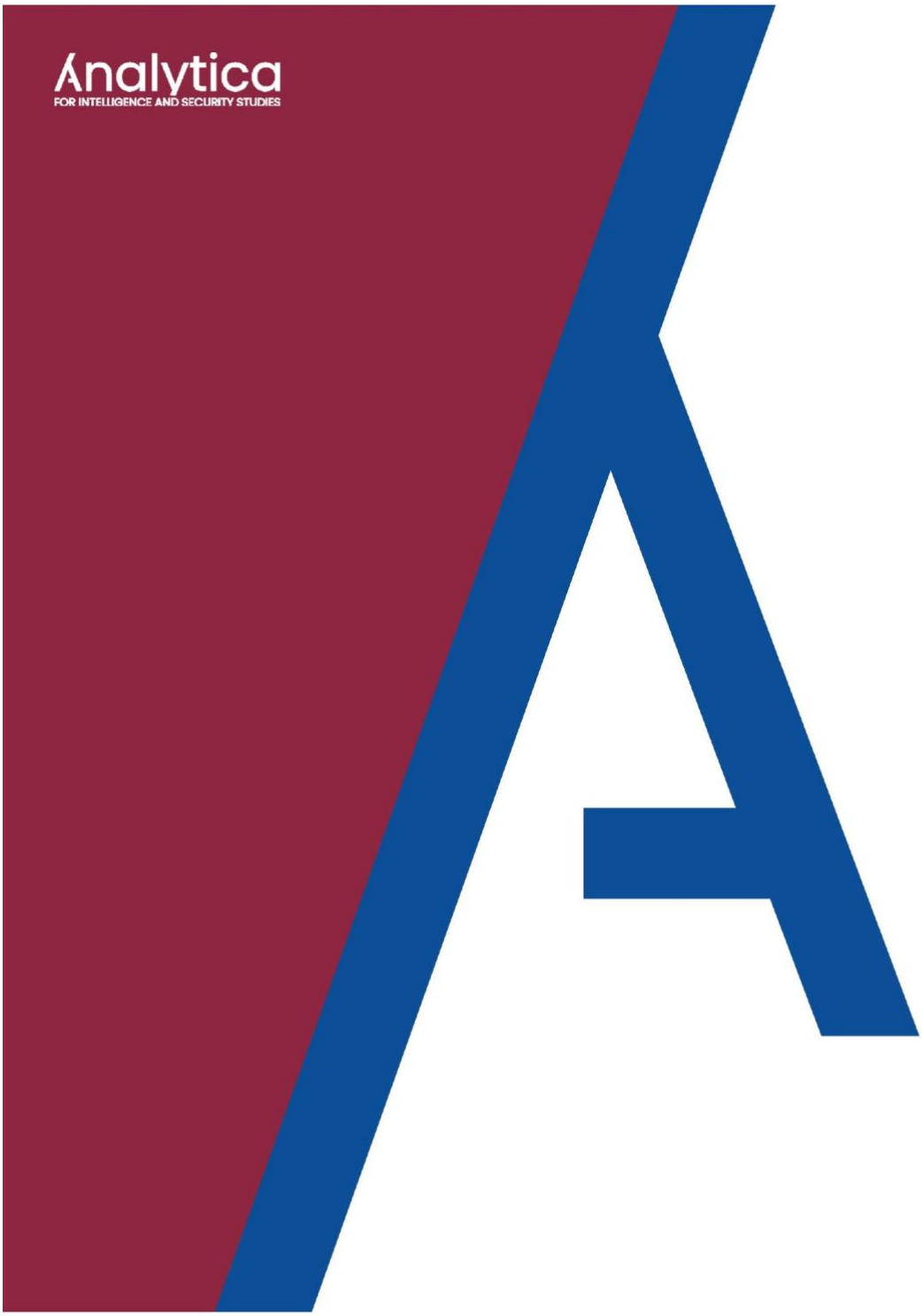

Il partenariato pubblico – privato nel contesto della cyber security. Una prospettiva europea.

Angela Lena

Analytica for intelligence and security studies

Paper Cyber security

Il partenariato pubblico – privato nel contesto della cyber security. Una prospettiva europea.

Angela Lena

Correzioni e revisioni a cura del Dottor PANEBIANCO Andrea

Torino, febbraio 2020

Il principio del successo è la cooperazione. Se l'equilibrio di Nash lo ha dimostrato in ambito scientifico, la profonda interdipendenza globale rende questo principio valido anche quando parliamo di sicurezza dello spazio cibernetico[1].
Nel *Global Risks Report* del 2020 il *World Economic Forum* ha qualificato gli attacchi cibernetici alle infrastrutture critiche dei settori strategici, quali la sanità, l'energia e i trasporti come "la nuova normalità".
La maggior parte di queste infrastrutture opera in un ambiente digitale, è posseduta e gestita da privati e regolamentata dal settore pubblico; di conseguenza, uno degli strumenti più proficui per garantire la sicurezza dalle minacce provenienti dal *cyberspace* è proprio **un elevato livello di cooperazione tra il settore pubblico e quello privato.**
Lo scopo del presente lavoro è quello di esplorare il tema della collaborazione pubblico-privata nel settore della *cyber security* per costruire la resilienza dei sistemi informatici ed informativi.
Grazie alla diffusione delle tecnologie dell'informazione e della comunicazione (ICT), negli ultimi due decenni abbiamo assistito ad una trasformazione del modo in cui vengono svolte le attività economiche, politiche e sociali, che fanno affidamento sulle tecnologie digitali per il loro pieno e corretto svolgimento. Tuttavia, le innumerevoli opportunità e i vantaggi offerti dalla digitalizzazione devono fare i conti con i potenziali rischi a cui tale progresso espone sia il settore pubblico che quello privato che operano in settori strategici.
La tecnologia ha fornito gli strumenti per erogare servizi essenziali in tutto il mondo. È indubbio, infatti, che oggi **attraverso il *cyberspace* venga gestita un'ampia gamma di attività**, dal controllo del traffico aereo, marittimo e ferroviario al funzionamento di una centrale elettrica o di una diga, fino alla gestione degli apparecchi domestici o dispositivi medici. Questa interconnessione rende la *cybersecurity* un settore cruciale in cui investire, dove **la collaborazione tra pubblico e privato appare imprescindibile.**
Con il tempo, anche **le minacce alle strutture portanti del Paese** si sono evolute, passando dalle manomissioni e attacchi fisici, a volte drammaticamente devastanti come gli episodi dell'11 settembre, ad altri meno fragorosi ma con un potenziale altrettanto deleterio, come quelli cibernetici, che non colpiscono direttamente le strutture fisiche, ma **sono in grado di inficiare le fondamenta su cui esse poggiano: *software, computer, network.***
Un attacco informatico potrebbe colpire le **infrastrutture critiche** di un Paese che, data la complessità delle tecnologie coinvolte, dei processi che le governano e il numero di attori che le progettano, implementano e controllano, rappresentano le entità a più alto livello di rischio.

Se garantire la riservatezza dei dati, assicurarne l'integrità e mantenerne la disponibilità sono le tipiche priorità della sicurezza dei sistemi IT (*Information Technology*), i sistemi OT (*Operational Technology*) hanno spesso privilegiato la disponibilità dei sistemi a discapito della loro sicurezza, spesso operando con sistemi obsoleti (*legacy systems*), per i quali le *patch* di sicurezza non sono

[1] Quando al premio nobel per l'economia John Nash, venne chiesto di spiegare in "quattro parole" quello che nella teoria dei giochi è conosciuto come equilibrio di Nash, egli rispose : l'equilibrio c'è, quando nessuno riesce a migliorare in maniera unilaterale il proprio comportamento. Per cambiare, occorre agire insieme" [...] "perché unilateralmente possiamo solo evitare il peggio, mentre per raggiungere il meglio abbiamo bisogno di cooperazione. L'intera intervista è consultabile *online*: P. Odifreddi, "*John Nash genio e follia*" in *L'Espresso,* 11 Marzo 2008.

disponibili e, qualora lo fossero, i tempi di inattività per eseguirle non sono contemplati, con il risultato che detti sistemi presentano innumerevoli vulnerabilità e risultano altamente esposti agli attacchi informatici[2].

