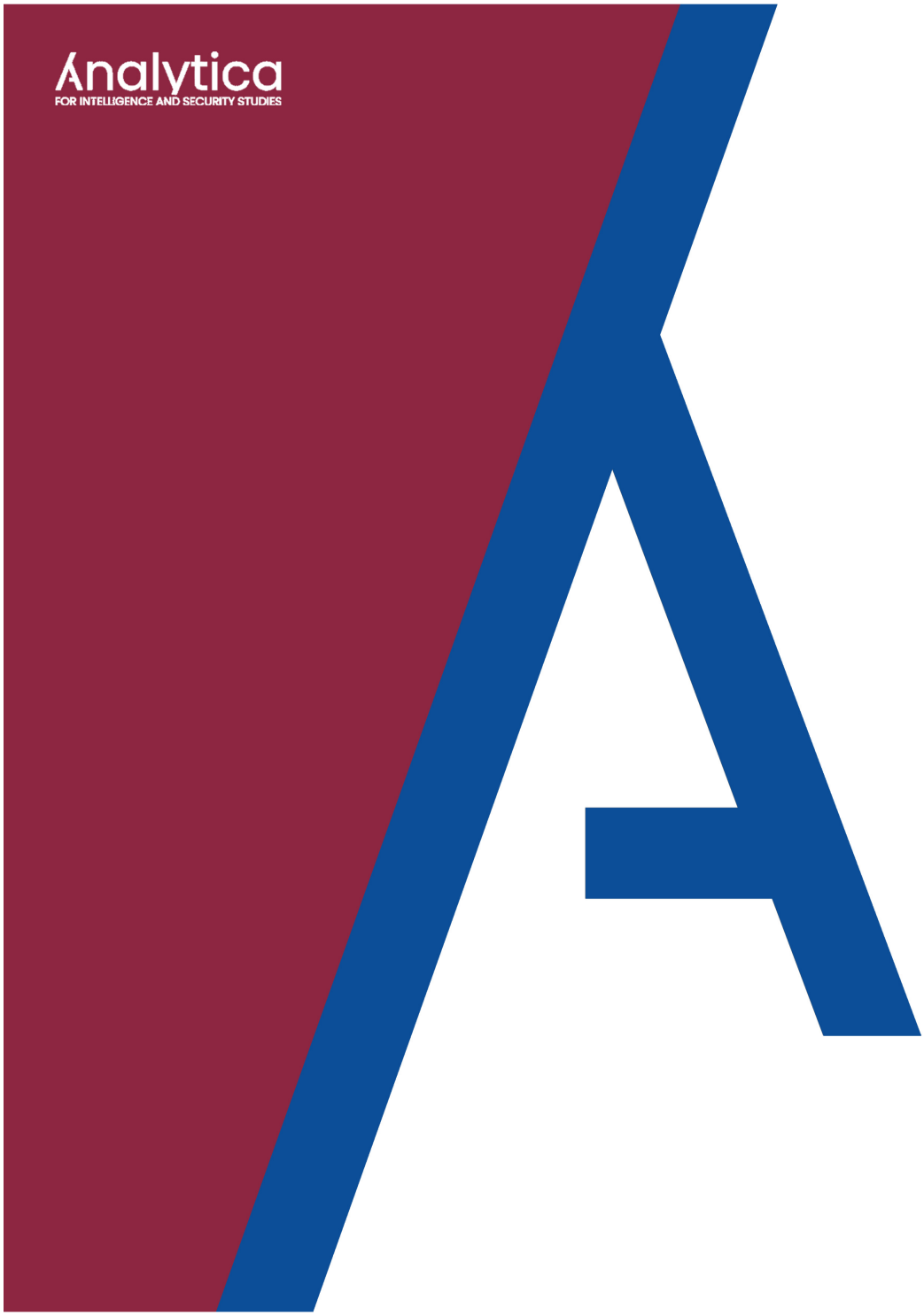

Digital Single Market: la certificazione europea nel nuovo mandato permanente dell'Enisa.

Angela Lena

Analytica for intelligence and security studies

Paper Cyber Security

Digital Single Market: la certificazione europea nel nuovo mandato permanente dell'Enisa.

Angela Lena

Correzioni e revisioni a cura del Dottor PANEBIANCO Andrea

Torino, dicembre 2020

Introduzione

Negli ultimi vent'anni la tecnologia ha pervaso completamente la nostra realtà, contribuendo a creare una società globalizzata e sempre più eterogeneamente interconnessa, che svolge gran parte delle **attività essenziali** *online,* passando così dall'era industriale ad una società dell'informazione sempre più dipendente dalle **tecnologie dell'informazione e della comunicazione** (TIC o *ICT* dall'acronimo inglese *Information and Communications Technology*).

Le politiche per la sicurezza informatica rivestono un ruolo cruciale per lo **sviluppo sociale ed economico**, poiché lo svolgimento degli affari, le interazioni personali e professionali e la tutela dei nostri diritti, oggi più che mai, dipendono dalla disponibilità e dal corretto funzionamento delle ICT. Se è vero, dunque, che le tecnologie digitali possono essere fonti di **innumerevoli vantaggi,** è altrettanto vero che un uso malevolo delle stesse, da parte di attori statali e non, può costituire una **minaccia** non solo per i singoli, ma anche **per la pace e la sicurezza internazionale**.

Come si legge nella Strategia dell'Unione europea per la *cybersecurity*, "non è possibile assicurare i diritti delle persone senza disporre di reti e sistemi sicuri"[1]. Partendo da questo assunto, l'Unione Europea ha sempre avuto come fine ultimo quello di **estendere i suoi valori costitutivi**, di protezione della democrazia, di tutela delle libertà e dei diritti dei cittadini anche **allo spazio cibernetico**, perché solo così è possibile raggiungere quella cyber-resilienza capace di garantire l'*availability,* unitamente alla *confidentiality* ed all'*integrity,* dell'intero sistema ICT e creare un **mercato unico digitale**[2] in grado di superare gli ostacoli esistenti *online* e abbattere i costi per cittadini, imprese e governi, favorendo le opportunità di crescita.

Le **caratteristiche *sui generis*** di questo dominio, che si presenta come uno spazio virtuale che trascende i confini dei singoli Stati, **azzerano i concetti classici di spazio e tempo**[3] e **impongono un'azione coesa** da parte dei singoli Stati, in quanto misure differenziate costituiscono un limite alla *governance* della *cybersecurity*, proprio in virtù del terreno peculiare su cui si gioca questa partita. Nel settembre del 2017[4], la Commissione Europea ha infatti manifestato la necessità di ulteriori sinergie e di un'azione più incisiva da parte degli Stati, passando da un "approccio reattivo ad uno proattivo".

---

[1] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 7 febbraio 2013, Strategia dell'Unione europea per la cibersicurezza: uno spazio aperto e sicuro, JOIN/2013/01 final, p. 4.

[2] Il Digital Single Market è stato definito come un mercato in cui è garantita la libera circolazione di merci, persone, servizi e capitali e in cui i cittadini, gli individui e le imprese possono accedere ed esercitare senza problemi attività online in condizioni di concorrenza leale e con un elevato livello di protezione dei dati personali e dei consumatori, indipendentemente dalla loro nazionalità o luogo di residenza. Definizione contenuta nella Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe" {COM(2015) 192 final}.

[3] Strategia Militare Nazionale D.C. 20318 del Dipartimento di Difesa degli Stati Uniti dell'11 dicembre 2006, La strategia militare nazionale per le operazioni del cyberspazio, pp. 3-5.

[4] Comunicazione congiunta al Parlamento europeo e al Consiglio del 13 settembre 2017, Resilienza, Deterrenza e Difesa: verso una Cibersicurezza forte per l'UE.

A supporto di tale obiettivo, è stata avanzata la proposta[5] di un nuovo mandato permanente per l'ENISA (*European Union Agency for Network and Information Security*) e l'elaborazione di un quadro per la politica europea sulla certificazione della *cybersecurity* per le ICT. La proposta affronta una questione molto importante che è quella di **preservare la fiducia e la sicurezza** dei prodotti e dei servizi ICT, ottemperando ad un dovere di diligenza per gli architetti e i produttori che dovranno implementare le caratteristiche di sicurezza sin dalle prime fasi di progettazione del prodotto o servizio (*security by design*).

Questo documento si pone l'obiettivo di ripercorrere, *in primis,* le tappe più importanti nell'ambito delle politiche europee per favorire lo sviluppo di un mercato unico digitale e che hanno portato alla previsione di uno schema di certificazioni per la *cybersecurity.*

In secondo luogo, intende esaminare il ruolo dell'ENISA nell'ambito del suo nuovo mandato, con un focus sullo EUCC, di cui ne verranno esaminati limiti e vantaggi, vale a dire lo schema europeo di certificazione della sicurezza informatica basato su criteri comuni che si pone come il successore del SOG-IS (Senior Officials Group Information Systems Security) MRA (Mutual Recognition Agreement).

Per concludere, infine, con una *roadmap* sugli sviluppi futuri della *cybersecurity* nell'Unione europea, che ha l'ambizione di conquistare la fiducia nelle tecnologie digitali per un virtuoso sviluppo del *digital single market*.

Background

L'Unione Europea ha iniziato ad occuparsi di *cybersecurity* in tempi relativamente recenti, dal momento che i primi atti ufficiali risalgono agli inizi del 2000[6]. Tuttavia, le forti aspirazioni dell'Unione nel diventare una società dell'informazione e di creare un **mercato unico digitale**, hanno portato alla promozione di molte iniziative che hanno contribuito a porre le basi per una **cultura digitale** e a dare un approccio unitario alla sicurezza delle reti e delle informazioni.

Un'agenzia indipendente al servizio degli Stati Membri

In un contesto socio-economico in cui l'*Information Technology* (IT) aveva già dimostrato di svolgere un ruolo determinante, l'Unione europea ha manifestato la crescente preoccupazione nei confronti della minaccia cibernetica con l'istituzione dell'ENISA (*European Union Agency for*

[5] Proposta COM(2017) 477 final della Commissione Europea del 13 settembre 2017, per un Regolamento del Parlamento europeo e del Consiglio sull'ENISA, l'Agenzia europea per la cybersecurity", e che abroga il regolamento (UE) 526/2013, e sulla certificazione della cybersecurity per le tecnologie dell'informazione e della comunicazione ("Cybersecurity Act").

[6] Una delle prime iniziative è stata la Comunicazione dal titolo "eEurope - una società dell'informazione per tutti", approvata dal Consiglio europeo di Lisbona nel marzo 2000 con il fine di collegare l'Europa *online*, fornendo ai cittadini, alle imprese, alle scuole e alle amministrazioni un collegamento alla rete.

Network and Information Security) avvenuta con il Regolamento (CE) n. 460/2004[7], sottolineando, in questo modo, l'importanza di adottare misure efficaci in materia di **sicurezza delle reti di comunicazione e dei sistemi informativi,** oramai divenuti "strumenti altrettanto comuni dell'acqua corrente o dell'energia elettrica[8]" e, di conseguenza, fondamentali per il benessere dei cittadini e la tutela dei loro diritti.

