativo sito *web* e in consultazione pubblica. Contengono misure di tipo organizzativo, funzionale e operativo, suddivise tra azioni da svolgere prima, durante e dopo la fase di *procurement*. Tali indicazioni sono obbligatorie per le forniture ritenute critiche dall'amministrazione committente, mentre vanno intese come semplici suggerimenti per le forniture non critiche. Nell'ambito del gruppo di lavoro è emersa la necessità di provvedimenti legislativi per consentire di adeguare la normativa sugli appalti, in modo da equiparare la *cyber security* alla sicurezza sui luoghi di lavoro, così da poter evitare l'affidamento delle gare secondo il principio del massimo ribasso, prevedendo altresì la presenza di almeno un esperto di sicurezza informatica nelle commissioni aggiudicatrici delle gare ICT[20].

Infine viene attribuito al **Ministero dello sviluppo economico** il compito di istituire un centro di valutazione e certificazione

[20] Cfr. resoconto stenografico della seduta della Commissione Trasporti del 7 maggio 2019 nel corso della quale ha avuto luogo l'audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri, nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5g ed alla gestione dei *big data*.

nazionale per la verifica dell'affidabilità della componentistica delle apparecchiature ICT che vengono utilizzate da parte della pubblica amministrazione nelle strutture critiche e nelle strutture strategiche ed è stato inoltre previsto l'accesso alle banche dati dei soggetti privati e ai cosiddetti SOC (*Security Operation Center*) dal parte del DIS, in modo tale da poter avere una visione unitaria del sistema.

Il **Centro di valutazione e certificazione nazionale** è stato istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019. Il centro è stato istituito presso l'Istituto Superiore delle comunicazioni e tecnologie dell'informazione. Il 19 aprile 2019 è stato firmato il decreto che descrive il modello di funzionamento, l'organizzazione e il piano di sviluppo del CVCN, così come previsto dal richiamato decreto del Ministro dello sviluppo economico[21].

Al riguardo si segnala che il recente decreto legge n. 105 del 2019 sul "**perimetro di sicurezza nazionale cibernetica"** in corso di conversione, rafforza i poteri del Cenro di valutazione e certificazione nazionale che potrà imporre "test di *hardware* e *software*" in caso di "affidamento di forniture di beni, sistemi e servizi Ict destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici" dei soggetti inseriti nel perimetro.

In particolare ai sensi del comma 7 dell'articolo 1 il Centro:

a) contribuisce all'elaborazione delle misure di sicurezza, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;
b) svolge attività di valutazione del rischio e di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, dettando, se del caso, prescrizioni di utilizzo al committente;
c) elabora e adotta (previo conforme avviso dell'organismo tecnico di supporto al Comitato interministeriale per la sicurezza della Repubblica - CISR) schemi di certificazione cibernetica, qualora gli schemi di certificazione esistenti non siano ritenuti, per ragioni di sicurezza nazionale, adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

[21] Per un approfondimento si veda resoconto stenografico della seduta della Commissione Trasporti del 19 giugno 2019, cit, audizione di rappresentanti dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) del Ministero dello sviluppo economico dell' indagine conoscitiva richiamata nella precedente nota.

Ai fini delle attività di cui alla lettera b), il CVCN si avvale anche di laboratori che esso accredita. I criteri per tale accreditamento sono da stabilirsi con D.P.C.M. entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto-legge.

Siffatto D.P.C.M. è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR).

Si segnala, inoltre, che il decreto legge n. 105 del 2019 prevede l'istituzione, presso il Ministero della **Difesa,** di un apposito **Centro di valutazione** definendone gli specifici poteri nell'ambito delle misure di *cyber defence* previste dal medesimo decreto (cfr. *infra).*

3. Il decreto legislativo n. 65 del 18 maggio 2018 (attuazione della cosiddetta "direttiva NIS")

Con il decreto legislativo n. 65 del 18 maggio 2018, adottato in attuazione della direttiva (UE) 2016/1148 (c.d. direttiva NIS *Network and Information Security*) è stata ulteriormente definita la cornice legislativa relativa alla sicurezza delle reti e dei sistemi informativi con espressa individuazione dei soggetti competenti a dare attuazione agli obblighi previsti dalla richiamata direttiva.

Al contempo è stata prevista l'istituzione di uno CSIRT italiano presso la Presidenza del Consiglio dei ministri nel quale confluiranno il CERT nazionale e quello della Pubblica amministrazione (cfr. *infra*).

In particolare, la direttiva NIS ha stabilito misure per uno *standard* comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea". La Direttiva rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza cibernetica e delinea le azioni in capo agli Stati membri volte a migliorare le capacità di sicurezza dei singoli Paesi dell'Unione Europea. La Direttiva si pone inoltre l'obiettivo di aumentare il livello di collaborazione nella prevenzione delle minacce cibernetiche e nell'implementazione di misure di risposta agli attacchi *cyber*.

Per una ricognizione delle disposizioni del provvedimento si consiglia la lettura del *dossier* del Servizio Studi della Camera dei deputati e del Senato delle Repubblica;

Nel dettaglio, il D.Lgs. 65/2018 ha stabilito:

a) **l'inclusione** nella strategia nazionale di **sicurezza cibernetica** delle previsioni **in materia di sicurezza delle reti** e dei sistemi informativi rientranti nell'ambito di applicazione del decreto;
b) la designazione delle **autorità nazionali competenti** e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti previsti all'allegato I del decreto medesimo;
c) il rispetto di obblighi da parte degli **operatori di servizi** essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;
d) la partecipazione nazionale al gruppo di cooperazione europeo, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea, nonché dell'incremento della fiducia tra di essi;
e) la partecipazione nazionale alla **rete CSIRT** nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace.

Viene altresì specificato che, fatto salvo quanto previsto dall'articolo 346 del trattato sul funzionamento dell'Unione europea, le informazioni riservate secondo quanto disposto dalla normativa dell'Unione europea e nazionale, in particolare per quanto concerne la riservatezza degli affari, sono scambiate con la Commissione europea e con altre autorità competenti NIS solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione del decreto. Le informazioni scambiate devono essere pertinenti e commisurate allo scopo e deve essere tutelata la riservatezza e la protezione della sicurezza e degli interessi commerciali degli operatori di servizi essenziali e dei fornitori di servizi digitali.

Restano inoltre impregiudicate le misure adottate per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, nei casi in cui la divulgazione sia ritenuta contraria agli interessi essenziali di sicurezza e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati.

Per quanto riguarda **l'architettura istituzionale** definita dal D.Lgs. 65/2018 è stata in primo luogo attribuita al **Presidente del Consiglio dei ministri**, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), la competenza alla definizione

della **strategia nazionale di sicurezza cibernetica** per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

Con la medesima procedura sono adottate **linee di indirizzo** per l'attuazione della strategia nazionale di sicurezza cibernetica.

La qualifica di "**autorità competente NIS**" viene attribuita ai singoli ministeri in base ai settori di competenza (Ministero dello sviluppo economico, Ministero delle infrastrutture e trasporti, Ministero dell'economia e delle finanze, Ministero della salute e Ministero dell'ambiente e della tutela del territorio) e, per taluni ambiti, alle regioni e alle province autonome di Trento e di Bolzano.

Tali autorità sono i **soggetti competenti per settore** - settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali - in materia di sicurezza delle reti e dei sistemi informativi; verificano, in particolare, l'applicazione della direttiva a livello nazionale ed individuano gli operatori di servizi essenziali nell'ambito dei criteri ivi definiti.

L'**autorità di contrasto** è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione al quale è attualmente attribuita la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Gli operatori di servizi essenziali, ai fini del provvedimento, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS.

Il decreto legislativo 65/2018 definisce inoltre **gli obblighi** posti in capo agli operatori dei servizi essenziali e ai fornitori dei servizi digitali con riferimento alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III.

È posto a loro carico l'obbligo di individuare le misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti e, sotto il profilo procedurale, sono definite le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti individuando altresì le condizioni e le modalità secondo le quali potranno essere coinvolti gli organismi di altri Paesi.

Sono poi individuati i **poteri di controllo delle autorità NIS** sia nei confronti degli operatori di servizi essenziali, che dei fornitori di servizi digitali anche prevedendo poteri di verifica e di ispezione oltre che l'irrogazione di sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti.

4. Il decreto legge n. 105 del 2019 sul perimetro di sicurezza nazionale cibernatica

Il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il **decreto n.105 del 2019** (pubblicato nella Gazzetta Ufficiale del 21 settembre 2019) che introduce disposizioni urgenti in materia di "perimetro" di sicurezza nazionale cibernetica.

Il decreto, come si legge nel comunicato, mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di **un perimetro di sicurezza nazionale cibernetica** e la previsione di misure idonee a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

In particolare, il decreto fa riferimento ad amministrazioni pubbliche, nonché ad enti oppure operatori nazionali, pubblici e privati i cui sistemi informatici:

- sono necessari per l'esercizio di una funzione essenziale dello Stato;
- sono necessari per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

• il cui malfunzionamento, interruzione o uso improprio possono pregiudicare la sicurezza nazionale.

Resta ferma, per gli organismi di informazione e sicurezza, la specifica disciplina di cui alla legge 3 agosto 2007, n. 124 (recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto").

Una volta stabilito il perimetro, verranno definite le **procedure** con le quali i soggetti che ne fanno parte dovranno notificare gli eventuali incidenti "aventi impatto su reti, sistemi informativi e servizi informatici" e vengono stabilite le misure "volte a garantire elevati livelli di sicurezza".

In particolare, il comma 3 demanda ad un D.P.C.M. - da adottare entro dieci mesi dalla conversione del decreto legge - la definizione:

1. delle procedure in base alle quali i soggetti del perimetro di sicurezza nazionale cibernetica segnalino gli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici (lett. a));
2. delle misure volte a garantirne elevati livelli di sicurezza (lett. b)).

All'elaborazione delle richiamate misure provvedono, secondo gli ambiti di competenza delineati dal medesimo decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

Per quanto riguarda le **procedure di segnalazione** degli incidenti su reti, sistemi informativi e sistemi digitali rientranti nel perimetro di sicurezza nazionale cibernetica, i relativi soggetti (amministrazioni pubbliche, nonché enti oppure operatori nazionali, pubblici e privati) devono **notificare l'incidente** al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano. Il CSIRT procede poi a inoltrare tempestivamente tali notifiche al Dipartimento delle informazioni della sicurezza (DIS). Siffatta trasmissione è prevista anche qualora siano interessate attività demandate al Nucleo per la sicurezza cibernetica. A sua volta il DIS assicura una ulteriore trasmissione all'organo del Ministero dell'interno preposto alla sicurezza e regolarità dei servizi di telecomunicazioni; alla Presidenza del Consiglio dei ministri (se le notifiche degli incidenti giungano da un soggetto pubblico - o da un soggetto fornitore di servizi fiduciari qualificati o svolgente l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale, ai sensi dell'art. 29 del Codice dell'amministrazione digitale, decreto legislativo n. 82 del 2005) ovvero al Ministero dello sviluppo economico (se le notifiche

giungano da un soggetto privato del perimetro di sicurezza nazionale cibernetica). Le **misure di sicurezza** - di cui alla lettera b) - esse devono assicurare elevati livelli di prevenzione e salvaguardia delle reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica.

Il testo integra e adegua, inoltre, il quadro normativo in materia di esercizio dei **poteri speciali** da parte del Governo, con particolare riferimento a quanto previsto dal decreto-legge 15 marzo 2012, n. 21, in modo da coordinare l'attuazione del Regolamento (UE) 2019/452, sul controllo degli investimenti esteri, e apprestare idonee misure di tutela di infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione del decreto-legge 15 marzo 2012, n. 21.

L'articolo 4 modifica il decreto legge n. 21 del 2012 in tema di poteri speciali del Governo nei settori ad alta intensità tecnologica (cd. *golden power*). In particolare, viene ampliato il perimetro dei settori che possono essere individuati con regolamento ai fini dell'applicazione della disciplina, con riferimento alla sussistenza di un pericolo per la sicurezza e l'ordine pubblico (comma 1). Viene altresì stabilito (comma 2) che, fino all'adozione del regolamento che individua i settori rilevanti, è soggetto a notifica l'acquisto a qualsiasi titolo, da parte di un soggetto esterno all'Unione europea, di partecipazioni in società che detengono beni e rapporti in specifici settori, fra i quali quelli legati alla cibersicurezza, di rilevanza tale da determinare l'insediamento stabile dell'acquirente in ragione dell'assunzione del controllo della società. Il comma 2 prevede altresì che tali notifiche possano dar luogo all'esercizio di poteri speciali da parte del Governo, mediante l'imposizione di condizioni e impegni diretti a garantire la tutela degli interessi essenziali dello Stato nonché l'opposizione all'acquisto della partecipazione.

Le nuove norme, tra l'altro:

- istituiscono un meccanismo teso ad assicurare un ***procurement*** più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi di *information and communication technology* (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti. Con specifico riferimento al **comparto della Difesa** si prevede che per le forniture di beni, sistemi e servizi ICT da

impiegare su reti, sistemi informativi e servizi informatici del Ministero della difesa, il Ministero proceda, **attraverso un proprio Centro di valutazione** in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza.

- prevedono che l'esercizio dei **poteri speciali** in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa e, con riferimento alle autorizzazioni già rilasciate ai sensi del decreto-legge 15 marzo 2012, n. 21, la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi *standard*;

- **rafforzano i poteri** del Centro di valutazione e certificazione nazionale (il Cvcn, istituito al Mise), che potrà imporre "test di hardware e software" in caso di "affidamento di forniture di beni, sistemi e servizi Ict destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici" dei soggetti inseriti nel perimetro.

- attribuiscono al **Presidente del Consiglio dei Ministri**, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi, **il potere di eliminare**, ove indispensabile e per il tempo strettamente necessario, **lo specifico fattore di rischio** o di mitigarlo, secondo un criterio di proporzionalità, disattivando totalmente o parzialmente, uno o più apparati o prodotti impiegati nelle reti e nei sistemi".

Nello specifico il decreto legge stabilisce in **quattro mesi** il termine per **individuare le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati** che entreranno a far parte del cosiddetto perimetro cibernetico, a tutela della sicurezza di reti e servizi definiti "strategici". Sempre in **quattro mesi** l'organismo tecnico di supporto al **CISR** il Comitato Interministeriale per la Sicurezza della Repubblica, con un **rappresentante della Presidenza del Consiglio** dei ministri, dovranno stabilire i criteri in

base ai quali i soggetti predisporranno e aggiorneranno "**con cadenza almeno annuale** un elenco delle reti, dei sistemi informativi e dei servizi informatici sensibili di rispettiva pertinenza, comprensivo della relativa architettura e componentistica", che verrà poi diffuso agli organismi di competenza. Entro **dieci mesi** dovranno essere definite le procedure secondo cui i soggetti che fanno capo al perimetro **notifichino gli incidenti** che hanno impatto su reti, sistemi e servizi. Sempre entro **dieci mesi** è prevista la definizione delle misure volte a **garantire gli elevati livelli di sicurezza** previsti per i soggetti identificati, relative alle politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio e alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza; alla protezione fisica e logica e dei dati; all'integrità delle reti e dei sistemi informativi; alla gestione operativa, ivi compresa la continuità del servizio; al monitoraggio, test e controllo; alla formazione e consapevolezza; all'affidamento di forniture di beni, sistemi e servizi di *information and communication technology* (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.

Per un approfondimento del contenuto del decreto legge si rinvia al relativo *dossier*.

5. Il Sistema di informazione per la sicurezza della Repubblica nell'ambito della sicurezza cibernetica

Nello sviluppo dell'architettura nazionale della *cyber* sicurezza il Sistema di informazione per la sicurezza della Repubblica ha acquisito un ruolo strategico, prima con il DPCM 24 gennaio 2013 e, successivamente, con il DPCM 17 febbraio 2017 e il D.Lgs. 65/2018.

Come noto il **Sistema di informazione per la sicurezza della Repubblica** è l'insieme degli organi e delle autorità che nel nostro Paese hanno il compito di assicurare le attività informative allo scopo di salvaguardare la Repubblica dai pericoli e dalle minacce provenienti sia dall'interno sia dall'esterno.

Disciplinato principalmente dalla L. 124/2007, il Sistema di informazione per la sicurezza della Repubblica è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità eventualmente delegata dal Presidente del Consiglio, dal Dipartimento delle informazioni per la sicurezza (DIS), e dai servizi

di informazione: Agenzia informazioni e sicurezza esterna (AISE) e Agenzia informazioni e sicurezza interna (AISI).

A sua volta il Comitato parlamentare per la sicurezza della Repubblica (Copasir), composto da cinque deputati e cinque senatori, è l'organo di controllo parlamentare della legittimità e della correttezza costituzionale dell'attività degli organismi informativi (L. 124/2007, artt. 30-38).

Nel dettaglio il **Presidente del Consiglio dei ministri** dirige ed ha la responsabilità generale della politica dell'informazione e della sicurezza (L. 124/2007, art. 1).

Egli provvede alla **tutela della sicurezza nazionale anche nello spazio cibernetico** (DPCM 17 febbraio 2017).

In particolare, in questo settore:

- provvede, nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale, a convocare il CISR;
- adotta e aggiorna, su proposta del CISR, il quadro strategico nazionale per la sicurezza dello spazio cibernetico;
- adotta, su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica contenente gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale;
- emana le direttive per l'attuazione del Piano nazionale;
- impartisce, sentito il CISR, le direttive al DIS e alle Agenzie per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali.

Inoltre, adotta, sentito il CISR, la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale e le linee di indirizzo per l'attuazione della strategia di sicurezza cibernetica (D.Lgs. 65/2018, art. 6).

Ulteriori poteri in ambito di sicurezza cibernetica sono assegnati al Presidente del Consiglio dal recente decreto legge n. 105 del 2019, in corso di conversione.

Nello specifico il Presidente del Consiglio - su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR) - può disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi posti nel perimetro di sicurezza nazionale cibernetica nel caso in cui si verifichi un **rischio grave e imminente per la sicurezza nazionale** connesso alla vulnerabilità di reti, sistemi e servizi del perimetro di sicurezza nazionale cibernetica, **e comunque nei casi di crisi cibernetica**.

Situazione di **crisi cibernetica** è - secondo la definizione reca dall'articolo 2, comma 1, lettera o) del D.P.C.M del 17 febbraio 2017 - una "situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale".

Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è organo istituzionale di raccordo politico-strategico sul tema della sicurezza nazionale, con compiti di consulenza, proposta e deliberazione. È presieduto dal Presidente del Consiglio e composto dai ministri degli esteri, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, dello sviluppo economico. Il CISR ha funzioni consultive e di proposta, elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza e delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi (L. 124/2007, art. 5).

In materia di *cyber security* il CISR, oltre ai generali poteri di consulenza e proposta nei confronti del Presidente del Consiglio visti sopra, **ha autonomi poteri di impulso** e vigilanza indicati nel DPCM 17 febbraio 2017 (art. 4) quali:

- l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;
- l'approvazione di linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati

interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di *best pratices* e di misure rivolte all'obiettivo della sicurezza cibernetica;
- l'elaborazione di indirizzi generali e obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali;
- la promozione di iniziative necessarie per assicurare la piena partecipazione dell'Italia ai consessi di cooperazione internazionale, quali quelli in ambito NATO e UE.

Infine, il CISR può formulare proposte di intervento normativo ed organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi.

Il supporto tecnico all'attività del CISR, è assicurato dall'organismo collegiale di coordinamento istituito presso il DIS dal DPCM 24 gennaio 2013 e presieduto dallo stesso direttore del DIS. L'organismo è stato denominato **CISR tecnico** dal DPCM 17 febbraio 2017 (art. 3) che ne ha confermato sostanzialmente le competenze originariamente fissate dal DPCM del 2013.

Il **Dipartimento delle informazioni per la sicurezza (DIS)** presso la Presidenza del Consiglio ha come compito principale quello di coordinare il complesso delle attività informative e di assicurare l'unitarietà dell'azione dei servizi di informazione per la sicurezza verificando altresì i risultati delle attività svolte da:
- l'Agenzia informazioni e sicurezza esterna (**AISE**) operante all'estero (L. 124/2007, art. 6);
- l'Agenzia informazioni e sicurezza interna (**AISI**) che agisce sul territorio nazionale (art. 7).

La funzione di coordinamento del DIS comprende l'attività di verifica dei risultati e di elaborazione di analisi globali da sottoporre al CISR, e di progetti di ricerca informativa sui quali decide il Presidente del Consiglio, sentito il CISR (L. 124/2007, art. 4).

Il DIS svolge tali funzioni anche riguardo la sicurezza cibernetica. Infatti, il DPCM del 2017, confermando il precedente DPCM del 2013, specifica che l'attività di coordinamento delle attività di ricerca informativa è finalizzata anche a rafforzare la protezione cibernetica e la sicurezza informatica nazionali (DPCM 17 febbraio 2017, art. 7, comma 2). Così come le attività di formulazione di analisi, valutazioni e previsioni e di trasmissione di informazioni alle p.a. e a tutti i soggetti interessati, di competenza del DIS, sono svolte anche riguardo alla minaccia cibernetica (DPCM 17 febbraio 2017, art. 7, comma 3).

Come anticipato in precedenza, il DPCM del 2017 rafforza il ruolo del DIS: nello specifico è **il direttore generale del DIS** ad adottare le iniziative idonee a definire le linee di azione necessarie per innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati e avanzati supporti tecnologici in funzione di prevenzione e contrasto, da parte sia delle p.a., sia dei privati, in caso di crisi cibernetica. Per la realizzazione di tali iniziative, è previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore Infatti, il direttore del DIS è chiamato a predisporre gli opportuni moduli organizzativi, di coordinamento e di raccordo, prevedendo il ricorso anche a professionalità delle pubbliche amministrazioni, degli enti di ricerca pubblici e privati, delle università e di operatori economici privati (DPCM 17 febbraio 2017, art. 6).

Il ruolo centrale del DIS nella sicurezza cibernetica è confermato dal decreto legislativo di recepimento della direttiva NIS che lo ha designato ***Punto di contatto unico NIS*** in materia di sicurezza delle reti e dei sistemi informativi. In tale veste, il DIS svolge una funzione di collegamento per garantire la cooperazione tra le autorità competenti NIS nazionali (ministeri dello sviluppo economico, infrastrutture e trasporti, economia e finanze, salute e ambiente) e le autorità competenti NIS degli altri Stati dell'Unione europea, il Gruppo di cooperazione europeo e la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente - CSIRT (D.Lgs. 65/2018, art. 7).

Presso il DIS è incardinato il **Nucleo per la sicurezza cibernetica** (NSC), struttura di supporto del Presidente e del CISR, nella materia della sicurezza dello spazio cibernetico, relativamente alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento (DPCM 17 febbraio 2017).

Il NSC è presieduto da un **Vice Direttore generale del DIS**, designato dal Direttore generale, ed è composto dal Consigliere militare del Presidente del Consiglio e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale.

Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza (UCSe) operante presso il DIS.

In particolare, spetta al Nucleo per la sicurezza cibernetica:

- promuovere la **programmazione** e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e curare l'elaborazione delle necessarie procedure di coordinamento interministeriale;
- mantenere costantemente attiva **l'unità per l'allertamento** e la risposta a situazioni di crisi cibernetica;
- valutare e promuovere procedure di **condivisione delle informazioni**, anche con gli operatori privati, al fine di diffondere gli allarmi relativi ad eventi cibernetici e per la gestione delle crisi;
- acquisire le comunicazioni circa i **casi di violazione** o dei tentativi di violazione della sicurezza o di perdita dell'integrità dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), nonché dalle strutture del Ministero della difesa e dai CERT;

- promuovere e coordinare, in raccordo con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale lo **svolgimento di esercitazioni** anche internazionali che riguardano la simulazione di eventi di natura cibernetica;
- costituire il **punto di riferimento nazionale** per i rapporti con l'ONU, la NATO, l'UE e le altre organizzazioni internazionali e gli altri Stati.

Nello specifico campo dell'attivazione delle azioni di risposta e ripristino rispetto a situazioni di crisi cibernetica, il Nucleo per la sicurezza cibernetica:

- riceve, anche dall'estero, le segnalazioni di eventi cibernetici e dirama gli allarmi alle amministrazioni e agli operatori privati;
- valuta se l'evento assuma dimensioni, intensità o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richieda l'assunzione di decisioni coordinate in sede interministeriale;
- informa tempestivamente il Presidente del Consiglio, per il tramite del Direttore generale del DIS, sulla situazione in atto.

6. Il CSIRT Italia e il CNAIPIC

Il D.Lgs. 65/2018 di recepimento all'interno dell'ordinamento nazionale italiano della direttiva NIS ha previsto l'istituzione presso la Presidenza del Consiglio di un unico *Computer Security Incident Response Team*, il CSIRT italiano, destinato a svolgere i compiti e le funzioni del CERT-PA e CERT-nazionale.

Il CSIRT italiano ha compiti di natura tecnica finalizzati a supportare la p.a., i cittadini e le imprese attraverso azioni di sensibilizzazione, prevenzione e coordinamento della risposta ad eventi cibernetici su vasta scala, anche in cooperazione con gli altri CERT europei. In particolare, secondo quanto disposto dal decreto di recepimento, ha i seguenti compiti:

- definire le procedure per la prevenzione e la gestione degli incidenti informatici;
- ricevere le notifiche di incidente, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e

preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al NSC;
- fornire al soggetto che ha effettuato la notifica le informazioni che possono facilitare la gestione efficace dell'evento;
- informare gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali o del fornitore di servizi digitali nonché la riservatezza delle informazioni fornite;
- garantire la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di *best practices*.

La disciplina dell'organizzazione e il funzionamento del CSIRT Italia è demandata ad un DPCM non ancora adottato. Nelle more dell'adozione di tale provvedimento, le funzioni sono svolte dal CERT-Nazionale e dal CERT-PA.

È in corso di definizione un modello nazionale di riferimento per i CERT regionali (AgID, Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali, 14 maggio 2019).

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) è una struttura che afferisce al Servizio di Polizia postale e delle comunicazioni nell'ambito del Dipartimento della pubblica sicurezza del Ministero dell'interno.

Il CNAIPIC ha il compito di prevenzione e repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale. Si avvale di tecnologie e di personale specializzati nel contrasto del *cyber crime*.

L'operatività del CNAIPIC si realizza attraverso l'esercizio di un Settore operativo e di un Settore tecnico. Il Settore operativo supporta le funzioni di: Sala operativa, Intelligence e Analisi. Il Settore tecnico è deputato alla gestione ed all'esercizio dell'infrastruttura tecnologica del CNAIPIC e dei collegamenti telematici con le Infrastrutture Critiche convenzionate, ai processi di

individuazione, *testing* ed acquisizione di risorse strumentali ed alla pianificazione di cicli di formazione ed aggiornamento del personale.

7. Il CERT Difesa, il CERT Technical Center e il Security Operation Center

Tra i soggetti pubblici che fanno parte dell'architettura strategica nazionale di *cyber security* un posto di rilievo assumono **le strutture della Difesa** preposte alla difesa delle **reti e dei sistemi digitali** delle Forze armate quale elemento essenziale di sicurezza per la condotta delle operazioni, la protezione delle informazioni e la tutela delle Forze armate.