Ormai la quasi totalità delle industrie mondiali si affida alle **tecnologie OT,** ovvero all'utilizzo di *hardware* e *software* per monitorare e controllare i dispositivi fisici e gestire le operazioni industriali, così come ai **sistemi di controllo industriale (ICS),** una parte importante dell'ambiente OT.

Storicamente, la sicurezza informatica delle tecnologie operative negli impianti industriali non era prevista, per il semplice motivo che i loro sistemi non erano collegati a Internet. Gli impianti, dunque, se da un lato non presentavano il rischio di un accesso non autorizzato, in quanto isolati, dall'altro comportavano dei costi di gestione molto alti, perché richiedevano l'intervento fisico di tecnici che ne assicurassero il loro corretto funzionamento. Di conseguenza, con l'espansione dell'automazione è stata colta l'opportunità di ridurre i costi introducendo la possibilità di gestire da remoto il controllo e la manutenzione di tali impianti.

Aver reso accessibile attraverso internet i sistemi legati all'industria, **non progettati per operare in tali condizioni,** e dunque privi dei meccanismi di sicurezza, di autenticazione e di autorizzazione, **ha creato innumerevoli vulnerabilità che possono essere sfruttate per scopi dannosi.**

Le OT comprendono componenti essenziali all'interno dei settori delle *Critical Information Infrastructure* (CII), come il settore energetico, idrico e dei trasporti, e l'aumento globale degli attacchi informatici a tali sistemi[3], dovrebbe **intensificare il coinvolgimento del governo e dei responsabili delle operations**, nella definizione delle *policy* per la protezione dei sistemi industriali e delle OT connesse, e **tendere alla mitigazione del rischio e al rafforzamento della resilienza nel contesto industriale.**

I passi in questa direzione possono essere molteplici, ad esempio:

- **sviluppare**, con il coinvolgimento degli *stakeholders* di OT, **strategie di *cybersecurity*** per tali sistemi;
- **predisporre linee guida** per gli operatori delle infrastrutture critiche circa la sicurezza informatica OT, facendo riferimento alle *best practices* e agli standard consolidati nel settore;
- **creare** degli ***hub* di condivisione delle informazioni** sulle minacce per le aziende che operano con le infrastrutture critiche, in modo da assicurare un canale per lo scambio di informazioni sicuro sugli attacchi registrati e **aiutare nella prevenzione e mitigazione dei danni futuri**[4].

Ad oggi non esiste un consenso generale su cosa debba intendersi per infrastruttura critica, poiché, come affermato dall'Assemblea Generale delle Nazioni Unite, la portata della definizione sarà

---

[2] Di recente, la casa automobilistica Honda e una delle società di Enel Argentina, Edesur SA, che opera nel *business* della distribuzione di energia nella città di Buenos Aires, sono state vittime di attacchi che, secondo i ricercatori di Malwarebytes, sarebbero riconducibili alla famiglia dei *ransomware* EKANS/ SNAKE. Purtroppo, la lista delle società bersaglio di tali attività dannose è molto lunga.

[3] Nel Report "Cy*bersecurity in Operational Technology*, *7 insights you need to know*", pubblicato nel 2019, Ponemon Institute ha dichiarato che il 62% delle organizzazioni nei settori che si affidano alla tecnologia operativa ha subito due o più attacchi informatici con conseguenze sul proprio *business* nei 24 mesi precedenti alla stesura del rapporto.

[4] Merita di essere citato, a tal proposito, l*'Operational Technology Information Sharing and Analysis Center* (OT-ISAC) che collabora sia con aziende che con i governi per ridurre i rischi di sicurezza informatica per la tecnologia operativa e l'infrastruttura delle informazioni critiche.

stabilita da ogni singolo Stato[5]. In termini generali, comunque, l'infrastruttura critica è spesso definita come "**il patrimonio essenziale per il funzionamento di una società e di un'economia"**[6].
Come è intuibile, in una realtà altamente digitalizzata come quella odierna, tale patrimonio include una vasta gamma di servizi: telecomunicazioni, *database* sensibili delle forze dell'ordine, approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, trasporti, finanza etc., alcuni dei quali sono erogati direttamente dallo stato; altri invece sono nelle mani di privati, come fornitori di servizi internet, banche e aziende che spesso per offrire tali servizi hanno bisogno anche del supporto di infrastrutture controllate da organizzazioni straniere. Ecco, dunque, che **il partenariato pubblico-privato (PPP) diventa un'esigenza funzionale** per mitigare i rischi e proteggere i settori strategici.

È stato, peraltro, ampiamente dimostrato come, sempre più spesso, attori statali (e non) abbiano le capacità, tecniche ed economiche, di sfruttare le vulnerabilità delle infrastrutture erogatrici di servizi essenziali, mettendo a rischio l'intera sicurezza nazionale; il virus STUXNET, che modificava l'andamento delle centrifughe della centrale nucleare di Natanz o il *malware* BlackEnergy 3 che nel 2015 colpì i sistemi ICS/SCADA della rete elettrica di una regione dell'Ucraina, causandone un *blackout*, sono solo alcuni esempi delle sfide poste a carico di coloro che operano con le *Critical information infrastructure* (CII).
Ad oggi, fortunatamente, episodi di *Cyber Warfare*, intesi come uno scenario caratterizzato dall'impiego di operazioni cibernetiche offensive che abbiano raggiunto la soglia di attacco armato, non sono noti all'opinione pubblica. Gli effetti sinora prodotti sono stati limitati e gli autori non hanno mai raggiunto un livello di aggressività tale da poter fare dei parallelismi con l'11 settembre.
Tuttavia, se consideriamo che gli attacchi informatici sono uno strumento particolarmente attraente, sia da un punto di vista economico che per l'accessibilità, e consideriamo l'aumento della dipendenza delle infrastrutture critiche dalle reti di computer, **le potenziali conseguenze di un attacco informatico potrebbero avere effetti catastrofici,** come il tracollo dell'economia, la distruzione dei sistemi di trasporto, nonché la distruzione di beni e la perdita di vite umane, innescando un pericoloso effetto a cascata dovuto proprio alla complessa interdipendenza dell'attuale sistema globale.
É allora giusto chiederci cosa è possibile fare per proteggerci e quali sono le strategie messe in campo.
Il presente lavoro vuole indagare alcune implicazioni derivanti dai moderni progressi della tecnologia, illustrando come lo sviluppo della rete abbia innescato un cambiamento fondamentale nelle questioni di sicurezza, inclusa quella informatica, ponendoci di fronte a nuove e complesse sfide.
In questo scenario, in cui da un lato vi è **il dovere fondamentale dello Stato di garantire la sicurezza nazionale** e dall'altro **l'esigenza di delegare parte di questo compito al settore privato,** pare opportuno analizzare le pratiche esistenti ed indagare il modo in cui i governi e il settore privato abbiano diviso i rispettivi ruoli e collaborino per assicurare la sicurezza nel quinto dominio. A tal fine verrà presentato un *background* storico e cronologico per illustrare gli sforzi compiuti sino ad ora dall'Unione Europea; osserveremo l'evoluzione del ruolo del settore privato nella *governance* dello spazio cibernetico*;* esamineremo, quindi, l'attuale panorama dei partenariati pubblico-privati per individuarne i vantaggi, le criticità e indicare modelli virtuosi.

---

[5] Risoluzione A/RES/58/199 dell'Assemblea Generale delle Nazioni Unite, 30 gennaio 2004.
[6] C. Focarelli, *Self-defence in cyberspace*, in N. Tsagourias, R. Buchan (a cura di), Research Handbook on *International Law and Cyberspace*, Cheltenham, 2015, cap. 12, p. 268.