Il riconoscimento della complessità di tale materia, dell'impossibilità di trovare soluzioni univoche ed il rischio di incorrere in risposte eterogenee inefficaci, fece emergere l'esigenza di istituire un punto di riferimento che fosse in grado di creare un **clima di fiducia** sulla base di consulenza ed assistenza di qualità, trasparenza delle sue procedure, nonché diligenza nello svolgimento delle proprie mansioni; un'entità centrale e indipendente che collaborasse con gli Stati membri e mantenesse le relazioni con gli altri *stakeholders*. L'ENISA, la cui operatività era stata inizialmente prevista per la durata di 5 anni, poi costantemente prorogata[9], è ora diventata ufficialmente l'agenzia europea per la *cybersecurity* in virtù del **mandato permanente** che le è stato conferito dal Regolamento UE 2019/881, entrato in vigore il 27 giugno 2019, noto al grande pubblico come "Cybersecurity Act"[10].

La Strategia per uno spazio cibernetico aperto e sicuro

Un primo importante spartiacque nel percorso volto ad **armonizzare il sistema di sicurezza informatico europeo** è stata la proposta da parte della Commissione e dell'Alto Rappresentante di una Strategia per la sicurezza cibernetica volta a creare "un *cyber* spazio aperto e sicuro"[11], con cui si invitavano gli Stati Membri ad adottare specifiche normative nazionali al fine di **contrastare la minaccia cibernetica** in Europa e veniva messo in luce il problema di come le lacune nella sicurezza informatica minassero la fiducia dei cittadini nei confronti delle ICT, generando, di conseguenza, **un arresto nel processo di completamento del mercato unico digitale**.

---

[7] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004, relativo all'istituzione dell'Agenzia europea per la sicurezza delle reti e dell'informazione, art. 1.1.

[8] *Ibidem*.

[9] Regolamento (CE) n. 1007/2008 del Parlamento Europeo e Consiglio dell'Unione Europea del 24 settembre 2008, che modifica il Regolamento n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia. Regolamento (UE) n. 580/2011 del Parlamento Europeo e del Consiglio dell'Unione Europea dell'8 giugno 2011, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia.

[10] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, 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 («regolamento sulla cibersicurezza»).

[11] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni del 7 febbraio 2013, Strategia dell'Unione europea per la cibersicurezza: uno ciberspazio aperto e sicuro, JOIN/2013/01 final.

L'introduzione alla Strategia descrive un contesto in cui vi è la necessità di proteggere la libertà e l'apertura del *cyber*spazio che, nell'arco di due decenni, ha favorito l'abbattimento delle barriere tra Paesi, rendendo possibile lo scambio di informazioni ed idee in tutto il pianeta e diventando "la spina dorsale" della crescita economica;
Per questi motivi e a causa del ritmo preoccupante con cui crescono gli incidenti a carico della *cybersecurity*, l'Unione ha deciso di delineare la sua visione in questa materia, chiarendo ruoli e responsabilità e definendo gli interventi necessari per una protezione forte ed effettiva, con l'auspicio di poter rendere il *cyber*spazio dell'Unione Europea l'ambiente *online* più sicuro al mondo.
I principi contenuti nella Strategia sono:

- protezione dei diritti fondamentali, della libertà d'espressione, dei dati personali e della *privacy*;
- garanzia di accesso ad internet per tutti;
- *governance* partecipativa che coinvolga qualsiasi entità, comprese quelle commerciali e non governative;
- responsabilità condivisa tra tutti gli attori implicati: cittadini, imprese ed autorità pubbliche[12].

Con lo scopo di affrontare al meglio queste ambiziose sfide, la Strategia ha delineato una serie di azioni e **priorità strategiche** che possono rafforzare l'efficienza complessiva dell'UE e non solo quella degli Stati Membri:

- raggiungere la cyberresilienza;
- ridurre drasticamente il *cyber*crimine;
- sviluppare una politica e capacità di *cyber*difesa connesse alla Politica di Sicurezza e di Difesa Comune (PSDC);
- sviluppare risorse industriali e tecnologiche per la *cyber*sicurezza;
- creare una politica internazionale dell'UE in materia di *cyber*spazio[13].

Rafforzare le capacità di difesa, deterrenza e resilienza

Se la strategia per la *cybersecurity* del 2013 rappresentava la visione generale su come l'Unione intendesse supportare gli Stati membri e gli altri attori coinvolti nella prevenzione e risposta agli attacchi cibernetici, questo approccio reattivo ed imperniato sul concetto di un *cyberspace "open, safe and secure",* si è scontrato con un aumento esponenziale degli attacchi che ha messo a dura prova la resilienza dei sistemi di informazione ed ha reso evidente un cambio di rotta.

[12] Ivi, p. 4.
[13] Ivi, p. 5.

Con la strategia del 2017[14] si passa dunque ad una modalità d'azione più proattiva, che punta ad una implementazione delle capacità di difesa, deterrenza e resilienza dei singoli Stati e dunque dell'Unione.
La nuova strategia si basa su tre assi fondamentali:

- **rafforzare la resilienza dell'UE agli attacchi**, intesa sia come la capacità di dotarsi di strutture più solide ed efficaci e formare esperti qualificati, ma anche come la necessità di immettere sul mercato europeo tecnologie più sicure con l'istituzione di un quadro europeo di certificazione della cybersicurezza[15];
- **creare una deterrenza efficace,** che scoraggi gli autori, statali e non, ad intraprendere operazioni offensive contro l'UE, nonché potenziare la risposta operativa per prevenire e reagire prontamente agli attacchi;
- **rafforzare la cooperazione internazionale**, che si sostanzia nell'applicazione del diritto internazionale, e dunque della Carta delle Nazioni Unite al dominio cibernetico, e nella promozione di una convergenza degli interessi di tutti gli *stakeholders* per instaurare proficue alleanze e garantire la sicurezza internazionale.

Uno strumento ambizioso: la Direttiva NIS

Nell'ambito della strategia europea volta ad incrementare il livello complessivo di sicurezza delle reti e dei sistemi informativi, soprattutto nei settori che fanno largo uso delle tecnologie digitali e che sono considerati essenziali per il funzionamento del mercato interno[16], il 6 luglio 2016 è stata adottata dal Parlamento europeo la Direttiva UE 2016/1148, meglio nota come "Direttiva NIS" (*Network and Information Security*)[17].
Con essa, il Parlamento ha ritenuto fondamentale considerare che i livelli di preparazione degli Stati Membri, in quanto molto diversi tra loro, hanno caratterizzato una **frammentazione degli approcci** in materia di sicurezza informatica e generato uno stato di protezione non omogeneo, che **compromette il livello di sicurezza delle reti e dei sistemi dell'Unione**.

[14] Comunicazione congiunta JOIN(2017) 450 final al Parlamento europeo e al Consiglio del 13 settembre 2017, Resilienza, Deterrenza e Difesa: verso una Cibersicurezza forte per l'UE.
[15] COM(2017) 477.
[16] I settori citati nella Direttiva NIS sono: energia, trasporti, fornitura e distribuzione di acqua potabile, servizi bancari, infrastrutture dei mercati finanziari, sanità, infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di *cloud computing* e mercati *online*).
[17] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio dell'Unione Europea del 6 luglio 2016, recante misure per un livello elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Tale considerazione ha portato a concludere che è assolutamente necessario un **approccio globale,** che favorisca la creazione di **capacità e disposizioni minime comuni** in materia di cooperazione, scambio di informazioni ed obblighi comuni di sicurezza per gli operatori di servizi essenziali ed i fornitori di servizi digitali che, applicando misure di sicurezza più rigorose, possono contribuire ad estendere la copertura di rischi ed incidenti. Tra i servizi essenziali si annoverano energia, trasporti, credito, finanza, salute e risorse idriche, mentre tra quelli digitali: motori di ricerca *online*, mercato *online* e servizi nella nuvola (*cloud computing)*.
Un elemento ricorrente in tutta la Direttiva è il concetto della **fiducia** per il quale, trattandosi di uno dei pilastri fondamentali delle transazioni commerciali, la *cybersecurity* assume un ruolo fondamentale anche per il mantenimento di livelli di corretta e legittima **competitività nel contesto del mercato unico digitale**.
Nell'ottica di contribuire allo sviluppo della fiducia ma anche del miglioramento del livello di capacità tecniche ed organizzative necessarie a prevenire, individuare e rispondere ai rischi e agli incidenti di reti e sistemi informativi, gli Stati Membri dovrebbero assicurare la disponibilità di squadre di pronto intervento CSIRT ben funzionanti e rispondenti a requisiti minimi essenziali.
In merito alle Autorità Competenti, la Direttiva esplicita che ogni Stato Membro deve:

- designare pubblicamente una o più autorità nazionali, anche già esistenti, che abbiano competenze in materia di sicurezza informatica e che si occupino dei settori dei servizi essenziali e digitali e che vigilino sull'applicazione della Direttiva a livello nazionale;
- designare pubblicamente un Punto di Contatto Unico nazionale selezionandolo tra le Autorità Competenti esistenti;
- comunicare alla Commissione i compiti delle Autorità Competenti e del Punto Unico e qualsiasi modifica effettuata sui medesimi.

Risulta interessante anche un'altra considerazione rivolta agli Stati Membri che, con il recepimento della Direttiva, non vedranno limitare la propria possibilità di adottare misure necessarie per assicurare la tutela degli interessi essenziali della propria sicurezza, salvaguardare l'ordine pubblico e perseguire i reati; inoltre, in conformità con l'articolo 346 del trattato sul funzionamento dell'Unione Europea, nessuno Stato Membro è tenuto a fornire informazioni la cui divulgazione possa risultare contraria agli interessi essenziali della propria sicurezza.

La procedura di *follow up* della Direttiva

In linea con quanto previsto dall'art 23 della Direttiva NIS e al fine di sostenere la cooperazione strategica tra gli Stati, la Commissione ha il compito di **riesaminare** periodicamente il funzionamento della stessa, presentando una relazione al Parlamento e al Consiglio in cui si esaminano: le metodologie di identificazione degli operatori dei servizi essenziali (OSE) adottate dai singoli Stati, i servizi che le autorità nazionali ritengono essenziali, le soglie di identificazione e i numeri degli operatori di servizi essenziali identificati nei vari settori a cui si applica la Direttiva[18]. In un contesto in cui la digitalizzazione a tappeto che stiamo vivendo comporta un aumento non solo nei numeri ma anche nella sofisticazione delle minacce, è vieppiù evidente che sia necessario un **approccio flessibile e adattivo** per rispondere alle nuove esigenze. Per questo motivo il 25 giugno 2020 la Commissione europea ha avviato una consultazione pubblica[19], conclusa lo scorso 2 ottobre ed aperta alla partecipazione di tutti: cittadini, università, enti pubblici etc. e che ha avuto lo scopo di raccogliere informazioni e punti di vista eterogenei da parte dei soggetti interessati, sia sul funzionamento della Direttiva che su aspetti non ancora disciplinati dalla stessa. Il riesame dovrebbe avvenire entro la fine dell'anno, anticipando di qualche mese la data originariamente prevista nel maggio 2021.