Per l'analisi delle capacità cyber della difesa e le line di sviluppo capacitivo si rinvia al primo capitolo della sezione terza del dossier

Allo stato il **CERT Difesa** si articola in due organismi: il **CERT *Coordination Center***, costituito in seno al II Reparto (Informazioni e Sicurezza) dello stato maggiore della difesa e il CERT *Technical Center*, costituito in seno al Comando C4 Difesa, a sua volta inserito nel VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa. I due CERT svolgono attività di indirizzo, coordinamento e informazione rispetto ai CERT delle singole Forze armate. Nelle **situazioni di crisi** riguardanti i sistemi della difesa, il **CERT Difesa** coordina le attività da porre in essere. In sintesi, il CERT *Coordination Center* svolge attività di informazione e di allertamento anche a scopo di prevenzione e collabora e condivide informazioni con i corrispondenti CERT nazionali e internazionali (quello della NATO, il Nato *Computer Incident Response Capability* o NCIRC).
A sua volta il CERT *Technical Center* è invece preposto a prevenire, rilevare e contenere sul piano tecnico-operativo gli incidenti informatici, oltre che a coordinare e supportare l'azione dei CERT di Forza armata in caso di emergenza cibernetica. Il CERT **Technical Center** è quindi l'organo preposto alla **gestione tecnico-operativa** di tutti gli assetti e sistemi di *Information and Communication Technology* del comparto Difesa.

Il Comando C4 – nel quale è costituito il CERT *Technical Center* – svolge le proprie funzioni in tre ambiti di attività.
Il primo è **l'area del *networking***, che comprende la gestione dell'intera infrastruttura di rete. In quest'ambito opera il *Network Operation Center* (NOC). Il secondo è **l'area dei servizi informativi** (di natura sia gestionale, sia operativa) erogati agli utenti attraverso l'infrastruttura di rete, che comprende la gestione dei data center che ospitano quei servizi. In quest'ambito opera *l'Infrastructure Operation Center* (IOC). Il terzo è **l'area della sicurezza**, preposta a garantire l'applicazione degli indirizzi di settore in materia e a dare attuazione alle misure di *information assurance e cyber defence*. In quest'ambito operano il *Security Operation Center* (SOC), preposto a garantire servizi di sicurezza finalizzati alla protezione dell'infrastruttura ICT del comparto e a rilevare ogni forma di anomalia di natura di sicurezza su tale infrastruttura, e il CERT *Technical Center*, che garantisce i servizi di sicurezza finalizzati alla prevenzione, alla reazione e al contenimento di incidenti informatici.

Nell'ambito delle strutture sopra richiamate la Difesa ha dato vita nel 2017 ad un apposito **Comando Interforze per le operazioni cibernetiche (CIOC)** in fase di implementazione posto alle dirette dipendenze del capo di Smd, quale *Cyber command* nazionale abilitato a svolgere operazioni militari nel dominio cibernetico" (*infra*).

IL CONTRASTO DELLA CRIMINALITÀ INFORMATICA E LA TUTELA DEI DIRITTI NEL DOMINIO CIBERNETICO

1. L'elaborazione a livello sovranazionale e la Convenzione del Consiglio d'Europa sui crimini informatici (c.d. Convenzione di Budapest

Tra i primi documenti normativi che hanno posto il problema della tutela dei diritti nello spazio cibernetico e del contrasto dei reati che vengono commessi avvalendosi degli strumenti offerti dalla tecnologia e dall'ambiente informatici è da individuare nella **Convenzione del Consiglio d'Europa sul crimine cibernetico**, fatta a **Budapest** il 23 novembre **2001** ed entrata in vigore il 1° luglio 2004.

La firma della Convenzione fu l'esito del lavoro di una commissione istituita dal Comitato dei ministri del Consiglio d'Europa nel 1997 (la quale, a sua volta, proseguì il tracciato già indicato dalle Raccomandazioni del medesimo Consiglio d'Europa del 1989 n. 9 e del 1995 n. 13).

Ratificata dall'Italia con **la legge n. 48 del 2008**, la Convenzione sul crimine cibernetico è stata seguita dal Protocollo addizionale del 28 gennaio 2003 (entrato in vigore il 1° marzo 2006), inerente al contrasto dei crimini di matrice razzista e xenofoba commessi mediante strumenti informatici. Tale Protocollo – viceversa non è stato ancora ratificato dall'Italia.

Le considerazioni di sistema contenute nel preambolo della Convenzione di Budapest appaiono di particolare rilievo. Vi si sottolinea la necessità di perseguire una **politica comune in campo penale**, finalizzata alla protezione della società contro la criminalità informatica, adottando misure legislative appropriate e sviluppando la cooperazione internazionale, nella consapevolezza dei profondi cambiamenti dipendenti dall'introduzione della tecnologia digitale, dalla convergenza e costante globalizzazione delle reti informatiche.

Il preambolo premette altresì la preoccupazione per i rischi che le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati e che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti.

La Convenzione è pertanto finalizzata ad offrire un deterrente per le condotte dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi, reti ed informazioni, attraverso la tipizzazione penale dei comportamenti indicati nella medesima Convenzione.

La Convenzione, nondimeno, tiene presente la necessità di garantire un equo bilanciamento tra l'interesse per l'azione repressiva e il rispetto dei diritti umani fondamentali come previsto nella Convenzione europea dei diritti dell'uomo del 1950, la Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici e gli altri trattati applicabili sui diritti umani che riaffermano il diritto di ciascuno di avere opinioni senza condizionamenti, come anche il diritto alla libertà di espressione, incluso il diritto di cercare, ricevere, e trasmettere informazioni e idee di ogni tipo, senza limiti di frontiere, e il diritto al rispetto della privacy.

I contenuti della Convenzione si distribuiscono lungo **tre assi**.

In sintesi:

- il primo concerne l'impegno dei Paesi sottoscrittori a **tipizzare nel proprio diritto interno**, come fattispecie penalmente sanzionate, le condotte che mettono a rischio la sicurezza dell'infrastruttura informativa pubblica o privata, comr per esempio l'accesso abusivo a sistemi informatici o il loro danneggiamento, la captazione abusiva di flussi informatici riservati, l'apprestamento di mezzi informatici per commettere uno dei fatti appena descritti, il danneggiamento dei dati contenuti nei sistemi e la pornografia minorile diffusa con mezzi informatici;
- il secondo inerisce al **potenziamento dei mezzi di indagine** e di ricerca e conservazione delle prove dei reati informatici e impegna gli Stati a predisporre un quadro normativo che consenta la rapida ed efficace ricostruzione dei flussi a al fine di contrastarli, ivi compresa la possibilità di ordinare a persone fisiche residenti nei propri territori di rilasciare le informazioni necessarie, di accedere ai sistemi informatici e di conservare dati utili a fini repressivi e stabilire con apposite norme che la

giurisdizione dello Stato sottoscrittore si possa affermare anche sulla base del fatto che l'offesa del bene giuridico tutelato si sia realizzata sul proprio territorio;
- il terzo riguarda la **cooperazione internazionale** tra i Paesi sottoscrittori.

Le acquisizioni dell'ordinamento del Consiglio d'Europa sono rifluite anche nell'ambito dell'Unione europea. L'art. 83 TFUE (comma 1) – infatti – prevede che il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni. Tali sfere di criminalità comprendono – oltre, tra gli altri, al traffico illecito di stupefacenti e di armi, al riciclaggio di denaro, alla corruzione, alla criminalità organizzata - la criminalità informatica.

Per quanto concerne le politiche UE in materia di criminalità informatica si rinvia allo specifico capitolo della sezione terza di questo lavoro

2. Il contrasto alla criminalità informatica nell'ordinamento giuridico nazionale

Come in precedenza rilevato lo sviluppo della rete *internet* e di sempre nuovi prodotti tecnologici ha comportato cambiamenti rilevanti in ogni settore della vita umana, ha offerto molteplici opportunità di sviluppo, sul piano sociale, culturale ed economico, ma ha rappresentato anche un terreno fertile per nuove condotte di rilievo penale.

L'era di internet ha dunque aperto anche una nuova frontiera nella lotta alla criminalità, che può offrire innovativi strumenti e mezzi per la ricerca delle prove e, in generale, per il contrasto a gravi fenomeni criminosi. In questa costante evoluzione le manifestazioni criminose che si realizzano "in rete" hanno assunto nuove e differenti configurazioni, che trovano crescente rilievo offensivo ed allarmante impatto sociale e che necessitano di una risposta normativa.

In via preliminare è opportuno sottolineare che la "**criminalità informatica**" non consiste in una categoria definita giuridicamente, anche se compare in fonti europee e sovranazionali[22].

Si pensi alle Raccomandazioni n. R (89) 9 - sui profili di diritto penale sostanziale concernenti la lotta alla criminalità informatica - e n. R (95) 13, relativa ai problemi di procedura penale legati alla tecnologia dell'informazione, del Consiglio d'Europa; alla Convenzione del Consiglio d'Europa *Cybercrime* adottata a Budapest il 23 novembre 2001; al Trattato di Lisbona che ha inserito la "criminalità informatica" nell'art. 83 TFUE, fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale.

Sul piano del diritto penale sostanziale, sono ricondotti alla categoria della "criminalità informatica":

- **reati informatici in senso stretto**, cioè fattispecie penali che fanno dei procedimenti di automatizzazione di dati o informazioni ovvero degli oggetti e delle attività di carattere tecnologico elementi di tipizzazione dell'illecito. Si pensi, nel nostro ordinamento, all'accesso abusivo a sistemi informatici (art. 615-ter c.p.) o alla frode informatica (art. 640-ter c.p.). Questa categoria di reati informatici si connota per un nuovo oggetto passivo su cui la condotta va a cadere (quali i dati, le informazioni, i programmi od altri "prodotti" informatici o digitali, compresi i "sistemi informatici" in genere) oppure per il fatto che il computer ed i prodotti informatici in genere costituiscono lo strumento tipico di realizzazione del 'fatto' criminoso;
- **reati informatici in senso lato**, cioè tutte quelle fattispecie incriminatrici "comuni" che, pur non presentando espressamente elementi tipici caratterizzati dalla tecnologia, possono essere realizzate anche tramite la tecnologia, la rete o nel cyberspace. Si consideri, nel sistema italiano, la truffa

[22] In merito si vedano L. Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in Riv. trim. dir. pen. ec., 4, 2011, 827 e ss.; R. Flor, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet* (Relazione al convegno internazionale su "Lo sviluppo delle scienze penalistiche alle soglie del nuovo millennio", Tirana, 20-21 aprile 2012), in Diritto penale contemporaneo.it, 20 settembre 2012.

comune (art. 640 c.p.), che può essere commessa attraverso l'invio di email ingannevoli che inducono in errore il destinatario determinandolo ad effettuare un atto di disposizione patrimoniale su conti correnti *online*.

3. Interventi di diritto penale sostanziale

Nel nostro ordinamento, lo sviluppo di una normativa in materia di criminalità informatica è avvenuto senza un previo disegno sistematico, perché condizionato da contingenti necessità di tutela, cui il legislatore ha inteso via via far fronte, ovvero dall'urgenza di adeguarsi ad indicazioni e raccomandazioni di fonte sovranazionale.

Sulla spinta delle Raccomandazioni del Consiglio d'Europa il legislatore ha approvato la legge 23 dicembre 1993, n. 547 (Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica), con la quale ha novellato il codice penale introducendovi nuove fattispecie di reato e modificando le fattispecie esistenti con riferimento ai beni informatici. Ulteriori modifiche alla legislazione penale sono state poi apportate dalla legge 18 marzo 2008 n. 48, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001.

Dal combinato disposto delle due leggi si ricavano le seguenti innovazioni penali:

- in riferimento ai delitti contro l'amministrazione della giustizia, l'integrazione dell'art. 392 c.p., prevedendo che il reato di esercizio arbitrario delle proprie ragioni con violenza sulle cose comprenda anche una fattispecie di violenza sulle cose realizzata attraverso il **danneggiamento di software** o l'impedimento del funzionamento di un sistema informatico;
- l'inserimento fra i delitti di falso in atti l'art. **491-*bis***, che prevede l'applicazione delle pene previste dal codice anche quando i documenti falsificati sono documenti informatici pubblici aventi efficacia probatoria;

- l'inserimento, nel capo dedicato alla falsità personale, dell'art. 495-bis c.p., che punisce chiunque dichiara o attesta falsamente al certificatore - ovvero al soggetto che presta servizi di certificazione delle firme elettroniche - l'identità, lo stato o altre condizioni proprie o altrui;
- l'introduzione di nuove fattispecie penali, il cui bene giuridico tutelato è costituito sia dalla libertà individuale sia dalla tutela del bene patrimoniale costituto dal mezzo informatico. In particolare, l'art. 615-ter (Accesso abusivo ad un sistema informatico o telematico) sanziona chiunque si introduce abusivamente in un **sistema informatico o telematico protetto** o vi si mantiene contro la volontà espressa o tacita del titolare (la norma intende sanzionare i c.d. hackers); l'art. 615-quater (Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici) punisce l'appropriazione indebita delle parole chiave e dei codici segreti per accedere ai sistemi; l'art. 615-quinquies (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) punisce la diffusione dei c.d. virus informatici, ossia di programmi che diffusi nei sistemi informatici danneggiano irrimediabilmente i programmi residenti, i dati immagazzinati e i sistemi operativi;
- in riferimento all'inviolabilità dei segreti, la previsione che la fattispecie di violazione, **sottrazione e soppressione di corrispondenza** (art. 616 c.p.) si applica anche in riferimento alla **corrispondenza informatica**, quale la posta elettronica; l'applicabilità dell'art. 621 c.p., relativo alla rivelazione del contenuto di documenti segreti, anche quando i documenti segreti sono supporti informatici contenenti dati; l'introduzione, con l'art. 623-bis c.p., di una norma di chiusura, che stabilisce che le norme penali della sezione V del codice, relativa ai delitti contro l'inviolabilità dei segreti, si applicano anche ad ogni altra trasmissione a distanza di suoni, immagini o altri dati, con ciò precostituendo un sistema sanzionatorio penale adatto alle successive modificazioni tecnologiche;
- l'inserimento di tre nuove fattispecie di reato: l'intercettazione, impedimento, **interruzione illecita di comunicazioni**

informatiche o telematiche (art. 617-quater c.p.); l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) e la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-sexies c.p.);

- in riferimento ai delitti contro il patrimonio, l'introduzione di quattro fattispecie speciali di danneggiamento: le prime due (artt. 635-bis e 635-ter c.p.) relative al **danneggiamento di informazioni, dati e programmi informatici** anche utilizzati dallo Stato o comunque di pubblica utilità, e le seconde due (artt. 635-quater e 635-quinquies c.p.) relative al danneggiamento di sistemi informatici e telematici, anche di pubblica utilità;
- l'introduzione di due nuove fattispecie di frode: la **frode informatica** (art. 640-ter c.p.), nella quale il **sistema informatico** non è l'oggetto del reato, bensì lo strumento con il quale viene leso il patrimonio della vittima, e la frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

Inoltre, novità significativa introdotta dalla legge n. 48 del 2008, di ratifica della richiamata Convenzione di Budapest è rappresentata dall'estensione della **responsabilità amministrativa delle aziende** per una ampia serie di **reati informatici**.

Novellando il decreto legislativo n. 231 del 2001, in tema di responsabilità amministrativa delle persone giuridiche derivante da reato, la legge ha stabilito che qualora i delitti di **criminalità informatica** (491-bis, 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies, 640-quinquies) siano commessi nell'interesse della persona giuridica, quest'ultima è soggetta a **sanzioni amministrative pecuniarie e interdittive**.

Al di là di quanto previsto dalle leggi del 1993 e 2008, anche in interventi legislativi più recenti sono state introdotte modifiche al codice penale per consentire la punibilità di altre condotte realizzate

con il mezzo informatico. Si pensi, ad esempio, alle aggravanti dei delitti di addestramento ad attività con finalità di terrorismo anche internazionale, di istigazione a delinquere o di atti persecutori, quando i fatti siano commessi attraverso strumenti informatici o telematici (cfr. artt. 270-quinquies, 302 e 414 c.p., come modificati dal decreto-legge n. 5 del 2017 e art. 612-bis c.p., come modificato dal decreto-legge n. 93 del 2013).

Peraltro, le disposizioni contenute nel codice penale **non esauriscono** il quadro dei reati informatici: per completezza occorre infatti ricordare che ulteriori fattispecie sono previste dalla legislazione speciale. Si ricordano le disposizioni incriminatrici contenute nella legislazione in materia di tutela dei dati personali (D.Lgs. n. 196 del 2003), che puniscono la comunicazione e diffusione illecita di un archivio automatizzato contenente dati personali, oggetto di trattamento su larga scala (art. 167-bis) oppure la disciplina specifica in materia di tutela del diritto d'autore rispetto ai programmi per elaboratore (legge 22 aprile 1941, n. 633).

Resta tuttora da ratificare nel nostro ordinamento, invece, il Protocollo addizionale alla Convenzione del Consiglio d'Europa sulla **criminalità informatica** (entrato in vigore a livello internazionale il 1° marzo 2006) che mira a includere nel perimetro della Convenzione anche i reati legati alla propaganda a sfondo razzistico e xenofobo, consentendo in tal modo alle Parti di poter utilizzare gli strumenti della cooperazione internazionale stabiliti nella Convenzione anche per il contrasto di tali reati. In particolare, il Protocollo prevede che gli Stati parte definiscano come reato la diffusione o altre forme di messa a disposizione del pubblico per il tramite di un sistema informatico:

- di materiale razzista e xenofobico (articolo 3);
- di materiale che neghi, minimizzi in modo palese, approvi o giustifichi degli atti che costituiscano la fattispecie di genocidio o crimine contro l'umanità, come definiti dal diritto internazionale e riconosciuti come tali da una decisione definitiva del Tribunale militare internazionale o ogni altra corte internazionale (articolo 6).

4. Interventi di diritto processuale penale

L'innovazione-rivoluzione tecnologica offre anche **nuovi strumenti e mezzi per la ricerca delle prove**, e consente di perseguire altresì finalità di prevenzione dei reati.

Sempre attraverso le due leggi **del 1993 e del 2008**, il legislatore è allora intervenuto anche sulla procedura penale e, in particolare:

- modificando l'art. 51 del codice di procedura penale (comma 1-quinquies), ha attribuito la competenza per i reati di criminalità informatica alla procura distrettuale;
- è intervenuto sulla disciplina dei mezzi di ricerca della prova, novellando le disposizioni in tema di ispezioni (art. 244 c.p.p.) e perquisizioni (artt. 247, 248 e 352 c.p.p.) per specificare che l'autorità giudiziaria può disporre rilievi anche in relazione a sistemi informatici o telematici.

  In relazione ai sequestri, ha integrato la disciplina del sequestro di corrispondenza (art. 254 c.p.p., aggiungendo la corrispondenza inoltrata per via telematica) prevedendo anche il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni (art. 254-bis c.p.p.) ed ha disciplinato la custodia delle cose sequestrate (art. 259 c.p.p.) disponendo che se la custodia riguarda dati informatici il custode deve essere anche avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi;
- ha introdotto l'art. 266-bis c.p.p., che consente l'intercettazione di comunicazioni informatiche o telematiche negli stessi casi in cui il precedente art. 266 consente le intercettazioni telefoniche o di conversazioni, oltre ai casi in cui si perseguano reati informatici; ha modificato l'art. 268 c.p.p., precisando le modalità con le quali le intercettazioni possono essere eseguite; ha esteso la possibilità di intercettazioni preventive rispetto alla commissione di reati di criminalità organizzata, anche alle intercettazioni informatiche.

E' poi intervenuta la legge 15 **febbraio 2012**, n. 12 che, nel disciplinare nuove misure per il contrasto della criminalità informatica, ha modificato l'art. 240 c.**p. prevedendo la confisca obbligatoria dei beni e degli strumenti informatici** o telematici

che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati informatici. La legge, inoltre, prevede che tali beni sequestrati e poi confiscati siano destinati a particolari esigenze di ordine pubblico; sono, infatti, affidati all'autorità giudiziaria in custodia, con facoltà d'uso alle forze di polizia che li richiedano per l'impiego nel contrasto alla criminalità informatica ovvero ad altri organi dello Stato per finalità di giustizia.

5. Misure per la prevenzione e l'accertamento dei reati

La concreta esigenza di misure efficaci di contrasto a gravi forme di criminalità vale anche rispetto a reati "tradizionali", che trovano nelle nuove tecnologie un essenziale ausilio per la loro realizzazione. Si pensi solo alle attività preparatorie di attentati terroristici, che possono trovare in Internet un formidabile mezzo di comunicazione e di pianificazione degli attacchi, oppure alla lotta contro la diffusione di materiale pedopornografico online.

In questa direzione, alcune novità sul fronte della prevenzione dei reati e dei **mezzi di ricerca delle prove** sono state introdotte dal decreto-legge n. 7 del 2015, prevalentemente volto a contrastare il terrorismo internazionale.

Il provvedimento ha infatti modificato la disciplina delle norme di attuazione del codice processuale penale sulle intercettazioni preventive, anche in relazione ad indagini per delitti in materia di terrorismo commessi con l'impiego di tecnologie informatiche o telematiche, e con riguardo all'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico.

Ha demandato poi alla **polizia postale** e delle comunicazioni il compito di tenere aggiornata una ***black-list*** dei siti Internet che vengano utilizzati per la commissione di reati di terrorismo, anche al fine di favorire lo svolgimento delle indagini della polizia giudiziaria, effettuate anche **sottocopertura** ed ha introdotto in capo agli Internet providers specifici obblighi di **oscuramento dei siti** e di rimozione dei contenuti illeciti connessi a reati di terrorismo pubblicati sulla rete.

Sulla *black list* e sui provvedimenti di oscuramento e rimozione adottati, sono introdotti obblighi di relazione in capo al Ministro dell'interno in apposita sezione della Relazione annuale sull'attività delle forze di polizia e sullo stato dell'ordine e della sicurezza pubblica.

Il decreto-legge n. 7 del **2015** ha poi introdotto una deroga alla disciplina relativa **alla conservazione dei dati di traffico telefonico e telematico** contenuta nel Codice della privacy deroga originariamente temporanea e poi stabilizzata nell'ordinamento dalla legge n. 127 del 2017.

L'art. 132 del Codice della privacy, infatti, dispone che i dati relativi al traffico telefonico sono conservati dal fornitore per **24 mesi dalla data della comunicazione**, per finalità di accertamento e repressione di reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, **sono conservati dal fornitore per 12 mesi dalla data della comunicazione.** I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per 30 giorni.

Rispetto a questa disciplina l'art. 4-bis del decreto-legge n. 7 del 2015 ha stabilito che per finalità di accertamento e repressione dei reati di terrorismo, **fino al 30 giugno 2017**, il fornitore deve conservare i dati relativi al traffico telematico (esclusi i contenuti della comunicazione) ed i dati relativi al traffico telefonico. Analogamente, dovranno essere conservati, fino a tale data, anche i dati sulle chiamate senza risposta.

E' poi intervenuto l'art. 24 della **legge n. 167 del 2017** (Legge europea 2017) in base al quale, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione di tali reati il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, **è stabilito in 72 mesi**, in deroga a quanto previsto dall'articolo 132 del Codice della privacy.

L'esempio della ***data retention*** è emblematico di quanto le esigenze repressive e preventive di attività criminose che trovano nel *cyberspac*e l'ambiente esclusivo ed ideale di manifestazione ponga problemi in termini di bilanciamento con altri interessi contrapposti, a partire dai diritti fondamentali dell'individuo, quali il diritto all'integrità, sicurezza e riservatezza dei sistemi informatici ed il diritto all'autodeterminazione informativa, da elevare ad espressioni di "tradizionali" diritti fondamentali, in particolare da ricondurre alle manifestazioni dei diritti della personalità.

Parte seconda: Politiche di sicurezza e difesa cibernetica

LA DIFESA CIBERNETICA: IL QUADRO CAPACITIVO ATTUALE E I PROGETTI DI RAFFORZAMENTO

1. Le capacità cyber della Difesa

La Difesa italiana, al pari dei principali paesi della comunità internazionale, sta da tempo rafforzando le proprie **capacità militari** nel dominio cibernetico, sia attraverso apposite strutture di comando e controllo per lo svolgimento di operazioni nel *cyber space*, sia "studiando le **diverse sfaccettature** di tale dominio al fine di poter operare (…) in contesti interconnessi e/o federati, tenendo conto che evidentemente l'assenza di capacità in questo settore rappresenta la non possibilità di operare in modo credibile in un contesto interalleato"[23] .

L'estensione dei domini d'azione a quello cibernetico e dello spazio comporta infatti che a tali ambiti siano dedicate specifiche capacità operative difensive, al fine di preservare la sicurezza del "Sistema Paese" e di rafforzare la tenuta delle strutture politiche, economiche e sociali[24].

Al riguardo il Libro bianco per la difesa e la sicurezza internazionale 2015 descrive lo spazio cibernetico come un "dominio [...] che dovrà essere presidiato e difeso" e definisce particolarmente distruttivi possibili attacchi alle reti informatiche dei Paesi occidentali (…) idonei a produrre "effetti sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali" (punto 32).

A sua volta il Quadro strategico nazionale per la sicurezza dello spazio cibernetico attribuisce al Ministero della Difesa il compito di dotarsi della capacità di pianificare, condurre e sostenere operazioni nello spazio cibernetico e questo per prevenire, localizzare,

[23] Cfr. Audizione del capo di Stato maggiore della Difesa *pro tempore*, Generale Graziano, presso la Commissione difesa della Camera, seduta del 25 gennaio 2017

[24] Punto 103 del Libro bianco per la difesa e la sicurezza internazionale 2015 cit.

difendere, contrastare e neutralizzare le minacce e le azioni avversarie a danno dei sistemi e dei servizi della difesa, sia sul territorio nazionale, sia sui teatri operativi fuori dai confini nazionali, nel quadro delle missioni militari.

Nel dettaglio in base a quanto previsto nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico spetta al Ministero della Difesa definire e coordinare la politica militare, la *Governance* e le capacità militari nell'ambiente cibernetico; pianificare, condurre e sostenere operazioni (*Computer Network Operations* – CNO) nello spazio cibernetico atte a prevenire, localizzare, difendere (attivamente e in profondità), contrastare e neutralizzare ogni possibile minaccia e/o azione avversaria cibernetica, portata alle reti, ai sistemi ed ai servizi della Difesa sul territorio nazionale o nei teatri operativi fuori dai confini nazionali, nel quadro della propria missione istituzionale. In tale quadro, la Difesa negozia le intese e gli accordi internazionali di disciplina della materia, coordina le proprie attività nel settore cyber- militare con NATO, EU e le Difese di atri Paesi amici e alleati;

A sua volta il Piano nazionale per la protezione cibernetica ha previsto la realizzazione del Comando interforze per le operazioni cibernetiche (**CIOC**) deputato alla protezione dei sistemi e delle reti del Dicastero della Difesa, nonché all'effettuazione delle operazioni in campo cibernetico.

L'istituzione del CIOC e il conseguimento della specifica capacità di **condurre operazioni nel dominio cibernetico** rappresenta la principale iniziativa volta a rafforzare le capacità *cyber* della Difesa.

A tal proposito si ricorda che nell'ottobre 2018 la NATO ha annunciato l'istituzione a Mons, nell'ambito della struttura di Comando NATO, del *Cyberspace Operations Centre* (CYOC) che sarà pienamente operativo nel 2023.

Da collegare all'istituzione del CIOC la definizione di un apposito protocollo d'intesa attraverso il quale il Comparto intelligence e lo Stato Maggiore della Difesa hanno elaborato un quadro strategico e tattico allineato, tale da permettere il miglior posizionamento del costituendo CIOC con riguardo all'operatività nel dominio digitale anche alla luce dell'esperienze in corso di sedimentazione nell'Alleanza Atlantica.