La sicurezza delle reti e dell'informazione

L' esperienza europea

La *cybersecurity* è diventata una priorità nell'agenda politica dell'intera comunità internazionale, e l'Unione Europea ha ravvisato sin da subito la necessità di dotarsi di un quadro legislativo efficace per far fronte alle nuove sfide e parificare il rispetto dei diritti fondamentali anche nello spazio cibernetico.
Con la Strategia del febbraio 2013[7] l'Europa ha dimostrato di voler garantire un *cyberspace* "aperto, libero e sicuro", e di considerare la sicurezza di questo dominio una questione di primaria rilevanza poiché, come si legge nella sua introduzione, **le ICT sono diventate "la spina dorsale" della crescita economica da cui dipendono i sistemi complessi che fanno funzionare le nostre società**.

In realtà, l'Unione europea ha iniziato ad occuparsi della sicurezza delle reti e dell'informazione sin dai primi anni del 2000, avanzando nel giugno del 2001 una proposta per un approccio strategico alla loro protezione[8]. In questo documento compare per la prima volta la definizione di *Network and Information Security* (NIS), intesa come "*la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema*"[9], e un'elencazione delle minacce che possono verificarsi a causa di un inadeguato livello di sicurezza.
Questa proposta segnò un importante spartiacque circa la collocazione del settore privato nella nuova arena strategico-politica. Prima di allora infatti, gran parte dei servizi erano ancora forniti dallo stato, con **un ruolo del tutto marginale per il settore privato**, considerato esclusivamente "parte lesa" dagli attacchi senza avere la responsabilità di agire ed essere resiliente a tali eventi.
Questo ruolo passivo è stato ben presto superato, poiché, come riconosce la stessa Commissione, alcuni servizi non sono stati più affidati soltanto alle società statali ma anche ad operatori e fornitori che agiscono in regime di concorrenza e in un mercato libero che considera "la sicurezza un aspetto dell'offerta di mercato.[10]"
Non essendo più esclusivo appannaggio dello stato, il settore della protezione della sicurezza delle reti e dell'informazione necessitava di un **riesame del quadro normativo**.
A seguito del riconoscimento della complessità tecnica di reti e sistemi, l'assenza di soluzioni semplici in grado di proteggerli ed il rischio di inefficacia di risposte eterogenee, nel 2004 venne manifestata l'esigenza di istituire un punto di riferimento che fosse in grado di creare un clima di fiducia sulla base di un'elevata competenza ed assistenza, che supportasse gli Stati Membri e curasse le relazioni con altri *stakeholders*. A questo fine, con il Regolamento (CE) n. 460/2004 del 10 marzo 2004[11] venne istituita l'ENISA (*European Union Agency for Network and Information Security*), con l'obiettivo di

---

[7] 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 cybersicurezza: uno spazio aperto e sicuro, JOIN/2013/01 final.

[8] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 6 giugno 2001, Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo, COM(2001)298 definitivo, par. 2.1, p. 10.

[9] Ivi, p. 2.

[10] Ivi, p. 8.

[11] 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.

"*assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione*"[12].
Dalla lettura del Regolamento istitutivo, si evince che **l'Agenzia collabora con la comunità degli operatori economici**, al fine di aiutarli a **soddisfare i requisiti di sicurezza delle reti e dell'informazione[13]**, inoltre, tra i suoi obiettivi c'è quello di stimolare **un'ampia cooperazione tra gli attori del settore pubblico e privato**, servendosi delle elevate competenze sviluppate sulla base degli sforzi compiuti a livello interno e comunitario[14]. Affinché vengano rispettati questi obiettivi, l'ENISA ha anche il compito, previsto all'art. 3, lett. c), di **migliorare la cooperazione** tra coloro che operano nel settore della sicurezza delle reti e dell'informazione, organizzando periodicamente consultazioni con l'industria, le università e le altre parti interessate, "ricreando una sinergia tra le iniziative del settore pubblico e privato"[15].
Un altro riconoscimento importante lo troviamo nel considerando 24 del Regolamento n. 460/2004, in cui viene esplicitamente attribuito un **ruolo attivo al settore privato**, che deve contribuire alla messa in sicurezza delle reti e dei sistemi informativi mettendo a disposizione le sue competenze, e viene ritenuto responsabile di tutelare la stabilità del mercato interno (considerando 3).

Su questa scia l'Unione europea ha continuato ad adottare decisioni quadro e comunicazioni[16].
Purtroppo, la necessità di intensificare gli sforzi in materia di sicurezza è stata amplificata anche dagli attentati terroristici compiuti a Madrid l'11 marzo 2004; in seguito a questi tragici eventi in ambito europeo è apparso quanto mai opportuno aprire un dialogo sullo sviluppo di strategie nazionali di *cybersecurity*, sulla cooperazione tra i vari CSIRT (*Computer Security Incident Response Team*) e l'identificazione delle minacce informatiche. Nell'ottobre dello stesso anno la Commissione europea ha adottato tre comunicazioni[17] sui temi considerati prioritari, tra cui una Comunicazione in materia di protezione delle infrastrutture critiche nella lotta contro il terrorismo[18], che **incoraggia la promozione di un partenariato pubblico-privato sulle questioni di sicurezza** e mette in guardia sulle potenziali conseguenze materiali di un attacco informatico, come ad esempio ad una rete elettrica o ai sistemi di controllo di impianti chimici o di gas naturale liquido.
A completamento di questo percorso, nel novembre 2005, la Commissione ha adottato il Libro verde relativo ad un programma europeo per la protezione delle infrastrutture critiche (EPCIP)"[19], coinvolgendo gran parte di coloro che operano in tale settore, in quanto **un'efficace protezione delle stesse richiede necessariamente una cooperazione tra tutte le parti interessate** (tra queste la Commissione menziona: i proprietari e i gestori delle infrastrutture critiche, le autorità di

[12] Ivi, art.1, par. 1.
[13] Ivi, art. 1, par. 2.
[14] Ivi, art. 2, par. 3.
[15] Ivi, art.3, lett. e).
[16] Ad esempio: Decisione quadro del Consiglio del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione, 2005/222/GAI;
Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni del 1 giugno 2005, *i*2010- Una società europea dell'informazione per la crescita e l'occupazione, COM (2005)229 definitivo.
[17] Comunicazioni della Commissione "Prevenire e combattere il finanziamento del terrorismo" [COM (2004) 700], "Preparazione e gestione delle conseguenze nella lotta al terrorismo" [COM (2004) 701], e "La protezione delle infrastrutture critiche nella lotta contro il terrorismo" [COM (2004) 702].
[18] Comunicazione della Commissione al Consiglio e al Parlamento europeo del 20 ottobre 2004, La protezione delle infrastrutture critiche nella lotta contro il terrorismo, COM (2004) 702 definitivo.
[19] Libro verde della Commissione del 17 novembre 2005, relativo ad un programma europeo per la protezione delle infrastrutture critiche, COM (2005) 576 definitivo, par. 2.

regolamentazione e le associazioni professionali e industriali in cooperazione con i diversi livelli del settore pubblico e con il settore privato).

Nell'anno successivo seguirono due importanti documenti, una **Strategia per una società dell'informazione sicura**[20], basata sul dialogo, il partenariato e la responsabilizzazione, in cui si sottolinea l'importanza della disponibilità, affidabilità e sicurezza delle reti e dei sistemi informativi per l'economia e il tessuto della nostra società, e una Comunicazione della Commissione relativa ad un **programma europeo per la protezione delle infrastrutture critiche**, con cui viene istituito il CIIP (*Critical Information Infrastructure Protection*)[21], inteso ad attuare la legislazione europea in materia di protezione delle infrastrutture critiche e garantire la tutela dalle minacce provenienti dal quinto dominio.

Con il primo documento si sancisce definitivamente **il passaggio del settore privato da attore che si limita a recepire la normativa prevista dai decisori politici, ad attore che è coinvolto attivamente nel processo decisionale che ne determina il contenuto**[22]. Data l'alta dipendenza tra le reti e le infrastrutture critiche, la sicurezza della NIS è considerata una priorità e una sfida che le parti coinvolte non possono affrontare prescindendo dalla condivisione delle informazioni sugli incidenti e da una profonda conoscenza delle minacce[23]. Per garantire la resilienza dei sistemi informativi, **la Commissione riconosce il ruolo complementare del settore privato, sia nella raccolta e condivisione dei dati sugli incidenti, che nella diffusione di buone pratiche in materia di sicurezza per gli operatori della rete,** e lo invita a definire **le responsabilità dei produttori di *software* e dei fornitori di servizi internet** in relazione alla fornitura di livelli di sicurezza adeguati e verificabili[24].