Poiché la Direttiva è stata concepita con l'obiettivo di innalzare il livello di sicurezza nei diversi settori essenziali, tra cui appunto le infrastrutture e i servizi digitali, **il *follow up* della stessa vuole esaminare l'efficacia delle misure previste, il modo in cui sono state implementate dagli Stati, nonché i costi e i benefici sostenuti.**

Vista la sua giovane età, sarebbe prematuro giudicare l'impatto della Direttiva nel lungo periodo, mancando dati qualitativi e quantitativi a supporto di una siffatta valutazione. Esiste sicuramente un certo grado di frammentazione nel modo in cui la normativa europea è stata applicata dagli Stati membri, favorendo un approccio disomogeneo che non aiuta lo sviluppo del *digital single market*. Nonostante questo, è possibile notare che molte organizzazioni sono state motivate a migliorare la resilienza delle reti e dei loro sistemi proprio in vista del recepimento della Direttiva (e dell'applicazione del GDPR)[20], facendo sì che nell'ottica del breve periodo sia tangibile un miglioramento in alcuni settori.

---

[18] Relazione COM(2019) 546 final della Commissione al Parlamento e al Consiglio del 28 ottobre 2019, sulla valutazione della coerenza degli approcci adottati dagli Stati membri per l'identificazione degli operatori di servizi essenziali conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi.

[19] Per maggiori informazioni sull'iniziativa, si rinvia al seguente *link:* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive.

[20] 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 (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE).

Un modello di revisione biennale, ad avviso di chi scrive, rimane preferibile almeno per questa fase iniziale, soprattutto nell'ottica di una efficace gestione dei rischi delle minacce, in cui è per definizione necessario un approccio dinamico ed evitare che leggi inutili indeboliscano quelle necessarie, come sosteneva Montesquieu.
La società subisce cambiamenti dinamici che spesso sono troppo rapidi perché la legge possa tenere il passo, questo è particolarmente evidente nel mondo *cyber,* in cui il rischio di creare leggi inutili è tutt'altro che raro, dal momento che lo sviluppo tecnologico cresce in maniera esponenziale.

Il piano di risposta agli incidenti informatici su larga scala

La Direttiva NIS costituisce il fulcro delle misure adottate dall'UE per fronteggiare i sempre più frequenti incidenti a carico della sicurezza delle reti e dei sistemi informativi, ed è stata pensata per **aumentare le capacità di risposta dei singoli Stati**, favorire la cooperazione in modo da essere più preparati agli incidenti informatici, **stimolare** i principali attori economici **ad adottare *best practices*** efficaci, e a **segnalare gli incidenti** alle autorità nazionali competenti.
Nonostante gli sforzi e gli enormi passi in avanti registrati, l'Unione europea resta vulnerabile agli attacchi informatici, e questa vulnerabilità può incidere sul mercato unico digitale e più in generale sulla vita economica e sociale dell'Unione, che fa affidamento sulle reti e i sistemi informativi per lo svolgimento delle sue attività; tuttavia, data la repentinità con cui tali minacce evolvono, a maggior ragione nel caso di quelle ibride[21], questi eventi possono incidere anche su aspetti che trascendono la sfera economica e perturbare il mantenimento dell'ordine pubblico.
Ecco perché risulta di fondamentale importanza che le vittime e coloro che hanno la possibilità di reagire e mitigare la propagazione delle conseguenze, agiscano per coordinare una risposta efficace in tempi rapidissimi.
Sulla scia di due dilaganti pandemie, intercorse a poca distanza l'una dall'altra nella primavera-estate del 2017, quando prima il *ransomware WannaCry* e subito dopo *NotPetya* mostrarono a tutti la potenza infettiva di tali minacce, **è stato adottato un pacchetto di misure** nel settembre dello stesso anno che comprendeva anche una raccomandazione[22] della Commissione su una risposta coordinata a crisi e incidenti informatici su larga scala, la c.d. raccomandazione *Blueprint* o *incident response*.

[21] Per minacce ibride si intende "la combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali (cioè diplomatici, militari, economici e tecnologici), che possono essere usati in modo coordinato da entità statali o non statali per raggiungere determinati obiettivi, rimanendo però sempre al di sotto della soglia di una guerra ufficialmente dichiarata". Comunicazione JOIN(2016) 18 final della Commissione al Parlamento europeo e al Consiglio del 6 aprile 2016, Quadro congiunto per contrastare le minacce ibride. La risposta dell'Unione europea, p. 2.
[22] Raccomandazione C(2017)6100 final della Commissione europea del 13 settembre 2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

Come si evince dal considerando 2 della raccomandazione, Blueprint è pensato per far fronte a quelle crisi innescate da incidenti informatici che non colpiscono un solo Stato membro ma hanno, o possono avere, delle ripercussioni su tutta l'Unione e che pertanto per essere efficacemente gestite richiedono un'azione sinergica di tutte le istituzioni europee.
La sua finalità è quella di **dotare gli Stati membri di procedure di cooperazione** stabilite in maniera preventiva, che definiscano un quadro preciso circa **le modalità** con cui rispondere alle crisi e **fornire comunicazioni al pubblico**, attenendosi alla divisione dei ruoli e responsabilità definite a livello nazionale ed europeo; in particolare sono stati individuati dei quadri di risposta stratificati, a livello tecnico, operativo e strategico.
A livello **tecnico**, lo scopo dell'attività è consentire una risposta efficace che si sostanzia nel **"trattamento dell'incidente"**[23], vale a dire "tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente"[24]. Gli attori principali di questa fase sono i CSIRT, l'ENISA, l'Europol/EC3, la Commissione europea, i punti di contatto unici, il CERT-UE, il Servizio per l'azione esterna (Seae), e gli altri soggetti indicati nell'Allegato 1 della Raccomandazione.
A livello **operativo** l'obiettivo è quello di coordinare la risposta per **gestire la crisi** e **valutare l'impatto a livello europeo**, proponendo misure di mitigazione. I soggetti coinvolti in questo livello sono appartenenti alle stesse entità del primo, ma si tratta di personale con un livello gerarchico superiore, per consentire una valutazione strategica a 360 gradi.
A livello **politico** è previsto l'intervento dei maggiori decisori, dunque del Consiglio dell'UE, della Commissione europea, del Comitato politico e di sicurezza e dell'Alto rappresentante, che valuteranno la scelta di ricorrere ad altri strumenti quali la risposta diplomatica dell'UE alle attività informatiche dolose, mentre a livello nazionale verranno coinvolti i ministri responsabili per la sicurezza cibernetica.
Per ottemperare ad uno degli inviti avanzati dalla Commissione al fine di verificare la risposta agli incidenti e alle crisi cibernetiche su vasta scala, è opportuno tenere regolarmente delle **esercitazioni** coinvolgendo sia gli Stati membri che le istituzioni europee.
A questa proposta ha fatto seguito un'iniziativa franco-spagnola, che prende il nome di **Blue OLEx** , tenutasi per la prima volta a Parigi il 2 e il 3 luglio 2019, che ha riunito gli attori interessati in un'esercitazione che coinvolge tutte le autorità nazionali per la *cybersecurity* dei singoli Stati, la Commissione europea e l'ENISA, per **documentare il livello operativo** del quadro europeo di risposta alle crisi scatenate da attacchi informatici e **valutare i diversi meccanismi** a cui ricorrere per gestire collettivamente e in maniera efficace tali eventi.
L'esperienza è stata replicata lo scorso 29 settembre, questa volta su iniziativa dei Paesi Bassi, i lavori si sono svolti *online* a causa delle restrizioni imposte dalla pandemia di COVID-19.

[23] Ivi, Allegato 1.
[24] *Ibidem.*

Lo scopo di questa esercitazione è stato quello di **consolidare** le relazioni tra i diversi interlocutori che si occupano di sicurezza informatica, **rafforzare** la condivisione della conoscenza situazionale in modo tale che le informazioni giungano a tutti in modo rapido e nelle modalità opportune, oltre che **promuovere la condivisione** delle *best practices,* ed ha anche portato all'attenzione la necessità di **approfondire** le questioni strategiche su come gestire le crisi a livello europeo.
Blue OLEx 2019 è stata anche l'occasione per lanciare un'altra iniziativa: **CyCLONe** – *Cyber Crisis Liaison Organisation Network,* frutto del lavoro svolto dal *NIS Cooperation Group* sotto l'egida del DIS italiano e dell'Agenzia francese per la sicurezza dei sistemi informatici (l'Anssi), che si presenta come una **rete di cooperazione per gli Stati membri** pensata per rispondere prontamente a qualsivoglia tipologia di attacco cibernetico che dovesse colpire uno Stato dell'UE. Si fa carico, infatti, di riprendere i temi proposti nella Raccomandazione Blueprint, favorendo la collaborazione sia sul piano tecnico tra i vari CSIRT, che a livello politico tra gli IPCT (*Integrated Political Crisis Response*) cioè quegli strumenti che devono rendere fluido il processo decisionale in corso di crisi, tra cui vi rientrano una piattaforma *web*, punti di contatto 24 ore su 24, 7 giorni su 7 e rapporti.
Tutto questo farà in modo che le risposte siano prese a seguito di una **consultazione strategica rapida e coordinata,** che valuta gli impatti degli attacchi su più fronti, facilitando il ruolo dei decisori politici nazionali e dell'Unione, nonché apportando un consistente contributo alla **costruzione di un'Unione Europea resiliente agli attacchi informatici.**

La governance italiana della cybersecurity

Il 18 maggio 2018, in leggero ritardo rispetto al termine indicato dal Parlamento Europeo, è stato approvato in Consiglio dei Ministri il Decreto Legislativo n. 65/2018[25] recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione. Il Decreto, atto al recepimento della Direttiva NIS (2016/1148/UE) ed in pieno rispetto della stessa, definisce **l'oggetto** e l'**ambito di applicazione,** nonché gli **obblighi** a carico delle pubbliche amministrazioni, degli operatori di servizi essenziali e dei fornitori di servizi digitali **per garantire la sicurezza delle proprie reti e dei sistemi informatici**.
A tal fine il Decreto prevede, nell'articolo 1, comma 2, lettera b) la designazione delle autorità nazionali competenti, del punto di contatto unico e del gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT).

[25] D.lgs. 18 maggio 2018, n. 65, in materia di "Attuazione della 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".