2. Il Comando interforze per le operazioni cibernetiche e le computer network operations

Il Comando interforze per le operazioni cibernetiche (CIOC) è stato costituito nel 2017 con l'obiettivo di raggiungere la piena capacità operativa della struttura entro la fine del 2019.

Posto alle dirette dipendenze del Capo di Stato maggiore della Difesa il Comando, una volta raggiunta la piena capacità operatività, dovrà adempiere sia alla funzione di **protezione delle reti strategiche** e tattiche della Difesa dalle quali dipende l'esercizio della capacità di comando e controllo, sia sviluppare capacità di pianificazione e conduzione di ***computer network operations*** a supporto delle operazioni militari sia in Italia, che al di fuori dei confini nazionali.

Per quanto concerne la protezione delle reti la difesa si avvale di due tipi di dominio di rete: l'uno chiuso, per le informazioni classificate; e l'altro aperto, cioè in collegamento con la rete di pubblico accesso e con internet, per le informazioni non classificate. Le diverse Forze armate condividono la componente materiale dell'infrastruttura di rete (il *layer* fisico, ossia il supporto trasmissivo, la rete fisica). Le dorsali – formate dalla rete numerica nazionale e dai ponti radio – sono della difesa. La rete in fibra ottica è una delle più estese nell'ambito dalla pubblica amministrazione: 13.000 chilometri che coprono l'intero territorio nazionale, comprese le isole. Ogni Forza armata è poi organizzata col proprio dominio e ha la sua intranet. Le intranet di Forza armata e l'intranet dell'area di vertice interforze sono federate in una relazione di trust reciproca. Pertanto, i servizi vengono condivisi in maniera pienamente interoperabile, come se si trattasse di un'unica rete. Inoltre ogni Forza armata, ed anche l'Arma dei carabinieri, ha costituito un proprio CERT per la tutela dei rispettivi sistemi informatici, mentre la difesa nel suo insieme ha costituito un CERT difesa, che ha il compito di prevenire la minaccia cibernetica, rilevare le attività di natura malevola e reagire contro gli incidenti informatici che interessano il sistema della difesa nel suo insieme[25].

[25] I dati relativi alle reti della Difesa sopra riportati sono stati acquisiti nell'ambito Documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, cit. con particolare riferimento alle audizioni del Capo di Stato maggiore della Difesa, del Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa, e del Comandante del Centro *Intelligence* Interforze (CII), nonché Capo del Nucleo iniziale di formazione dell'allora costituendo Comando interforze per le operazioni cibernetiche (CIOC).

Il nucleo iniziale del CIOC è rappresentato dal **CERT Difesa** e dal ***Security Operation Center*** (SOC), strutture entrambe già esistenti in ambito Difesa (cfr. *supra).*

Su queste strutture la Difesa sta edificando la capacità di svolgere le *computer network operations* oltre alla predisposizione di poligoni virtuali per l'addestramento del personale alcuni dei quali giù operativi

Da un punto di vista teorico le *computer network operations* si articolano in operazioni di **difesa attiva** (*Computer network defence*), di **raccolta informativa** (*Computer network exploitation*) e di **attacco** (*Computer network attack*).

Nello specifico le ***Computer Network Defence*** (CND), consistono in azioni tese a proteggere le infrastrutture e gli assetti della Difesa da attività cibernetiche ostili. Questa attività si sostanzia nella difesa, analisi e sfruttamento dei dati. Le *Computer Network Exploitation* (CNE), sono azioni tese ad acquisire ed analizzare dati e informazioni contenute su computer e network d'interesse, al fine di ottenere un vantaggio. Le *Computer Network Attack* (CNA) sono azioni volte a rendere inaccessibili, degradare o distruggere informazioni contenute in un *computer* o in rete, oppure la rete di *computer* stessa degli avversari.

In relazione all'utilizzo di questa futura capacità il Ministro della Difesa *pro tempore,* in data 13 febbraio 2019, ha reso noto che la medesima "sarà implementata anche nei teatri operativi in cui sono impegnati i nostri contingenti, nell'ambito dei comandi militari delle forze proiettate, attraverso **Cellule operative cibernetiche** (Coc). Esse opereranno anche in sistema con il Cioc in madrepatria e garantiranno, da un lato, la protezione degli assetti militari, ormai sempre più digitalizzati e, dall'altro, la condotta delle possibili operazioni cibernetiche nell'area delle operazioni militari, secondo la missione istituzionale, le direttive operative e le regole d'ingaggio stabilite".

A questo riguardo, si segnala, inoltre, che a livello parlamentare, nelle diverse occasione in cui è stato illustrato l'avvio e lo sviluppo del "progetto CIOC", è stata sempre ribadita la necessaria riconducibilità di queste future operazione nell'alveo di precise

regole d'ingaggio che dovranno essere necessariamente definite in relazione allo sviluppo di questa nuova tipologia di operazioni militari[26], nel doveroso rispetto dell'ordinamento giuridico nazionale con particolare riferimento **all'articolo 11 della Costituzione** in forza del quale il nostro Paese ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo di risoluzione delle controversie internazionali.

Per quanto riguarda, invece, la realizzazione di **appositi ambienti virtuali** finalizzati allo sviluppo di capacità *cyber* è in via di completamento presso la scuola telecomunicazioni delle Forze Armate (STELTMIT) di Chiavari il *Cyber Range* "UNAVOX", piattaforma di addestramento degli operatori cibenetici militari che potrebbe essere resa disponibile quale laboratorio tecnico alle Università di settore. Il progetto prevede il completamento nel 2020 della fase di perfezionamento del dimostratore tecnologico "UNAVOX".

A sua volta il *Cyber Lab* sarà realizzato nella sede del Comando

strumenti necessari per studiare i *malware* e trovare i rimedi contro la minaccia, oltre a fornire supporto ai responsabili della progettazione, sviluppo e gestione delle reti, man mano che la minaccia viene identificata e neutralizzata.

In relazione a Centri specializzati si ricorda che in Estonia, a Tallin, ha sede il Centro di eccellenza NATO per la Difesa cibernetica (CCD CoE - NATO *Cooperative Cyber Defence Centre of Excellence)*, inaugurato il 14 maggio 2008. una struttura di ricerca e addestramento che si occupa di difesa cibernetica sotto l'aspetto educativo, di consulenza, di esperienze apprese, ricerca e sviluppo. Non fa parte della struttura di Comando NATO, ma certamente riveste un importante ruolo di sostegno. Il Centro di Tallin organizza, ogni anno, due esercitazioni: la *Crossed Swords*, evento riservato a personale tecnico dei *Red Team* e la *Locked Shields*.

[26] Cfr, Audizione del Capo di Stato maggiore della Difesa *pro tempore*, Generale Graziano, cit.; conf. Comandante del Comando Interforze per le Operazioni cibernetiche, Generale Vestito, Commissione difesa della Camera, seduta del 12 febbraio 2019.

La *Locked Shields*, in particolare, è la *flagship exercise* del Centro ed è la più complessa esercitazione *live-fire* (ovvero attacco-difesa in tempo reale) al mondo,
L'edizione del 2019, *Locked Shields* 2019 (LS19), si è conclusa nell'aprile 2019 e ha visto la partecipazione di oltre 1000 esperi di *cyber* difesa provenienti da 30 differenti nazioni. La simulazione, che vede la Nato assumere il ruolo di 'Blue Team', ha come obiettivo quello di valutare la preparazione dell'Alleanza atlantica sia nella risposta ad un attacco informatico esterno, sia per quanto concerne la capacità di mantenere attivi i servizi e difendere le reti vittime delle intrusioni.
La squadra italiana "Blue Team 22" era costituta da esperti informatici del Comando Interforze per le Operazioni Cibernetiche (CIOC), delle Forze Armate, del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAPIC), dell'Industria e delle Università, che insieme rispondono agli attacchi informatici virtuali.
La simulazione è stata vinta quest'anno dalla Francia.

3. Le linee di sviluppo capacitivo della Difesa cibernetica nel triennio 2019 – 2021

Il tema della Difesa cibernetica è trattato in diverse parti del documento programmatico pluriennale per la Difesa per il triennio 2019-2021 (Doc. CCXXXIV, n. 1).

Al riguardo, si ricorda che l'articolo 536 del Codice dell'ordinamento militare, ha previsto la presentazione annuale, entro la data del 30 aprile, di un piano di impiego pluriennale finalizzato a riassumere:

- il quadro generale delle esigenze operative delle Forze armate, comprensive degli indirizzi strategici e delle linee di sviluppo capacitive;
- l'elenco dei programmi d'armamento e di ricerca in corso ed il relativo piano di programmazione finanziaria, indicante le risorse assegnate a ciascuno dei programmi per un periodo non inferiore a tre anni, compresi i programmi di ricerca o di sviluppo finanziati nello stato di previsione del Ministero dello sviluppo economico. Nell'elenco sono altresì indicate le condizioni contrattuali, con particolare riguardo alle eventuali clausole penali;
- le spese relative alla funzione difesa, comprensive delle risorse assegnate da altri Ministeri.

Al riguardo, si dà conto del fatto che il crescente aumento della minaccia *cyber* nella complessità e nella frequenza degli attacchi e le conseguenti iniziative scaturite sia a livello internazionale, sia al livello nazionale, hanno spinto la Difesa a **migliorare** e rendere più efficiente gli aspetti connessi alla **sicurezza del *cyberspace***. In particolare, sono stati avviati una serie di programmi finalizzati alla resilienza, **protezione ed efficienza delle reti** e delle infrastrutture della Difesa e sono proseguiti i programmi già avviati nel 2017 volti a fornire alla componente CIOC, gli strumenti e gli assetti necessari a pianificare e condurre operazioni militari nel dominio cibernetico, garantire la *Cyber Situation Awareness*, addestrare il personale e gestire gli incidenti informatici attraverso il CERT Difesa.
Nello specifico, nell'ambito delle attività oggetto di potenziamento nel prossimo triennio si prevede la realizzazione di un **idoneo livello di sicurezza** a tutte le componenti che erogano servizi (sicurezza delle applicazioni); la **protezione delle postazioni** di lavoro, dei dispositivi in mobilita e dei dati in essi contenuti secondo criteri di confidenzialità, disponibilità e integrità (Protezione

dell'End Point); le attività rivolte alla **protezione delle reti** e in particolare alla riduzione del perimetro d'attacco (Protezione Perimetrale); l'**acquisizione** di **strumenti per visualizzare** e tenere sotto controllo **tutti gli eventi di sicurezza**; l'implementazione di un **sistema di *Governance* di sicurezza** unitaria secondo un modello che permetta, da un lato, una direzione centralizzata attraverso il CERT Difesa e dall'altro, l'esecuzione decentrata delle attività di *Cyber Defence* attraverso i SOC/CIRT Interforze e delle Forze armate.

Si segnala, infine che per quanto concerne il tema delle fornitura di servizi ICT alla Difesa il richiamato decreto legge n. 105 del 2019, in corso di conversione reca talune specifiche prescrizioni.
In via generale ai sensi del comma 6 dell'articolo 1 le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano **procedere all'affidamento di forniture** di beni, sistemi e **servizi ICT** destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici sono tenuti a dare comunicazione al Centro di valutazione e certificazione nazionale dell'intendimento di provvedere all'affidamento di tali forniture. Il CVCN sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, può, entro trenta giorni, imporre condizioni e test di hardware e software. In tale ipotesi, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.
Per le forniture di beni, **sistemi e servizi ICT** da impiegare su reti, sistemi informativi e servizi informatici del **Ministero della difesa**, il Ministero procede, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal decreto-legge all'esame, attraverso un **proprio Centro di valutazione** in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza.

I fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici individuati nell'elenco che deve essere trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico secondo quanto previsto dalla lettera b) del comma dell'articolo 1 del decreto legge, **assicurano** al CVCN e, limitatamente agli ambiti di specifica competenza, al **Centro di valutazione operante presso il Ministero della difesa**, la **propria collaborazione** per l'effettuazione delle attività di test, sostenendone gli oneri.

4. La sicurezza energetica nel settore della difesa

Le questioni energetiche hanno assunto particolare rilievo nel settore della Difesa che ha recentemente avviato il percorso verso la definizione della **Strategia Energetica della Difesa** in linea con i documenti programmatici nazionali in materia.

L'energia costituisce un aspetto estremamente vulnerabile per le capacità operative dello strumento militare, e ciò assume tanto più rilievo in considerazione della diffusione degli apparati e dei principi cardine della c.d. *Internet of Things* (IoT, cfr. Appendice) anche nel settore energetico e della conseguente accresciuta necessità di proteggere le infrastrutture critiche della Difesa dalle crescenti minacce di natura cibernetica.

Si ricorda al riguardo come sia attiva la Struttura di Progetto Energia, costituita a gennaio 2015 con decreto del Ministero della Difesa e potenziata a gennaio 2016.

Con il Decreto ministeriale dell'8 marzo 2018 e il relativo Decreto dirigenziale del 9 aprile 2018, la Struttura è stata ulteriormente confermata e riconfigurata per l'attuazione del Documento di Indirizzo Programmatico Strategico(DISP) e il sostegno all'adozione della Strategia Energetica della Difesa (SED).

In relazione al tema della sicurezza, il Ministro della Difesa *pro tempore*, in data 26 luglio 2018, in sede di illustrazione delle linee programmatiche del suo dicastero presso le Commissioni difesa congiunte della Camera e del Senato, ha osservato che il tema della sicurezza energetica "si pone come condizione basilare per garantire

la **sicurezza nazionale**. Nel medio e lungo termine la Difesa italiana mira al raggiungimento di elevate capacità di resilienza energetica, produzione e approvvigionamento da fonti sostenibili tali da assorbire e mitigare gli **effetti dovuti a eventuali attacchi** o a calamità e assicurare il mantenimento della capacità e della prontezza operativa dello strumento militare, sia in Patria che nei teatri operativi. In particolare, nel settore delle infrastrutture, a partire dai siti a valenza strategica, l'intento è la realizzazione di distretti energetici intelligenti (definiti *smart military district*) nei quali sia massimizzato il ricorso all'autoconsumo e la gestione dei flussi energetici avvenga in tempo reale in un alveo certo di ***cyber* security**.

In tale ambito la Difesa italiana potrà giocare un ruolo cruciale, anche a sostegno degli altri Dicasteri, con riferimento alla protezione delle infrastrutture critiche energetiche, sia come possibile entità istituzionale ospitante dei nodi di rilevanza strategica della rete di approvvigionamento/distribuzione, sia per il fattivo contributo alla difesa cibernetica del Paese, nell'ottica del consolidato paradigma del binomio *energy security-cyber security"*.

Proprio al fine di potenziare gli interventi e le dotazioni strumentali in materia di difesa cybernetica nonché rafforzare le capacità di resilienza energetica nazionale, la legge di bilancio 2019 (articolo 1, comma 227, legge n. 145/2018) **ha istituito**, nello stato di previsione del Ministero della difesa, **un Fondo**, con dotazione finanziaria di 1 milione di euro per ciascuno degli anni del triennio 2019 – 2021.

La ripartizione del Fondo tra i diversi interventi è operata con decreto del Ministro della Difesa, adottato di concerto con il Ministero dello sviluppo economico, da comunicare alle competenti commissioni competenti.

Ministero della Difesa
Struttura di Progetto Energia

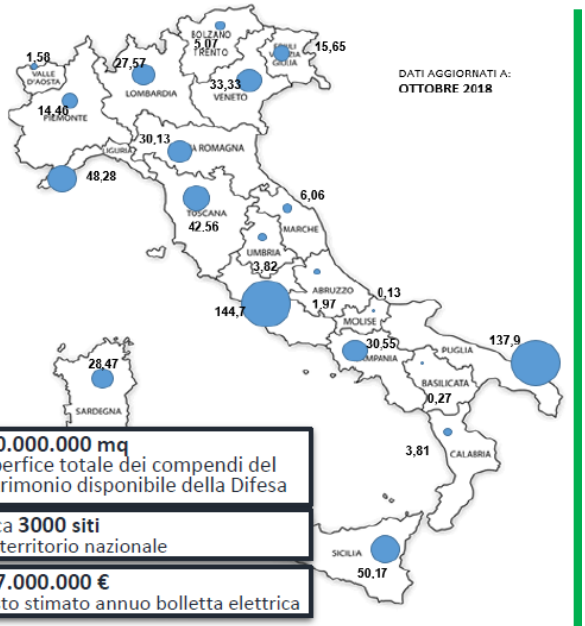
Profilazione energetica della Difesa

MINISTERO DELLA DIFESA		
CONSUMI ANNUI DI ENERGIA ELETTRICA (2017)		
ORD.	GWh	ENTE DIFESA
1	53,0	MARISTANAV TARANTO
2	37,0	MARINARSEN LA SPEZIA
4	20,2	MARINARSEN TARANTO
5	13,3	AEROPORTO MILITARE DI PRATICA DI MARE (ROMA)
3	12,0	MARINARSEN AUGUSTA (SR)
6	10,2	COMPRENSORIO CASTROPRETORIO AM (ROMA)
7	9,0	6° STORMO GHEDI (BS)
8	8,8	QUARTGENMARINA SANTA ROSA (ROMA)
9	8,5	4° STORMO GROSSETO
10	7,5	46ª BRIGATA AEREA PISA
11	7,3	AEROPORTO MILITARE DI CENTOCELLE (ROMA)
12	7,2	36° STORMO GIOIA DEL COLLE (BA)
13	6,7	32° STORMO AMENDOLA (FG)
14	6,6	PALAZZO ESERCITO (ROMA)
15	6,5	AEROPORTO MILITARE DI DECIMOMANNU (CA)
16	6,5	COMANDO OPERAZIONI AEREE POGGIO RENATICO (FE)
17	6,0	MARINARSEN BRINDISI
18	6,0	CII DIFESA
19	5,8	AEROPORTO MILITARE DI SIGONELLA (CT)
20	5,7	MARINARSEN MESSINA

	SMD-UGPPB SPESA PREV.* [M-€]	STIMA CONSUMO	U.M.
EN. ELETTRICA	127,8	632,90	GWh
GAS NATURALE	30,2	75,50	M-smc
GASOLIO RISCALD.	48,3	92,0	M-litri
ACQUA	30,7	12,29	M-mc
TOTALE	246,5		

*: FABBISOGNO PREVISIONALE 2016 [M€]

MINISTERO DELLA DIFESA - Struttura di Progetto Energia



760.000.000 mq
superfice totale dei compendi del patrimonio disponibile della Difesa

circa **3000 siti**
sul territorio nazionale

127.000.000 €
Costo stimato annuo bolletta elettrica

CONSUMI ELETTRICI DELLA DIFESA - Distribuzione geografica [GWh/anno]
Elaborazione dati da AU-SII (agg. Ottobre 2018) – Revisione in corso


Ministero della Difesa
Struttura di Progetto Energia
LE TAPPE DELLA STRATEGIA ENERGETICA
26/01/2015
Costituzione Struttura Progetto Energia
Attività prodromiche per lo sviluppo del Piano SED
19/04/2019
Adozione della SED
27/02/2017
Avvio fasi esecutive sviluppo e redazione del Piano SED
Nuova struttura di Governance
Attività strutturate in attuazione della SED
SPE
Resilienza energetica
Protezione delle infrastrutture Critiche energetiche
SPE
Efficientamento/Produzione/Consumi/ Contenimento della spesa/Recupero_situazione debitoria/ Data_collection/Gestione/ Contrattualistica/Visione strategica/Protocolli/ rapporti esterni/ Energy Security


Ministero della Difesa
Struttura di Progetto Energia
PNRM NEFERIS
Protezione ed efficienza delle Infrastrutture Strategiche della Difesa - Sistema Centrale di Monitoraggio e Controllo Performance Energetiche - Analisi Resilienza, sicurezza cyber e supporto decisionale per azioni proattive
OBIETTIVI DELLA PIATTAFORMA
• Monitoraggio energetico con allarmistica integrata di efficientamento e valutazione del rischio cyber
• Analisi predittiva dei consumi
• Supporto decisionale in linea per cambi di scenario energetico
• Valutazione in linea della resilienza
FASI PROGRAMMA
• Assessment di sicurezza cyber e resilienza energetica
• Progettazione, Realizzazione, Approntamento prototipo
• Monitoraggio, Definizione Interventi e Contromisure tramite lo strumento
PROTEZIONE CYBER
EFFICIENZA ENERGETICA
AWARENESS RESILIENZA
NEFERIS PORTAL
CYBER THREATS DETECTION
ENERGY EFFICIENCY MANAGEMENT
STATE & RESILIENCY AWARENESS
VULNERABILITIES & THREATS DETECION
CYBER ASSET PROTECTION
EFFICIENCY KPI & ALARMS
LOAD FORECASTING
DEMAND PLANNING
RESILIENCY KPIs & ALARMS
STATE MONITORING & DSS
IDS ANALYTIC ENGINES (NETWORK, PROTOCOLS)
RULES ENGINE
DATA SERIES CONSOLIDATION
BUILDING EFFICIENCY MODEL
RESILIENCE ESTIMATION
CONTROL NODES, NETWORK, PROTOCOL BASELINES
POWERFLOW MODEL
RESILIENCE ASSESSMENT MODELS
SCADA GUARDIANS
PROTOCOL ADAPTERS
IOT GATEWAY
SIMULATION OF EXTENDED SCENARIOES
Simulated Scenario
BMS EMS
Energy Sources
Energy Metering Devices
Energy Loads
Target System / Field

L'AMMINISTRAZIONE DIGITALE E LA SICUREZZA DEI DATI

1. Il processo di digitalizzazione delle pubbliche amministrazioni

Nell'ambito delle politiche di innovazione del settore pubblico un ruolo fondamentale è svolto dalla **digitalizzazione delle amministrazioni pubbliche**.

Per amministrazione digitale - o *eGovernment* – "si intende l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di **migliorare i servizi pubblici** e i processi democratici e di rafforzare il sostegno alle politiche pubbliche" (Commissione delle Comunità europee, Il ruolo dell'*eGovernment* per il futuro dell'Europa, 26 settembre 2003, p. 8).

In Italia il processo di informatizzazione della PA prende **avvio** negli anni '90 del secolo scorso con gli obiettivi di progettazione, sviluppo e gestione dei sistemi informativi automatizzati delle amministrazioni statali.

Successivamente, a tali finalità si affianca la semplificazione dei rapporti tra pubblica amministrazione e cittadino, fino a quando - con l'adozione del Codice dell'amministrazione digitale (CAD) nel 2005 - **si introduce** per la prima volta **la possibilità** per cittadini e imprese di **relazionarsi ufficialmente** con le pubbliche amministrazioni attraverso **tecnologie informatiche**.

Il CAD viene modificato più volte nel corso degli anni, fino alla riforma del 2016, finalizzata a rendere effettivi i diritti di **cittadinanza digitali** dei cittadini e delle imprese, attraverso l'introduzione di una Carta delle cittadinanza digitale (Camera dei deputati, Commissione parlamentare di inchiesta sul livello di digitalizzazione e innovazione delle pubbliche amministrazioni, Relazione sull'attività svolta, 26 ottobre 2017).

L'informatizzazione delle amministrazioni pubbliche è tra i temi centrali del dibattito pubblico anche negli ultimi anni, soprattutto al fine di dare piena attuazione all'Agenda digitale europea.

Nella Relazione 2018 del Team per la trasformazione digitale nella pubblica amministrazione si enucleano alcune

raccomandazioni rivolte al Governo per proseguire lungo la strada tracciata in sede di programmazione: le raccomandazioni riguardano in particolare la *governance*, le risorse, il *procurement* dei servizi tecnologici per la p.a.

Il Presidente del Consiglio dei ministri è la figura di coordinamento delle politiche di digitalizzazione della pubblica amministrazione. Nell'attuale Governo è stato nominato il Ministro senza portafoglio per l'innovazione tecnologica e la digitalizzazione (D.P.R 4 settembre 2019).

Presso la Presidenza del Consiglio è stato istituito il Dipartimento per la trasformazione digitale, struttura di supporto al Presidente del Consiglio per la promozione ed il coordinamento delle azioni di Governo finalizzate alla definizione di una strategia unitaria in materia di trasformazione digitale e di modernizzazione del Paese attraverso le tecnologie digitali (D.P.C.M. 19 giugno 2019).

L'Agenzia per l'Italia digitale (AGID) è l'organismo tecnico del Governo che ha il compito di garantire, sulla base degli indirizzi del Presidente del Consiglio, la realizzazione gli obiettivi dell'Agenda Digitale Italiana. Più in generale l'AGID promuove sia l'innovazione digitale del sistema Paese, sia la digitalizzazione delle pubbliche amministrazioni anche nel rapporto con cittadini e imprese.

Nel **marzo 2019** è stato approvato il Piano triennale per l'informatica nella pubblica amministrazione 2019-2021 che definisce le linee operative di sviluppo dell'informatica pubblica nei prossimi anni. Tra i requisiti strategici da soddisfare, viene considerato prioritario il principio del ***digital by default***, ovvero "digitale per definizione": le pubbliche amministrazioni devono fornire servizi digitali come opzione predefinita.

Nel confronto internazionale, l'Italia si colloca al 24° posto fra i 28 Stati membri dell'Unione europea nell'indice di digitalizzazione dell'economia e della società (Digital Economy & Society Index - DESI) della Commissione europea per il 2019 (era al 25° posto nel 2018).

Tuttavia, l'Italia è in buona posizione, sebbene ancora al di sotto della media dell'UE, in materia di connettività e servizi pubblici digitali (per quest'ultimo aspetto è 18esima nella classifica). Secondo il DESI (v. *supra*), i servizi pubblici online e *open data* sono prontamente disponibili e la diffusione dei servizi medici digitali è ben consolidata. La copertura a banda larga veloce e la diffusione del suo utilizzo sono in crescita (pur se quest'ultima rimane sotto la media), mentre sono ancora molto lenti i progressi nella connettività superveloce. L'Italia è a buon punto per quanto riguarda l'assegnazione dello spettro 5G.

2. La sicurezza informatica nel sistema informativo della p.a.

Il tema della **sicurezza informatica** della pubblica amministrazione riveste un'importanza fondamentale perché necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni del Sistema informativo della Pubblica amministrazione.

Essa è inoltre direttamente collegata ai principi di *privacy* previsti dall'ordinamento giuridico.

A livello nazionale la questione della sicurezza si pone in rilievo già nel documento Strategia per la crescita digitale 2014 – 2020 approvato dal Consiglio dei ministri nel marzo 2015.

In quella sede viene dato nuovo impulso al Progetto di *Digital Security* per la p.a. volto ad aumentare il livello di sicurezza delle informazioni e delle comunicazioni digitali per consentire nuovi livelli di servizi per i cittadini e le imprese. Il fine ultimo è di tutelare la *privacy*, l'integrità e la continuità dei servizi della p.a., vera e propria infrastruttura critica per il paese. In questo progetto rientra anche il CERT-PA.

Successivamente, il "Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione", punto di riferimento del Piano triennale per l'informatica 2017 – 2019, indica i requisiti strategici da soddisfare, tra cui l'adozione di un approccio architetturale basato sulla separazione dei livelli di *back end* e *front end*, con logiche aperte e standard pubblici che garantiscano ad altri

attori, pubblici e privati, accessibilità e massima interoperabilità di dati e servizi.

Secondo il modello strategico, tale architettura a più livelli - che assicuri la separazione tra *back end* e *front end* e permetta l'accesso ai *back end* solo in modo controllato e tramite API (*Application programming interface*) standard - costituisce un fattore di miglioramento della sicurezza del Sistema informativo della pubblica amministrazione.