Nel biennio 2009-2010 sono stati compiuti altri passi in avanti nel **rafforzamento del ruolo degli attori privati come parte attiva nella definizione delle politiche in materia di NIS**, *in primis* con una Risoluzione del Consiglio[25], in cui si riconosce l'importanza dei partenariati pubblico-privati per attenuare i rischi e garantire un elevato livello di resilienza delle reti[26], si sottolinea il ruolo cruciale che il settore privato svolge nella fornitura di infrastrutture di comunicazioni elettroniche solide e resilienti[27], e si invitano i soggetti interessati a proseguire i lavori sulla standardizzazione della sicurezza delle reti e dell'informazione per cercare di trovare soluzioni armonizzate e interoperabili[28].

Sempre nel 2009, viene poi istituito l'EP3R (*European Public-Private Partnership for Resilience*)[29] nell'ambito di un'iniziativa più ampia, conosciuta come il Piano d'azione per proteggere le

---

[20] Comunicazione della Commissione europea del 31 maggio 2006, Una strategia per una società dell'informazione sicura. Dialogo, partenariato e responsabilizzazione, COM(2006)251.

[21] Comunicazione della Commissione del 12 dicembre 2006, relativa ad un programma europeo per la sicurezza delle infrastrutture critiche, COM(2006)786 definitivo.

[22] COM(2006)251, p. 6

[23] *Ibidem*.

[24] Ivi, pp. 8-9.

[25] Risoluzione del Consiglio, del 18 dicembre 2009, su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione, 2009/C 321/01.

[26] Ivi, sez. 4, par. 7.

[27] Ivi, sez. 4, par. 8.

[28] Ivi, sez. 9, par. 4. Maggiori informazioni sul tema possono essere rinvenute nella pubblicazione: H. Carrapico, B. Farrand, *"Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers"*, in *Crime Law Soc Change*, 11 Ottobre 2016, reperibile *online*.

[29] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni del 30 Marzo 2009, Proteggere le infrastrutture critiche informatizzate "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai cyberattacco e dalle cyberperturbazioni, COM(2009)149 definitivo.

infrastrutture critiche informatizzate (CIIP), fondamentale per attuare la già citata Strategia del 2006[30]. Le valutazioni posteriori dello EP3R, da parte della stessa ENISA, hanno tuttavia dimostrato che nonostante gli sforzi, non si è riusciti a conseguire tutti i risultati sperati. Il mancato successo è riconducibile a diversi fattori, tra cui la diversità degli *stakeholders,* la prospettiva di costose misure di sicurezza obbligatorie e i vari conflitti di interesse circa la riservatezza dei dati; è importante però ricordarlo come il primo tentativo, a livello paneuropeo, di utilizzare la cooperazione tra il settore pubblico e quello privato, per affrontare i problemi di sicurezza e resilienza transfrontalieri nel settore delle telecomunicazioni e definire insieme le *best practices* politiche*,* gli obiettivi strategici, le misure e le priorità operative necessarie[31].
Del 2010 ricordiamo la strategia Europa 2020[32], nell'ambito della quale la Commissione ha presentato sette diverse iniziative, tra cui **l'agenda digitale europea,** con l'obiettivo di sfruttare al meglio il potenziale delle ICT per favorire l'innovazione e la crescita economica[33]. Una parte importante dell'agenda sostiene che **è necessario organizzare a livello mondiale la cooperazione tra gli attori coinvolti,** in modo da combattere in maniera efficace le minacce e contenerle[34]. L' agenda prevede, inoltre, una serie di azioni fondamentali che la Commissione deve intraprendere, tra cui presentare misure volte a raggiungere una politica rafforzata e di alto livello in materia di sicurezza delle reti e delle informazioni, che comprenda iniziative legislative come un rinnovo dell'ENISA, nonché misure che permettano di rispondere più rapidamente ai cyber-attacchi, compreso un CERT per le istituzioni dell'UE[35].

Nel 2013 l'Unione europea si è dotata della sua prima Cyber Strategy[36] segnando un punto di svolta fondamentale. Innanzitutto riconosce esplicitamente che **la *cybersecurity* è una responsabilità condivisa con il settore privato che deve attivarsi per proteggersi e, se necessario, assicurare una risposta coordinata ed efficace**[37]. Propone anche di migliorare la preparazione e l'impegno di questo settore, che detiene la maggior parte delle reti e dei sistemi informativi, coinvolgendolo maggiormente attraverso lo **sviluppo e la condivisione di proprie capacità di resilienza informatica**, cosicché anche il settore pubblico ne possa beneficiare[38].
Nella Strategia del 2013 viene anche annunciata la creazione della c.d. *European Network and Information Security Platform* (NIS Platform), successore dello E3PR, con lo scopo di promuovere la resilienza delle reti e dei sistemi informativi. Con tale presupposto sono stati creati tre gruppi di lavoro, tra cui quello sullo scambio di informazioni e il coordinamento degli incidenti, registrando

[30] COM(2006)251.
[31] Lionel Dupré, "*EP3R 2010-2013 Four Years of Pan-European Public Private Cooperation",* in *European Union Agency for Network and Information Security* (ENISA), Novembre 2014, reperibile *online*.
[32] Comunicazione della Commissione, del 3 Marzo 2010, EUROPA 2020 Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 definitivo.
[33] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni del 19 Maggio 2010, Un'agenda digitale europea, COM(2010)245 definitivo.
[34] Ivi, p. 19.
[35] Ivi, Azione fondamentale n. 6.
[36] 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 cybersicurezza: uno spazio aperto e sicuro, JOIN/2013/01 final.
[37] Ivi, p. 4.
[38] Ivi, p. 6.

uno sforzo considerevole in termini di cooperazione pubblico-privata, soprattutto se consideriamo che già nel 2015 contava oltre 200 partecipanti, tra organizzazioni e membri, di cui 110 erano portatori di istanze commerciali.

Nel Maggio 2015 è stata adottata la **Strategia per il mercato unico digitale in Europa**[39], che contiene una serie di iniziative volte a rafforzare la fiducia e la sicurezza di Internet, in modo da creare un ambiente appropriato per l'economia digitale, tra cui **l'istituzione di un partenariato pubblico-privato sulla cybersicurezza nel settore delle tecnologie e soluzioni per la sicurezza delle reti**[40], poiché la costruzione di un mercato unico digitale efficiente non può prescindere dalla comprensione reciproca dei bisogni e una collaborazione tra industria e governo. Il 5 luglio del 2016 la Commissione ha firmato con l'Organizzazione europea per la sicurezza informatica (ECSO) **il primo partenariato pubblico-privato (PPP) dell'Unione europea,** investendo, nel quadro del programma di ricerca e innovazione Orizzonte 2020, 450 milioni di euro. Un'iniziativa che ha dimostrato di essere determinante nello sviluppo di soluzioni di *cybersecurity* per i settori cruciali come energia, trasporti, finanza etc., che ha promosso la cooperazione tra il settore pubblico e quello privato e ha stimolato l'industria della sicurezza informatica[41].

Esattamente il giorno successivo alla firma del primo partenariato pubblico-privato europeo, è stata adottata la Direttiva (UE) 2016/1148, concernente misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, nota anche come **Direttiva NIS**[42], e che presenta diversi aspetti che coinvolgono le *partnership* pubblico-private. Più volte, infatti, all'interno del testo ricorre il concetto di **sensibilizzazione del pubblico** (cittadini e operatori dei servizi essenziali - OSE) **nel campo della sicurezza informatica**, per realizzare lo scopo a cui la direttiva è preordinata: raggiungere un livello elevato di *cybersecurity* nell'Unione. Questo aspetto può essere affrontato attraverso la cooperazione tra pubblico e privato, con lo scambio di informazioni e la condivisione delle *best practices,* chiedendo alle imprese che operano in settori economici cruciali di adottare pratiche efficaci di gestione dei rischi e di segnalare gli incidenti gravi alle autorità nazionali[43].