Quanto alla designazione delle **autorità nazionali competenti**, all'articolo 7, vengono indentificati ben cinque ministeri responsabili per uno o più settori di propria competenza: Ministero dello Sviluppo Economico, Ministero delle Infrastrutture e dei Trasporti, Ministero dell'Economia, Ministero della Salute e Ministero dell'Ambiente, che devono tenere conto dei criteri di cui all'Articolo 5(2) della Direttiva per identificare gli operatori di servizi essenziali.
Per ciò che concerne il **punto di contatto unico**, invece, il Decreto prevede la designazione del DIS che svolgerà **funzioni di collegamento** con l'Unione Europea e **di coordinamento** con le autorità competenti in materia di sicurezza informatica negli altri Stati membri.
La designazione del CSIRT, infine, prevede una fusione dei preesistenti CERT Nazionale, che operano presso il Ministero dello Sviluppo Economico, e CERT-PA, operante presso l'Agenzia per l'Italia Digitale (AgID). Per ciò che concerne l'organizzazione dei CSIRT e le procedure atte a realizzare le b*est practices*, il Decreto in esame risulta abbastanza disomogeneo e, specialmente a causa di una ripartizione delle competenze molto ampia, non incarna un'efficace schematizzazione.
Il Decreto di recepimento prevede anche degli obblighi in tema di **notifica degli incidenti informatici** che dovranno essere inoltrati dagli operatori di servizi essenziali e dai fornitori di servizi digitali al CSIRT e all'autorità competente NIS, in un arco temporale che seppur non specificato deve intendersi scevro da ogni "ingiustificato ritardo" come si legge nell'12, comma 5.

Un *framework* nazionale per il quinto dominio

Più di recente in Italia, sempre a completamento della Direttiva NIS, il Decreto Legge n. 105 del 2019 convertito, con modificazioni, dalla legge n. 133 del 18 novembre 2019[26], ha introdotto il c.d. **perimetro di sicurezza cibernetica nazionale,** un *framework* importantissimo, che ha lo scopo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici per tutti quei soggetti "pubblici e privati aventi una sede nel territorio nazionale, **da cui dipende l'esercizio di una funzione essenziale dello Stato**, [...] e **dal cui malfunzionamento**, **interruzione**, anche parziali, ovvero **utilizzo improprio**, possa derivare un **pregiudizio per la sicurezza nazionale**"[27].
L'individuazione dei soggetti rientranti nel perimetro è stata demandata ad un decreto del Presidente del Consiglio dei ministri (DPCM), che entrerà in vigore il 5 novembre 2020[28] e che individua **i criteri tramite i quali i ministeri determinano i soggetti che svolgono funzioni essenziali per lo Stato** e che pertanto rientrano in tale perimetro, nonché le modalità con cui gli stessi dovranno procedere ad un censimento, da aggiornare su base annuale, delle proprie infrastrutture che dovrà includere "l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi

[26] Per maggiori informazioni si rinvia ai lavori parlamentari del disegno di legge, reperibili *online*.
[27] Art. 1, comma 2, del citato decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n.133.
[28] Decreto del Presidente del Consiglio dei ministri, n.131 del 30 luglio 2020, Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (20G00150) (GU Serie Generale n.261 del 21-10-2020).

informativi e dei servizi informatici che li compongono"[29].

Un'altra innovazione si registra nell'ambito delle **procedure di segnalazione degli incidenti**, che infatti dovranno essere comunicati al CSIRT entro 6 ore.

L'aspetto che qui si vuole sottolineare, soprattutto in vista dell'incremento dell'utilizzo dell'IoT[30] e dei *big data* nella nostra società, che inevitabilmente si tradurrà in un aumento di vulnerabilità che vanno comprese e prevenute, è che il perimetro di sicurezza nazionale si applica anche in materia di **reti di telecomunicazione elettronica a banda larga con tecnologia 5G**, qualificata come un'attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale.

Più precisamente, i c.d. *golden power* sono stati estesi con una novella contenuta nel c.d. decreto BREXIT[31], mediante l'introduzione dell'art. 1-bis, e pertanto non più circoscritti soltanto ai settori individuati originariamente dal d.l. 15 marzo 2012, n. 21; con questo ampliamento della sfera di applicazione *ratione materia* **è stato incluso nel novero** delle attività di rilevanza strategica, in modo da comprendere quanto previsto dall'art. 4, par. 1, del Regolamento UE 2019/452, **anche quello della sicurezza informatica e delle tecnologie di quinta generazione.**

La decisione se esercitare o meno i poteri speciali[32], come descritto dall'art 3, comma 2, verrà presa "previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano", inoltre al comma 3, viene prevista l'adozione di "**misure aggiuntive** necessarie al fine di assicurare livelli di sicurezza equivalenti", per quelle **autorizzazioni già rilasciate**, qualora fossero indispensabili per risolvere le vulnerabilità riscontrate.

L'Esecutivo si riserva[33] la possibilità di esercitare i *golden power* anche nell'ambito delle acquisizioni di componenti ad alta intensità tecnologica, tra cui : "l'immagazzinamento e la gestione dei dati e le infrastrutture finanziarie; le tecnologie critiche, compresa l'intelligenza artificiale, la robotica, i semiconduttori, le tecnologie con potenziali applicazioni a doppio uso, la sicurezza in rete e la tecnologia spaziale o nucleare"[34].

---

[29] Ivi, art 7, comma 1.

[30] Business Insider Intelligence prevede che entro il 2026 saranno installati oltre 64 miliardi di dispositivi IoT in tutto il mondo.

[31] Decreto Legge 25 marzo 2019, n. 22, Misure urgenti per assicurare sicurezza, stabilità finanziaria e integrità dei mercati, nonché tutela della salute e della libertà di soggiorno dei cittadini italiani e di quelli del Regno Unito, in caso di recesso di quest'ultimo dall'Unione europea. (19G00032).

[32] L'esercizio di tali poteri è stato esercitato per la prima volta con il DPCM del 26 giugno 2019, recante imposizione di prescrizioni e condizioni nei confronti della società Fastweb Spa in relazione all'accordo commerciale 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.

[33] Decreto-legge n.148 del 2017 coordinato con la legge di conversione 4 dicembre 2017, n. 172, recante "Disposizioni urgenti in materia finanziaria e per esigenze indifferibili. Modifica alla disciplina dell'estinzione del reato per condotte riparatorie.

[34] Art. 14 del Decreto-legge 16 ottobre 2017, n. 148 (in Gazzetta Ufficiale - Serie generale - n. 242 del 16 ottobre 2017), coordinato con la legge di conversione 4 dicembre 2017, n. 172 (in questa stessa Gazzetta Ufficiale - alla pag. 1), recante: "Disposizioni urgenti in materia finanziaria e per esigenze indifferibili.

L'art. 5 del decreto-legge n. 105 del settembre 2019, prevede inoltre che 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 interessa**ti".

Il dispiegamento della tecnologia di quinta generazione è un tassello importantissimo per consentire all'Europa di **competere sul mercato globale.** Secondo le stime della Commissione europea il 5G genererà un fatturato di 225 miliardi di euro in cinque anni. È evidente, pertanto, che la possibilità di ottenere il primato nella diffusione di componenti, apparati e sistemi rappresenta un'opportunità di grande valore sia per gli operatori delle telecomunicazioni (Tel.Co.) che permettono l'accesso alla rete, che per i produttori di apparati di reti e per i responsabili di *procurement* di soluzioni ICT.

La Commissione europea ha colto il potenziale di questa nuova rivoluzione digitale già nel 2016, con l'adozione di un vero e proprio **piano d'azione**[35] per consentire all'Unione di ottenere una posizione di *leadership* e trarne vantaggi economici. Il piano punta a garantire le infrastrutture di connettività necessarie in tempi relativamente brevi, prevedendo sei punti chiave per dare un coordinamento agli Stati, e un impulso agli investimenti pubblici e privati nelle reti 5G[36].

Secondo la Commissione[37], poiché molti servizi dipenderanno dalle nuove reti, si deve garantire una solida *cybersecurity* ed evitare che malfunzionamenti o, peggio ancora, attacchi dolosi paralizzino il funzionamento del mercato interno e la gestione degli *asset* strategici come l'energia, i trasporti, i servizi bancari e sanitari nonché quello democratico, dal momento che anche i processi democratici si stanno sempre più affidando a soluzioni digitali. Molto utile è anche il rapporto del *NIS Cooperation Group,* basato sui risultati delle valutazioni fornite dagli Stati membri contenenti una mappatura dei rischi connessi alle reti del 5G, che fornisce le basi per identificare le **misure di mitigazione** che possono essere applicate sia a livello nazionale che europeo.

Nell'ottica di definire un approccio europeo coordinato, la Commissione ha pubblicato un pacchetto di misure[38], con l'obiettivo di fornire orientamenti utili nelle strategie da applicare a livello interno per mitigare i principali rischi per la sicurezza informatica delle reti 5G. Come ulteriore contributo, è intervenuta una Comunicazione[39] che invita gli Stati membri ad

---

Modifica alla disciplina dell'estinzione del reato per condotte riparatorie". (17A08254).

[35] Comunicazione, COM(2016) 588 final della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 14 settembre 2016, il 5G per l'Europa: un piano d'azione {SWD(2016) 306 final}.

[36] C. Giustozzi, *What Does the EU Say About 5G?* in Aa.Vv., The Geopolitics of 5G, cur. S. Dominioni, F. Rugge, in *ISPI - Istituto per gli studi di politica internazionale*, settembre 2020, pp. 8-10, reperibile *online.*

[37] Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019, Cibersicurezza delle reti 5G.

[38] NIS Cooperation Group, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures,* gennaio 2020, reperibile *online.*

[39] Comunicazione, COM(2020) 50 final della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 29 gennaio 2020, Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE.

intraprendere azioni concrete e misurabili per attuare la serie di misure chiave raccomandate nelle conclusioni del pacchetto di strumenti dell'UE e a presentare una relazione sullo stato dei lavori. Queste relazioni hanno permesso al *NIS Cooperation Group* di fornire una panoramica sui progressi compiuti nel processo di attuazione del pacchetto di misure da parte degli Stati[40], da cui emerge un risultato incoraggiante, con l'adozione in molti Stati di misure di sicurezza avanzate per garantire una solida *cybersecurity* alle reti 5G. Tuttavia, ci sono ancora diversi Stati in cui non sono stati definiti contenuto e portata delle misure e, in alcuni casi, devono ancora essere prese decisioni politiche a riguardo. L'azione europea è accolta con favore anche dal Consiglio dell'Unione europea, il quale nelle sue Conclusioni del 9 giugno scorso ha affermato che: "gli Stati membri e le istituzioni dell'UE dovrebbero continuare a **intensificare gli sforzi tesi a promuovere la digitalizzazione del mercato unico,** in cui l'economia digitale sia caratterizzata da un elevato livello di fiducia, di sicurezza, anche in termini di *safety*, e di possibilità di scelta per i consumatori, oltre che da una forte competitività basata su un quadro che promuova la trasparenza, la concorrenza e l'innovazione e che sia tecnologicamente neutro"[41].

Il Nuovo Ecosistema della sicurezza

Digital Single Market e nuove sfide

Il lavoro dell'Unione europea per abbattere la dicotomia tra mondo *online* e *offline* è un vero e proprio *work in progress,* come abbiamo visto ripercorrendo brevemente le tappe più significative del percorso teso alla **creazione di un dominio cibernetico sicuro e resiliente,** a cui estendere i valori europei di tutela dello Stato di Diritto, rispetto dei diritti fondamentali e mantenimento dell'assetto democratico ma anche volto a **rendere il mercato unico adatto all'era digitale,** affrontando la frammentazione e le barriere che esistono nel mercato digitale europeo.
Senza disconoscere quanto fatto finora, negli ultimi anni è divenuta evidente la necessità di un'azione più energica, che non si limitasse più a mitigare gli attacchi e a gestirne le conseguenze. É su questa scia che già nella Strategia del 2017 la Commissione europea aveva inserito la proposta di riforma dell'ENISA, che includeva un mandato permanente dell'agenzia e il suo sostegno per l'elaborazione della politica dell'UE sulla certificazione della *cybersecurity* per le tecnologie dell'informazione e della comunicazione (ICT)[42].