Parallelamente alla definizione dell'impianto teorico della **gestione della sicurezza** dei sistemi informativi pubblici sopra brevemente delineato, si è proceduto all'implementazione pratica di tali principi, attraverso l'adozione di **linee guida** per la sicurezza ICT delle pubbliche amministrazioni, aventi lo scopo di fornire indicazioni sulle misure da adottare in ciascuna soggetto del sistema.

Tali misure tengono conto anche delle indicazioni generali in materia di sicurezza dello spazio cibernetico contenute, tra l'altro, nella direttiva del Presidente del Consiglio 1° agosto 2019.

In questo contesto si inseriscono le Misure minime di sicurezza ICT per le pubbliche amministrazioni e le Linee guida per lo sviluppo del software sicuro nella pubblica amministrazione, entrambe adottate dall'AgID nel 2017.

Le misure minime di sicurezza ICT, che devono essere adottate da parte di tutte le pubbliche amministrazioni entro il 31 dicembre 2017, sono uno strumento pratico per valutare e **migliorare il livello di sicurezza informatica** delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle amministrazioni per valutare il proprio livello di sicurezza informatica.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'amministrazione, le **misure minime** possono essere implementate in modo graduale seguendo tre livelli di attuazione.

- **minimo:** è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere conforme;
- ***standard***: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della pubblica amministrazione italiana;
- **avanzato**: è il livello che essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

A **livello più evoluto**, le linee guida per lo sviluppo del *software* sicuro hanno l'obiettivo di pervenire a un'architettura della sicurezza per servizi, sia critici sia non critici, che definisca i **principi e le linee guida del modello architetturale** di gestione dei servizi e contestualizzazione rispetto al *cluster* dei dati gestiti.

Le linee guida contengono quattro allegati tecnici relativi alle seguenti tematiche:

- ciclo di sviluppo di *software* sicuro;
- sviluppo sicuro di codice
- sicurezza del *software* di base
- modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del *Secure/Privacy by Design*.

3. La sicurezza informatica e il Piano triennale 2019-2021

Il **Piano triennale per l'informatic**a nella pubblica amministrazione fissa gli obiettivi e individua i principali interventi di **sviluppo e gestione die sistemi informativi** delle p.a. (art. 14-bis CAD).

Il Piano è redatto dall'AgID, che ne cura anche la verifica dell'attuazione, e approvato dal Presidente del Consiglio, o dal ministro delegato per l'informatizzazione.

Nel marzo 2019 è stato varato il **Piano triennale 2019-2021**, che prosegue e integra le linee di azione del Piano 2017-2019 in un quadro di collaborazione con tutti gli interlocutori.

Le principali novità del Piano riguardano:

- il recepimento delle modifiche introdotte del Codice dell'amministrazione digitale (CAD) e delle direttive e regolamenti europei sull'innovazione digitale;
- il **rafforzamento del paradigma *cloud* della PA** con l'applicazione del principio *cloud first* (cfr. *infra*);
- la definizione di modelli e strumenti per l'innovazione per la PA con un'attenzione ai temi dell'*open innovation* e al paradigma *smart landscape*;
- un maggiore risalto al ruolo delle amministrazioni territoriali, che saranno accompagnate nel loro percorso di trasformazione digitale, attraverso la condivisione di strategie e piani operativi, ma anche di buone pratiche già adottate che aiutino a colmare rapidamente il divario digitale tra i diversi territori del Paese;
- la condivisione con le amministrazioni degli strumenti di monitoraggio delle azioni;
- il rafforzamento del tema delle competenze manageriali e digitali all'interno delle pubbliche amministrazioni, con iniziative concrete di sensibilizzazione e formazione;
- l'adozione di una nuova chiave di lettura delle linee d'azione, che individua le aree di intervento e l'impatto su cittadini, imprese e pubbliche amministrazioni.

La **strategia della trasformazione digitale** della pubblica amministrazione contenuta nel Piano triennale è coerente con il Piano di azione europeo sull'eGovernment 2016-2020, in riferimento al quale gli Stati membri sono impegnati a definire le proprie politiche interne sulla base di alcuni principi chiave tra cui il principio di "fiducia e sicurezza", secondo il quale sin dalla fase di progettazione devono essere integrati i profili relativi alla **protezione dei dati personali**, alla tutela della vita privata e alla sicurezza informatica.

L'esperienza condotta nel corso degli anni 2017-2018 e l'evoluzione dei progetti indicati nel Piano 2017 - 2019 porta, nel Piano Triennale 2019 - 2021, ad un aggiornamento del Modello strategico. Esso fornisce una definizione di sicurezza informatica, la quale comprende "le attività per la regolazione e regolamentazione della *cybersecurity* nella PA per l'*Assessment test* e il CERT-PA quale strumento operativo per supportare l'adozione dei corretti livelli di sicurezza presso la Pubblica Amministrazione. Sono inoltre identificati tutti gli altri aspetti che concorrono a rendere sicuri e affidabili i sistemi informatici, nonché le attività di indirizzo e la strumentazione correlata agli adempimenti per il rispetto della riservatezza (*privacy*)" (Piano triennale 2019-2021, pag. 16).

Come si è anticipato sopra, uno dei princìpi che ispirano il nuovo Piano triennale è quello del c.d. ***cloud first***, secondo il quale le pubbliche amministrazioni per la definizione di nuovi progetti e per la progettazione dei nuovi servizi, devono, in via prioritaria, adottare il paradigma *cloud* e in particolare i servizi SaaS (*software as a service)*, prima di qualsiasi altra opzione tecnologica, in coerenza con il modello *cloud* della PA e le linee guida su acquisizione e riuso di *software* per le pubbliche amministrazioni (Piano triennale 2019.2021, pag. 46).

L'utilizzo del ***cloud*** da parte delle p.a. pone sicuramente come **centrale la questione della sicurezza**.

Infatti, da un lato, il modello ***cloud*** viene incontro alle esigenze di sicurezza dei trattamenti dei dati delle pubbliche amministrazioni, facilitando la separazione delle problematiche di sicurezza per l'infrastruttura fisica, per il *software* e per la gestione logica delle applicazioni. Inoltre, le applicazioni *cloud* sono in grado di mettere a disposizione dell'amministratore strumenti di *auditing* e controllo delle informazioni che consentono interventi puntuali all'insorgere di eventuali problemi.

Tuttavia, la soluzione del *cloud* non è sufficiente per assicurare la *privacy* ai propri utenti e la sicurezza delle infrastrutture e servizi IT. È necessario un processo continuo di vigilanza e controllo che fin dalla prima fase di progettazione dei servizi, agisca trasversalmente su tutte le aree di interesse, e che sia costantemente aggiornato

rispetto allo stato dell'arte delle principali misure di sicurezza (Il Cloud della Pubblica Amministrazione, 15 luglio 2019, paragrafo 2.5: *Sicurezza e* Privacy).

Il Piano triennale affronta in modo sistematico il problema della **sicurezza informatica** nel Capitolo 8 (pag. 129 e seguenti).

Partendo dalla constatazione che il presente momento storico vede "la minaccia cibernetica crescere continuamente in quantità e qualità" e che i servizi informatici erogati dalla pubblica amministrazione "diventano sempre più cruciali per il funzionamento del sistema Paese", il Piano attribuisce alla sicurezza informatica un ruolo fondamentale in quanto può garantire "non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della pubblica amministrazione, ma anche la resilienza della complessa macchina amministrativa. Essa è inoltre direttamente collegata ai principi di *privacy* previsti dall'ordinamento giuridico".

Il Piano Triennale individua alcuni interventi per **aumentare** il **livello di sicurezza** complessivo dell'amministrazione. Tra questi, in primo luogo, la razionalizzazione delle risorse ICT. La razionalizzazione è al centro dell'analisi dell'architettura infrastrutturale dell'informatica della p.a., trattata nel Capitolo 3 del Piano, è viene declinata in tre settori: *Cloud* della p.a., *data center* e connettività.

La razionalizzazione permette di ridurre la "superficie" esposta agli **attacchi informatici**, uno degli aspetti di maggiore criticità: "Solo riducendo la superficie di attacco si può pensare id gestire in modo efficace la sicurezza di una infrastruttura nazionale. Questo oggi si può fare attraverso appropriati *data center*, per esempio dislocati su base regionale, che possono portare anche ingenti risparmi all'erario pubblico" (2014 Italian Cyber Security Report, dicembre 2015. p. 3. In proposito si veda anche il Rapporto Clusit 2018 sulla sicurezza ICT in Italia).

Un altro aspetto di criticità evidenziato dal Piano triennale risiede nella "mancanza nelle pubbliche amministrazioni della consapevolezza sulla minaccia e l'assenza di strutture organizzative locali in grado di operare efficacemente un'attività di preparazione e risposta agli incidenti". Le misure di risposta a tale criticità

consistono nell'attività di *awareness* condotta dal CERT-PA e nella pubblicazione da parte dell'AgID di documenti di indirizzo ed operativi (linee guida, regole tecniche) finalizzati ad accrescere la consapevolezza e la capacità di difesa delle amministrazioni interessate.

Nel dettaglio, il Piano triennale individua i seguenti obbiettivi prioritari per il miglioramento della sicurezza:

- definire i **profili di sicurezza** dei componenti ICT della pubblica amministrazione e fornire i riferimenti tecnici e normativi che le pubbliche amministrazioni dovranno adottare. La mancata attuazione dei profili di sicurezza potrebbe comportare, proporzionalmente al tipo di inadempimento, anche la necessità di interrompere l'erogazione dei servizi connessi;
- offrire alle pubbliche amministrazioni supporto alla prevenzione e al trattamento degli **incidenti di sicurezza** informatica;
- provvedere a effettuare *assessment* e **verifiche di sicurezza** onde accertare l'applicazione delle regole di sicurezza informatica individuate da parte delle pubbliche amministrazioni;
- elaborare e pubblicare un modello organizzativo standard per la realizzazione di "CERT di prossimità", ossia CERT di secondo livello sia "orizzontali" (territoriali) che "verticali" (tematici o di settore), il quale costituirà il riferimento normativo per la eventuale costituzione di tali strutture aventi funzione di **snodo tra il CERT-PA** e le amministrazioni locali;
- elaborare e pubblicare lo standard nazionale per **l'interscambio automatizzato** tra operatori accreditati (CERT, strutture di sicurezza) di informazioni di sicurezza e indicatori di compromissione qualificati mediante protocolli STIX e TAXII, utilizzando piattaforme per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di **sicurezza informatica e minacce relative all'analisi** degli **incidenti** di sicurezza informatica e all'analisi del *malware*, e adottando la tassonomia specificamente definita;

- potenziare ulteriormente il *National Vulnerability Database* e i relativi strumenti informativi a supporto, mettendo a disposizione delle amministrazioni e dei ricercatori funzionalità più estese per il supporto all'analisi ed alle ricerche.

Il Piano triennale **non esamina** le possibili ricadute in materia di sicurezza di nuove tecnologie quali ***blockchain*** **e intelligenza artificiale** (cfr. Appendice), ma prevede che esse potranno essere approfondite nella prossima edizione del Piano alla luce delle attività avviate e che diventeranno parte integrante dell'intera strategia di trasformazione digitale della p.a.

LA SICUREZZA CIBERNETICA DEL SISTEMA FINANZIARIO E IL RUOLO DELLE AUTORITÀ DI SETTORE

1. La sicurezza cibernetica del sistema finanziario

Il settore finanziario, data la centralità nel sistema produttivo, rappresenta un **obiettivo primario** sia per attacchi motivati dalla ricerca del profitto, sia per quelli rivolti a compromettere l'ordinato funzionamento del sistema economico. Tale settore risulta quindi **tra i più esposti** ad aggressioni cibernetiche anche in considerazione dell'uso intensivo di tecnologie informatiche da parte dell'industria finanziaria; si pensi a tale proposito al recente sviluppo delle nuove forme di intermediazione bancaria, finanziaria e assicurativa *online* (FinTech).

Con il **termine FinTech** si faceva in origine riferimento alle applicazioni informatiche a supporto dell'attività di banche e imprese di investimento. Col tempo, invece, la definizione si è allargata a una grande varietà di servizi e tecnologie per le imprese e i privati, includendo un insieme di innovazioni relative a prodotti e servizi bancari, finanziari e assicurativi: pagamenti elettronici (*cashless*), piattaforme *on-line* per il prestito fra privati (*peer-to-peer lending*) o per l'investimento in progetti innovativi (*crowdfunding*), negoziazione automatizzata (*algo-trading*), consulenza automatizzata (*robo-advice*) e nuovi sistemi di gestione dei rischi assicurativi (*InsurTech*), per citare i più diffusi.

Per una panoramica dettagliata sulle nuove forme digitali di intermediazione bancaria, finanziaria e assicurativa si consiglia la lettura del tema *web* Fintech realizzato dal Servizio Studi-Dipartimento Finanze della Camera dei deputati nonché del documento Lo sviluppo del FinTech della Consob.

Gli attacchi al sistema finanziario sono talvolta condotti con **metodi molto semplici**, come il **furto di credenziali** di accesso ai conti mediante il *phishing*, o il *denial of service* (DDoS cfr. Appendice), che, sovraccaricando i *server* con milioni di richieste simultanee di dati, **rende inutilizzabili i servizi bancari** erogati via rete. Altre volte le intrusioni sono condotte con metodi complessi e portano alla sottrazione di fondi o di dati su larga scala.

Nella Relazione Annuale per il 2017 della Banca d'Italia (Sezione monografica-Il rischio cibernetico nell'economia italiana) si rappresenta che nel 2017 la diffusione dei due *virus* informatici WannaCry (un programma che blocca il funzionamento di un

computer cifrando i dati per poi chiedere un riscatto, *ransomware*, in Bitcoin per decifrarli) e NotPetya (*software* che cifra i dati ma non dà la possibilità di decifrarli, di fatto distruggendo i contenuti dei dispositivi colpiti) ha causato **danni economici** a imprese e istituzioni pubbliche valutabili in centinaia di milioni di dollari, colpendo tra gli altri il British National Health Service, il gigante danese del trasporto marittimo Moller-Maersk e la multinazionale farmaceutica Reckitt Benckiser. Tra il 2016 e il 2017 ulteriori aggressioni informatiche sono state rivolte contro istituzioni finanziarie connesse con il sistema dei pagamenti interbancari attraverso la rete SWIFT (rete che connette più di 11.000 soggetti finanziari in oltre 200 Paesi) determinando la sottrazione di ingenti somme di denaro e coinvolgendo anche alcune banche centrali, come quella del Bangladesh, a cui sono stati sottratti circa 80 milioni di dollari.

La **difesa del sistema finanziario**, pertanto, risulta assai complessa e il settore, in **quanto interconnesso a livello globale**, sembra orientato verso una politica di forte **cooperazione internazionale**, anche al fine della condivisione delle informazioni sugli attacchi (*information sharing*).

In questa direzione, i modelli prevalenti di condivisione a livello internazionale ed europeo dell'informazione sugli incidenti informatici sono due: gli ***information sharing and analysis centers*** (ISAC), che sono piattaforme che abilitano i partecipanti a condividere informazioni e analisi, ma non prevedono attività operative di risposta congiunta; i **CERT** - *computer emergency response team* e i **CSIRT** - *computer security incident response team*, che consentono sia la condivisione delle informazioni che un rapido coordinamento nella risposta a eventuali incidenti.

La **cooperazione internazionale in materia di sicurezza cibernetica** del **settore finanziario** ha luogo in una **molteplicità di sedi** in quanto riflette lo stratificarsi di competenze settoriali e nazionali. Come ricordato nella relazione della Banca d'Italia precedentemente richiamata, per quanto riguarda le infrastrutture di mercato e i sistemi di pagamento, il principale *forum* è costituito dal Comitato sui sistemi di pagamento e sulle infrastrutture di mercato (*Committee on Payments and Market Infrastructures*, CPMI) della Banca dei regolamenti internazionali (BRI); in tema di vigilanza sono rilevanti il Consiglio per la stabilità finanziaria (*Financial Stability Board*, FSB) e il Comitato di Basilea per la vigilanza bancaria (*Basel Committee for Banking Supervision*, BCBS) della BRI. Un ruolo importante è svolto anche dal **G7** in

particolare dal ***Cyber Expert Group*** **del G7 finanziario** (G7-CEG), che è impegnato nella definizione di un protocollo di cooperazione internazionale tra autorità per la risposta a incidenti transfrontalieri.

Nell'ambito dell'Unione europea il **Comitato europeo per il rischio sistemico** (*European Systemic Risk Board*, ESRB) garantisce un raccordo di alto livello ai fini della stabilità finanziaria tra la Commissione europea, le autorità di settore europee, l'Eurosistema e le autorità macroprudenziali nazionali. All'interno dell'ESRB è istituito lo *European Cyber Risk Group*, che **analizza i potenziali impatti sistemici** degli attacchi cibernetici con particolare riferimento all'economia europea. Il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 Cybersecurity Act ha rafforzato il ruolo dell'Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Network and Information Security* — ENISA) assegnandole il compito di aiutare gli Stati membri a proteggersi dalle incursioni *hacker* e di stilare le nuove linee guida per le certificazioni europee.

Per quanto riguarda la **vigilanza bancaria**, l'EBA (*European Banking Authority* - Autorità indipendente dell'Unione europea che opera per assicurare un livello di regolamentazione e di vigilanza prudenziale efficace e uniforme nel settore bancario europeo) ha emanato **linee guida per le autorità di vigilanza** sulla valutazione del rischio informatico e raccomandazioni sull'esternalizzazione dei servizi di *cloud computing*, definendo anche requisiti di sicurezza per i prestatori di servizi di pagamento e regole di supervisione armonizzate. Nell'Eurosistema il rispetto di questi requisiti da parte delle banche significative è verificato dal **Meccanismo di vigilanza unico** (*Single Supervisory Mechanism*, SSM), che raccoglie anche le segnalazioni di incidenti cibernetici subiti e ha costituito una un'apposita *task force* (*Cyber Crisis Group*) per gestire eventuali crisi. In funzione di specifici indicatori di rischio derivanti da segnalazioni di incidenti o da debolezze riscontrate nell'attività di vigilanza cartolare, l'SSM avvia ispezioni dedicate all'analisi del rischio cibernetico.

Con riferimento ai sistemi di pagamento, il gruppo di lavoro sulla **resilienza cibernetica** (*cyber resilience)* delle infrastrutture finanziarie della BRI è impegnato a monitorare l'applicazione della Cyber *guidance* del CPMI-Iosco e a diffonderla oltre i Paesi del G20. In ambito CPMI è stata inoltre definita una **strategia per la sicurezza dei pagamenti all'ingrosso**, elaborata in seguito ad alcuni casi gravi di frodi cibernetiche. Nel 2017 la Banca centrale europea ha approvato la strategia di supervisione per la *cyber resilience* delle infrastrutture di mercato e di pagamento europee con l'obiettivo di armonizzare il recepimento della *Cyber guidance*, rafforzare le capacità di risposta agli attacchi delle singole istituzioni finanziarie e dei loro *provider* e promuovere la cooperazione pubblico-privato; a quest'ultimo scopo ha costituito un *forum* (*European Cyber Resilience Board*).

2. Il ruolo delle autorità di settore

La Banca d'Italia svolge un **ruolo centrale** per garantire la **sicurezza informatica** del sistema finanziario. In passato questa funzione si manifestava principalmente attraverso il presidio dei rischi operativi e della continuità di servizio (***business continuity***).

A tal fine la Banca presiede il Comitato per la continuità di servizio della piazza finanziaria italiana (Codise), istituito nel 2003 per gestire il coordinamento delle eventuali crisi operative della piazza stessa. Al Comitato partecipano gli operatori del settore finanziario rilevanti sul piano sistemico e la Consob. Il Codise svolge periodicamente **simulazioni di crisi a scopo** di esercitazione; già nel 2008 queste contemplavano l'eventualità di attacchi informatici.

Con lo svilupparsi della tecnologia e la proliferazione degli attacchi, alla tematica della continuità operativa se ne sono aggiunte altre.

Attualmente, in quanto **autorità di sorveglianza** sul sistema dei pagamenti e di supervisione sulle altre infrastrutture di mercato, l'Istituto persegue l'obiettivo **dell'innalzamento della resilienza cibernetica delle infrastrutture** del mercato finanziario. Esponenti della Banca, quindi, hanno partecipato alla stesura delle principali linee guida internazionali e seguono lo sviluppo della strategia dell'Eurosistema. Nell'ambito della sorveglianza cooperativa su SWIFT, la Banca d'Italia collabora al monitoraggio del *Customer Security Programme* (SWIFT-CSP), che consiste in una serie di requisiti e controlli di sicurezza richiesti agli utenti a seguito dei recenti attacchi informatici su scala globale. In qualità di autorità di vigilanza sul sistema bancario e finanziario in ambito nazionale, ha introdotto requisiti specifici per la gestione dei sistemi informativi delle banche con la revisione della circolare 285/2013 (Disposizioni di vigilanza 31 per le banche). L'Istituto partecipa inoltre alla redazione delle linee guida dell'EBA sulla sicurezza informatica per gli intermediari bancari e finanziari. A livello internazionale, nell'ambito del *Senior Supervisory Group* e del Comitato di Basilea per la vigilanza bancaria, collabora alla definizione delle migliori prassi sulla sicurezza cibernetica.

Inoltre, come descritto nel documento Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass, redatto a cura del Gruppo di coordinamento sulla sicurezza cibernetica (gruppo che riunisce esperti di informatica, di vigilanza sugli intermediari bancari, finanziari e assicurativi e di sorveglianza sul sistema di pagamenti e di ricerca economica), la Banca d'Italia in materia di sicurezza cibernetica del sistema finanziario:

- è gestore di infrastruttura critica informatizzata di interesse nazionale, come definita dal DM 9 gennaio 2008 del Ministero dell'Interno. In questa veste

collabora al contrasto delle minacce cibernetiche con il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) del Servizio centrale della Polizia postale e delle comunicazioni;
- eroga servizi digitali a favore dell'Eurosistema (ad esempio mediante le piattaforme del sistema di pagamento TARGET2 e TARGET2-Securities) e servizi a favore di enti governativi nazionali quali la tesoreria dello Stato, le aste del debito pubblico, il Sistema informativo delle operazioni degli enti pubblici (Siope);
- è titolare del trattamento di dati personali in formato elettronico ai sensi del regolamento GDPR.

Nel Piano Strategico 2017-2019 la Banca d'Italia ha precisato che, al fine di rafforzare la *cyber security* in relazione ai nuovi scenari di rischio, l'Istituto prende iniziative volte a costituire e sviluppare le attività del ***Computer Emergency Response Team*** (CERT) della Banca d'Italia fornendo il supporto tecnico e operativo al CERTFin; ad analizzare l'esposizione dei processi di *business* alle minacce di attacchi informatici, individuando opportune modalità di risposta; a sviluppare, adeguare e gestire architetture informatiche resilienti coerenti con i *framework* internazionali.

Si ricorda che il CERTFin – CERT Finanziario Italiano – è un'iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione dei rischi *cyber* degli operatori bancari e finanziari e la *cyber resilience* del sistema finanziario italiano attraverso il supporto operativo e strategico alle attività di prevenzione, preparazione e risposta agli attacchi informatici e agli incidenti di sicurezza. In linea con la strategia nazionale in tema di *cyber security*, il CERTFin svolge le proprie attività in coerenza con tutte le altre iniziative istituzionali avviate nel Paese in tema di sicurezza cibernetica e protezione delle infrastrutture critiche, ampliando ulteriormente la rete di interlocutori istituzionali e di esperti a livello nazionale e internazionale. Le linee di indirizzo sono affidate al lavoro di un comitato strategico ai vertici del quale troviamo la Banca d'Italia e l'ABI; i vari servizi sono invece coordinati da un comparto gestito direttamente dal Consorzio ABI Lab. IVASS e ANIA hanno aderito nel dicembre 2018 al CERTFin e partecipano negli organi direttivi in rappresentanza del settore assicurativo. I servizi sono messi a disposizione dei partecipanti su base cooperativa, grazie al coinvolgimento degli operatori finanziari italiani. Il CERTFin eroga servizi qualificati di sicurezza informatica a beneficio dei propri aderenti attraverso lo svolgimento delle funzioni di: centro per l'analisi e la condivisione delle informazioni (FinISAC); Osservatorio *Cyber Knowledge and Security Awareness*; centrale operativa per la gestione delle emergenze *cyber*. Inoltre, il CERTFin collabora con un'ampia comunità di soggetti pubblici e privati e si configura come punto di raccordo del settore finanziario con gli altri settori strategici in tema di *cyber security*.

Dal 2016 la Banca d'Italia raccoglie inoltre i **dati sul rischio cibernetico** nel sistema produttivo italiano analizzando gli investimenti in sicurezza informatica delle imprese, l'incidenza e l'impatto economico degli attacchi, nonché il ricorso alle assicurazioni specializzate contro i rischi *cyber*.

Va ricordato che in **tema di sicurezza delle reti** e dei sistemi informativi è intervenuta la direttiva UE/2016/1148 (*Directive on Security of Network and Information Systems*, NIS) che ha previsto che gli Stati membri si dotino di un'organizzazione nazionale in grado di vincolare a stringenti misure di protezione i maggiori operatori di servizi essenziali per l'economia (la direttiva ha introdotto, tra l'altro, a carico di questi operatori un obbligo di notifica alle autorità degli incidenti con effetti negativi rilevanti). Il decreto legislativo n. 65 del 2018 che recepisce la direttiva richiamata individua come autorità competente NIS **per il settore bancario** e delle infrastrutture dei mercati finanziari **il Ministero dell'Economia e delle finanze**. Al Mef, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, spetta il controllo dell'applicazione della direttiva a livello nazionale.

La Consob, oltre al richiamato ruolo di collaborazione con il MEF e la Banca d'Italia, nella sua attività di regolamentazione e di vigilanza sui mercati finanziari, svolge un ruolo fondamentale nel rafforzare la sicurezza informatica per contrastare i rischi di *cybercrime* e migliorare gli strumenti tecnologici per la gestione e la condivisione dei dati e delle informazioni.

Come riportato nel Piano strategico 2019-2021 l'Istituto intende ampliare il presidio sulle politiche e sul governo della sicurezza informatica in particolare potenziando il gruppo interno di specialisti in materia, incrementando l'impegno nelle attività operative (es.monitoraggio, verifiche di sicurezza), anche mediante l'affidamento a un *partner* esterno particolarmente qualificato in materia, sviluppando il *networking* con le altre autorità nei comitati internazionali e con le organizzazioni incaricate di raccogliere le segnalazioni di incidenti informatici e vulnerabilità (Polizia Postale e *Computer Emergency Response Team*, CERT). In questa direzione recentemente (3 giugno 2019) è stato siglato un accordo tra Consob e Polizia di Stato per la prevenzione e il contrasto dei crimini

informatici, basato sulla condivisione informativa e sulla cooperazione operativa.

L'Ivass sin dal 2014 monitora lo stato di **esposizione al rischio cibernetico** del comparto assicurativo, anche attraverso un questionario nell'ambito delle rilevazioni trimestrali delle vulnerabilità e dei rischi delle imprese e mediante indagini sulla sicurezza di agenti e *broker*. In linea con l'evoluzione regolamentare e del contesto operativo del settore assicurativo, l'Istituto è impegnato nella revisione della normativa di riferimento per imprese e intermediari. In questa direzione, nel luglio 2018, è stato emanato il nuovo regolamento sul governo societario delle imprese e dei gruppi assicurativi, che disciplina anche i presìdi in materia di rischio cibernetico nell'ambito delle regole sulla *governance* aziendale.