Inoltre, dal momento che la responsabilità di garantire la sicurezza delle reti e dei sistemi informativi incombe in larga misura sugli operatori di servizi essenziali e fornitori di servizi digitali[44], è necessario stabilire una stretta cooperazione tra le autorità nazionali competenti e gli operatori di servizi essenziali, peraltro identificati dagli Stati membri. Sempre nel luglio 2016 la Commissione presenta un'importante Comunicazione[45] in cui si sottolineano le iniziative necessarie affinché l'Unione possa ricoprire un ruolo di *leadership* nel settore della *cybersecurity* e in quest'ottica pone tre obiettivi da raggiungere:

- rafforzare la cooperazione in modo da essere più preparati agli incidenti informatici e gestirli adeguatamente;
- incoraggiare lo sviluppo di capacità industriali nel campo della cibersicurezza;

---

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

[40] Ivi, p. 14.

[41] European cyber security organisation (ECSO), "*European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*", in *European cyber security organisation*, luglio 2016, reperibile *online*.

[42] 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.

[43] Ivi, considerando 35.

[44] Ivi, considerando 44.

[45] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 5 Luglio 2016, Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza, COM(2016) 410 final.

- reagire alle sfide che il mercato unico della cybersicurezza europeo si trova ad affrontare[46].

Nel 2017 la Commissione adotta una Comunicazione[47] volta a **rafforzare la resilienza dell'Unione europea per consentire una gestione efficace degli incidenti informatici**, anche in previsione dell'aumento del numero di dispositivi connessi alla rete e della trasformazione digitale che farà crescere il numero delle vulnerabilità. L'approccio presentato nel documento richiede il pieno coinvolgimento di tutte le parti interessate, e sostiene **la necessità di rafforzare la fiducia per lo scambio di informazioni tra il pubblico e il privato** ritenendo fondamentale a questo proposito il ruolo svolto dai centri di condivisione e di analisi delle informazioni. A questa dichiarazione d'intenti ha fatto seguito la creazione di un Centro europeo per la sicurezza informatica nell'aviazione (*European Centre for Cyber Security in Aviation* - ECCSA), una piattaforma di condivisione e gestione delle informazioni sulla sicurezza informatica rilevanti per il settore dell'aviazione, come le vulnerabilità che possono essere utilizzate per scopi dannosi, nonché eventi e incidenti che potrebbero facilitare la conoscenza delle minacce.
Nel 2019 è stato adottato il Regolamento 2019/881, altrimenti noto come "**Cybersecurity Act**"[48], che rafforza il ruolo dell'ENISA con un mandato permanente, e delinea il processo per la predisposizione di un sistema europeo per la certificazione della *cybersecurity* dei dispositivi connessi alla rete e di altri prodotti e servizi digitali, al fine di stabilire e mantenere la fiducia e la sicurezza dei prodotti e servizi ICT, ma anche per abbattere i costi per le imprese e tutelare i consumatori.
Nell'ambito del suo nuovo mandato, all'ENISA viene richiesto di operare come centro di informazioni e conoscenze, **promuovendo lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato**[49]. Nel patrocinare la collaborazione pubblico-privata, soprattutto quella coinvolta nella protezione delle infrastrutture critiche, l'Agenzia deve fornire orientamenti sugli strumenti e procedure disponibili e indicazioni su come affrontare le questioni normative relative alla condivisione delle informazioni, ad esempio **agevolando la creazione di centri settoriali di condivisione e di analisi delle informazioni**[50].

Inoltre, per contribuire ad una risposta efficace in caso di incidenti transfrontalieri su vasta scala, è previsto che l'ENISA supporti sia una **cooperazione operativa** tra gli Stati membri, agevolando il confronto sulle soluzioni tecniche e contribuendo alla comunicazione pubblica, che una **cooperazione tecnica,** monitorando periodicamente il livello generale di sicurezza nell'Unione di concerto con gli Stati membri.
Poiché la ricerca è fondamentale in un settore in continua evoluzione come quello della *cybersecurity,* e la capacità di rispondere alle sfide è strettamente legata alla produzione di conoscenza e alla capacità di convertirla in strategie efficaci, **le partnership non dovrebbero essere instaurate esclusivamente con l'industria, ma anche con il mondo accademico:** il Regolamento, infatti, propone di istituire partenariati con le università che abbiano avviato studi o che si occupano di sicurezza informatica[51].

---

[46] Ivi, p. 3.
[47] Comunicazione congiunta al Parlamento europeo e al Consiglio del 13 settembre 2017, Resilienza, Deterrenza e Difesa: verso una Cybersicurezza forte per l'UE.
[48] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).
[49] Ivi, considerando 17.
[50] Ivi, considerando 29.
[51] Ivi, considerando 45.

In linea con questa filosofia è il programma **Digital Europe**, che ha l'obiettivo di sostenere la transizione digitale dell'Europa attraverso la costruzione delle sue capacità digitali. Nell'ambito di questo progetto è stata avviata anche una consultazione pubblica (conclusa il 9 novembre 2019) per conoscere le opinioni e gli interessi delle parti interessate e sensibilizzare il pubblico sui cinque settori chiave, tra cui quello della sicurezza informatica, riscuotendo una considerevole partecipazione di cittadini (34%) e aziende (18%).
Nel programma rientra anche l'iniziativa **Horizon Europe (2021-2027)**, il più grande programma di ricerca e innovazione per cui sono stati stanziati 95,5 miliardi di euro per i prossimi sette anni (il 30% in più rispetto al suo predecessore Horizon 2020) e che vedrà la formazione di diversi partenariati in diverse aree critiche come l'energia, i trasporti, la biodiversità, la salute e l'alimentazione.
Questo *excursus* ha ripercorso le iniziative fondamentali dell'Unione europea, a partire dall'inizio degli anni duemila, volte a **costruire e alimentare la collaborazione tra il settore pubblico e quello privato**. Non è un percorso facile, sia per **fattori culturali molto eterogenei** che rendono difficile individuare un modello unico di cooperazione adatto per tutti i Paesi, sia perché **la fiducia** su cui nasce un PPP con il tempo **può essere erosa**[52].

Ad ogni modo, sulla scia delle iniziative europee citate, con il supporto dell'ENISA[53] e motivata anche dalla crescente preoccupazione per l'aumento, sia in termini di quantità che di sofisticazione, delle minacce, possiamo affermare che negli ultimi anni c'è stata una crescita nella collaborazione per migliorare la *cybersecurity* a livello nazionale[54].

Il nuovo pacchetto di misure per la cybersecurity

L'ultimo tassello presentato dalla Commissione e dall'Alto Rappresentante, in materia di sicurezza informatica, è la nuova **Strategia per il decennio digitale**[55], complementare al documento "Plasmare il futuro digitale dell'Europa"[56], al piano per la ripresa europea[57] e alla strategia per l'Unione della sicurezza 2020-2025[58].

Il documento parte dalla constatazione che gli attacchi dolosi alle infrastrutture sono un rischio che

---

[52] I motivi per cui un PPP può fallire sono molteplici, per esempio la mancanza di fondi o di una solida base giuridica, così come la mancanza di una *leadership*.

[53] Negli anni l'ENISA ha supportato l'azione degli Stati nella creazione di PPP in molti modi, tra questi vi è la pubblicazione di vere e proprie linee guida e *best practices* per creare una partnership di successo. Per maggiori informazioni si rimanda al testo:
The European Network and Information Security Agency (ENISA), "*Cooperative Models for Effective Public Private Partnerships Good Practice Guide*", in ENISA, 2011, reperibile *online.*

[54] Prima del 2012 solo 12 Paesi si erano dotati di una Strategia sulla sicurezza informatica, oggi tutti i Paesi dell'UE ne hanno adottato una. Inoltre, sono aumentati i PPP settoriali, cioè gli *Information Sharing and Analysis Centers* (ISACs), che sono un modello più formale di cooperazione rispetto ai normali PPP e si basano principalmente sulla condivisione di informazioni e analisi degli incidenti nel settore della sicurezza informatica.

[55] Comunicazione congiunta al Parlamento europeo e al Consiglio del 16 dicembre 2020 , La strategia dell'UE in materia di cybersicurezza per il decennio digitale, JOIN(2020) 18 final.