---

[40] NIS Cooperation Group, *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity,* luglio 2020, reperibile *online.*
[41] Conclusioni 8711/20 del Consiglio dell'Unione Europea del 9 giugno 2020, Plasmare il futuro digitale dell'Europa.
[42] JOIN(2017) 450, p. 4.

Completamento della strategia europea per la cybersecurity

In un contesto di grande apprensione per la sofisticazione raggiunta nella conduzione delle minacce e la progressiva erosione della fiducia dei cittadini nelle tecnologie digitali, si conclude con 586 voti favorevoli, 44 contrari e 36 astensioni il lungo *iter* che ha portato all'adozione da parte del Parlamento europeo, in seduta plenaria, del Regolamento (UE) 2019/881- c.d. *Cybersecurity Act*- immediatamente esecutivo per tutti gli Stati Membri in virtù della sua natura giuridica. Il Regolamento, risolve una volta per tutte la mancanza di struttura ed i limiti strategici nell'azione dell'ENISA, che ora può contare su un **mandato permanente** che ne amplia il raggio d'azione, sia nei rapporti con i singoli Stati membri che con i Paesi terzi, disponendo anche di maggiori risorse finanziarie ed umane.

L'altra innovazione introdotta, riguarda il **sistema europeo per la certificazione della *cybersecurity* dei dispositivi connessi alla rete e di altri prodotti e servizi digitali**, che si presenta come la risposta volta ad abbattere i costi per le imprese e a tutelare i consumatori.

La **base giuridica** su cui poggia il Regolamento è l'art. 114 del Trattato sul funzionamento dell'Unione europea (TFUE), che attiene al **ravvicinamento delle legislazioni dei singoli Stati membri** nell'ambito dell'instaurazione e del corretto funzionamento del mercato interno, di all'art. 26 dello stesso TFUE.

Il sistema di sicurezza europeo by design

L'uso massivo delle reti e dei sistemi informativi in ogni strato della società non è destinato a diminuire, tutt'altro, in una realtà sempre più *digital,* intensificata anche dalla pandemia di COVID-19, la moltitudine di *endpoints*[43] che possono essere sfruttati per un uso malevolo, aumentano i rischi connessi alla sicurezza e generano un clima di grande apprensione da parte di cittadini, imprese e governi.

Al fine di attenuare questi rischi e garantire il raggiungimento del mercato unico è necessario rafforzare le difese attraverso **un'azione sinergica di tutte le parti coinvolte**. Tali esigenze non possono essere conseguite in misura sufficiente dagli Stati membri ma possono, a motivo della portata e degli effetti in questione, essere conseguite meglio a livello di Unione, e pertanto, legittimano il legislatore europeo ad intervenire in virtù del **principio di sussidiarietà.**

Una delle possibili **soluzioni** per ridurre i rischi legati all'uso delle ICT è appunto l'introduzione di una certificazione circa le caratteristiche dei prodotti, servizi e processi ICT in termini di *cybersecurity*.

In realtà, questa non è una preoccupazione del tutto nuova per l'Unione europea, che già negli anni 90' aveva adottato due atti importanti, che potremmo definire gli antecessori delle moderne misure legislative in questo settore e che hanno condotto alla formazione del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (*Senior Officials Group - Information Systems Security* - SOG-IS):

[43] Punti di accesso potenzialmente vulnerabili.

- Decisione (92/242/CEE) del Consiglio, del 31 marzo 1992 nel settore della sicurezza dei sistemi di informazione;
- Raccomandazione (94/144/CE) del Consiglio, del 7 aprile 1995 sui criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione[44].

Il SOG-IS ha creato il primo piano d'azione nel settore della sicurezza dei sistemi di informazione con l'adozione del *Mutual Recognition Agreement* (MRA) che, già dalla sua seconda versione del 1999 prevedeva nelle valutazioni l'utilizzo del nuovo standard ISO/IEC IS-15408 (*Common Criteria*[45]) ed è riconosciuto da tutti come un modello di cooperazione efficace ma con una portata limitata, perché comprende solo alcuni Stati e non consente un pieno sviluppo del mercato interno. Si è reso necessario, dunque, estendere i vantaggi della certificazione a tutti gli Stati membri per ridurre i costi ed evitare la frammentazione del mercato.
Il nuovo sistema europeo è pensato per invertire la tendenza secondo cui gli addetti ai lavori si preoccupano della *cybersecurity* quando ormai è troppo tardi. Se guardiamo alle aziende che lavorano in questo settore, ci rendiamo conto di come esista un **approccio principalmente reattivo**, che consiste nell'aggiornare i sistemi esistenti spuntando gli elementi nelle liste di controllo di conformità, piuttosto che un approccio teso ad incorporare la sicurezza nei nuovi prodotti e servizi sin dalla progettazione. Questa tendenza, che può essere efficace dal punto di vista del *management* che mira ad innovare rapidamente per essere competitivi sul mercato, non lo è sul versante della sicurezza, ed ha contribuito a creare **una frammentazione del mercato dei prodotti e servizi ICT** che hanno giocato al ribasso sugli investimenti della sicurezza, considerando i *chief information security officer* (CISO) e i reparti di *cybersecurity* come degli oneri a cui ottemperare piuttosto che un valore aggiunto. Questo ha contribuito ad **abbassare il livello generale di sicurezza, aumentato le vulnerabilità e reso fertile il terreno per gli attacchi, con una ovvia perdita di fiducia da parte degli utilizzatori che hanno visto compromessa la riservatezza, l'integrità o la disponibilità dei propri dati.**
Le certificazioni europee vogliono stimolare l'inversione di questa tendenza con un approccio proattivo che consideri il rischio sin dall'inizio e foraggi la fiducia dei consumatori. Questo è l'obiettivo della *security by design.*
Come più volte sottolineato nel presente documento, l'idea sottesa al *digital single market* è quella di **adeguare il mercato unico già esistente ai cambiamenti tecnologici** al fine di rendere l'Europa "adatta all'era digitale".

---

[44] Senior Officer Group Information Security, *Introduction*, disponibile *online* al seguente link: https://www.sogis.eu/index_en.html.
[45] L'utilizzo dei *Common Criteria* per la valutazione e la certificazione di sistemi e prodotti ICT permette di ottenere la garanzia circa il soddisfacimento di specifici requisiti di sicurezza di tali sistemi e prodotti, in modo da aumentare il livello generale di fiducia sull'effettiva sicurezza dei prodotti ICT. Sono stati ampiamente utilizzati per la certificazione di *chip* e *smartcard*, innalzando il livello di sicurezza dei dispositivi di firma elettronica per mezzo di identificazione come passaporti e carte bancarie e anche per certificare la sicurezza informatica dei prodotti software ICT.

Oltre al quadro di certificazioni per la *cybersecurity,* un considerevole contributo, atto ad aumentare la fiducia e la sicurezza dei consumatori in tale mercato, è dato anche dal Regolamento (UE) 2016/679[46], noto con l'acronimo GDPR (*General Data Protection Regulation*), poiché in un mercato alimentato dai *big data*[47], **il rispetto dei principi della *privacy* e protezione dei dati personali è una componente fondamentale della fiducia, che sta alla base della relazione tra utenti e fornitori di servizi digitali**[48].

La *ratio* sottesa alla previsione del GDPR, che introduce un concetto importante ossia quello di *privacy by design,* è che **la sicurezza digitale dell'Europa si può costruire solo sul concetto di *trust,*** e questo è anche uno dei fini cui tende il Regolamento sulla protezione dei dati, che **rafforza la fiducia nei servizi digitali con la tutela delle persone fisiche riguardo al trattamento dei propri dati**, e consente alle aziende di operare in un mercato digitale che abbia regole comuni, **eliminando le barriere alla libera circolazione dei dati** e rimuovendo la frammentazione legislativa dei singoli Stati.

Come si evince da una lettura combinata dei Considerando 7 e 13 del GDPR è necessario trovare un **equilibrio tra innovazione e protezione dei dati** per consentire **lo sviluppo dell'economia digitale**, facendo in modo che le persone abbiano maggiore controllo sui propri dati personali e che le imprese non vengano ostacolate dalla burocrazia ma anzi, traggano beneficio non solo dalla fiducia dei consumatori, ma anche da un quadro giuridico omogeneo che accresce la certezza del diritto e dalla parità di condizioni che devono garantire in materia di trattamento dei dati, impegnandosi in una concorrenza leale.

Solo così è possibile garantire **la libera circolazione dei dati personali** all'interno dell'UE e consentire il corretto funzionamento del mercato unico digitale.

Poiché la realizzazione del *digital single market* è una priorità per l'Europa, già nella Strategia del 2015[49] venivano affrontate diverse componenti chiavi per l'UE, tra cui il diritto fondamentale alla protezione dei dati personali sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea (in seguito, "Carta") e il principio che garantisce un elevato livello di tutela dei consumatori, sancito dall'art. 38 della Carta.

---

[46] Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio dell'Unione Europea 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.

[47] Grandi quantità di dati che non possono essere memorizzati o processati utilizzando basi di dati tradizionali.

[48] L'esistenza di una stretta connessione tra la disciplina della *privacy* e quella della *security* è stata sottolineata per la prima volta da Ann Cavoukian, ex Commissaria per le Informazioni e la *Privacy* della provincia canadese dell'Ontario, che ha aperto il dibattito su come la *privacy* debba essere considerata parte integrante di una solida *security*. Per approfondire, si rinvia al testo Ann Cavoukian, Mark Dixon, "*Privacy and Security by Design: An Enterprise Architecture Approach*" in *Information and Privacy Commissioner Ontario*, Canada, settembre 2013.

[49] Comunicazione COM(2015) 192 final della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 6 maggio 2015, Strategia per il mercato unico digitale in Europa.

A tal proposito, il perno intorno al quale ruota il concetto di *privacy* sin dalla progettazione e per impostazione predefinita (*privacy by default),* di cui all'articolo 25 del GDPR, è inteso a tutelare i diritti e le libertà degli interessati con riguardo al trattamento dei dati personali, attraverso l'attuazione da parte del titolare del trattamento di **adeguate misure tecniche e organizzative che prevedano che la protezione dei dati sia integrata nell'intero ciclo di vita del trattamento stesso,** dalla fase di progettazione fino alla sua ultima di distribuzione, utilizzo e di eliminazione finale e che nel secondo caso, siano rispettati i principi generali della protezione dei dati, quali la minimizzazione e la limitazione delle finalità.
Dunque, così come per la *security by design,* la protezione dei dati personali deve essere affrontata contestualmente alla realizzazione del trattamento e dei sistemi, e non può essere considerata un *optional* da aggiungere *ex post facto.* È necessario fornire strumenti significativi agli utenti e consentire loro di esprimere una scelta consapevole, garantendo la trasparenza, e permettendo loro di controllare ed eseguire il riutilizzo dei propri dati. Solo così si potrà **facilitare la fruizione dei servizi digitali** e **costruire la fiducia degli utenti** nell'elaborazione dei propri dati.