L'Ivass ha inoltre avviato, in collaborazione con la Banca d'Italia, iniziative per monitorare l'esposizione al rischio cibernetico dell'industria assicurativa italiana e il mercato dei nuovi prodotti assicurativi a copertura dei rischi di attacco *cyber*. Per quanto riguarda la diffusione di queste polizze assicurative, il mercato italiano presenta andamenti in parte analoghi a quelli europei: la commercializzazione dei prodotti di copertura specializzati – su cui negli anni precedenti si riscontrava molta prudenza – mostra segnali di sviluppo, con un maggior numero di imprese attive, seppure con volumi ancora molto contenuti.

L'*ASSET* STRATEGICO IN MATERIA DI SICUREZZA ENERGETICA

1. Cyber sicurezza nel settore energetico

Il settore europeo dell'energia sta attraversando un momento di transizione verso un'economia decarbonizzata. Nel contesto di questa transizione e del correlato decentramento della produzione di energia da fonti rinnovabili, il progresso tecnologico, l'integrazione settoriale e la digitalizzazione stanno trasformando la rete energetica europea, in particolare quella elettrica, in una «rete intelligente». Tutto ciò comporta però anche **nuovi rischi** poiché la **digitalizzazione** espone sempre più il sistema energetico ad attacchi e incidenti informatici che possono compromettere la **sicurezza dell'approvvigionamento**.

Nel pacchetto legislativo sulla *governance* europea dell'energia, cd. "*Clean energy package*"[27] viene riconosciuta l'importanza della *cyber* sicurezza nel settore dell'energia.

In particolare, il nuovo Regolamento sul mercato interno dell'energia elettrica (Regolamento (UE) n. 2019/943/UE) prevede l'adozione di **norme tecniche per l'energia elettrica**, e l'adozione, da parte della Commissione europea, di un codice di rete concernente norme settoriali per gli aspetti relativi alla *cyber*

[27] Il pacchetto è composto dai seguenti otto atti legislativi:
- **Regolamento UE n. 2018/1999** del Parlamento europeo e del Consiglio dell'11 dicembre 2018 sulla ***governance* dell'Unione dell'energia**.
- **Direttiva UE 2018/2002** sull'**efficienza energetica c**he modifica la Direttiva 2012/27/UE
- **Direttiva UE 2018/2001** sulla promozione dell'uso dell'energia da **fonti rinnovabili**
- **Direttiva (UE) 2018/844** che modifica la direttiva 2010/31/UE sulla prestazione energetica nell'edilizia e la direttiva 2012/27/UE sull'efficienza energetica (Direttiva EPBD-*Energy Performance of Buildings Directive*)
- **Regolamento (UE) n. 2019/943/UE**, sul **mercato interno dell'energia elettrica** (testo per rifusione);
- **Direttiva (UE) 2019/944** relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE
- **Regolamento (UE) n. 2019/941** sulla **preparazione ai rischi nel settore dell'energia elettrica**, che abroga la direttiva 2005/89/CE
- **Regolamento (UE) 2019/942** che istituisce un'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia.

sicurezza dei flussi transfrontalieri di energia elettrica, e ai requisiti minimi comuni, la pianificazione, il monitoraggio, la rendicontazione e la gestione delle crisi (articolo 59, par. 2, lett. *e)*).

Il Regolamento (UE) n. 2019/941 sulla preparazione ai rischi nel settore dell'energia elettrica – che segue in larga misura l'approccio scelto nel Regolamento sulla sicurezza dell'approvvigionamento di gas (Regolamento (UE) 2017/1938) - sottolinea la necessità di valutare adeguatamente tutti i rischi, compresi quelli connessi alla *cyber* sicurezza. Le misure adottate per risolverli devono essere adeguatamente indicate nei Piani nazionali di preparazione ai rischi (articolo 10). La Commissione europea ha poi recentemente adottato la Raccomandazione (UE) n. 2019/553 sulla *cyber* sicurezza nel settore dell'energia.

Pertanto, le norme generali in materia di sicurezza delle reti e dei sistemi informativi contenute nella Direttiva (UE) n. 2016/1148, cd. Direttiva NIS e nel Regolamento (UE) 2019/881, cd. *Cyber security Act*, sono destinate a trovare una loro specificazione e declinazione, per ciò che concerne la ***cyber* sicurezza nel settore energetico**, nel **Codice di rete di cui al Regolamento** (UE) n. 2019/943 e nelle specifiche misure per fronteggiare i rischi connessi alla *cyber* sicurezza nel settore elettrico contenute nei Piani nazionali di preparazione ai rischi, di cui al Regolamento (UE) n. 2019/941.

Si ricorda in proposito che la Direttiva NIS – ed il Decreto Legislativo 68/2018 che la attua in Italia – si applicano agli operatori di servizi essenziali, quali quelli del **settore energetico**.

Gli Stati membri, nell'elaborazione della propria disciplina nazionale sulla *cyber* sicurezza nel settore energetico dovranno peraltro tenere in considerazione la Raccomandazione n. 2019/553, che in sostanza costituisce attuazione e completamento della disciplina europea in materia.

La Raccomandazione individua le **principali misure che i gestori di reti** energetiche dovrebbero adottare in materia di sicurezza cibernetica, dividendole in tre categorie:

- misure connesse alle esigenze delle componenti dell'infrastruttura energetica operanti in tempo reale;

- misure volte a prevenire "effetti a cascata";
- misure relative alla coesistenza nel settore energetico di tecnologie preesitenti e tecnologie all'avanguardia.

La Raccomandazione considera in primo luogo che alcune delle componenti dei sistemi energetici devono operare in «tempo reale», ossia eseguendo i comandi entro pochi millisecondi, il che rende difficile, se non addirittura impossibile, introdurre misure di *cyber* sicurezza a causa della mancanza di tempo.

Per soddisfare le esigenze di queste componenti dell'infrastruttura energetica, la Raccomandazione incoraggia i **gestori di reti energetiche** ad applicare le più **recenti norme tecniche di sicurezz**a per le nuove installazioni e a prendere in considerazione misure di sicurezza fisica complementari qualora la base installata dei vecchi impianti non possa essere sufficientemente protetta da meccanismi di sicurezza informatica.

Inoltre, gli operatori dovrebbero attuare le **norme tecniche** internazionali in materia di ***cyber* sicurezza e norme tecniche specifiche** adeguate per la comunicazione sicura in tempo reale non appena i prodotti in questione diventano disponibili sul mercato.

Gli operatori dovrebbero poi considerare l'utilizzo di reti private per i sistemi di tele **protezione al fine di garantire il livello di qualità** del servizio richiesto per le contingenze in tempo reale.

La Raccomandazione invita poi gli operatori a suddividere il proprio sistema complessivo in zone logiche e a definire, all'interno di ciascuna zona, i limiti di tempo e i vincoli di processo al fine di consentire l'applicazione di adeguate misure di sicurezza cibernetica o di prendere in considerazione altri metodi di protezione.

I gestori di reti di comunicazione pubbliche dovrebbero valutare la possibilità di assicurare un'assegnazione della larghezza di banda, requisiti di latenza e misure di sicurezza della comunicazione.

Se possibile, i gestori delle reti energetiche dovrebbero inoltre:

a) scegliere un protocollo di comunicazione sicuro, tenendo conto delle esigenze di un contesto in tempo reale, ad esempio per la comunicazione tra un impianto e i relativi sistemi di gestione (sistema di gestione dell'energia/sistema di gestione della distribuzione);
b) introdurre un adeguato meccanismo di autenticazione per la comunicazione tra macchine (M2M) al fine di affrontare le esigenze di un contesto in tempo reale.

La Raccomandazione parte dalla considerazione che **le reti elettriche** e i **gasdotti** sono **strettamente interconnessi in tutta Europa** e un attacco informatico che causa indisponibilità o interruzioni in una parte del sistema energetico potrebbe innescare effetti a cascata di vasta portata in altre sue

parti. Per evitare tali effetti a cascata, la Raccomandazione invita i gestori di reti energetiche a provvedere affinché i nuovi dispositivi, compresi i dispositivi IoT (*Internet* delle cose), abbiano e mantengano un **livello di sicurezza cybernetica adeguato alle criticità del sito**; a tenere debitamente conto degli effetti *cyber* fisici al momento della definizione e della revisione periodica dei piani di continuità operativa; ed a stabilire criteri di progettazione ed un'architettura atti a garantire la resilienza delle reti.

La raccomandazione considera inoltre che di fatto, nell'attuale sistema energetico, coesistono due diversi tipi di tecnologie: tecnologie più vecchie con una durata di vita di 30-60 anni, progettate prima che si tenesse conto delle questioni connesse alla *cyber* sicurezza, e apparecchiature moderne che riflettono lo stato dell'arte della digitalizzazione e dei dispositivi intelligenti.

La Raccomandazione esorta in proposito i gestori delle reti energetiche ad adottare una serie di misure per ovviare a questo problema.

In particolare, i gestori delle reti energetiche dovrebbero:

a) **analizzare i rischi** inerenti alla connessione della tecnologia preesistente e di quella basata sull'*Internet* delle cose;
b) adottare **misure adeguate contro gli attacchi dolosi** provenienti da un numero elevato di applicazioni o dispositivi di largo consumo controllati da malintenzionati;
c) stabilire una capacità automatizzata di monitoraggio e analisi per gli eventi relativi alla **sicurezza negli ambienti preesistenti o IoT**, come i tentativi di accesso falliti, allarmi sulle porte per l'apertura delle cabine o altri eventi;
d) effettuare periodicamente un'analisi dei rischi specifici per la *cyber* sicurezza su tutti gli impianti preesistenti, anche per classi di *asset*, soprattutto quando si connettono tecnologie vecchie e nuove;
e) aggiornare se del caso alla versione più recente il *software* e l'*hardware* dei sistemi preesistenti e dei sistemi IoT;
f) **formulare i bandi** delle gare di appalto tenendo conto delle **questioni connesse alla *cyber* sicurezza,** esigere il rispetto delle norme tecniche esistenti in materia di *cyber* sicurezza, provvedere a che siano proposte ininterrottamente misure di segnalazione, correzione (*patch*) e attenuazione qualora emergano vulnerabilità; chiarire inoltre le responsabilità del fornitore in caso di attacchi o incidenti informatici;
g) collaborare con i fornitori di tecnologia per sostituire i sistemi preesistenti ogni volta in cui ciò potrebbe apportare benefici in termini di sicurezza, tenendo tuttavia conto delle funzionalità essenziali del sistema.

LA SICUREZZA DELLE RETI E LA TECNOLOGIA 5G

1. Premessa

Il prossimo dispiegamento della tecnologia di rete 5G di quinta generazione costituirà un fattore abilitante per lo sviluppo di molti servizi digitali e le relative reti 5G saranno l'**infrastruttura portante** non solo di nuovi servizi di comunicazione elettronica, ma anche di una vasta gamma di servizi essenziali, quali l'energia, i trasporti, i servizi bancari e sanitari, i sistemi di controllo industriale.

Il 5G, inoltre, tramite le sue soluzioni tecniche, basate sullo sfruttamento di elevate porzioni dello spettro elettromagnetico e anche sulla diffusione capillare di antenne e microcelle, assicurando estesa copertura della rete, grande velocità di trasferimento, elevato numero di connessioni simultanee a bassissima latenza, **incrementerà** in maniera esponenziale l'utilizzo dell'*internet of thing* e dei *big data* all'interno della società[28].

Come rilevano gli esperti si tratta di un insieme molto ampio di servizi che presenteranno diversi aspetti di **vulnerabilità** che dovranno essere presi in considerazione ai fini della messa in sicurezza della relativa rete.

2. La tecnologia 5G

La **tecnologia 5G** fa riferimento agli *standard* di quinta generazione per le **telecomunicazioni mobili**. A sua volta il termine 5G viene generalmente impiegato per indicare tecnologie e *standard*, successivi a quelli di quarta generazione, tali da soddisfare determinati requisiti per aumentare sia le prestazioni dei servizi attualmente offerti, che supportare nuovi servizi, come *l'Internet of Things*" (IoT), incluse le cosiddette comunicazioni di tipo M2M

[28] Cfr. Audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei ministri, svolta lo scorso 12 giugno 2019 presso la Commissione Trasporti della Camera dei deputati nell'ambito dell'indagine conoscitiva "sulle nuove tecnologie delle telecomunicazioni" con particolare riguardo alla transizione verso il 5g ed alla gestione dei *big data*".

(*Machine to Machine*), nonché i servizi di trasmissione e comunicazione in situazioni di emergenza e di pubblica sicurezza.

Dal punto di vista dell'utilizzatore la differenza tra il 4G e il 5G è rappresentata principalmente da un insieme di caratteristiche del sistema, tra cui una **maggiore qualità del servizio** in termini di maggiore velocità e di minore latenza della trasmissione dati, con possibilità di ottenere elevate capacità trasmissive e/o ritardi molto bassi, che consentono lo sviluppo di applicazioni fortemente innovative in molteplici settori.

Il 5G costituirà pertanto un *framework* che **dovrà anche integrare le tecnologie esistenti** e supportare un ambiente estremamente eterogeneo di reti fisse e mobili, caratterizzate da una **molteplicità di interfacce** radio e potrà pertanto consentire la connessione simultanea di un più elevato numero di dispositivi, una maggiore efficienza nell'utilizzo dello spettro radio (maggior volume di dati per unità di area), un più basso consumo delle batterie, una minore probabilità di interruzione del servizio.

L'**importanza strategica** del 5G, sia per le funzioni vitali della società e dell'economia, come l'energia, i trasporti, le banche e la sanità, sia nel contesto della protezione del processo democratico contro le interferenze e la disinformazione, ha recentemente indotto l'UE ad avviare l'elaborazione di strumenti volti a garantire a tale infrastruttura digitale un livello adeguato di sicurezza.

Come sottolineano gli esperti la nuova tecnologia 5G presenta, infatti, una **flessibilità architetturale** tale da rendere **complessa** la predisposizione della relativa **rete di sicurezza**, in quanto queste architetture innovative saranno composte da una pluralità di segmenti, che vanno dalla parte di accesso più esterna (la parte radio) fino alla rete *core*, quella di gestione e con una vastità di terminali che svolgono funzioni sempre più complesse[29].

Per quanto concerne le iniziative in ambito europeo si rinvia al paragrafo "Cibersicurezza e 5G" della sezione IV del dossier .

[29] Cfr. seduta della Commissione Trasporti del 7 maggio 2019 nel corso della quale ha avuto luogo l' audizione di rappresentanti dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) del Ministero dello sviluppo economico dell' indagine conoscitiva richiamata nella precedente nota.

In Italia, in attuazione del "*5G Action Plan*" della Commissione europea (Comunicazione CE n. 2016/588), è stata avviata dal MISE, la **sperimentazione del 5G** in 5 città, Milano, Bari, L'Aquila, Matera, Prato, con l'assegnazione (in seguito ad avviso pubblico per progetti sperimentali sul 5G -2018-2020) del diritto d'uso di 100 Mhz nella porzione di spettro 3.6-3.8 Ghz a Vodafone Italia (Milano), Wind Tre-Open Fiber (Prato e L'Aquila), Telecom Italia-Fastweb-Huawei Technologies Italia (Bari e Matera).

Per quanto riguarda la **liberazione delle frequenze** per favorire lo sviluppo delle reti 5G, con la decisione (UE) 2017/899 del 17 maggio 2017 è stato previsto che la c.d. banda dei 700 Mhz (frequenze da 694 a 790 MHz), venga liberata a favore dei servizi 5G, secondo una specifica Roadmap che fissa al 2020 per tutta Europa lo *swicth off*, prevedendo la possibilità per gli Stati membri di arrivare fino al 2022 per completare il percorso.

In tale quadro, la legge di bilancio per il 2018 (legge n. 205 del 2017- commi 1026-1046) ha quindi previsto un articolato programma di redistribuzione delle frequenze. Oltre alla banda dei 700 Mhz (la banda di frequenza 694-790 Mhz), le bande di frequenze interessate dal 5G sono la banda 3,6-3,8 GHz e quella 26,5-27,5 GHz.

Il Ministero dello sviluppo economico ha quindi svolto, sulla base dei criteri definiti dall'AGCOM con delibera 231/18/CONS, le procedure di gara per l'assegnazione dei diritti d'uso di frequenze radioelettriche da destinare a servizi di comunicazione elettronica 5G nelle bande 694-790 MHz, 3600-3800 MHz e 26.5-27.5 GHz, che si è conclusa il 2 ottobre 2018 con offerte che hanno raggiunto i 6.550.422.258 euro. Con l'asta sono stati messi a gara 1275 MHz di spettro nelle bande pioniere per il 5G attuando il 5G Action Plan europeo.

Con riferimento alle più recenti iniziative normative adottate in ambito nazionale il **decreto legge n. 22/2019** ha recentemente modificato la disciplina dei poteri speciali (cd. *golden power*) sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, di cui al decreto-legge n. 21/2012[30], qualificando i servizi di comunicazione elettronica a

[30] Il decreto reca Misure urgenti per assicurare sicurezza, stabilità finanziaria e integrità dei mercati, nonché tutela della salute e della libertà di soggiorno dei

banda larga basati sulla **tecnologia 5G** come attività di **rilevanza strategica** per il sistema di **difesa e sicurezza nazionale**, ai fini dell'esercizio dei poteri speciali.

Con tale norme è stata aggiornata la normativa in materia di poteri speciali in conseguenza dell'evoluzione tecnologica intercorsa, con particolare riferimento alla tecnologia 5G e ai connessi rischi di un uso improprio dei dati con implicazioni sulla sicurezza nazionale. La disposizione prevede **l'obbligo di notifica** per i contratti o gli accordi con soggetti esterni all'Unione europea, che abbiano ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G; altresì soggette a notifica sono le acquisizioni di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione.

L'**esercizio di poteri speciali** in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, **è stato esercitato** con il decreto del Presidente del Consiglio dei ministri 26 giugno 2019, recante imposizione di prescrizioni e condizioni nei confronti della società Fastweb Spa in relazione all'accordo con la società Samsung Electronics Co. Ltd. per la progettazione, fornitura, configurazione e manutenzione di apparati *software* relativi alle componenti radio e *core network* necessari alla realizzazione della rete 5G *Fixed Wireless Access* nelle città pilota di Bolzano e Biella.

Inoltre in data 11 luglio 2019 è stato approvato dal Consiglio dei Ministri il decreto legge n. 64 del 2019 (**non convertito in legge**) che modificava ulteriormente la disciplina organica di tali **poteri speciali**, con particolare riferimento alla disciplina dei poteri speciali in tema di tecnologie **5G**[31].

cittadini italiani e di quelli del Regno Unito, in caso di recesso di quest'ultimo dall'Unione europea.

[31] Sulla "sanatoria degli effetti" del richiamato decreto legge n. 64 del 2019 si veda l'articolo 1 del ddl di conversione del decreto legge n. 75 del 2019 (A.C. 2107).

Al riguardo, il Consiglio dei Ministri, nel corso della riunione dello scorso 5 settembre, su proposta del Ministro dello sviluppo economico Stefano Patuanelli, a norma dell'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, ha deliberato:

1. l'esercizio dei poteri speciali in relazione alla informativa notificata dalla società LINKEM S.p.a. relativa a contratti o accordi aventi ad oggetto l'acquisto di beni e servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga su tecnologia 5G e acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione;
2. l'esercizio di poteri speciali, con condizioni e prescrizioni, in relazione all'operazione notificata dalla società Vodafone S.p.a. consistente in accordi aventi ad oggetto l'acquisto di beni e servizi per la realizzazione e la gestione di reti di comunicazione elettronica basate sulla tecnologia 5G;
3. l'esercizio dei poteri speciali in relazione all'informativa notificata dalla società TIM S.p.a. relativa agli accordi conclusi prima del 26 marzo relativi ad apparati e sistemi di comunicazione rispetto ai quali la tecnologia 5G può essere considerata una naturale evoluzione;
4. l'esercizio dei poteri speciali, con prescrizioni, in relazione all'informativa notificata dalla società Wind Tre S.p.a. circa gli accordi stipulati con la società Huawei, aventi ad oggetto l'acquisto di beni e servizi per la realizzazione e la gestione di reti di comunicazione elettronica basate sulla tecnologia 5G;
5. l'esercizio dei poteri speciali in relazione all'informativa notificata dalla società FASTWEB S.p.a. relativa all'acquisto dalla società ZTE Corporation degli apparati relativi alle componenti radio per la realizzazione dell'ultima tratta della rete 5G FWA.

Da ultimo, come in precedenza rilevato, il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il decreto n.105 del 2019 (pubblicato nella Gazzetta Ufficiale del 21 settembre 2019) che introduce disposizioni urgenti in materia di "**perimetro**" di sicurezza nazionale cibernetica. Per quanto riguarda la **tecnologia 5G**, il decreto legge n.105 del 2019 fa riferimento alla citata legge sul *golden power* in relazione agli assetti societari nei settori della difesa e della sicurezza nazionale e stabilisce che le condizioni dei contratti

già autorizzati dal presidente del Consiglio che rientrano nel 'perimetro' "possono essere modificate o integrate" con "misure aggiuntive necessarie al fine di assicurare livelli di sicurezza" in linea con lo stesso decreto "anche prescrivendo, ove necessario, la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza".
Infine lo stesso **Presidente del Consiglio "può comunque disporre**, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, **la disattivazione, totale o parziale,** di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati".
Per un approfondimento si rinvia al *dossier* schede di lettura sul provvedimento.

PROTEZIONE DELLA FILIERA INDUSTRIALE AUTOMATIZZATA E INTERCONNESSA (PROGETTO INDUSTRIA 4.0)

1. Industria 4.0

L'espressione Industria 4.0 indica un **processo** generato da trasformazioni tecnologiche nella progettazione, nella produzione e nella distribuzione di sistemi e prodotti manifatturieri, finalizzato alla **produzione industriale automatizzata e interconnessa**.

In particolare, Industria 4.0 identifica un'organizzazione dei processi produttivi basata sulla digitalizzazione di tutte le fasi degli stessi: un modello di "*smart factory*" (fabbrica intelligente) del futuro, nel quale l'utilizzo delle tecnologie digitali permette di monitorare i processi fisici e assumere decisioni decentralizzate, basate su meccanismi di autoorganizzazione, orientati alla gestione efficiente delle risorse, alla flessibilità, alla produttività e alla competitività del prodotto, che generano fruttuose sinergie tra produzione e servizi.

La chiave di volta dell'industria 4.0 sono i **sistemi ciberfisici** (*Cyber Physical System-CPS*), ovvero sistemi fisici strettamente connessi con i sistemi informatici, che possono interagire e collaborare con altri sistemi **CPS**.

L'espressione Industria 4.0 è stata **utilizzata per la prima volta in Germania**, ma si sovrappone per gran parte alle esperienze maturate a livello internazionale: *Manufacturing USA* negli USA, *Smart Industry* nei Paesi Bassi, in Slovacchia e in Svezia o *Industrie du Futur* in Francia. L'esperienza tedesca è indubbiamente la più strutturata ed è stata considerata come punto di riferimento, in ragione sia del considerevole anticipo con cui le autorità pubbliche hanno avviato l'iniziativa, sia della forte sinergia con i *leader* industriali privati.

In Germania, essa è nata al fine di creare le condizioni per preservare e favorire la competitività. Nel 2012 Industria 4.0 rientrava tra i dieci progetti della strategia High-Tech del Governo tedesco. Nel 2013, sulla base dei risultati di un gruppo di lavoro formato da rappresentanti dell'industria, accademici e scienziati, il Ministero dell'istruzione e della ricerca tedesco ha individuato le otto priorità della strategia Industria 4.0, dalla standardizzazione alla formazione continua. Nel 2015, tali impegni sono stati istituzionalizzati attraverso la creazione di una piattaforma composta da imprese, ricercatori e sindacati e guidata dai Ministri dell'economia e della ricerca, convinti che la digitalizzazione dei prodotti e dei servizi di Industria 4.0 potesse consentire

guadagni annuali in termini di efficienza nel settore manifatturiero, nonché la creazione di nuovi posti di lavoro. Un'attenzione particolare è stata rivolta alle piccole e medie imprese, anche in Germania diffidenti nei confronti della transizione verso metodi di produzione digitalizzati. Alle proposte degli esperti, il Ministero della ricerca ha finora dato seguito autorizzando la sovvenzione di progetti di ricerca e, parallelamente, anche il Ministero federale per l'economia e l'energia ha adottato programmi di sostegno a favore della ricerca e dello sviluppo di importanti innovazioni nell'ambito di Industria 4.0.

Industria 4.0 è strettamente connessa alla cosiddetta "**quarta rivoluzione industriale**", che fa seguito alle tre precedenti rivoluzioni industriali (legate, rispettivamente, all'utilizzo della macchina a vapore, all'introduzione dell'elettricità, dei prodotti chimici e del petrolio e all'avvento dell'informatica e dell'elettronica).

Resa possibile dalla **disponibilità di sensori** e di **connessioni *wireless*** a basso costo, essa si associa a un impiego sempre più pervasivo di dati e informazioni, di tecnologie digitali e analisi dei dati, di nuovi materiali e componenti e di sistemi totalmente digitalizzati e connessi (*internet of things and machines*).

Nella visione del futuro dell'Industria 4.0, infatti, gli impianti, i lavoratori, i materiali in *input* e i prodotti finiti saranno dotati di **sensori** che li identificheranno e ne rileveranno costantemente posizione, stato e attività. Tali sensori consentiranno la **raccolta di dati** che, una volta analizzati, potranno migliorare la capacità produttiva, l'efficienza, la sicurezza e la continuità operativa.

L'approccio Industria 4.0 facilita pertanto gli operatori nelle loro mansioni grazie a ***robot* collaborativi** e a nuove **interfacce uomo-macchina** che ne potenzieranno sia la capacità esecutiva sia quella decisionale.

Infine, tutta la fabbrica sarà connessa al resto del sistema logistico-produttivo e ai clienti tramite **piattaforme *cloud***; i dati relativi all'utilizzo dei prodotti saranno utilizzati per facilitare l'assistenza post-vendita e lo sviluppo di nuovi prodotti e servizi, nonché per abilitare nuovi modelli di *business*.

La Commissione europea, già nella Comunicazione COM(2016)180 aveva sottolineato la **rilevanza delle innovazioni digitali nell'industria**, che "costituiscono un'opportunità unica per attrarre ulteriori investimenti in Europa". La Commissione europea ha posto pertanto l'accento sull'esigenza di

rafforzare la competitività dell'UE nell'ambito delle tecnologie digitali e di fare in modo che qualsiasi industria in Europa possa beneficiare appieno delle innovazioni digitali, indipendentemente dal settore in cui opera, dal luogo in cui si trova e dalle sue dimensioni. I cambiamenti tecnologici in atto nel settore dell'industria mondiale investono non solo le modalità di produzione e l'organizzazione delle fabbriche, ma anche l'intera organizzazione sociale e il sistema culturale e saranno assunti come standard a livello globale.

2. Le soluzioni tecnologiche individuate dalla logica Industria 4.0

Le **soluzioni tecnologiche** individuate dalla logica **Industria 4.0 sono** dunque **finalizzate** a:

- ottimizzare i processi produttivi;
- migliorare la qualità del prodotto;
- supportare i processi di automazione industriale;
- incrementare la flessibilità della produzione;
- favorire la collaborazione produttiva tra imprese attraverso tecniche avanzate di pianificazione distribuita, gestione integrata della logistica in rete e interoperabilità dei sistemi informativi.