[56] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 19 febbraio 2020, Plasmare il futuro digitale dell'Europa, COM(2020)67 final.

[57] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, dell'11 marzo 2020, Un nuovo piano d'azione per l'economia circolare Per un'Europa più pulita e più competitiva, COM(2020)98 final.

[58] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 24 luglio 2020, sulla strategia dell'UE per l'Unione della sicurezza, COM(2020) 605 final.

riguarda l'intera comunità internazionale e nessuno può sottrarsi alla responsabilità di rendere lo spazio cibernetico un dominio sicuro; tuttavia, nella nuova Strategia si prende atto che **l'Unione è priva di consapevolezza situazionale collettiva in materia di minacce informatiche**[59], questo a causa del fatto che le autorità nazionali non prevedono la raccolta e la condivisione sistematica di informazioni, come quelle disponibili nel settore privato sulle notifiche di incidenti ricevute, che aiuterebbero ad avere una visione d'insieme sul panorama delle minacce e quindi ad essere piu preparati ad affrontarle.

L'intera Strategia delinea tre linee d'azione in tre aree distinte, volte rispettivamente alla "creazione della resilienza, sovranità tecnologica e leadership", alla "costruzione di una capacità operativa di prevenzione, dissuasione e risposta" e alla "promozione di uno spazio cibernetico globale e aperto attraverso una maggiore cooperazione".
Nell'ottica di stimolare un approccio maggiormente attivo degli Stati membri, il primo indirizzo prevede la costituzione di un centro europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza e la rete di centri nazionali di coordinamento (CCCN) che dovrebbe avvalersi del prezioso contributo del settore industriale e del mondo accademico **per sviluppare la sovranità tecnologica dell'UE** in materia di sicurezza informatica, **garantire la sicurezza di infrastrutture sensibili,** e **sostenere la ricerca e l'innovazione** per ridurre la dipendenza esterna per le tecnologie più importanti[60].
Nell'ambito del secondo indirizzo è stata prevista la creazione di una **Unità Cibernetica Congiunta** (*Joint Cyber Unit*), nella forma di una piattaforma fisica e virtuale per la cooperazione tra le varie autorità di *cybersecurity* all'interno dell'UE, per dare una risposta coordinata ed efficace agli attacchi e sopperire anche alla mancanza di una piattaforma che consenta la cooperazione operativa con il settore privato; a tal proposito, nel documento si prevede **la creazione di partenariati strutturati con una base industriale di fiducia**[61].
Lo sviluppo di tale Unità è stato proposto dalla presidente della Commissione europea, Ursula von der Leyen, ed è pensato per favorire **un approccio più centralizzato alla *cybersecurity*** e completare il quadro europeo di gestione delle crisi informatiche. L'iniziativa, inoltre, mira a **combattere le carenze nella risposta agli attacchi informatici,** che purtroppo sono in costante aumento, mettendo a disposizione di tutte le autorità coinvolte uno spazio comune per **attuare una cooperazione strutturata** e **facilitare la cooperazione operativa** tra gli *stakeholders*.
Almeno nelle intenzioni, la *Joint Cyber Unit* è pensata per essere il fulcro della cooperazione operativa dell'Unione europea e **rafforzare le capacità di risposta con l'aiuto, fondamentale, del settore industriale e dei partner esterni**, in cui verrà garantito **un canale sicuro per lo scambio di informazioni**, che di riflesso aiuterà anche ad ottenere una panoramica generale ed aggiornata sulle minacce, e verrà **incentivato il supporto reciproco e lo scambio di competenze tra le parti** per accrescere la propria preparazione e resilienza. A breve, dovrebbero essere presentate le scadenze per la definizione, la preparazione, la realizzazione e l'espansione della nuova Unità.
Infine, sostenendo il modello multipartecipativo per le questioni che riguardano la sicurezza informatica e il cyberspazio, la Commissione e l'Alto Rappresentante rafforzeranno la comunicazione con i portatori di interessi, compreso il settore privato, il mondo accademico e la società civile, a riprova del fatto che **l'interdipendenza dello spazio cibernetico coinvolge tutti e nessuno è esente dalla responsabilità di renderlo uno spazio *open, safe* e *secure,* rafforzando la resilienza collettiva dell'Europa contro le minacce informatiche e permettendo ai cittadini e alle imprese**

[59] JOIN(2020) 18 final, p. 4.
[60] Ivi, p. 13.
[61] Ivi, p. 16.

di godere appieno dei vantaggi delle tecnologie digitali.
Di conseguenza, la Commissione ha presentato due nuove proposte: una proposta legislativa volta ad aggiornare la Direttiva NIS (denominata NIS 2[62]) e una nuova direttiva sulla resilienza delle entità critiche[63].
La revisione della NIS, in linea con la priorità di rendere l'Europa "adatta all'era digitale", **si è resa ancor più evidente con l'arrivo della pandemia di COVID-19,** che ha portato alla luce tutte le sue lacune, tra cui la risposta spesso incoerente di alcuni Stati nell'adeguamento alle disposizioni previste. Nel testo della proposta, infatti, viene sottolineato il paradosso di come in alcuni Stati gli ospedali non rientrino tra gli enti tenuti ad adottare le misure di sicurezza contenute nella NIS, mentre in altri Paesi i servizi di assistenza sanitaria sono coperti dai requisiti menzionati dalla Direttiva[64]**: questo approccio disomogeneo non contribuisce ad aumentare il livello di resilienza informatica dell'Unione e vanifica gli sforzi compiuti.**
A fronte di ciò, la nuova proposta abolisce la distinzione tra Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD) e classifica le entità in base alla loro importanza, dividendole in categorie essenziali ed importanti[65], inoltre **estende gli obblighi della NIS anche ad alcuni settori che finora non rientravano nel novero di applicazione**[66], aggiungendo una lista di specifiche misure di sicurezza che dovranno essere implementate, e introduce un limite dimensionale, ricomprendendo tutte le aziende medie e grandi dei settori elencati, con l'esclusione delle micro e piccole imprese, eccezion fatta per quelle che abbiano un profilo di rischio elevato[67].

Rilevante ai fini della presente analisi è l'innovazione sotto il profilo della **gestione del rischio informatico.** Mentre nella prima Direttiva il dovere di adottare misure idonee per la gestione del rischio e la notifica degli incidenti significativi alle autorità nazionali ricadeva in capo agli OSE e agli FDS, nella nuova proposta legislativa **sono gli organi di gestione degli operatori essenziali e importanti,** vale a dire il *management,* a dover rispondere per la violazione degli obblighi nel garantire il rispetto e l'aderenza alle misure di sicurezza di cui all'art. 18 della proposta. Si rileva, inoltre, che i membri dell'organo di gestione dovranno munirsi, attraverso dei corsi di formazione specifici e regolari, delle conoscenze e competenze necessarie per individuare le migliori pratiche, valutare i rischi e il loro potenziale impatto[68].
La seconda proposta presentata è volta a **migliorare la fornitura dei servizi essenziali nel mercato interno**, su cui si basa il funzionamento dell'economia e della società, aumentando la resilienza delle infrastrutture critiche che offrono tali servizi.
A seguito della valutazione della Direttiva 2008/114/CE [69] sulle infrastrutture critiche europee, effettuata lo scorso 2019, è stata rilevata **la necessità di garantire maggiormente la resilienza delle entità critiche,** poiché, a causa della marcata interconnessione tra settori, le misure previste non

[62] Proposta della Commissione europea al Parlamento e al Consiglio del 16 dicembre 2020, sulle misure per un livello comune elevato di cybersicurezza in tutta l'Unione, che abroga la direttiva (UE) 2016/1148, COM(2020) 823 final.
[63] Proposta della Commissione europea del 16 dicembre 2020, sulla resilienza delle entità critiche, COM(2020) 829 final.
[64] COM(2020) 823 final, p. 1.
[65] Commissione Europea, "*Proposta di Direttiva sulle misure per un livello comune elevato di cybersicurezza in tutta l'Unione*", 16 Dicembre 2020, reperibile *online.*
[66] COM(2020) 823 final, p. 9 per l'elenco dei nuovi settori inclusi.
[67] COM(2020) 823 final, p. 9.
[68] Ivi, art. 17, par. 2.
[69] Direttiva 2008/114/CE del Consiglio dell'8 Dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

risultano più adeguate all'era altamente digitalizzata in cui viviamo e all'evoluzione delle minacce con cui devono confrontarsi. Questa carenza ha messo in evidenza anche la scarsa preparazione, dei soggetti che gestiscono tali infrastrutture, nel far fronte ad eventuali attacchi che potrebbero generare l'interruzione della fornitura dei servizi, con conseguenze a cascata sia per le funzioni essenziali della società che per l'economia[70].
Inoltre, ciò che è considerato critico in alcuni Stati non lo è per altri, e questo genera confusione e difficoltà per coloro che operano in più Stati. Per permettere un corretto funzionamento del mercato interno, la proposta presentata lo scorso Dicembre, auspica la **creazione di norme minime armonizzate** per garantire la fornitura di servizi essenziali e rafforzare la resilienza delle entità critiche[71].