Il Nuovo mandato dell'ENISA

Nell'ambito del *Cybersecurity Act* viene delineato un nuovo mandato per l'ENISA, che in virtù dell'art. 48(2) del Regolamento, è investita di una nuova competenza, vale a dire preparare il primo programma di certificazione della *cybersecurity,* il "*Common Criteria based European candidate cybersecurity certification scheme*" (EUCC), che mira a sostituire i sistemi esistenti che operano nell'ambito del SOG-IS - MRA (Senior Officials Group – Information Systems Security - Mutual Recognition Agreement) per i prodotti ICT, aggiungendo nuovi elementi e rendendolo applicabile per tutti gli Stati membri dell'Unione.
In seguito a tale richiesta, l'ENISA ha istituito un gruppo di lavoro ad hoc composto dai rappresentanti delle parti interessate (AHWG) per essere di supporto alla preparazione del programma di certificazione, e grazie anche al confronto continuo con il Gruppo Europeo per la Certificazione di Sicurezza (ECCG)[50], istituito dal Regolamento come organo consultivo dell'Agenzia, ha consolidato uno Schema di Certificazione europeo per la sicurezza dei servizi, processi e prodotti ICT, che sarà applicabile da giugno 2021, avrà carattere volontario, e prevede il rilascio di certificati aventi validità per 5 anni, rinnovabili[51].

[50] Per ulteriori informazioni sui compiti del Gruppo Europeo per la Certificazione di Sicurezza (ECCG) si rinvia al seguente link: https://ec.europa.eu/digital-single-market/en/european-cybersecurity-certification-group.
[51] European Union Agency for Cybersecurity (ENISA), *"Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS",* del 1 luglio 2020, V 1.0., cap.20, p. 65.

L'idoneità dell'ENISA, come agenzia che mette a disposizione le sue competenze per aggiornare e sviluppare la normativa europea nel settore della sicurezza delle reti e dell'informazione e dunque favorire lo sviluppo del mercato interno, è stata confermata anche dalla Corte di Giustizia nella famosa sentenza del 2006, C-217/04 (Regno Unito *vs.* Parlamento europeo e Consiglio dell'Unione europea).

La necessità di un quadro di certificazione europea ha motivato l'intervento dell'ENISA, volto a dare un **contributo alle politiche dell'Unione in materia di *cybersecurity*** e a creare delle **condizioni di mercato migliori**[52]. Lo scopo precipuo del quadro di certificazione, così come precisato nel CSA, è quello di **stabilire e mantenere la fiducia e la sicurezza dei prodotti, servizi e processi ICT**, pertanto la predisposizione dei sistemi di certificazione mira a fornire criteri per eseguire valutazioni di conformità e determinare il grado di aderenza di questi rispetto ai requisiti fissati. In questo modo, sia i consumatori che i fornitori di servizi hanno cognizione del livello di affidabilità dei prodotti che acquistano o utilizzano, e nel secondo caso possono determinare il grado di sicurezza di ciò che immettono sul mercato.

In merito ai livelli di affidabilità, il nuovo schema prevede tre livelli di certificazione della sicurezza dei servizi, processi e prodotti ICT: un **livello base**, un **livello sostanziale** e un **livello elevato,** lo EUCC copre però solo gli ultimi due.

Un certificato europeo che si riferisca al livello di garanzia sostanziale assicura il rispetto dei requisiti di sicurezza e che i prodotti/servizi/processi ICT siano in grado di **ridurre al minimo i rischi noti connessi alla *cybersecurity* e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate.** Tra le attività di valutazione da effettuare c'è un **riesame** per dimostrare **l'assenza di vulnerabilità pubblicamente note** e un **test** per dimostrare **che i prodotti, i servizi o i processi ICT attuino correttamente le necessarie funzionalità di sicurezza**[53].

Un certificato europeo che si riferisca al livello di affidabilità **elevato,** assicura che i prodotti, i servizi e i processi ICT per i quali è rilasciato rispettino i corrispondenti requisiti , comprese le funzionalità di sicurezza, e che siano stati valutati ad un livello inteso a **ridurre al minimo il rischio di attacchi informatici avanzati, commessi da attori che dispongono di abilità e risorse significative**. Le attività di valutazione da intraprendere includono: un **riesame** per dimostrare l'assenza di vulnerabilità pubblicamente note, un **test** per dimostrare che i prodotti, i servizi o i processi ICT attuino correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una **valutazione** della loro resistenza agli attacchi commessi da soggetti qualificati **mediante test di penetrazione**[54].

---

[52] Art. 54 (1), lett. b) del CSA, un sistema europeo di certificazione della cibersicurezza comprende almeno: "una chiara descrizione dello scopo del sistema e delle modalità con cui le norme, i metodi di valutazione e i livelli di affidabilità selezionati corrispondono alle esigenze degli utenti del sistema previsti".

[53] Art. 52 (6) del Regolamento UE 2019/881.

[54] Art. 53 (7) del Regolamento UE 2019/881.

Il nuovo schema europeo non copre il livello di affidabilità di base, che prevede la possibilità di effettuare un ***self-assessment* di conformità sotto la responsabilità del fornitore** per tutti quei servizi, processi e prodotti ICT che presentano un livello di rischio basso, ai sensi dell'articolo 53(1) della CSA.

La previsione di tre livelli rende sicuramente lo schema molto **flessibile** ma apre la porta anche ad alcuni **rischi**.

Se un'autovalutazione di conformità è adatta per il fabbricante o il fornitore che effettuano direttamente tutti i controlli sui **servizi e processi ICT** a bassa complessità, garantendo il rispetto dei requisiti dello EUCC e che rispondono dei rischi associati ad essi, questa idoneità non è adatta a scongiurare i rischi in relazione ai **prodotti ICT**, innanzitutto perché le minacce alla sicurezza in questo caso non gravano sul produttore ma su chi utilizza il prodotto.

Inoltre, ci sono due aspetti da tenere in considerazione, il primo è quello relativo al ruolo che il *management* può esercitare per assicurare l'uscita di prodotti che devono rispettare il *time to market* (TTM), e che potrebbe risolversi in indebite pressioni; il secondo, attiene alle conseguenze che potrebbero verificarsi in caso di aspetti negativi che l'autovalutazione di conformità potrebbe mettere in luce, anche in questo caso, il *management* potrebbe esercitare pressioni affinché vengano trovate delle soluzioni rapide, che spesso non sono altrettanto sicure.

Al di là di questi aspetti da tenere in forte considerazione, la possibilità di effettuare un'autovalutazione della conformità per prodotti ICT con un livello di affidabilità "di base", presenta anche dei vantaggi, soprattutto in termini di velocità e costi, perché il produttore che effettua la valutazione è già in possesso del *know-how* del prodotto e quindi abbatte le tempistiche che servirebbero ad una parte terza per conoscere il prodotto e poterlo valutare[55].

Per questo motivo è importante **potenziare il sistema di controllo** che, come stabilito nel CSA[56], ricade sulle Autorità Nazionali di Certificazione che devono controllare la conformità agli obblighi e far applicare gli stessi ai fabbricanti o ai fornitori di prodotti ICT, e devono avvalersi del mezzo dissuasivo delle **sanzioni** previsto dal Regolamento[57], chiedendo contestualmente la cessazione immediata delle violazioni riscontrate.

Uno degli aspetti trattati nel quadro delle certificazioni dall'ENISA è poi la **gestione delle vulnerabilità riscontrate** in un prodotto ICT[58].

Secondo lo schema, i produttori e i fornitori di prodotti ICT dovranno utilizzare le fasi generali della ISO/IEC 30111 per la gestione delle vulnerabilità, vale a dire: *preparation, receipt, verification, remediation development, release* e *post-release.*

---

[55] G. Conte, H. Kurth, *Il vendor self-assessment in ambito Cybersecurity Act: rischi e opportunità,* 2 dicembre 2019, in *Network Digital 360,* consultabile *online.*

[56] Art. 58 (7) lett. b) del Regolamento UE 2019/881.

[57] Art. 58 (7) lett. f) del Regolamento UE 2019/881.

[58] European Union Agency for Cybersecurity (ENISA), *"Cybersecurity Certification EUCC",* cit. cap.14, p. 50.

Per quanto riguarda la prima fase, i produttori e fornitori devono sviluppare metodi per **ricevere informazioni sulle vulnerabilità** e hanno il dovere di renderle pubbliche[59]. Questo è un passaggio molto importante nell'ottica della divulgazione e conoscenza delle vulnerabilità, non solo per gli addetti ai lavori ma anche per gli utilizzatori finali dei prodotti ICT e la loro sicurezza.

Una volta che il produttore o il fornitore abbia ricevuto informazioni su una vulnerabilità del suo prodotto ICT, deve riferire immediatamente all'organo che ha emesso il certificato e deve fornire una data in cui verrà stabilita **l'analisi della vulnerabilità**. Se invece è l'organo di certificazione ad acquisire per prima le informazioni sulla vulnerabilità, dovrà informare immediatamente il produttore o il fornitore, richiedendo l'analisi della vulnerabilità da effettuarsi entro una data da concordare.

Anche questa è una fase importante, poiché se il produttore o il fornitore non informa l'organo di certificazione, non fornisce l'analisi o non la fornisce nei tempi concordati, **il certificato verrà sospeso**.

In caso contrario, l'analisi delle vulnerabilità sarà documentata e la documentazione dovrà essere conservata per un minimo di cinque anni. Tale analisi dovrà contenere il c.d. *Required Attack Potential* (RAP)[60], che misura lo sforzo necessario per attaccare l'obiettivo, espresso in termini di competenza, risorse e motivazione dell'attaccante, che servirà per stabilire se la vulnerabilità è confutata o confermata. Nel caso in cui la vulnerabilità sia smentita, il processo si interrompe e le informazioni devono essere conservate per eventuali ulteriori controlli. Nel caso in cui la vulnerabilità venga confermata, l'analisi dovrà contenere **la valutazione dell'impatto che la vulnerabilità può avere sul prodotto ICT** e **la possibile risoluzione della stessa** (con l'indicazione dei rischi del possibile attacco e il livello di modifiche che dovranno essere applicate)[61] e, infine, deve contenere una valutazione sulla possibilità di aggirare la vulnerabilità che, ove non fosse possibile, comporterebbe la **revoca del certificato.**

A supporto del processo di gestione delle vulnerabilità di cui abbiamo appena parlato, lo EUCC prevede anche **due metodologie di gestione delle patch[62]**; infatti un prodotto può includere o meno un patch management all'interno della sua certificazione, che consentirebbe agli sviluppatori di implementare la sicurezza del prodotto rimanendo sotto l'ombrello del certificato.