Più in dettaglio i sei grandi insiemi di **tecnologie digitali innovative alla base dell'Industria 4.0 ("*Smart Technologies*")** sono individuati nelle seguenti applicazioni:

1) *Industrial Internet (of Things);*
2) *Industrial Analytics;*
3) *Cloud Manufacturing;*
4) *Advanced Automation;*
5) *Advanced Human Machine Interface (Advanced HMI);*
6) *Additive Manufacturing*[32].

Le richiamate tecnologie presentano un fondamentale tratto comune: abilitare una forte **interconnessione** tra le risorse utilizzate nei processi operativi. Nella visione del futuro dell'Industria 4.0, infatti, gli impianti, i lavoratori, i materiali in *input* e i prodotti finiti saranno dotati di **sensori** che li identificheranno e

[32] Per un approfondimento di queste tecnologie si rinvia all'Appendice di questo lavoro.

ne rileveranno costantemente posizione, stato e attività. Tali sensori consentiranno la **raccolta di dati** che, una volta analizzati, potranno migliorare la capacità produttiva, l'efficienza, la sicurezza e la continuità operativa.

3. Cyber security e industria 4.0

Secondo una ricerca dell'Osservatorio I*nformation Security & Privacy della School of Management* del Politecnico di Milano per le imprese che stanno evolvendo verso l'Industria 4.0, le *principali criticità* sono legate alle tecnologie IoT (cfr. Appendice). Nello specifico i **principali fattori di minaccia informatica** sono rappresentati dalla mancanza di una logica di *security by design* (indicata dal 73% delle imprese), dalla **scarsa consapevolezza** da parte degli utenti sui possibili problemi legati a questi dispositivi (58%) e dal**l'assenza di standard tecnologici** e di sicurezza (53%).

Le principali sfide per la sicurezza nell'Industria 4.0 riguarderanno soprattutto la **mancanza di consapevolezza** dei problemi di sicurezza da parte delle funzioni *Operation*s (56%), l'interconnessione crescente tra impianti industriali e infrastruttura IT (55%), l'**obsolescenza** degli impianti industriali (40%) e la mancanza di figure con adeguate competenze (37%).

Dello studio di questi aspetti si occupa da tempo l'**ENISA** (*European Union Agency for Network and Information Security*), che nel novembre 2018 ha pubblicato delle **linee guida per la sicurezza** informatica nel settore dell'IoT, con un *focus* particolare sulle *smart manufacturing* (cfr. paragrafo successivo e Appendice) e sull'Industria 4.0. L'obiettivo della pubblicazione era promuovere e favorire la **cultura della sicurezza informatica** nell'Industria 4.0 e in tutte le aziende che prevedono di adottare dispositivi e soluzioni IoT nelle proprie operazioni industriali.

A **maggio 2019** ENISA ha pubblicato un secondo rapporto, che identifica le principali sfide che l'Industria 4.0 e il settore IoT devono affrontare per incrementare la sicurezza informatica.

Secondo l'ENISA, le principali *new skills* richieste saranno:

- competenze di sicurezza operativa e abilità nel monitorare, prevenire e rilevare anomalie dovute a violazioni della sicurezza;

- conoscenza dei nuovi protocolli di sicurezza utilizzati dalle soluzioni *Industry* 4.0 e *Industry IoT*;
- padronanza delle funzionalità di sicurezza dei componenti delle nuove macchine e dei servizi connessi;
- sicurezza dei sistemi di informazione sulla *supply chain* (cfr. Appendice).

Con riferimento alle più recenti iniziative legislativa, il D. L. n. 34 del 2019 ha previsto una serie di misure finalizzate a favorire la **trasformazione tecnologica e digitale** dei processi produttivi delle micro, piccole e medie imprese, coerenti con le linee strategiche del Piano triennale per l'informatica nella pubblica amministrazione 2019-2021, tramite l'inclusione tra le tecnologie abilitanti del Piano Impresa 4.0, alla cui implementazione sono disposte agevolazioni, di alcune voci, tra le quali **rientrano gli investimenti in cybersecurity**.

Si segnala, inoltre che la legge di Bilancio per il 2019 (l. n. 145 del 2018), all'articolo 1, comma 226, ha previsto l'istituzione di un **Fondo per favorire** lo sviluppo delle tecnologie e delle applicazioni di Intelligenza Artificiale, *blockchain* e *Internet of Things*, con una dotazione di 15 milioni di euro per ciascuno degli anni 2019, 2020 e 2021, per finanziare progetti di ricerca e sfide competitive in questi campi.

Parte terza: Politiche UE in materia di cibersicurezza

(a cura dell'Ufficio Rapporti con l'Unione europea)

1. L'approccio UE all'azione di contrasto al cybercrime

L'**UE ha** progressivamente **rafforzato** le misure volte a **contrastare** la **criminalità informatica**, articolando il proprio intervento con riferimento a tre principali categorie di illeciti:

- gli attacchi alle reti e ai sistemi informatici;
- la perpetrazione di reati di tipo comune (ad esempio, crimini essenzialmente predatori) tramite l'uso di sistemi informatici;
- la diffusione di contenuti illeciti (ed esempio, pedopornografia, propaganda terroristica, hate speech/discorso di odio, etc.) per mezzo di sistemi informatici.

Le politiche di contrasto alle attività illecite e dolose basate sull'uso di sistemi informatici (comprese le iniziative in materia di disinformazione: vedi infra) sono state trattate nei più recenti Consigli europei, in occasione dei quali i leader dell'UE hanno, tra l'altro, chiesto la conclusione dei procedimenti legislativi dei principali strumenti normativi proposti dalla Commissione europea, e dato impulso a nuove iniziative nel campo della cibersicurezza (per approfondimenti si vedano i temi web su: Consiglio europeo 28-29 giugno 2018, Consiglio europeo 17-18 ottobre 2018; Consiglio europeo 13-14 dicembre 2018; Consiglio europeo 20-21 giugno 2019).

2. Le minacce alle reti e ai sistemi informatici

La prima categoria di illeciti è considerata di particolare rilievo, attesa l'importanza delle reti e dei sistemi informatici rispetto al funzionamento delle infrastrutture critiche (tra tutte, il sistema dei trasporti, le strutture ospedaliere, quelle energetiche), la cui sicurezza attiene peraltro al normale svolgimento della vita democratica di un Paese. L'intervento dell'UE al riguardo si è sviluppato su diversi piani, inclusa la politica estera, di sicurezza e di

difesa europea, stante la natura di vera e propria minaccia ibrida di alcune tipologie di attacchi informatici[33].

In particolare, con la direttiva (UE) n. 2016/1148, sulla **sicurezza delle reti e dell'informazione** (direttiva NIS) *(recepita in Italia con il decreto legislativo 18 maggio 2018, n. 65)*, l'Unione europea ha posto le basi per un miglioramento della cooperazione operativa tra Stati membri in caso di incidenti di cibersicurezza e della condivisione delle informazioni sui rischi (cfr. *supra)*.

La direttiva definisce **obblighi di sicurezza** per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, l'assistenza sanitaria e la finanza) e i fornitori di servizi digitali (mercati *online*, motori di ricerca e servizi di *cloud*); inoltre, ogni Paese dell'UE è tenuto a designare una o più autorità nazionali con il compito, tra l'altro, di monitorare l'applicazione della direttiva, nonché a elaborare una strategia per affrontare le minacce informatiche.

L'UE ha recentemente consolidato tale quadro mediante l'adozione del regolamento sulla cibersicurezza[34] (cosiddetto *cybersecurity act*), recante una serie di disposizioni per:

- il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) che si intende trasformare nell'Agenzia UE per la cibersicurezza;
- l'introduzione di sistemi europei di certificazione della cibersicurezza dei prodotti e dei servizi TIC nell'Unione (che consisterebbero in una serie di norme, requisiti tecnici e procedure).

[33] Per minacce ibride – nozione per la quale non esiste una definizione sul piano giuridico universalmente accettata – la Commissione europea intende una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali pur senza oltrepassare la soglia di guerra formalmente dichiarata. Il loro obiettivo non consiste soltanto nel provocare danni diretti e nello sfruttare le vulnerabilità, ma anche nel destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

[34] Regolamento (UE) n. 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013.

Nello stesso ambito, inoltre, il 17 aprile 2019, il Parlamento europeo ha adottato la propria posizione in prima lettura circa la proposta di regolamento istitutiva di un **centro europeo di ricerca** e di competenza sulla cibersicurezza, affiancato da una rete di centri analoghi a livello di Stati membri. Tra gli obiettivi chiave della proposta, il miglioramento del coordinamento dei finanziamenti disponibili per la cooperazione, la ricerca e l'innovazione in tale ambito. La proposta è in attesa dell'adozione da parte del Consiglio dell'UE.

Disposizioni volte alla sicurezza delle reti sono altresì contenute nel Codice delle comunicazioni elettroniche[35].

3. Cibersicurezza e 5G

Il 5G viene considerato cruciale per una connettività di alta qualità nell'intero territorio dell'Unione, ai fini del completamento del mercato unico digitale e a sostegno dell'innovazione in tutti settori.

A tal proposito, si ricorda che la citata direttiva (UE) n. 2018/1972, che istituisce il Codice delle comunicazioni elettroniche, prevede che entro il 2020 **tutti gli Stati membri dell'UE** assegnino le frequenze necessarie per l'introduzione della rete 5G.

A tal proposito si ricordano:

- la risoluzione non legislativa (2019/2575 (RSP), adottata dal Parlamento europeo il 12 marzo 2019, sulle "minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce".

Nell'atto di indirizzo si esprime forte preoccupazione in relazione alla possibilità che le infrastrutture cinesi per le reti 5G possano avere incorporate delle '*backdoors*' in grado di consentire a fornitori ed autorità cinesi un accesso non autorizzato ai dati personali e alle telecomunicazioni nell'UE. La legislazione cinese

[35] Direttiva (UE) n. 2018/1972, che istituisce il codice europeo delle comunicazioni elettroniche.

contempla una definizione estesa della sicurezza nazionale tale da comportare l'obbligo per le imprese di cooperare con lo Stato, pertanto vi è il timore che i fornitori di dispositivi di un paese terzo come la Cina possano costituire un rischio per la sicurezza dell'Unione europea;

- la comunicazione congiunta[36] del "UE - Cina una prospettiva strategica" della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, nella quale si sottolinea la necessità di un approccio comune per la cibersicurezza delle reti 5G;
- la raccomandazione[37] del 26 marzo 2019, con la quale la Commissione europea (in attuazione dell'indirizzo espresso dal Consiglio europeo del 22 marzo 2019 a favore di un approccio concertato alla sicurezza delle reti 5G) propone un approccio comune dell'UE ai rischi per la sicurezza delle reti 5G, basato su una valutazione coordinata dei rischi e su misure coordinate di gestione dei rischi, su un quadro efficace per la cooperazione e lo scambio di informazioni e su una conoscenza comune della situazione delle reti di comunicazione.

La Commissione europea ha reso noto che, dando seguito alla raccomandazione, 24 Stati membri dell'UE hanno presentato le valutazioni nazionali dei rischi, che dovrebbero confluire nella prossima fase, costituita dalla valutazione dei rischi a livello dell'UE il cui completamento è previsto entro il 1° ottobre. Le valutazioni nazionali dei rischi offrono una panoramica dei seguenti elementi: principali minacce e attori che incidono sulle reti 5G; grado di sensibilità di componenti e funzioni delle reti 5G e di altre risorse; vulnerabilità di vario tipo, di ordine tecnico ma non solo, ad esempio quelle potenzialmente derivanti dalla catena di approvvigionamento del 5G. La raccomandazione prevede che entro il 31 dicembre 2019 il gruppo di cooperazione NIS previsto dalla citata direttiva sulla sicurezza delle reti e dell'informazione approvi un insieme di misure di attenuazione

[36] Comunicazione JOIN(2019)5 del 12 marzo 2019.
[37] Raccomandazione (UE) 2019/534 della Commissione, Cibersicurezza delle reti 5G.

per affrontare i rischi individuati nelle valutazioni a livello di Stati membri e dell'UE.

4. L'uso dei sistemi informatici a fini criminali

L'intervento normativo dell'UE più recente in tale settore è la direttiva (UE) n. 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. Gli elementi chiave della direttiva, sostitutiva della precedente decisione quadro 2001/413/GAI del Consiglio, sono: **l'ampliamento della portata dei reati,** che secondo il nuovo regime include, tra l'altro, le transazioni mediante **valute virtuali**; l'armonizzazione delle definizioni di alcuni reati *online*, quali la pirateria informatica o il *phishing*; l'introduzione di livelli minimi per le **sanzioni** più elevate per le persone fisiche; norme in materia di competenza giurisdizionale riguardo le **frodi transfrontaliere**; il miglioramento della cooperazione in materia di giustizia penale; la prevenzione e le attività di sensibilizzazione per ridurre i rischi di frodi.

Nell'ambito degli strumenti per la cibersicurezza, la Commissione europea ha, altresì, presentato proposte legislative volte a migliorare **l'acquisizione transfrontaliera di prove elettroniche** per i procedimenti penali. Si tratta di una proposta di regolamento[38] relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali, e di una proposta di direttiva[39] che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali. Le proposte sono tuttora all'esame delle Istituzioni legislative europee.

La materia è stata da ultimo trattata dall'UE anche per i profili di politica estera. A tal proposito, il 6 giugno 2019, il Consiglio dell'UE ha conferito alla Commissione europea due mandati per svolgere negoziati internazionali intesi a migliorare l'accesso transfrontaliero alle prove elettroniche nelle indagini penali, da un lato, con gli Stati Uniti, dall'altro con particolare riguardo al secondo protocollo aggiuntivo alla **Convenzione di Budapest** del Consiglio d'Europa

[38] COM(2018)225.
[39] COM(2018)226

sulla criminalità informatica (cfr. capitolo 3, paragrafo 1, della sezione prima). I mandati includono disposizioni recanti garanzie a tutela dei diritti fondamentali in materia di protezione dei dati, *privacy* e diritti procedurali delle persone.

5. L'impiego dei sistemi informatici per la diffusione di contenuti illegali

Politiche di prevenzione e contrasto alla radicalizzazione e al linguaggio di odio

È tuttora oggetto di iter legislativo la proposta di regolamento COM(2018)640 presentata dalla Commissione nel settembre del 2018 al fine di **eliminare** rapidamente i contenuti terroristici dal ***web***. La proposta mira a introdurre un **termine vincolante** di un'ora per l'eliminazione dalla rete dei contenuti di stampo terroristico a seguito di un **ordine di rimozione** emesso dalle autorità nazionali competenti. Sono altresì previsti: un quadro di cooperazione rafforzata tra prestatori di servizi di *hosting*, Stati membri ed Europol, per facilitare l'esecuzione degli ordini di rimozione; **meccanismi di salvaguardia** (reclami e ricorsi giurisdizionali) per proteggere la libertà di espressione su Internet e per garantire che siano colpiti esclusivamente i contenuti terroristici; un apparato sanzionatorio per i prestatori di servizi nel caso di mancato rispetto (o ancora, di omissione sistematica) degli ordini di rimozione. Sulla proposta il Parlamento europeo, il 17 aprile 2019 ha approvato la propria posizione in prima lettura. Il neoeletto Parlamento europeo sarà incaricato di negoziare con il Consiglio dell'UE il testo definitivo del regolamento.

In tale settore, si ricorda che l'unità IRU (*Internet Referral Unit*), istituita nel 2015 in seno ad Europol - l'Agenzia europea per la cooperazione di polizia, ha il compito di segnalare ai fornitori di servizi *online* interessati i contenuti volti alla propaganda terroristica o all'estremismo violento su Internet ai fini della loro rimozione.

Nell'ambito del contrasto alla radicalizzazione, l'UE ha altresì messo in campo una serie **di strumenti di carattere preventivo** (processi di integrazione e inclusione sociale, di reinserimento e deradicalizzazione delle persone considerate a rischio e degli stessi

combattenti stranieri che fanno ritorno nei rispettivi Stati membri di provenienza).

Tra gli strumenti di prevenzione adottati a livello di Unione devono ricomprendersi il Gruppo di esperti di alto livello in materia di radicalizzazione, la **Rete per la sensibilizzazione** alla radicalizzazione (RAN), il ***Forum* dell'UE su Internet**, la Rete europea per le comunicazioni strategiche (ESCN).

Si ricorda infine che, il 6 giugno 2019, il Consiglio dell'UE giustizia e affari interni ha approvato una serie di conclusioni sulla prevenzione e la lotta alla radicalizzazione nelle carceri e sulla gestione degli autori di reati di terrorismo ed estremismo violento dopo la scarcerazione,

Nel quadro generale della **prevenzione e del contrasto** dei contenuti illeciti *online* si segnalano altresì: il *Code of conduct* siglato dalla Commissione con le principali imprese operanti nel settore dei *social media*, recante l'impegno da parte di queste di eliminare i messaggi illegali di incitamento all'odio (maggio 2016); gli orientamenti politici per le **piattaforme *online*** al fine di intensificare la lotta contro i contenuti illeciti in cooperazione con le autorità nazionali (settembre 2017); le raccomandazioni agli Stati membri recanti misure operative volte a garantire maggiore rapidità nella rilevazione e nella rimozione dei contenuti illegali *online* anche di stampo terroristico o riconducibili a reati di odio (marzo 2018).

Iniziative dell'UE per il contrasto alla disinformazione

Dal 2015 l'UE è sistematicamente impegnata in una serie di iniziative volte a proteggere le istituzioni e i processi democratici dall'attività di disinformazione.

A tale attività - secondo la definizione adottata dalla Commissione europea[40] - deve essere ricondotta "un'informazione rivelatasi **falsa** o **fuorviante** concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un **pregiudizio pubblico**. La disinformazione non include gli errori di segnalazione, la **satira** e la **parodia**, o notizie e commenti chiaramente identificabili come di parte". Secondo la

[40] Comunicazione congiunta "Relazione sull'attuazione del piano di azione contro la disinformazione (COM (2019) 12).

Commissione europea, "obiettivo della disinformazione è distrarre e dividere, insinuare il seme del dubbio distorcendo e falsando i fatti, al fine di disorientare i cittadini minando la loro fiducia nelle istituzioni e nei processi politici consolidati".

Data la sensibilità del tema, con particolare riguardo alla questione della **protezione delle elezioni europee**, il contrasto alla disinformazione è stato oggetto di conclusioni da parte dei Consigli europei del 13 -14 dicembre 2018, del 22 marzo e 20-21 giugno 2019.

In particolare, nella riunione del 20-21 giugno 2019, il Consiglio europeo ha chiesto un impegno costante per sensibilizzare sul tema della **disinformazione** e rafforzare la preparazione e la resilienza delle nostre democrazie di fronte a tale fenomeno; il Consiglio europeo ha, altresì, sottolineato la necessità di una valutazione costante e di una risposta adeguata nei confronti della **continua evoluzione delle minacce** e del crescente **rischio di interferenze dolose e manipolazioni *online***, associati allo sviluppo dell'intelligenza artificiale e di tecniche di raccolta dati.

Task force East StratCom

Tra le prime iniziative dell'UE in materia di disinformazione, le misure nell'ambito della azione esterna volte a **contrastare la diffusione di informazioni fuorvianti** o palesemente false da parte di enti e organismi situati in Stati terzi.

Le misure in tale settore sono spesso ricondotte dall'UE nel più ampio ambito dell'azione di difesa dalle minacce ibride. Secondo la Commissione europea, le campagne massicce di disinformazione, che usano i media sociali per controllare il discorso politico o per radicalizzare, reclutare e dirigere mandatari, possono essere vettori di minacce ibride[41].

[41] Comunicazione "Quadro congiunto per contrastare le minacce ibride" del 6 aprile 2016. Per minacce ibride – nozione per la quale non esiste una definizione sul piano giuridico universalmente accettata – la Commissione europea intende una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali pur senza oltrepassare la soglia di guerra formalmente dichiarata. Il loro obiettivo non consiste soltanto nel provocare danni diretti e nello sfruttare le vulnerabilità, ma anche nel destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

In particolare, a seguito della decisione del Consiglio europeo del marzo 2015 di contrastare le campagne di disinformazione da parte della Russia, il Servizio europeo per l'azione esterna (SEAE) ha istituito la *task force* East StratCom, con il compito di sviluppare prodotti e campagne di comunicazione incentrate sulla spiegazione delle politiche dell'UE nella regione del partenariato orientale (Armenia, Azerbaijan, Bielorussia, Georgia, Moldavia e Ucraina).

La *task force* si concentra sui seguenti obiettivi: comunicare efficacemente le politiche dell'UE al suo vicinato orientale; rafforzare l'ambiente mediatico generale nel vicinato orientale, anche sostenendo la libertà dei mezzi di informazione e consolidando i media indipendenti; migliorare le capacità dell'Unione di prevedere e affrontare le attività di disinformazione a favore del Cremlino e di sensibilizzare il pubblico in proposito. Sono state istituite altre due task *force* incentrate su aree geografiche diverse: la *task force* StratCom per i Balcani occidentali e la *task force South Med Stratcom* per il mondo di lingua araba.

In tale contesto, meritano di essere segnalati anche la cellula dell'UE per l'analisi delle minacce ibride (*Hybrid Fusion Cell*) creata nel SEAE nel 2016 per fungere da punto focale per l'analisi di tali attacchi e il Centro europeo di eccellenza per contrastare le minacce ibride, istituito a Helsinki nel 2017.

Approccio europeo per il contrasto alla disinformazione

Nell'aprile del 2018, la Commissione europea ha presentato la comunicazione COM(2018) 236 "Contrastare la disinformazione *online*: un approccio europeo" recante i principi e gli obiettivi generali che dovrebbero guidare le azioni volte a sensibilizzare l'opinione pubblica alla disinformazione e a contrastare efficacemente tale fenomeno, nonché una serie di iniziative considerate prioritarie. Tra le misure chiave indicate dalla Commissione europea, l'elaborazione da parte dei rappresentanti delle **piattaforme *online***, dell'industria della **pubblicità** e dei principali inserzionisti di un codice di buone pratiche dell'UE sulla disinformazione in regime di **autoregolamentazione**.

Il codice è stato adottato nell'ottobre del 2018 dalle principali piattaforme *online*, dalle società di *software*, e dalle organizzazioni che rappresentano il settore della **pubblicità**.

Il codice prevede una serie di impegni, che comprendono, tra l'altro: **vaglio delle inserzioni pubblicitarie** per ridurre gli introiti pubblicitari di coloro che diffondono disinformazione; garanzia della **trasparenza** dei **messaggi pubblicitari** di natura politica; contrasto all'abuso delle piattaforme da parte di **profili falsi** e di **"bot" automatizzati**; maggiore collaborazione con i **verificatori di fatti**; miglioramento della **visibilità** dei **contenuti** sottoposti a

verifica dei fatti; predisposizione di **strumenti** messi a disposizione degli **utenti** per individuare meglio la disinformazione.

Nel giugno del 2019, la Commissione europea ha manifestato l'intenzione di procedere ad una valutazione dell'efficacia del codice entro la fine del 2019, preannunciando peraltro ulteriori iniziative, anche di **natura regolamentare**, qualora i risultati di tale valutazione non fossero soddisfacenti.

Il pacchetto elezioni

In occasione del discorso sullo Stato dell'Unione del settembre 2018, la Commissione europea ha presentato una serie di iniziative per garantire **elezioni libere ed eque** (in vista della tornata elettorale del maggio del 2018) tra l'altro, anche in materia di contrasto alla disinformazione.

Si tratta, in particolare, di: una comunicazione della Commissione europea "Assicurare elezioni europee libere e corrette[42]; una raccomandazione (C(2018)5949) relativa alle reti di cooperazione in materia elettorale, alla trasparenza *online*, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione; orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di **protezione dei dati** nel contesto elettorale; una serie di modifiche[43] (entrate in vigore nel marzo del 2019) al regolamento relativo al **finanziamento dei partiti politici europei**, che introducono in particolare **sanzioni finanziarie** ai partiti politici europei e alle fondazioni politiche europee che **influenzano** deliberatamente, o tentano di influenzare, i **risultati** delle **elezioni** del PE approfittando di **violazioni** delle norme in materia di **protezione dei dati**.

Piano d'azione contro la disinformazione

Presentato dalla Commissione europea e dall'Alto rappresentante dell'unione per gli affari esteri e la politica di sicurezza nel dicembre del 2018, il Piano contiene una serie di iniziative per far fronte alle minacce provenienti dall'interno e dall'esterno dell'UE che possono riassumersi nelle seguenti linee di azione[44]:

- capacità di **individuazione** dei casi di **disinformazione**, in particolare tramite il rafforzamento delle *task force* di comunicazione strategica e della cellula dell'UE per l'analisi delle **minacce ibride** del Servizio europeo per l'azione esterna (SEAE);

[42] (COM(2018)637)

[43] Regolamento (UE, Euratom) n. 2019/493, del 25 marzo 2019, che modifica il regolamento (UE, Euratom) n. 1141/2014 per quanto riguarda la procedura di verifica relativa alle violazioni delle norme in materia di protezione dei dati personali nel contesto delle elezioni del Parlamento europeo.

[44] JOIN(2018)36. Si ricorda che, il 14 giugno 2019, è stata pubblicata una relazione sullo stato dell'arte dell'attuazione del piano.

- **risposta coordinata**, dotando istituzioni UE e Stati membri di un **sistema di allarme rapido** per la condivisione e valutazione delle campagne di disinformazione;
  Istituito nel marzo del 2019, il **sistema di allarme rapido** è una piattaforma digitale volta a consentire a istituzioni dell'UE e Stati membri la migliore condivisione di approfondimenti relativi alle campagne di disinformazione e il coordinamento delle loro risposte. Il sistema si basa su informazioni *open-source*, nonché su approfondimenti dal mondo accademico, *fact-checker*, piattaforme *online* e partner internazionali.
- mobilitazione del **settore privato** nelle attività di **contrasto** (in particolare, mediante l'attuazione efficace da parte delle **piattaforme *online*** e dell'industria firmatarie degli impegni nell'ambito del **codice di buone pratiche)**;
- **campagne di sensibilizzazione** e **di responsabilizzazione** dei **cittadini,** in particolare mediante l'alfabetizzazione mediatica.
  La diffusione di notizie da parte della Commissione europea sulle iniziative dell'UE, nonché sulla disinformazione nei confronti dell'Unione, avviene regolarmente attraverso i propri ***account social***.
  Obblighi a carico degli Stati membri circa il rafforzamento delle misure di **alfabetizzazione mediatica** sono in linea con le previsioni della recente direttiva UE n. 2018/1808 sui **servizi di media audiovisivi**.

Nell'ambito di tale settore si ricorda, infine, l'istituzione di una sezione europea della **rete internazionale di verificatori di fatti**, con il compito di approfondire le strutture che sostengono la disinformazione e dei meccanismi che ne determinano le modalità di diffusione online, e di scambiare le migliori pratiche per conseguire la più ampia copertura possibile di correzioni fattuali nell'UE.

Parte quarta: Iniziative in materia di *cyber security* in ambito comparato

(a cura del Servizio Biblioteca)

STRATEGIE NAZIONALI E MISURE LEGISLATIVE IN MATERIA DI CYBERSECURITY ADOTTATE IN FRANCIA, GERMANIA E REGNO UNITO

1. Francia

Nell'ottobre 2015 è stata annunciata la **Strategia nazionale per la sicurezza digitale** (*Stratégie nationale pour la sécurité du numérique*), diretta a sostenere la transizione digitale della società francese.