Su questa scia, gli Stati membri dovrebbero disporre di una **strategia che definisca gli obiettivi e le azioni da intraprendere per garantire la resilienza delle entità critiche ed eseguire valutazioni periodiche del rischio**[72], che aiuterebbero anche ad identificare altre entità critiche e supportarle nell'adeguamento alle misure di sicurezza richieste.
Occorre sottolineare come le entità relative al settore delle infrastrutture digitali rientrino nell'ambito di applicazione della direttiva NIS 2, e dunque non debbano sottostare agli obblighi previsti dalla suddetta proposta se non per quanto previsto dal Capitolo II della stessa, in modo tale che gli Stati membri, utilizzando *mutatis mutandi* i criteri e le procedure ivi previsti, identifichino i soggetti appartenenti al settore delle infrastrutture digitali e possano equiparali ad entità critiche[73].
L'ultima ambiziosa proposta della Commissione riguarda la previsione di **nuove regole per i servizi digitali** che ormai fanno parte della nostra quotidianità, compresi i social media, i mercati *online* e altre piattaforme digitali che operano nel territorio dell'Unione: ci riferiamo al **Digital Services Act** (DSA)[74] e al **Digital Markets Act** (DMA)[75].
Il primo fonda la sua origine nella direttiva e-commerce del 2000[76], e dunque il suo aggiornamento era particolarmente atteso e avrà un impatto su tutte le imprese che offrono servizi digitali.
È stato creato con l'intento di delineare uno spazio digitale sicuro in cui vi sia **il rispetto dei diritti fondamentali per gli utenti dei servizi digitali** e un quadro chiaro circa **la responsabilità per le piattaforme *online*.** In concreto, il DSA prevede una serie di obblighi per garantire tali diritti, tra cui il dovere in capo agli Stati di controllare la conformità agli obblighi previsti da parte dei prestatori di servizi digitali che operano sul proprio territorio.
Il secondo documento, invece, mira a ristabilire l'equilibrio che è stato sbilanciato dal comportamento delle grandi piattaforme digitali, c.d. "*gatekeeper*", per eliminare le barriere all'ingresso, creare parità di condizioni e permettere a tutte le imprese di essere competitive nel mercato digitale, dimodoché i consumatori avranno una maggiore possibilità di scelta e non solo quelle avanzate dalle grandi piattaforme digitali.

---

[70] COM(2020) 829 final, p. 14.
[71] *Ibidem*.
[72] Ivi, considerando 10.
[73] Ivi, considerando 14.
[74] Proposal for a regulation of the european Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.
[75] Proposal for a regulation of the european Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final.
[76] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

Il DMA in aggiunta, attribuisce anche poteri sanzionatori alla Commissione europea che, constatata la violazione, può imporre multe significative, penalità di mora e ulteriori rimedi in caso di recidiva.

L'attuale panorama sul partenariato pubblico-privato

Vantaggi, ostacoli ed elementi di successo

L'utilizzo dello strumento del partenariato pubblico-privato (PPP) è molto diffuso non solo per le questioni che attengono alla sicurezza informatica ma anche in altri settori (trasporti, assistenza sanitaria, istruzione etc.), e viene utilizzato per fornire beni e servizi che tendenzialmente sono gestiti dal settore pubblico.
Il presente lavoro parte dall'assunto che se un governo vuole costruire una solida resilienza per contrastare i potenziali attacchi cibernetici che dovessero colpire le reti elettriche, i sistemi idrici o altre infrastrutture critiche sul proprio territorio, non può prescindere dal coordinare gli sforzi con il settore privato che possiede molte di queste infrastrutture[77].
Benché, come emerge dalla trattazione sinora esposta, la Commissione europea abbia spesso incoraggiato l'utilizzo di questo strumento, predisponendo un quadro legislativo e organi che ne facilitassero la creazione, non sempre i progetti intrapresi hanno riportato il successo sperato. Molto spesso questo accade perché, per produrre i vantaggi a cui è preordinato, un partenariato deve fondarsi su una solida ***due diligence***, dovere che nella pratica non sempre viene rispettato.
I **vantaggi** che una buona *partnership* tra il settore pubblico e quello privato può dare sono molteplici, proprio perché si tratta di uno **strumento flessibile** e in quanto tale può:

- **aiutare nella gestione degli incidenti e delle crisi**: mentre il ruolo dello stato è quello di predisporre un quadro legislativo che aiuti nella pianificazione della resilienza, come una *cyber strategy* nazionale, e istituire meccanismi più snelli di condivisione delle informazioni; il settore privato può avere un impatto molto efficace nella risposta tempestiva agli attacchi, soprattutto grazie alla massiva raccolta di informazioni e alle competenze tecnologiche avanzate che spesso mancano nel settore pubblico. Ne consegue che lo **scambio di informazioni in tempo reale tra i due settori** può essere uno strumento utile nella gestione degli incidenti informatici;
- **sviluppare buone pratiche e *standard* di sicurezza:** lavorando insieme, il settore pubblico e quello privato possono contribuire allo sviluppo e alla diffusione di *best practices* e conseguentemente aumentare il livello generale di sicurezza, per esempio con informazioni relative alle modalità di sviluppo dei *software,* all'implementazione delle *patch* di sicurezza o confrontarsi sulle pratiche di risposta agli incidenti. Attraverso un'azione sinergica possono anche facilitare la definizione di *standard* di sicurezza e linee guida per gli operatori delle infrastrutture critiche;
- **sostenere lo sviluppo del settore della *cybersecurity:*** è possibile che un partenariato faccia luce sui bisogni e sulla domanda nel settore della sicurezza informatica e si concentri nella ricerca e lo sviluppo di nuove tecnologie per soddisfare tali richieste e, conseguentemente,

[77] S. Goldsmith, W. D. Eggers, *Governing by Network: The New Shape of the Public Sector*, Brookings Institution Press, 2009, Washington, DC.

dare una spinta al settore - a maggior ragione se vengono coinvolte le università e i ricercatori che hanno intrapreso studi sul tema;

- **essere di supporto nella pianificazione strategica:** la collaborazione tra settori potrebbe affrontare temi ritenuti strategici per la protezione delle infrastrutture critiche e stimolare il dialogo su disegni di legge e altre iniziative che garantiscano un maggiore livello di sicurezza.