---

[59] Art. 55 (1) lett. c) del Regolamento UE 2019/881.

[60] Secondo il *Common Methodology for Information Technology Security Evaluation* (CEM), nell'analisi dei diversi fattori che devono essere considerati durante il calcolo ci sono: a) tempo impiegato per identificare e sfruttare la vulnerabilità (*Elapsed Time*); b) competenza tecnica specialistica richiesta (*Specialist Expertise*); c) conoscenza della progettazione e del funzionamento dell'obiettivo (*Knowledge of the TOE*); d) finestra di opportunità (*Windows of Opportunity*); e) *hardware* / *software IT* o altre apparecchiature necessarie per lo sfruttamento. (*IT hardware/software or other equipment).* Per approfondire, si rinvia al testo: Common Methodology for Information Technology Security Evaluation (CEM), Evaluation methodology, Aprile 2017, Versione 3.1. Revisione 5, CCMB-2017-04-004, p 421, disponibile *online:* https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf.

[61] European Union Agency for Cybersecurity (ENISA), *"Cybersecurity Certification EUCC",* cit. Cap. 38, Allegato 11, "Assurance Continuity", pp. 256 ss.

[62] Ivi, p 53.

In entrambi i casi, il produttore o il fornitore deve decidere in merito alla riparazione e apportare le modifiche necessarie al prodotto ICT.
Una volta che la riparazione e le modifiche associate al prodotto sono state dichiarate idonee per la distribuzione, il produttore o il fornitore procederà alla loro implementazione o rilascio seguendo i requisiti dell'articolo 55 (1) del CSA.
Lo EUCC è il primo schema di certificazione proposto dall'ENISA nell'ambito del suo nuovo mandato, un secondo schema a cui l'Agenzia sta lavorando riguarda invece i servizi cloud, anche questi sempre più spesso bersaglio di attori malintenzionati in quanto in grado di generare ingenti profitti.

Conclusioni e roadmap per il futuro

Nel Global Risks 2020, il World Economic Forum (WEF) ha presentato gli attacchi *cyber* come il settimo rischio globale in termini di probabilità e l'ottavo in termini di impatto. Questi dati non devono sorprendere, poiché è ormai noto che le conseguenze di un *cyber attack* possono incidere su molti aspetti: economici[63], sociali e sulla vulnerabilità della sicurezza internazionale.
Basta chiedere ad un alto funzionario dell'*Office of Personnel Management* (OPM), un'agenzia federale americana che ha subito due attacchi informatici riportando il furto dei dati di impiegati ed ex impiegati che lavorano nella sicurezza nazionale ed hanno accesso a dati sensibili, o ad un dirigente della Sony Pictures o del colosso dell'*e-commerce* Target. Basta guardare alla capacità di propagazione che hanno registrato alcuni *malware,* come il famoso "WannaCry" *c*he ha colpito numerosi settori di ben 150 nazioni, tra cui quello sanitario, governativo e delle telecomunicazioni, criptando i *file* sul disco rigido di ben 230.000 *computer e* chiedendo un riscatto in cambio della chiave fondamentale per la decriptazione.
Neppure gli Stati sono immuni da attacchi informatici, la loro vulnerabilità è direttamente proporzionale al livello di sviluppo tecnologico di cui si avvalgono per gestire le proprie infrastrutture militari e civili. Se l'intera nazione è cablata in fibra ottica e le reti di *computer* diventano il motore delle principali infrastrutture, metterle fuori uso, significa paralizzare il paese. È ciò che è capitato nel 2007 in Estonia, quando attacchi di tipo DDoS (*Distributed Denial of Service*) hanno paralizzato per ben tre settimane: agenzie governative, banche e media nazionali in quello che è stato uno degli attacchi più massicci e prolungati fino ad ora realizzati. Il paese baltico si è trovato ad affrontare il primo attacco cibernetico, che di lì a poco sarebbe stato ribattezzato *Web War One*; un vero e proprio spartiacque che ha reso evidente il potenziale pericolo di un attacco non convenzionale che ha colpito un'intera nazione[64].

[63] Il Fondo monetario internazionale (FMI) ha stimato la perdita annua dovuta agli attacchi informatici al 9 % del reddito netto delle banche a livello mondiale, pari circa 100 miliardi di dollari.
[64] Il caso estone è rilevante anche ai fini dell'applicazione del diritto internazionale al dominio cibernetico, in quanto non solo rappresenta il primo episodio di *cybewarfare* il cui *casus belli* è legato a motivazioni politiche ma soprattutto per il fatto che il governo estone invocò l'articolo V del Trattato Nord Atlantico chiedendo l'intervento militare degli alleati in difesa di uno stato membro

Anche in questo caso la lista non si esaurisce qui, e il fragore prodotto dagli attacchi subiti dall'Estonia o dall'Ucraina[65] è in netta contrapposizione con gli eventi, subdoli e silenziosi ma non per questo privi di conseguenze, che interessarono l'Iran Centrale nel 2010[66].

É in tale contesto che le parole del Generale Peter Pace, Capo dello Stato Maggiore Congiunto, appaiono quanto mai emblematiche:

"Gli effetti catastrofici, [delle Armi di Distruzione di Massa] sono possibili anche nel cyberspazio a causa del legame esistente tra lo spazio cibernetico e le infrastrutture critiche dei sistemi SCADA. Attacchi ben pianificati a nodi chiave delle infrastrutture del cyberspazio hanno il potenziale di causare il collasso della rete ed effetti a cascata che possono danneggiare seriamente infrastrutture a livello locale, nazionale o finanche globale".

Il *trend* generale degli attacchi non è destinato a decrescere, ma il *target,* la pervasività, l'efficacia e il *modus operandi* degli attaccanti è cambiato negli ultimi anni, decretando un'evoluzione epocale delle minacce cibernetiche. Prendendo in prestito la definizione contenuta nel Rapporto CLUSIT di metà anno[67], che analizza i *cyber attacks* di dominio pubblico su scala globale in base a tre livelli di *severity,* siamo di fronte ad uno scenario di "gravità inaudita", che non può essere sottovalutato.

Innanzitutto sono mutati gli **intenti** che spingono gli attori ad agire, non si tratta più solo di *hacker* desiderosi di mettere alla prova le proprie abilità, o mossi da motivazioni ideologiche o politiche, siamo di fronte ad attaccanti che agiscono secondo una "logica industriale[68]" che punta a massimizzare i profitti. Molto spesso si tratta di veri e propri gruppi di criminali organizzati con fatturati esorbitanti, multinazionali ma anche attori statali che hanno capacità tecniche ed economiche avanzate, in grado di mettere a segno attacchi più o meno gravi ad infrastrutture strategiche, reti, *server*, *client* ma anche oggetti IoT e dispositivi mobili, causando un **deterioramento dei livelli di *cybersecurity*** e diffondendo un **clima generale di insicurezza nell'utilizzo delle tecnologie digitali.**

---

vittima di un attacco *web*. Data l'impossibilità di attribuire con certezza la paternità dell'attacco, a causa dell'uso di *botnet* l'intervento non ci fu, ma ha fatto sì che la sicurezza informatica sia diventata una preoccupazione generale della comunità internazionale.

[65] Nel dicembre del 2015 la regione Ivano-Frankivsk nell'Ucraina ovest vide spegnere improvvisamente circa 60 sottostazioni della sua rete elettrica, generando un *black-out* che coinvolse circa 230.000 residenti.

[66] Ci riferiamo al virus, inizialmente nominato dalla Symantec "W32.Themphid" ed in seguito "W31.Stuxnet", della famiglia dei *worm*, che colpì il sistema SCADA dell'impianto nucleare di Natanz. Nella fattispecie, obiettivo primario erano i PLCs (*Programmable Logic Controllers*) affinché venisse modificato il loro comportamento. Tale modifica sarebbe stata lenta e individuabile solo nel lungo periodo, poiché per svolgere il proprio compito, Stuxnet sfruttava ben quattro *zero-day exploits* del sistema operativo Windows al quale era connesso il dispositivo PLC, riuscendo a rimanere invisibile ai sensori del sistema SCADA tramite l'ausilio di un *rootkit (*un *software* che permette di ottenere costantemente i permessi di amministrazione su un *computer* o una rete di *computer* a cui non si è autorizzati ad accedere).

[67] CLUSIT, *Rapporto Clusit 2020 sulla sicurezza ICT in Italia,* ottobre 2020, reperibile *online.*

[68] Ivi p. 21.

Il *pool* di esperti ha stimato che rispetto al primo semestre del 2019 il numero di attacchi con una *severity* elevata, registrati nel primo semestre di quest'anno è aumentato del 6,7%[69].
Il *cybercrime* rimane ancora la principale causa di attacchi gravi, coprendo l'83% dei casi, con una crescita in termini assoluti del 7,1%[70].
Dall'analisi delle tecniche di attacco[71], emerge che il protagonista indiscusso è il *malware* con una crescita del 6,8%[72], molto interessante è notare poi l'incremento registrato dalla categoria *phishing/social engineering* (+26,1%)[73], un successo che va letto attraverso due lenti di osservazione.
La prima prende in esame **la pandemia di COVID-19** che ha costretto milioni di persone ad una "nuova normalità" con la ridefinizione delle norme sociali e del modo di lavorare.Tutto questo, unitamente alla paura per un virus sconosciuto e aggressivo, ha generato insicurezze e acuito vulnerabilità che i criminali informatici hanno saputo capitalizzare. Molti degli attacchi registrati nell'ultimo semestre iniziavano con campagne di *phishing* che, utilizzando una terminologia precisa inerente al COVID-19, induceva la vittima a scaricare *file* che erano dei vettori per *malware* pericolosi. Il contesto in cui tutto questo è accaduto è una realtà nuova, che ha colto molti impreparati e ha causato ingenti danni.
Il secondo aspetto coinvolge **il tema della formazione**; stante ai dati del Rapporto CLUSIT, l'80% degli attacchi è dovuto al **fattore umano**, a questo valore tuttavia, non segue una previsione capillare all'interno delle aziende, di programmi strutturati di *cybersecurity awareness* e *training* pluriennali, anche con vere e proprie simulazioni di attacchi, per minimizzare i rischi e aumentare la consapevolezza del personale.
Il problema della conoscenza di tali tematiche riguarda anche i profani del settore, poiché la consapevolezza circa i rischi informatici andrebbe affrontata in maniera più ampia, per raggiungere tutta la cittadinanza.
Ad avviso di chi scrive, questo è un problema di **maturazione culturale**, e dunque di tempo. Le tecnologie digitali, infatti, sono esplose immediatamente come tecnologie di massa e non c'è stato tempo per l'uomo della strada, la scuola, il formatore, il legislatore e il politico di comprenderlo e di assuefarsi.