La Strategia è caratterizzata da **cinque obiettivi**:

1. Garantire la sovranità della Francia e assicurare la sicurezza delle sue infrastrutture critiche nel caso di un grande attacco informatico. Questo obiettivo è perseguito rafforzando le capacità scientifiche, tecniche e industriali necessarie e la sicurezza delle infrastrutture vitali;
2. Proteggere i cittadini e le imprese e combattere la criminalità informatica. In questa direzione è promosso il percorso "*identité numérique*", allo scopo di rafforzare la fiducia degli utenti nella loro vita digitale, limitando il rischio di uno sfruttamento indesiderato dei loro dati, e creare altresì un dispositivo nazionale di assistenza alle vittime di atti di cyber-violenza;
3. Sensibilizzare i ragazzi sulla sicurezza digitale e sui comportamenti responsabili nel cyberspazio, a partire dall'età scolastica. Anche l'istruzione superiore e la formazione continua devono comprendere una sezione dedicata alla *sécurité numérique*;
4. Sviluppare un ecosistema favorevole alla ricerca e all'innovazione e rendere la sicurezza digitale un fattore di competitività. La Francia sostiene lo sviluppo dell'economia e la promozione internazionale dei suoi prodotti e servizi digitali e garantisce la disponibilità di prodotti e servizi digitali con livelli di fiducia e sicurezza adeguati agli usi e alle minacce informatiche;
5. Promuovere la cooperazione con gli Stati membri volontari in modo da favorire un'Autonomia strategica digitale europea

(*Autonomie stratégique numérique européenne*), giocando un ruolo attivo nella promozione di un cyberspazio sicuro, stabile e aperto.

Dal punto di vista operativo, i cinque obiettivi possono essere raggiunti grazie alla partecipazione di diversi soggetti.

Un ruolo fondamentale è svolto dall'**Agenzia nazionale della sicurezza dei sistemi di informazione** (*Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI*), che è il soggetto primario incaricato di misurare e valutare i rischi e gli effetti degli attacchi informatici, rivolti sia ai soggetti pubblici sia ai privati.

Il ruolo dell'ANSSI è quello di promuovere una risposta coordinata ed efficiente ai problemi di della sicurezza digitale in Francia.

L'Agenzia, istituita con il *Décret n. 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information»*, svolge in particolare le seguenti funzioni:

- assicura la funzione di autorità nazionale per la difesa dei sistemi di informazione. In questa veste, propone al Primo ministro misure per rispondere alle crisi che incidono o minacciano la sicurezza dei sistemi di informazione delle autorità pubbliche e degli operatori di vitale importanza e coordina, nel quadro degli orientamenti stabiliti dal Primo ministro, l'azione del governo in materia di difesa dei sistemi di informazione;
- progetta, fa realizzare e attua i mezzi interministeriali sicuri di comunicazioni elettroniche necessari per il Presidente della Repubblica e il Governo;
- anima e coordina i lavori interministeriali sulla sicurezza dei sistemi informativi;
- elabora le misure di protezione dei sistemi di informazione proposti al Primo ministro. Assicura l'applicazione delle misure adottate;
- effettua ispezioni dei sistemi informativi dei servizi statali e degli operatori pubblici o privati;

- implementa dispositivi di rilevamento degli eventi che possono influire sulla sicurezza dei sistemi di informazione dello Stato, delle autorità pubbliche e degli operatori pubblici e privati, e coordina la risposta a tali eventi; raccoglie le informazioni tecniche relative agli incidenti che interessano i sistemi di informazione di tali soggetti; può inoltre aiutare a rispondere a questi incidenti;
- rilascia le approvazioni per dispositivi e meccanismi di sicurezza destinati a proteggere, nei sistemi di informazione, le informazioni coperte dal segreto di difesa nazionale;
- partecipa ai negoziati internazionali e collabora con le controparti straniere;
- assicura la formazione del personale qualificato nel campo della sicurezza dei sistemi di informazione (art. 3 del Decreto del 2009, come modificato nel 2018).

L'ANSSI fa riferimento al Segretario della difesa e della sicurezza nazionale (*Secrétaire général de la défense et de la sécurité nationale*), che assiste il Primo ministro nell'esercizio delle sue responsabilità in materia di difesa e sicurezza.

La Direzione dell'ANSSI è affidata a un Direttore generale, nominato dal Primo ministro. L'ANSSI è articolata in cinque Sotto-direzioni:

1. Sotto-direzione Amministrazione (*Sous-direction Administration*, SDA);
2. Sotto-direzione Expertise (*Sous-direction Expertise*, SDE);
3. Sotto-direzione Digitale (*Sous-direction Numérique*, SDN);
4. Sotto-direzione Operazioni (*Sous-direction Opérations*, SDO);
5. Sotto-direzione Strategia (*Sous-direction Stratégie*, SDS).

All'interno della SDO opera il Centro governativo di vigilanza, allerta e risposta agli attacchi informatici (*Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*, CERT-FR), che fornisce supporto alla gestione degli incidenti a ministeri, istituzioni, giurisdizioni, autorità indipendenti, collettività territoriali e OIV (operatori di importanza vitale). È responsabile dell'assistenza agli

organi dell'amministrazione nell'attivare i mezzi di protezione necessari. Esso svolge funzioni di CERT (*computer emergency response team*) nazionale[45].

Ai sensi dell'art. L. 2321-1 del codice della difesa (inserito dalla *Loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*), nel quadro della strategia di sicurezza nazionale e della politica di difesa, il Primo ministro definisce la politica e coordina l'azione del Governo in materia di sicurezza e di difesa dei sistemi di informazione. Egli a tal fine ha a sua disposizione l'autorità nazionale di sicurezza dei sistemi di informazione.

La *Loi n. 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense* ha fissato gli orientamenti relativi alla politica di difesa e ha indicato la programmazione militare per il periodo 2019-2015. In materia di cybersicurezza, la legge consente agli operatori di comunicazioni elettroniche, per le esigenze della difesa e della sicurezza dei sistemi di informazione, di istituire dispositivi che consentano, a partire da marcatori tecnici, di rilevare gli eventi che possono incidere sulla sicurezza dei sistemi di informazione dei loro abbonati. Quando viene a conoscenza di una minaccia, l'ANSSI può chiedere a questi operatori di sfruttare i marcatori di attacco informatico che fornirà loro (art. L. 33-14 del codice delle poste e delle comunicazioni elettroniche, inserito dalla legge n. 2018-607).

L'ANSSI coordina i **Centri per la valutazione della sicurezza dell'informazione** (*Centres d'Évaluation de la Sécurité des Technologies de l'Information*, CESTI) che sono fornitori di servizi volti a certificare la sicurezza dei prodotti[46]. Un prodotto per essere certificato deve rispettare le regole del regime di certificazione francese, che permette due tipi di valutazione:

[45] I CERT sono organismi incaricati di raccogliere le segnalazioni di incidenti informatici e potenziali vulnerabilità nei software che provengono dalla comunità degli utenti interessati.

[46] Si veda anche il *Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*, relativo alla certificazione francese per i prodotti e i sistemi di sicurezza.

- la conformità al livello di garanzia della valutazione[47];
- la certificazione della sicurezza di primo livello (*Certification de Sécurité de Premier Niveau*, CSPN) dei prodotti informatici, istituita dall'ANSSI nel 2008.

L'ANSSI dispone di un proprio centro di formazione, il **Centro di formazione sulla sicurezza dei sistemi di informazione** (*Centre de formation à la sécurité des systèmes d'information*, CFSSI), che in particolare rilascia un Diploma di esperto in sicurezza dei sistemi di informazione (ESSI) riconosciuto come titolo di livello 1 e registrato nel Repertorio nazionale delle certificazioni professionali.

Un altro soggetto molto importante è la **Commissione nazionale dell'informatica e delle libertà** (*Commission Nationale de l'Informatique et des Libertés*, CNIL), istituita con la legge n. 78-17 (*Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*).

La CNIL è un'autorità amministrativa indipendente che è responsabile di garantire che l'informatica sia al servizio del cittadino e che non violi l'identità e i diritti umani, la privacy, la libertà individuale e quella pubblica. La CNIL analizza le ripercussioni delle innovazioni tecnologiche sulla privacy e sulla libertà e collabora con gli analoghi soggetti europei e internazionali per sviluppare una regolamentazione armonizzata.

La Commissione si compone di un collegio multidisciplinare di diciotto membri, di cui:

- 4 parlamentari (2 deputati, 2 senatori);
- 2 membri del Consiglio economico, sociale e ambientale;

[47] La *Evaluation Assurance Level* (livello di garanzia della valutazione) di un prodotto o sistema elettronico è un valore numerico che esprime una valutazione di sicurezza basata sui *Common Criteria*, standard internazionale in vigore dal 1999, poi riconosciuto dall'ISO mediante la ISO/IEC 15408. Il prodotto valutato, detto "TOE" (*Target of Evaluation*, in italiano ODV, oggetto della valutazione), può essere hardware, software o entrambi. Può variare da un minimo di EAL1 a un massimo di EAL7.

- 6 rappresentanti dei tribunali superiori (2 consiglieri di stato, 2 consiglieri della Corte di cassazione, 2 consiglieri della Corte dei conti);
- 5 persone qualificate designate dal Presidente dell'Assemblea nazionale (1 personalità), dal Presidente del Senato (1 personalità), dal Consiglio dei ministri (3 personalità). Il mandato dei commissari è di cinque anni o, per i parlamentari, di durata pari alla loro carica elettiva;
- il presidente della CADA (Commissione di accesso ai documenti amministrativi).

Il Presidente della CNIL è nominato con decreto del Presidente della Repubblica, tra i membri della Commissione stessa, il suo mandato è di cinque anni.

Le sue **missioni principali** sono:

1. Informare e proteggere i diritti. Svolge azioni di comunicazione pubblica attraverso la stampa, il sito web, la presenza sui social network o fornendo strumenti pedagogici. Può essere direttamente interpellata da organismi, società o istituzioni per condurre azioni di formazione e sensibilizzazione sul RGPD (Regolamento generale sulla protezione dei dati)[48], la CNIL partecipa anche a mostre o conferenze per informare e allo stesso tempo informarsi. Essa garantisce che i cittadini possano accedere efficacemente ai dati contenuti nei trattamenti che li riguardano. Chiunque può contattare la CNIL in caso di difficoltà nell'esercizio dei propri diritti inviando un reclamo concernente:

- la reputazione online;
- il commercio;
- le risorse umane;
- le banche e il credito;

[48] Il regolamento generale sulla protezione dei dati (in inglese *General Data Protection Regulation*) è il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. Adottato il 27 aprile 2016, esso è entrato in vigore il 25 maggio dello stesso anno e operativo a partire dal 25 maggio 2018.

2. Accompagnare e consigliare. Nel quadro del RGPD, la conformità è un indicatore di buona governance, che soddisfa la sfida della reputazione, della fiducia e costituisce un vantaggio competitivo per le aziende. Per aiutare gli organismi pubblici e privati a prepararsi all'implementazione del RGPD, la CNIL offre una serie di strumenti completa e adattata alle loro dimensioni ed esigenze. Le attività di consulenza e regolamentazione della CNIL sono varie: pareri su progetti di testi provenienti dal Governo riguardanti la protezione dei dati personali o la creazione di nuovi archivi, consigli, partecipazione alle audizioni parlamentari. Nell'ambito di questa attività, la CNIL assicura la ricerca di soluzioni che consentano agli organismi pubblici e privati di perseguire i loro legittimi obiettivi nel rigoroso rispetto dei diritti e delle libertà dei cittadini.

3. Anticipare e innovare. Partecipa alla costituzione di un dibattito sociale sulle questioni etiche dei dati. È un punto di contatto e di dialogo con gli ecosistemi dell'innovazione digitale (ricercatori, start-up, laboratori). Contribuisce allo sviluppo di soluzioni tecnologiche che tutelino la privacy, consigliando le aziende il più direttamente possibile, nello spirito della *privacy by design*[49].

Per contribuire ai dibattiti sul digitale, la CNIL ha lanciato LINC, un laboratorio di innovazione digitale, con riflessioni prospettiche, condivisione e sperimentazione in materia.

Al fine di rafforzare la sua missione di monitoraggio e di riflessione, la CNIL guida un comitato di esperti esterni (*Comité de la prospective*) composto da ventitre membri con profili e background diversi: sociologi, economisti, antropologi, filosofi, imprenditori, ricercatori, autori, giuristi, giornalisti.

La *Loi n. 2016-1321 du 7 octobre 2016 pour une République numérique* ha affidato alla CNIL la missione di condurre una riflessione sulle questioni etiche e le questioni sociali sollevate dall'evoluzione delle

[49] In base al principio della *privacy by design* la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali deve comportare l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione sia dell'esecuzione del trattamento medesimo.

tecnologie digitali (v. *Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle*, dicembre 2017).

4. Controllare e sanzionare. Il controllo successivo costituisce un mezzo privilegiato di intervento presso i gestori del trattamento dei dati personali. Permette alla CNIL di verificare in loco l'attuazione concreta della legge. Il programma dei controlli è elaborato in base ai temi di attualità e delle principali problematiche di cui viene interessata la CNIL.

Il Presidente della CNIL ha la possibilità di sollecitare gli organismi che non rispettano le disposizioni del RGDP o della legge a conformarsi entro un dato periodo. Tali comunicazioni formali possono essere rese pubbliche in base alla gravità delle violazioni accertate o al numero di persone interessate.

Dopo il controllo o i reclami, in caso di violazione delle disposizioni del RGPD o della legge da parte dei responsabili del trattamento e dei subappaltatori, la formazione ristretta della CNIL può imporre sanzioni ai responsabili di trattamenti che non rispettano le norme.

La formazione ristretta del CNIL è composta da 5 membri e un Presidente distinto dal Presidente della CNIL.

In base al RGPD, l'ammontare delle sanzioni pecuniarie può arrivare fino a 20 milioni di euro o, nel caso di un'impresa, fino al 4% del fatturato annuale globale. Queste sanzioni possono essere rese pubbliche.

Quando le violazioni del RGPD o della legge vengono portate alla sua attenzione, la formazione ristretta della CNIL può:

- pronunciare un richiamo all'ordine;
- ingiungere di rendere il trattamento conforme;
- limitare temporaneamente o permanentemente un trattamento;
- sospendere i flussi di dati;
- ordinare di soddisfare le richieste per l'esercizio dei diritti delle persone;
- pronunciare una sanzione amministrativa.

Dalla data di notifica della decisione della formazione ristretta, l'organizzazione coinvolta ha un periodo di due mesi per presentare appello al Consiglio di Stato contro la decisione della CNIL.

Per quanto concerne i **centri pubblici di ricerca**, molti sforzi sono stati dedicati alla sicurezza digitale. In particolare, il CNRS (*Centre National de la Recherche Scientifique*) ha dedicato l'anno 2016 alla sicurezza e ha creato un gruppo di ricerca (*Groupement De Recherche*, GDR) specifico sulla sicurezza digitale.

Il ***GDR Sécurité Informatique*** è uno strumento di stimolo per la ricerca scientifica. Gli argomenti trattati dal GDR comprendono la crittografia, la protezione della privacy, la sicurezza dei dati multimediali, la sicurezza di reti e infrastrutture, la sicurezza dei sistemi software e hardware e i metodi formali per la sicurezza.

Il GDR organizza annualmente vari eventi, tra i quali:

- le "giornate nazionali" presso la sede CNRS di Parigi, che riuniscono oltre 200 scienziati. Le giornate nazionali consistono in sessioni plenarie con presentazioni a livello di comunità e sessioni parallele dei gruppi di lavoro;
- una scuola estiva in cybersicurezza, principalmente per i giovani ricercatori che affrontano per una settimana alcuni argomenti sulla sicurezza informatica. Circa 40 giovani ricercatori frequentano ogni anno la scuola;
- una settimana di incontri tra aziende e studenti di dottorato (*Rencontres Entreprises-DOCtorants en Sécurité*, REDOCS), organizzata ogni anno in autunno nel campus CNRS di Gif-sur-Yvette, allo scopo di mettere in contatto i dottorandi con i principali attori economici nel campo della sicurezza informatica.

2. Germania

Strategia nazionale ed atti normativi in materia di cybersicurezza

I progressi compiuti dalla Germania in campo informatico e nell'*high tech* hanno fatto sì che il paese – leader europeo nel settore ICT e quarto al mondo – si confrontasse con le sfide della sicurezza

informatica e delle telecomunicazioni in anticipo rispetto ad altri stati europei. Una delle prime iniziative intraprese dal Governo federale è stata infatti l'istituzione dell'**Ufficio federale per la sicurezza informatica** (*Bundesamt für Sicherheit in der Informationstechnik* - BSI), che ha ufficialmente iniziato la sua attività il 1° gennaio 1991. Ai sensi del § 1 della vigente legge che lo regolamenta (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI-Gesetz* – BSIG del 14 agosto 2009), il BSI è competente per la sicurezza informatica a livello nazionale ed è subordinato al Ministero federale dell'interno. Le aree di competenza di questa agenzia federale con sede a Bonn e in cui lavorano attualmente circa 570 dipendenti, comprendono la protezione delle reti informatiche del Governo federale, la sicurezza delle applicazioni e installazioni informatiche, la verifica e certificazione dei *software* e dei servizi, e, più recentemente, l'allerta da infezioni da *malware*.

La **strategia nazionale sulla cybersicurezza e sulla sicurezza informatica** è stata inizialmente inserita in un contesto di innovazione più ampio che copre tutti i settori strategici ad alta tecnologia. Tale strategia, denominata "***High-Tech Strategie 2020***", è contenuta in una serie di documenti redatti a partire dal 2006 e aggiornata con cadenza quadriennale seguendo le raccomandazioni di un panel di esperti che dal 2006 al 2013 ha ospitato dapprima solo rappresentanti della ricerca e dell'industria, e, a partire dal 2014, anche membri della società civile.

Negli ultimi piani strategici sono state individuate come aree chiave:

- la ***cybersecurity***: le sfide in quest'area riguardano tutte le azioni criminali che possono violare privacy o segreti industriali, mirando all'accesso e all'intercettazione non autorizzata dei dati. Il Governo federale ha riconosciuto priorità alla ricerca sull'informatica forense e la criminologia. L'implementazione del programma è descritta nella ***Cyber-Sicherheitsstrategie für Deutschland***, adottata nel febbraio 2011 e poi aggiornata nel 2016;

- l'***IT Sicherheit***: ha come obiettivo pricipale l'affidabilità e la sicurezza delle reti. Il Governo federale supporta la ricerca nell'IT security con due programmi di finanziamento: "***Selbstbestimmt und sicher in der digitalen Welt 2015-2020***" per la ricerca accademica (attuato dal Ministero federale dell'istruzione e della ricerca), e "*IT Sicherheit in der Industrie*" per le piccole e medie imprese al fine di migliorare i loro livelli di sicurezza;
- le **identità sicure**: la sicurezza delle identità rappresenta un elemento di particolare interesse per il Governo federale. Esse sono alla base della privacy e del commercio elettroncio. Il Governo federale continua a sostenere la ricerca nella creazione di nuovi approcci interdisciplinari con il forum "*Privacy - Self-Determined Living in the Digital World*".

Un primo concreto esito dell'**Agenda digitale** (*Digitale Agenda 2014-2017*), adottata dal Governo federale nel 2014, è rappresentato dalla **Legge per aumentare la sicurezza dei sistemi informatici** (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, IT-Sicherheitsgesetz*) del 17 luglio 2015, con la quale sono state introdotte nuove disposizioni volte a garantire la sicurezza dei sistemi informatici in alcuni settori chiave come quello energetico, alimentare, idrico, sanitario, finanziario e dei trasporti (c.d. **infrastrutture critiche**, *Kritische Infrastrukturen* – **KRITIS**). L'obiettivo della legge è anche quello di migliorare la sicurezza informatica nelle aziende e nell'amministrazione federale, nonché offrire ai cittadini una migliore protezione online. Per la realizzazione di questi scopi sono state estese le funzioni e le competenze del già citato Ufficio federale per la sicurezza informatica che, ai sensi del *§ 8b BSI-Gesetz*, svolge anche la funzione di **Ufficio di registrazione centrale per gli operatori delle infrastrutture critiche** nelle questioni riguardanti la sicurezza informatica (*Zentrale Meldestelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen*).

L'*IT-Sicherheitsgesetz* prevede a carico degli operatori delle infrastrutture strategiche l'obbligo di adottare, entro limiti di costo ragionevoli, provvedimenti specifici in materia di cybersicurezza in linea con il costante progresso tecnologico, ossia quelle misure

organizzative e tecniche necessarie ad evitare inconvenienti tecnici inerenti alla disponibilità, integrità, autenticità e riservatezza dei loro sistemi informatici. Alcune norme specifiche, applicabili al settore delle telecomunicazioni, riguardano il monitoraggio e l'obbligo, per le imprese di questo settore, di avvisare i propri clienti se constatano un uso improprio della connessione mostrando le possibili soluzioni, mentre altre disposizioni *ad hoc* si applicano alle società di energia nucleare che devono rispettare uno *standard* di sicurezza più elevato. Specifiche previsioni riguardano i fornitori di servizi audiovisivi, i quali sono tenuti ad adottare misure volte ad impedire l'accesso non autorizzato ai sistemi utilizzati per la fornitura del servizio e il trattamento illecito dei dati personali.

Gli operatori delle infrastrutture critiche devono inviare ogni due anni all'Ufficio federale per la sicurezza informatica una valutazione recante le informazioni relative alle misure concretamente adottate e ai *bugs* registrati nei loro sistemi informatici. È inoltre previsto l'obbligo di notificare allo stesso Ufficio gravi episodi di *hacking* ed eventuali inadempienze in fatto di sicurezza, nonché il nominativo del referente aziendale in materia di sicurezza informatica. Il mancato rispetto degli obblighi previsto dalla legge è punito con una sanzione pecuniaria fino a 100 mila euro per le violazioni più gravi (*§ 14 BSI-Gesetz*).

Come previsto dal *§ 10 BSI-Gesetz*, in attuazione dell'*IT-Gesetz*, il 3 maggio 2016 è stata emanata la prima parte del regolamento sulle infrastrutture critiche (*Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*, BSI-Kritisverordnung - BSI-KritisV del 22 aprile 2016) che si applica ai settori dell'energia, dell'informatica, delle telecomunicazioni, dell'acqua e dell'alimentazione. Le disposizioni relative invece ai settori finanziario, assicurativo, sanitario e dei trasporti sono entrate in vigore il 30 giugno 2017 a seguito di alcune modifiche integrative al regolamento del 2016 (*Erste Verordnung zur Änderung der BSI-Kritisverordnung* del 21 giugno 2017).

Di recente è stata elaborata dal Ministero federale dell'interno una bozza di **disegno di legge relativo ad una seconda legge sulla sicurezza informatica** (*Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme*, *IT-Sicherheitsgesetz 2.0*), che è

stata resa pubblica il 27 marzo 2019. In base alle disposizioni contenute nel disegno di legge, non ancora presentato al Parlamento, dovrebbero ulteriormente amentare le competenze dell'Ufficio federale per la sicurezza informatica ed essere introdotte diverse norme di carattere penale.

Organismi ed enti federali preposti alla cybersicurezza

Elemento centrale della citata strategia di cybersicurezza è stata l'istituzione del **Centro di difesa cibernetica** (*Cyber-Abwehrzentrum* - Cyber-AZ), una struttura di cooperazione di autorità e organismi di sicurezza che operano a livello federale per la difesa da attacchi informatici alle infrastrutture tecnologiche e industriali della Germania. Il Cyber-Az, istituito in base a una decisione del Governo federale del 23 febbraio 2011, ha sede a Bonn presso l'Ufficio federale per la sicurezza informatica. I principali compiti del Centro sono la prevenzione, l'informazione e l'allerta precoce contro i c.d. attacchi informatici (*Cyber-Angriffe*) diretti contro uno o più sistemi informatici allo scopo di comprometterne la sicurezza.

Per quanto riguarda più specificamente il settore della difesa, che solo nei primi tre mesi del 2017 ha subito 284 mila attacchi informatici, tutte le funzioni relative alla cybersicurezza sono state accentrate in una **nuova struttura interforze** con quartier generale a Bonn, l'**Unità di cyberdifesa nazionale** (*Kommando Cyber- und Informationsraum* - **KdoCIR**) inaugurata alla presenza dell'allora Ministro federale della difesa Ursula von der Leyen ed entrata in funzione il 5 aprile 2017 per sovrintendere alle operazioni cybernetiche e coordinare l'infrastruttura IT, le comunicazioni militari, operative e i servizi di geolocalizzazione. Il KdoCIR rappresenta quindi l'equivalente del Cyber-AZ – creato solo per scopi civili – sul piano militare. L'Unità, che dispone di un *team* di 13.500 effettivi su tutto il territorio della Germania sotto il comando del generale *Ludwig Leinhos*, raggiungerà la piena operatività nel 2021. La Germania ha quindi ideato, come è stato definito dalla stampa, un corpo di *cyber marines* in grado di fronteggiare la difficile sfida della cybersicurezza a livello globale e che potrebbe rappresentare un primo passo verso la costituzione di una specie di corpo di armata unico per la cyberdifesa dell'Unione europea.

Successivamente, il 14 settembre 2017, è stata inaugurata a Monaco di Baviera una **nuova Agenzia per la cybersicurezza** (Ufficio centrale per l'informatica nel settore della sicurezza, *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* – **ZITiS***)* come parte di un tentativo centralizzato per affrontare la criminalità informatica e lo spionaggio digitale mediante la sorveglianza delle telecomunicazioni di massa, la crittografia dei dati e la raccolta delle informazioni. Dal punto di vista giuridico, lo ZIYiS è stato istituito come ente federale senza capacità giuridica nella sfera di competenza del Ministero federale dell'interno con un decreto ministeriale (*Erlass*), emanato il 6 aprile 2017 dall'allora Ministro federale dell'interno De Maizière.

Lo ZITiS, come ha dichiarato lo stesso Ministro federale dell'interno, rappresenta un investimento di grande importanza, destinato a diventare una risorsa tecnologica a servizio degli altri servizi di sicurezza della Germania. I compiti della nuova Agenzia includono anche la "scienza forense digitale" per poter sviluppare nuovi metodi finalizzati alla raccolta di prove provenienti da internet. Lo ZITiS, il cui organico iniziale è di 120 unità per un investimento iniziale di 10 milioni di euro, ricerca ed elabora strategie di sorveglianza delle telecomunicazioni per conto di altre agenzie.

Da ultimo, il 6 settembre 2018 il Governo federale ha approvato la creazione di un'**Agenzia per per l'innovazione nella cybersicurezza** (*Agentur für Innovation in der Cybersicherheit*) investendo 200 milioni di euro in un programma di durata quadriennale. La nuova agenzia governativa sarà guidata congiuntamente dal Ministero federale della difesa e dal Ministero federale dell'interno con l'obiettivo di proteggere e difendere lo Stato dalle minacce del futuro, *in primis* dai *cyber* attacchi. Come modello per la creazione di questa nuova organizzazione governativa è servita la Darpa del Pentagono USA (*Defense Advanced Research Projects Agency*). La nuova Agenzia avrà in forza un centinaio di operatori per diventare pienamente operativa nei prossimi 4 anni. Lo scopo dei funzionari del Ministero federale della difesa che lavoreranno al progetto è quello di rafforzare la rete di sicurezza informatica del paese con l'acquisizione di tecnologie adeguate,

garantendo la sicurezza dei dati sensibili e lo sviluppo di contromisure per difendere la Germania e i paesi alleati della Nato dai sofisticati attacchi di *hacker* (o *cracker*) che si sono moltiplicati nell'ultimo triennio.

Per completare il quadro delle istituzioni impegnate a livello federale nel realizzare gli obiettivi della strategia relativa alla cybersicurezza, si segnala infine la **risposta scritta del Governo federale** (stampato BT n. 19/2645 dell'11 giugno 2018) ad un'interrogazione presentata dai deputati del gruppo parlamentare liberale in merito all'esistenza di dipartimenti, nella sfera di competenza di vari Ministeri federali, che si occupano di cyberdifesa e di contro-attacchi informatici.

3. Regno Unito

Il tema della sicurezza delle **infrastrutture di interesse nazionale** (*critical national infrastructures* – CNI) e della loro esposizione al rischio di attacchi cibernetici è stato oggetto, negli ultimi anni, di specifiche iniziative del Governo e del Parlamento del Regno Unito. L'impatto dell'evoluzione tecnologica e il pericolo di *cyber-attacks*, con effetti potenzialmente dirompenti sull'organizzazione sociale ed economica nazionale, sono stati annoverati dal Governo tra le maggiori sfide poste al Paese al momento di sottoporre a verifica, nel 2018, lo stato di attuazione della strategia per la sicurezza e la difesa adottata nel 2015[50]. Tali iniziative, d'altra parte, si sono delineate in un quadro normativo e istituzionale assai articolato.

In tema è di riferimento generale la legislazione applicabile ai reati a carattere informatico, compresa l'intrusione abusiva in sistemi informatici; essa forma un *corpus* normativo stratificato di cui fanno parte, tra le altre, le previsioni in materia di *hacking* (*Computer Misuse Act 1990*), di furto di identità (*Fraud Act 2006*), di sicurezza riferita rispettivamente alle telecomunicazioni (*Communications Act 2003*) e ai dati personali (materia ora disciplinata dal Regolamento UE

[50] *National Security Capability Review* (marzo 2018), concernente il secondo anno di implementazione della *National Security Strategy 2015* e della *Strategic Defence and security Review 2015*.

2016/679 e dal *Data Protection Act 2018* quale disciplina nazionale di adattamento); nonché, per gli aspetti rilevanti, dalla disciplina sul contrasto delle attività di stampo terroristico (*Terrorism Act 2000*) e sulla intercettazione delle comunicazioni (*Investigatory Powers Act 2016*).

In relazione più specifica al tema della cibersicurezza, il Governo ha dato attuazione, con le *Network and Information System Regulations 2018*[51], alla recente disciplina euro-unitaria in materia, prevedendo misure di sicurezza[52] per le infrastrutture nazionali in tredici ambiti prioritari[53].

La portata innovativa delle *regulations* ben si comprende ove si consideri che la disciplina delle infrastrutture di interesse nazionale è stata prima applicata da *authorities* di regolazione, competenti a vigilare sull'assetto della concorrenza dei mercati di riferimento oppure anche su profili inerenti alla sicurezza (*economic* o *security regulators*), assolvendo in taluni casi ad entrambi i compiti (è il caso, dal 2011, di Ofcom, autorità di regolazione delle telecomunicazioni); per converso, l'introduzione del principio della **resilienza** rispetto ai rischi di *cyber-attacks* comporta ora il complessivo e uniforme incremento dei livelli di sicurezza nel settore dei servizi essenziali, in prospettiva soprattutto della continuità della loro erogazione.

Tale obiettivo è perseguito dalle *regulations* attraverso l'obbligo posto sugli operatori (incluse le pubbliche amministrazioni) di implementare misure di sicurezza "appropriate e proporzionate"; l'istituzione di *competent authorities*, ovvero di autorità di regolazione e controllo, in ciascun settore al quale si applica la disciplina, al fine di assicurarvi il rispetto delle prescrizioni; l'individuazione di un unitario "punto di contatto" nell'ambito del Governo nazionale, che

[51] S.I. 2018 n. 506.

[52] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[53] I tredici settori delle *critical national infrastructures* individuati dal Governo sono quelli della chimica, dell'energia nucleare civile, delle comunicazioni, della difesa, dei servizi di protezione civile, dell'energia, della finanza, delle risorse alimentari, dell'amministrazione pubblica, nonché la sanità, il settore aerospaziale, i trasporti e le risorse idriche.

sia di riferimento per gli altri Stati membri dell'Unione Europea, e la creazione di un *team* abilitato alla gestione degli incidenti (le cui funzioni, assieme a quelle del "*single point of contact*", sono assolte dal *National Cyber Security Centre* su cui *infra*).

Il raggio applicativo delle ***regulations*** si estende ai settori delle risorse idriche, della sanità, dei trasporti, delle telecomunicazioni, mentre ne è escluso l'ambito finanziario e bancario (pur contemplato dalla direttiva), nel presupposto esso sia già oggetto di normative specifiche. Gli operatori dei settori implicati (i cui servizi sono considerati "essenziali", ai fini della normativa, in relazione a soglie numeriche riferite alla platea dei rispettivi utenti), sono tenuti a conformarsi alle linee-guida predisposte dalle competenti autorità di regolazione (le quali a loro volta adottano a base della propria attività le regole di "buona pratica" stabilite dal *National Cyber Security Centre*). Le *regulations*, infine, fanno obbligo agli operatori di denunciare tempestivamente, entro 72 ore, gli incidenti il cui impatto superi soglie predeterminate dalle *authorities* di riferimento; e prevedono, per la violazione delle prescrizioni in materia di cyber-sicurezza, **sanzioni pecuniarie** di ammontare fino a 17 milioni di sterline.

Significative innovazioni in materia di cyber-sicurezza, peraltro, si correlano all'adozione, nel 2016, del **piano strategico nazionale** quinquennale ad essa specificamente dedicato (*National Cyber Security Strategy 2016-2021* - NCSS[54], dotata di uno stanziamento di 1,9 miliardi di sterline).

In questa occasione il Governo ha mutato l'impostazione accolta nel piano strategico riferito al quinquennio precedente[55], che assegnava ampio spazio all'iniziativa degli operatori privati e al mercato per la diffusione e l'implementazione di elevati standard di sicurezza nel settore sia privato che pubblico; constatando i limitati vantaggi di un simile approccio esso ha infatti riconosciuto, per il

[54] *National Cyber Security Strategy 2016-2021*.

[55] Si tratta della prima *National Cyber Security Strategy* riferita al periodo 2011-2016, adottata nel 2010 e finanziata con uno stanziamento di 860 milioni di sterline.

perseguimento del medesimo obiettivo, il ruolo dei poteri pubblici e la maggiore incisività del loro intervento[56].

In particolare, si è provveduto ad istituire un organismo tecnico *ad hoc*, il ***National Cyber Security Centre*** (NCSC)[57], preposto alla gestione degli incidenti di rilievo nazionale nel campo della cibersicurezza e all'assistenza tecnica diretta ai dipartimenti governativi, alle amministrazione pubbliche e alle imprese attraverso attività di analisi e di individuazione delle minacce, di consulenza, di promozione dell'innovazione e delle competenze professionali in materia[58]. Nell'espletamento dei suoi compiti il NCSC si inserisce nella rete di collaborazione tra gli organismi le cui competenze riguardano la sicurezza dello Stato (*Government Communications Headquarter* – GCHQ[59]) e la protezione delle infrastrutture di interesse nazionale (CPNI[60]).

Il piano strategico vigente condensa i propri obiettivi avvalendosi tre fondamentali parole-chiave: *Defend*, *Deter*, *Develop*. Ovvero si fa riferimento (*Defend*) alla resilienza delle reti di comunicazione nel settore pubblico e in quello privato ed imprenditoriale rispetto agli attacchi esterni, e in particolare lo schema (denominato *Active Cyber Defence*) che fa leva sull'adozione, in modo appropriato e "proattivo", di misure di sicurezza idonee a rafforzare i livelli di tutela. Viene altresì postulata la complessiva capacità del sistema a dispiegare un'azione di deterrenza (*Deter*) rispetto a simili minacce, elevando i costi necessari a metterle in atto e riducendo i benefici che da ciò possono trarsi, anche attraverso l'inasprimento delle sanzioni e il dispiegamento di misure diplomatiche, politiche, economiche. Infine, si persegue in ambito nazionale lo sviluppo

[56] "*Only Government can draw on the intelligence and other assets required to defend the country from the most threats. Only Government can drive cooperation across the public and private sectors and ensure information is shared between two. Government has a leading role, in consultation with industry, in defining what good cyber security looks like and it is implemented*": *National Cyber Security Strategy 2016-2021*, p. 27.

[57] Del NCSC può consultarsi la *Annual Review 2018*.

[58] Un bilancio dell'attività finora svolta dal NCSC v. la relazione del Cabinet Office, *National Cyber Security Strategy 2016-2021 – Progress report*.

[59] Si segnala al riguardo che il NCSC ha assorbito il CESG, precedentemente incardinato nel GCHQ come sua articolazione deputata alla *information security*.

[60] *Center for Protection of National Infrastructure*.

(*Develop*) delle competenze e capacità professionali e tecnologiche necessarie alla tutela del Paese dai rischi suddetti.

Nel piano strategico, infine, è fatto riferimento all'uscita del Regno Unito dall'Unione Europea, affermandosi al riguardo la necessità della continuazione degli accordi di **cooperazione internazionale** in questo ambito – specie con la *European Union Agency for Network and Information Security* (ENISA) -, stante l'evidente carattere transnazionale dei fenomeni considerati.

Sul versante parlamentare, deve segnalarsi l'**indagine** condotta dalla commissione bicamerale competente (*Joint Committee on National Security Strategy*) sull'attuazione del piano strategico da ultimo richiamato.

La commissione ha espresso, anche sulla base delle risultanze acquisite attraverso un ciclo di audizioni, alcune riserve circa la complessiva adeguatezza delle misure previste rispetto alla gravità dei rischi a cui sono esposte le infrastrutture vitali del Paese, dovendosi queste considerare come i possibili "bersagli naturali" di attacchi perpetrati attraverso le reti di telecomunicazione da gruppi criminali o da Stati stranieri al fine di interferire con il loro regolare funzionamento, o di violare segreti industriali e diritti di privativa, oppure di compiere atti di spionaggio. La commissione ha pertanto evidenziato, nella relazione pubblicata nel novembre 2018[61], una serie di aspetti per i quali ha segnalato al Governo l'esigenza di assicurare maggiori livelli di **resilienza** delle infrastrutture suddette, nella consapevolezza che sia impossibile garantirne la sicurezza assoluta e che la capacità di rispondere ad insidie ripetute e costanti, da parte di soggetti statali e non statali, rappresenti ormai il parametro della normalità[62].

D'altra parte il grado di interconnessione e di interdipendenza instauratosi tra le diverse infrastrutture, a giudizio della commissione, rende ormai inadeguata la designazione di ciascuna di queste come prioritaria, poiché gli incidenti che potrebbero colpirle avrebbero inevitabilmente ricadute sugli operatori di altri settori.

[61] *House of Lords – House of Commons, Joint Committee on National Security Strategy*, *Cyber security of the UK's Critical national Infrastructure* (Third Report of Session 2017-2019).

[62] V. il documento citato alla nota precedente, p. 12.

Pertanto, mentre si auspica l'adozione di un approccio "sistemico" in occasione della redazione del prossimo piano strategico in materia, è raccomandata la preposizione di un Ministro membro del *Cabinet Office* all'attività di coordinamento delle attuali misure di *cyber–resilience* concernenti i singoli ambiti infrastrutturali.

Inoltre, come già evidenziato in una precedente relazione del luglio 2018[63], il Regno Unito registra la perdurante carenza di **profili professionali** specialistici nei maggiori settori infrastrutturali; il tema è stato preso in specifico esame dalla commissione bicamerale, che proprio nel "cambiamento culturale" ha individuato la condizione affinché possa aversi un costante miglioramento al passo con l'evoluzione tecnologica.

La raccomandazione della commissione bicamerale generalmente rivolta ad un'espansione dell'intervento dello Stato in un ambito di tale complessità (e in cui, a suo avviso, si è registrato anche un "fallimento del mercato" le cui cause il Governo ha finora mancato di valutare adeguatamente), è stata seguita dall'annuncio (l'11 maggio 2019)di un progetto di legge dedicato al particolare profilo della cibersicurezza nell'ambito dell'"Internet delle cose" (***Internet of things***), di rilevante impatto sociale ove si consideri la pervasività delle correlate applicazioni tecnologiche, di crescente diffusione anche in ambito domestico[64].

Le linee fondamentali della disciplina, finalizzata ad introdurre, tra l'altro, requisiti minimi obbligatori di sicurezza incorporati nei dispositivi tecnologici fin dalla loro fabbricazione, è stata oggetto di una consultazione pubblica[65] promossa dal *Department for Digital, Culture, Media and Sport* nel quadro dell'iniziativa denominata *Secure by design*[66], concretizzatasi in una serie di documenti programmatici e

---

63 *House of Lords – House of Commons, Joint Committee on National Security Strategy*, *Cyber Security Skills and the UK's Critical National Infrastructure* (*Second Report of Session* 2017-2019). Sul tema dello *skill gap* in questo ambito vedasi la replica del Governo alla relazione parlamentare, del 13 novembre 2018.

64 *Plans announced to introduce new laws for internet connected devices (*press release, 1 May 2019)

65 *Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security*.

66 *Secure by Design*.

di codici di condotta concernenti gli standard di sicurezza e la tutela dei consumatori in questo settore.

Appendice: Definizioni

Advanced Automation

Espressione riferita ai più recenti sviluppi nei sistemi di produzione automatizzati, caratterizzati da elevata capacità cognitiva, interazione e adattamento al contesto, auto-apprendimento e riconfigurabilità. L'esempio più evidente di questa famiglia di tecnologie sono i robot collaborativi (co-bots), che sono progettati per lavorare al fianco degli operatori.

Advanced Human Machine Interface (Advanced HMI)

Espressione riferita ai recenti sviluppi nel campo dei dispositivi wearable e delle nuove interfacce uomo/macchina per l'acquisizione e/o la veicolazione di informazioni in formato vocale, visuale e tattile (per esempio display touch, scanner 3D, visori per la realtà aumentata).

Additive Manufacturing

Anche nota come Stampa 3D, ribalta l'approccio dei processi produttivi classici (asportazione o deformazione plastica di materiale) creando un oggetto attraverso la sua "stampa" strato per strato. Trova applicazione in 4 ambiti: Rapid Prototyping, Rapid Manufacturing, Rapid Maintenance Repair, Rapid Tooling.

Advanced Persistent Threat (APT).

Minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti bersaglio al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle reti dell'ente obiettivo

Apprendimento automatico

Denota la capacità di un software/computer di apprendere dal proprio ambiente o da una serie molto ampia di dati rappresentativi, consentendo ai sistemi di adattare il loro comportamento a circostanze mutevoli o di eseguire compiti per i quali non sono stati programmati esplicitamente.

Artificial Intelligence (AI)

Indica un'ampia gamma di sistemi basati su software che hanno la capacità di analizzare, sulla base di dati e attraverso algoritmi, operazioni

specifiche anche molto complesse nonché caratteristiche di contesto esterno e di fornire risposte in qualche misura autonome, basate sull'analisi complessa dei dati a disposizione: per tale motivo vengono definiti come sistemi "intelligenti". L' Artificial Intelligence abbraccia una vasta serie di sotto branche quali l'informatica cognitiva (cognitive computing: algoritmi capaci di ragionamento e comprensione a un livello superiore, ossia più simile alla mente umana), apprendimento automatico (machine learning: algoritmi in grado di apprendere autonomamente determinate mansioni), intelligenza aumentata (augmented intelligence: collaborazione tra uomo e macchina), robotica intelligente (AI robotics: intelligenza artificiale incorporata nei robot).

Attacchi Distributed Denial of Service Attacks

Aggressioni nelle quali un numero rilevante di computer, controllati dal medesimo attore, lanciano attacchi DDoS coordinati contro un sistemaobiettivo, per comprometterne il funzionamento (cfr *infra. DDoS).*

Blockchain (Registri distribuiti)

Consiste in uno strumento tecnologico innovativo che consente la creazione e gestione di archivi o registri distribuiti, che sono in grado di registrare e gestire transazioni di vario tipo, sia finanziarie che aventi ad oggetto beni o servizi di altra natura, le quali vengono controllate, validate secondo specifiche modalità di "consenso" e condivise da tutti i c.d. nodi che fanno parte della rete. La definizione di blockchain è stata inserita nel nostro ordinamento dall'articolo 8-ter del D.L. 14 dicembre 2018, n. 135. La norma definisce come "tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati, sia in chiaro che ulteriormente protetti da crittografia, verificabili da ciascun partecipante, non alterabili e non modificabili. La norma prevede inoltre che la memorizzazione di un documento informatico attraverso l'uso di tecnologie blockchain produca gli effetti giuridici della validazione temporale elettronica, ai sensi dell'articolo 41 del Regolamento UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Per quanto riguarda gli utilizzi della blockchain, il World Economic Forum nel documento: "Deep Shift Technology Tipping Points and Societal Impact" ritiene che entro il 2027 il 10% del PIL mondiale sarà prodotto da attività e servizi che passeranno attraverso le blockchain.

Blockchain permissionless e blockchain permissioned

Le *blockchain* possono essere *permissionless* e in tal caso tutti i nodi della medesima possono partecipare paritariamente alla validazione dei blocchi (questo è il sistema della più nota delle *blockchain* Bitcoin) ovvero *permissioned*. In tal caso il processo di validazione può essere riservato ad alcuni specifici nodi (*trusted*) e possono anche essere inseriti dei permessi che attribuiscono poteri di intervento diversi ai singoli nodi (ad esempio alcuni soltanto sono in grado di accedere a tutti i dati presenti nella *blockchain*). Questo modello di *blockchain* è generalmente riconosciuto come più adatto per organizzazioni pubbliche, finanziarie o a titolari di dati sensibili.

Botnet

Insieme di dispositivi (compromessi da *malware*) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo DDOS.

Cloud Manufacturing

Applicazione in ambito manifatturiero del paradigma del *cloud computing* che abilita, tramite la rete Internet, l'accesso diffuso, agevole e *on demand* a un insieme virtualizzato, condiviso e configurabile di risorse a supporto di processi produttivi e di gestione della *supply chain*. Le risorse possono andare dal livello infrastrutturale (IaaS), al livello di piattaforma (PaaS), al livello applicativo (SaaS). Sempre più spesso l'espressione *Cloud Manufacturing* viene utilizzata anche per indicare la virtualizzazione di risorse produttive (*Maas, Manufacturing as a Service*).

Cloud Marketplace

Programma gestito da AgID e consente alle amministrazioni di consultare e confrontare le infrastrutture e i servizi *Cloud* qualificati per la PA sulla base di requisiti tecnici e funzionali, rimandando la fase di acquisizione agli strumenti previsti dalla normativa vigente. La qualificazione delle infrastrutture *Cloud* e dei servizi di tipo IaaS, PaaS e SaaS, erogabili alle amministrazioni pubbliche è anch'essa gestita da AgID. Secondo quanto previsto dal "Piano Triennale per l'informatica nella Pubblica Amministrazione 2017-2019" nella fase di definizione di un nuovo progetto e/o sviluppo di servizi, prima di qualsiasi altra opzione

tecnologica, le PA sono tenute ad adottare il paradigma *Cloud*, in particolare soluzioni di tipo SaaS.

Compromised Counterfeit Hardware

Componenti *hardware* che presentano una preventiva installazione di *software* malevolo nascosto, anche all'interno del microprocessore.

Criptovalute

Sono valute virtuali (come *Bitcoin, LiteCoin, Ether e Ripple*) che, come sottolineato dalla Banca d'Italia, non rappresentano in forma digitale le comuni valute a corso legale (euro, dollaro, ecc.); non sono emesse o garantite da una banca centrale o da un'autorità pubblica e generalmente non sono regolamentate. Le valute virtuali non hanno corso legale e pertanto non devono per legge essere obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie, cioè non danno il diritto a utilizzarle come strumento di pagamento (come ad esempio l'euro nell'area geografica dell'Euro), ma possono essere utilizzate per acquistare beni o servizi solo se il venditore è disponibile ad accettarle.

Anche la BCE ha chiarito che, nonostante il B*itcoin* sia comunemente definito come una moneta, in realtà non ne ha le caratteristiche (non è emesso da un'Autorità centrale, non è riconosciuto legalmente come mezzo di pagamento ed ha una eccessiva volatilità) e si configura pertanto come un *asset* speculativo.

Cyber Physical System-CPS)

L'espressione, ricorrente nell'ambito dell'industria 4.0, indica sistemi fisici strettamente connessi con i sistemi informatici, che possono interagire e collaborare con altri sistemi CPS.

Distributed Denial of Service (DDoS)

Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (botnet), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server.

Internet of Things (IoT)

Costituisce un percorso evolutivo della Rete Internet attraverso la quale ogni oggetto fisico acquisisce una sua contropartita nel mondo digitale. Alla

base dell'*Internet of Things* vi sono oggetti intelligenti (capaci cioè di identificazione, localizzazione, diagnosi di stato, acquisizione di dati, elaborazione, attuazione e comunicazione) e reti intelligenti (aperte, standard e multifunzionali). Il loro funzionamento si basa su varie fonti di dati, su sensori incorporati che misurano automaticamente parametri ambientali o possono monitorare un'attività e trasferire i dati su database in modo autonomo, senza intervento umano. I dati sono accessibili, elaborati e analizzati da applicazioni che trasferiscono comandi ai dispositivi fisici nell'ecosistema Iot. Gli ecosistemi *Internet of Things* hanno la caratteristica di essere trasversali rispetto alle diverse aree e settori in cui possono operare (dalla produzione, ai trasporti, alla sanità, ai dispositivi con sensori di vario tipo) e pertanto si relazionano grazie a piattaforme comuni e trasversali. L'ecosistema IoT richiede una configurazione specifica per l'identificazione e la ricerca dell'oggetto, la condivisione di dati (aperta/chiusa), protocolli di comunicazione leggera, un bilanciamento tra l'elaborazione delle informazioni locali e in rete, l'integrazione *back-end* (programmazione che sta dietro le interfacce applicative).

Liability

Con particolare riferimento alle tecnologie innovative digitali l'espressione è utilizzata per indicare l'individuazione della responsabilità in caso di incidente o di attacco informatico.

Malware

Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

Phone hacking

Attività di *hacking* che ha come oggetto i sistemi telefonici (ad esempio mediante l'accesso illegittimo a caselle vocali).

Piano strategico banda ultralarga

La base giuridica del Piano strategico banda ultralarga è rappresentata dall'articolo 30 del decreto-legge 98 del 2011 che ha previsto che per il raggiungimento dell'obiettivo dell'Agenda digitale europea del diritto di accesso a internet per tutti i cittadini "ad una velocità di connessione superiore a 30 Mb/s" e almeno per il 50% "al di sopra di 100 Mb/s", il Ministero dello sviluppo economico, con il concorso delle imprese e gli enti

titolari di reti e impianti di comunicazione elettronica fissa o mobile, predisponga un progetto strategico per individuare gli interventi finalizzati alla realizzazione dell'infrastruttura di telecomunicazione a banda larga e ultralarga. Il *programma operativo del Piano Banda Ultra Larga*, è stato quindi approvato con la delibera n. 65-2015 del CIPE, che ha programmaticamente destinato, a valere sulle risorse del Fondo Sviluppo e Coesione (FSC) 2014-2020, 3,5 miliardi di euro, di cui 2,2 miliardi di euro per interventi di immediata attivazione, rinviando a una successiva delibera l'assegnazione di ulteriori risorse nel limite massimo di 1,3 miliardi di euro. Con la Delibera n. 71 del 7 agosto 2017 il CIPE, sempre a valere sul Fondo Sviluppo e Coesione ha approvato, per il completamento del Piano Banda Ultralarga, l'assegnazione di 1,3 miliardi € per interventi a sostegno della domanda degli utilizzatori.

La Strategia per la crescita digitale 2014-2020 e la Strategia italiana per la banda ultralarga forniscono il quadro per la realizzazione della banda larga e ultralarga.

Ransomware

Malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo.

Sistemi di trasporto intelligenti (ITS)

Sono definiti dal decreto del Ministro delle infrastrutture e dei trasporti 11 febbraio 2013 e rappresentano le tecnologie informatiche e della comunicazione applicate ai sistemi di trasporto, alle infrastrutture, ai veicoli e alla gestione del traffico e della mobilità. Essi comprendono un insieme di strumenti sia per la gestione delle reti di trasporto, che per i servizi ai viaggiatori, quali le informazioni in tempo reale sulle condizioni del traffico stradale o autostradale e le informazioni on-line per programmare un viaggio nonché per prendere decisioni relative (dati di traffico, controlli semaforici, controllo degli accessi, gestione dei parcheggi, pannelli a messaggio variabile, centri di supervisione e controllo integrati, instradamento parcheggi, *call center*, etc).

Smart cities

Concetto ampio e variamente elaborato in questi ultimi anni, ma che si sostanzia nell'idea di città nelle quali gli strumenti di *Information and Communication Technology* (ICT) sono largamente impiegati, con una visione

strategica e pianificata, a supporto dei servizi pubblici e delle infrastrutture, per lo sviluppo sostenibile delle città stesse. Una città intelligente è quindi un luogo in cui le reti e i servizi tradizionali sono resi più efficienti con l'uso delle tecnologie digitali e di telecomunicazione a beneficio dei suoi abitanti e delle sue attività. Nel Piano Triennale 2019-2021 il concetto di *smart cities and communities*, si sta evolvendo verso un modello più ampio di *Smart Landscape*, mediante l'utilizzo di tecnologie abilitanti quali IA, IoT e *Blockchain*, e che comprende anche l'idea di *Smart Logistic* finalizzata all'integrazione dei servizi e alla completa digitalizzazione della catena logistica, alla realizzazione di soluzioni *smart* basate sull'utilizzo di *fast corridor* e nodi logistici interconnessi, sulla ottimizzazione di tempi e costi di spostamento delle merci.

Smart contract

Programma per elaboratore che opera su tecnologie *blockchain* e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse (D.L. 14 dicembre 2018). Gli *smart contract* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia Digitale con linee guida da adottarsi entro 90 giorni dall'entrata in vigore della legge di conversione del decreto legge.

SQL injection

Tecnica di attacco basata sull'uso di *query* indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.

Supply chain

Espressione particolarmente utilizzata con riferimento all'industria 4.0- Indica un sistema di organizzazioni, persone, attività, informazioni e risorse coinvolte nel processo atto a trasferire o fornire un prodotto o un servizio dal fornitore al cliente.

Sviluppo delle reti a banda ultralarga

I progetti per lo sviluppo della banda ultra larga si riferiscono a connessioni da rete fissa. Tuttavia l'infrastruttura in fibra è essenziale anche per un miglioramento della connessione mobile in quanto il rilegamento in fibra delle stazioni radio base è la soluzione che crea le condizioni migliori

per sfruttare appieno le capacità delle reti LTE (cfr. *Piano strategico banda ultralarga)*.

Tecnologie innovative digitali

Espressione utilizzata con riferimento ad un vasto insieme di abilità tecnologiche che consentono di individuare, valutare, utilizzare, condividere e creare contenuti utilizzando le tecnologie informatiche e Internet. In continua evoluzione e implementazione queste nuove tecnologie, nonostante abbiano avuto uno sviluppo relativamente recente e risultino in parte ancora in fase di prima applicazione, hanno già assunto un carattere di natura strategica per la rilevanza del loro uso estensivo in molteplici settori di rilevo della società.