---

[69] Ivi p. 17.
[70] Ivi p. 19.
[71] Sulla base dell'analisi degli attacchi in Italia relativi al 2019, svolta da Fastweb sulla base dei dati rilevati dal *Fastweb Security Operations Center* (SOC) emerge che avalanche-Andromeda è stato il *malware* più utilizzato (28%), segue nella classifica ZeroAccess (22,69%) e al terzo posto troviamo QSnatch. La stessa analisi mostra, poi, come a fronte dell'aumento generale degli attacchi di tipo DDoS, soprattutto verso il settore del *Gaming* e *Finance/Insurance*, ci sia stata una riduzione della stessa tipologia di attacchi verso la p.a., facendo notare come questo calo sia legato alla introduzione di strumenti di difesa, attraverso l'adesione degli enti pubblici alla convenzione SPC per i servizi di *cybersecurity*, che contribuiscono a rendere il settore meno remunerativo e quindi meno appetibile per i criminali informatici.
[72] CLUSIT, *Rapporto Clusit 2020,* cit. p. 24.
[73] *Ibidem.*

Nella Strategia europea del 2013 si raccomanda agli Stati membri di inserire l'insegnamento della sicurezza già dalle scuole primarie: una cosa lodevole ma a questo invito non ha fatto seguito, almeno in Italia, una volontà politica che spingesse verso una maggiore formazione del cittadino, inoltre, l'introduzione di questa disciplina, dovrebbe affrontare anche il tema della mancanza di competenze degli attuali formatori su questi temi, che andrebbero a loro volta formati.
L'auspicio è che le cose possano cambiare con il *Digital Europe programme,* per il budget UE 2021-2027, che investirà 9,2 miliardi di euro per finanziare **la transizione digitale dell'Europa**, con l'obiettivo di aumentare la competitività internazionale e sviluppare e rafforzare le capacità digitali strategiche dell'Unione europea.
Uno dei cinque *pillar* del programma è rivolto, infatti, proprio all'acquisizione di **competenze digitali avanzate** per i cittadini, a cui sono destinati 700 milioni di euro dell'intero *budget* e che saranno utilizzati per supportare la formazione a breve e lungo termine, di studenti, lavoratori e imprenditori attraverso corsi di formazione, tirocini sul lavoro e programmi mirati, per aiutare le piccole e medie imprese nonché le pubbliche amministrazioni a dotare il proprio personale delle competenze digitali necessarie[74].
Decisivo è anche un altro pilastro del programma *Digital Europe*: *Cybersecurity and trust,* per il quale sono stanziati 2 miliardi di euro che saranno impiegati per la **salvaguardia dell'economia digitale**, della società e delle democrazie dell'UE attraverso i**l potenziamento della difesa informatica e del settore della *cybersecurity*,** supportando gli Stati membri nel *procurement* di attrezzature, infrastrutture di dati e strumenti avanzati per la sicurezza informatica, ed anche per sostenere lo sviluppo delle competenze necessarie e per aiutare gli Stati membri nell'adesione alla Direttiva NIS[75].
Sul tema della tutela e della protezione dello spazio cibernetico, degni di nota sono anche gli sforzi italiani. Dalle ultime analisi, l'Italia non è esente dall'aumento del numero di attacchi che ammonterebbero a 43 milioni nel 2019[76], pertanto, garantire una maggiore sicurezza è condizione essenziale per la prosperità del nostro Paese. Per rispondere a tale necessità, già il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica[77], ha evidenziato **la rilevanza delle varie componenti pubbliche e private** nonché della ricerca nel processo di evoluzione e cambiamento auspicato, e ha ritenuto necessario **sviluppare iniziative che coinvolgessero le principali imprese nazionali, le università e la ricerca scientifica,** con la realizzazione di un Centro Nazionale di Ricerca e Sviluppo in *Cybersecurity,* il cui ambito d'azione deve esprimersi nella protezione delle infrastrutture critiche e nei sistemi di analisi delle minacce cibernetiche.

---

[74] Proposta di Regolamento COM(2018) 434 final del Parlamento europeo e del Consiglio del 6 giugno 2018, che istituisce il programma Europa digitale per il periodo 2021-2027, art. 7.
[75] Ivi, art. 6.
[76] CLUIST, *Rapporto Clusit 2020,* cit. p. 33.
[77] Piano Nazionale, Presidenza del Consiglio dei Ministri, del marzo 2017, Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica.

L'annuncio della costituzione dell'Istituto italiano di Cybersecurity (IIC) è apparso nell'art. 96 della bozza della legge di bilancio del 2021, e al comma 13 prevedeva una spesa iniziale di 30 milioni di euro per il 2021, 70 milioni di euro per il 2022, di 60 milioni di euro per il 2023 e 50 milioni di euro per il 2024. Tuttavia, il testo bollinato e inviato al Parlamento, ha visto lo stralcio dell'Istituto a seguito di un forte contrasto della maggioranza politica. Non si esclude, però, che la sua previsione possa rientrare in un futuro disegno di legge a seguito di una maggiore concertazione tra le parti che forse è mancata in questo momento.

Nell'ambito delle sue funzioni, l'istituto avrebbe dovuto "sostenere **l'accrescimento delle competenze e delle capacità tecnologiche,** industriali e scientifiche nazionali nel campo della sicurezza cibernetica e della protezione informatica [...] **stipulare contratti, convenzioni, accordi o intese con soggetti pubblici e privati,** promuovere la costituzione di nuove società, associazioni o fondazioni, **partecipare a società, associazioni o fondazioni esistenti,** a strutture di ricerca, di alta formazione e di trasferimento tecnologico in Italia e all'estero, se tali soggetti svolgono attività comunque strumentali al perseguimento delle sue finalità". Emerge, dunque, che almeno nelle intenzioni, l'istituto sarebbe stato una sorta di **collettore per il settore pubblico e i privati** e in tal senso avrebbe contribuito a due dei principali temi di cui la Direttiva NIS si è fatta promotrice, vale a dire **intraprendere una *partnership* operativa con il settore privato** per condividere le informazioni sulle minacce cibernetiche (***information sharing***) e **aumentare la consapevolezza** del pericolo proveniente dal *cyberspace.*

Il quadro delineato e i dati riportati nel presente lavoro, sono dei chiari indicatori di un sistema complesso e in rapida evoluzione, che richiede un **cambio culturale** basato sulla cooperazione, prevenzione dei rischi, preparazione nella gestione degli incidenti e pianificazione delle strategie per risolvere le crisi. Gli episodi menzionati, che sono ovviamente parte di una narrazione parziale, mostrano a tutti la vulnerabilità delle società contemporanee e la necessità di raggiungere una maggiore regolamentazione dello spazio cibernetico. Infatti, se con la Strategia del 2017 l'Unione europea ha puntato a rafforzare le capacità di difesa, deterrenza e resilienza dei singoli Stati, con la nuova Strategia, che copre il periodo 2020-2025[78], vuole garantire che la *cybersecurity* sia adeguata alle sfide che la società deve affrontare. A tal proposito, ribadisce che il quadro delle misure previste in materia di protezione e resilienza delle infrastrutture critiche non è al passo con l'evoluzione dei rischi, e richiama l'importanza di **creare competenze** e **capacità** per garantire un ambiente di sicurezza al passo con l'era della trasformazione digitale. Nella nuova Strategia vengono definite le priorità strategiche e gli interventi necessari per affrontare i rischi nell'ambiente digitale, vale a dire: sostenere la resilienza delle infrastrutture critiche per creare "un ambiente sicuro adeguato alle future esigenze, affrontare le minacce in evoluzione, proteggere i cittadini europei dal terrorismo e dalla criminalità organizzata e creare un ecosistema europeo

[78] Comunicazione, COM(2020)605 final, della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 24 luglio 2020 sulla strategia dell'UE per l'Unione della sicurezza.

forte in materia di sicurezza"[79].

Visto il carattere globale, anche nell'ambito della politica estera e di sicurezza comune sono state stabilite alcune misure per la protezione degli Stati membri e dei loro cittadini da minacce e attività informatiche dolose, con l'adozione del c.d. "pacchetto di strumenti della diplomazia informatica"[80], che consente all'UE di imporre misure restrittive come deterrente alla commissione di attacchi informatici. Queste misure sono attuabili anche nei confronti di Stati terzi, organizzazioni internazionali nonché **persone fisiche** ed **entità** che si rendano autori o che in qualche modo supportano tali attività, tecnicamente o finanziariamente. In effetti, il 30 luglio 2020, per la prima volta, il Consiglio ha imposto misure restrittive nei confronti di sei persone e tre entità responsabili di aver compiuto attacchi informatici o di avervi a diverso titolo preso parte[81].

Le sanzioni sono una delle misure intese a fungere da deterrente per la commissione di attività informatiche dolose che possono incidere negativamente sulla sicurezza dei cittadini e sulla tenuta democratica dell'Unione, e che si inseriscono perfettamente nell'azione tesa a rafforzare la resilienza dello spazio cibernetico per renderlo uno spazio aperto, sicuro e pacifico.

Uno degli obiettivi da raggiungere è quello di **diffondere un nuovo approccio alla sicurezza informatica** che si basi sulla valutazione del rischio sin dall'inizio della progettazione; un grande contributo in tal senso è dato dal nuovo quadro di certificazione della *cybersecurity* di cui è stata investita l'ENISA.

Il momento è propizio perché l'UE sfrutti il potenziale della *digital economy* ed eviti la frammentazione del mercato, così da permettere ai consumatori di beneficiare delle opportunità offerte da una scelta più ampia di beni e da prezzi più vantaggiosi. É essenziale che venga raggiunto **l'obiettivo** a monte del quadro di certificazioni, ovvero **aumentare l'affidabilità dei prodotti, servizi e processi ICT in termini di sicurezza per nutrire la fiducia nelle tecnologie digitali,** che non sarà possibile finché la riservatezza, l'integrità o la disponibilità dei dati continueranno ad essere compromessi o quando i prodotti e i servizi non funzioneranno come previsto.

Un risultato auspicabile sarebbe quello in cui il sistema di certificazioni dell'Unione europea facesse appello ai mercati globali, per aver guadagnato una posizione di riconoscimento in termini di efficacia tra i maggiori sistemi accreditati. Lo schema proposto dall'ENISA va in questa direzione e apre la strada ad un **nuovo livello di cooperazione europea** in un settore fondamentale per una società altamente dipendente dalla tecnologia, in cui il confine tra mondo *online* e *offline* è sempre più labile. Il successo del nuovo schema proposto dipenderà da tutte le parti interessate, sia del settore pubblico che privato, perché **la *cybersecurity* è una responsabilità condivisa** e dipenderà anche dalla capacità di cambiare approccio, adottando una prospettiva che

---

[79] Ivi p. 7.

[80] Decisione (PESC) 2019/797 del Consiglio del 17 maggio 2019 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri.

[81] Decisione (PESC) 2020/1127 del Consiglio del 30 luglio 2020 che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri.

consideri i rischi sin dalle prime fasi di vita di qualsiasi prodotto o servizio, piuttosto che come fattore secondario. In questo modo, è possibile che i produttori e i fornitori saranno in grado di innovare nel mercato interno e l'Unione europea avrà la capacità di competere nello scenario globale della *cybersecurity* migliorando gli *standard* di sicurezza dei cittadini e delle imprese e il loro livello di fiducia, componente imprescindibile per un mercato unico digitalizzato che sia prospero, solido e dinamico.