Come anticipato, non sempre la collaborazione instaurata tra i due settori conduce agli esiti sperati. Analizzando la letteratura disponibile sulle *partnership* pubblico-private e le valutazioni dell'ENISA sui diversi modelli di partenariati, emerge che i motivi per cui una collaborazione può fallire sono diversi, poiché diversi sono gli ostacoli da superare:

- **mancanza di risorse (umane e finanziarie):** una delle principali difficoltà incontrate è lo scarso impiego di capitale umano e finanziario per la riuscita dei partenariati. La vasta portata e la lunga durata che caratterizzano i PPP richiedono costi elevati e un numero sufficiente di personale qualificato che spesso non viene allocato, in quanto non considerati prioritari. Tuttavia, essendo uno dei requisiti fondamentali, è un punto che andrebbe discusso a monte, prima di intraprendere qualsiasi tipo di collaborazione.
- **mandati differenti:** sotto questo profilo, il settore pubblico e quello privato registrano approcci diversi soprattutto nella pianificazione delle rispettive azioni. I governi tendenzialmente fanno dei piani di medio-lungo termine, mentre il settore privato si muove con tempistiche molto più contratte per rispondere a logiche di *business* dinamiche;
- **costruzione e mantenimento della fiducia:** il rapporto di fiducia viene spesso definito come uno degli impedimenti maggiori per la riuscita di un PPP, in quanto è il requisito di base che permette a due parti di poter costruire e portare avanti una collaborazione ed è, allo stesso tempo, uno degli elementi più difficili da mantenere nel tempo, poiché richiede impegno, volontà ed energie, che possono facilmente essere compromessi soprattutto con l'ingresso di nuovi *stakeholders,* causando il disallineamento degli obiettivi da raggiungere. L'ENISA suggerisce alcuni meccanismi per salvaguardare il rapporto fiduciario, tra cui la promozione di incontri regolari, la partecipazione di entrambe le parti ad eventi tematici per poter scambiare le rispettive idee, eventi sociali e la promozione dello scambio di informazioni circa gli incidenti informatici[78];
- **divergenze circa la tutela della *privacy*:** una preoccupazione ricorrente è la protezione dei dati, un tema affrontato molto seriamente in Europa e che viene coinvolto quando si parla di condivisione delle informazioni. I privati sono storicamente restii a scambiare informazioni per evitare il rischio di incorrere in azioni legali e tutelare la propria reputazione, inoltre devono modulare l'azione anche in base alla sensibilità dei propri clienti circa il diritto alla *privacy*, in alcuni Paesi più sentito che in altri, mentre per gli Stati un impedimento alla

[78] The European Union Agency for Network and Information Security (ENISA), "*Public Private Partnerships (PPP) Cooperative models",* Novembre 2017, p. 32, disponibile *online.*

condivisione è spesso dato dalla sicurezza nazionale e dalla volontà di non divulgare informazioni riservate per non comprometterla[79].

Avendo chiarito quali sono i vantaggi di un PPP e gli ostacoli che si frappongono alla sua efficace realizzazione, possiamo elencare i fattori che un partenariato di successo dovrebbe avere:

- **chiarezza nell'obiettivo e nelle norme da seguire:** è molto importante per la riuscita di una *partnership* che le parti siano chiare sin dall'inizio circa gli obiettivi che entrambe si aspettano di realizzare, che solitamente divergono e richiedono una mediazione. Idealmente, l'obiettivo di fondo dovrebbe tendere alla protezione del *cyberspace* e dunque il partenariato dovrebbe affrontare tutte le questioni per la realizzazione della sicurezza informatica, sviluppare capacità di prevenzione, risposta e ripristino contro gli attacchi informatici. Oggi la maggior parte dei partenariati si sostanzia nella condivisione di informazioni e nel coordinamento della risposta agli incidenti, ma sarebbe utile allargare la portata di queste collaborazioni e ricomprendere obiettivi di più ampia portata, sia in termini di ricerca e sviluppo di strumenti tecnologici per affrontare le minacce, sia nella preparazione del personale in questo settore, che da sempre è un profondo *gap* da colmare. Inoltre, è importante che ci sia una base giuridica comunemente accettata dalle parti (un atto giuridico o un *memorandum* d'intesa) perché il partenariato abbia successo, in modo che tutti i partecipanti conoscano esattamente il quadro giuridico in cui si muovono;
- **scelta dei partecipanti:** la scelta dei partner è sicuramente un punto fondamentale per la realizzazione degli obiettivi dichiarati. Circa i rappresentanti della sfera pubblica, questi dovrebbero partecipare attivamente e conferire un apporto significativo in termini di conoscenze e risorse; dovrebbero essere coinvolti i rappresentanti di qualsiasi livello, dalle amministrazioni locali ai livelli più alti, perché la *cybersecurity* coinvolge tutti gli strati dell'amministrazione[80]. Dal lato privato, sarebbe vantaggioso coinvolgere anche le piccole e medie imprese (PMI) e le *start-up* che spesso non hanno i fondi sufficienti per partecipare a questo tipo di collaborazioni, ma nell'ottica di aumentare il livello di protezione generale delle infrastrutture critiche digitali, sarebbe proficuo interessare anche gli attori più piccoli del *cyberspace*, che possono apportare un contributo importante e contemporaneamente acquisire buone pratiche da chi possiede e gestisce infrastrutture digitali ritenute *asset* nazionali strategici. La sfera privata dovrebbe comprendere anche *stakeholders* provenienti dal mondo accademico e coloro che si occupano di innovazione e ricerca in questo settore.

Conclusioni e raccomandazioni

Alla luce di quanto esposto finora, il partenariato pubblico-privato rimane uno strumento efficace per perseguire gli obiettivi nazionali ed internazionali di protezione dello spazio cibernetico

[79] United Nations Interregional Crime and Justice Research Institute, "*Information Sharing and Public-Private Partnerships: Perspectives and Proposals*", reperibile *online.*

[80] R. N. Thomas, *Securing Cyberspace through public-private partnership. A comparative Analysis of partnership models*, in *Center for Strategic & International Studies* (CSIS), 19 Agosto 2013, reperibile *online.*

attraverso una solida *cybersecurity.*
La proliferazione e l'evoluzione delle minacce richiedono necessariamente un'azione sinergica per mitigare i rischi e gestire le conseguenze che un incidente informatico può innescare, ed è la natura stessa di questo dominio a richiedere un approccio multi-stakeholders.
Abbiamo ripercorso il processo che ha portato alla consacrazione del settore privato come attore che gioca un ruolo determinante nella protezione dalle minacce cibernetiche, con il riconoscimento, prima, nel 2009 con la Risoluzione del Consiglio in cui si riconosce la **responsabilità condivisa della sicurezza delle reti e dell'informazione tra tutte le parti interessate**[81], e poi, nel 2013, con la prima Cyber Strategy dell'Unione europea[82], registrando i fallimenti e i successi nello sforzo di creare meccanismi di collaborazione tra le parti.
Considerati i ritmi vertiginosi con cui aumentano le minacce, sarebbe auspicabile la profusione di maggiori energie nella costruzione di *partnership* tra il settore pubblico e quello privato, e rafforzare la risposta tempestiva ed efficace agli incidenti informatici. Tuttavia, bisognerebbe lavorare meglio nella creazione di tali collaborazioni, poiché il loro successo dipende in gran parte dal progetto iniziale, dalle risorse allocate, dalla scelta di partner adeguati, da una condivisione simmetrica di responsabilità e dalla chiarezza degli obiettivi da raggiungere.

Nonostante la maggior parte dei PPP sinora realizzati si siano concentrati sull'*information sharing* delle minacce, molti esperti concordano sul fatto che gli obiettivi da perseguire siano di più ampio spettro, così come sarebbe opportuno allargare la soglia d'ingresso per ricomprendere non solo le grandi realtà industriali che gestiscono le infrastrutture critiche digitali considerate *asset* strategici, ma anche le piccole e medie imprese, le *start-up*, i ricercatori e gli accademici coinvolti in questo settore.
Ovviamente, questo non significa che la condivisione delle informazioni non sia essenziale, anzi andrebbe incoraggiata tenendo a mente però che è una strada a doppio senso, come suggerisce David Rockvam in un suo articolo, e in quanto tale dovrebbe esserci una reciproca condivisione e non uno scambio unidirezionale in cui a beneficiarne sia solo una parte. Proprio nel contesto delle iniziative di *information sharing,* un ruolo importante nella costruzione della resilienza e nella risposta agli attacchi, a vantaggio anche del settore privato, è ricoperto dai CSIRT nazionali che facilitano lo scambio di informazioni. La necessità di una maggiore regolamentazione di questo aspetto viene sottolineata anche nella già citata Strategia europea di sicurezza 2020-2025, che individua come obiettivo importante quello di "*elaborare norme comuni obbligatorie e rigorose per lo scambio sicuro di informazioni e la sicurezza delle infrastrutture e dei sistemi digitali in tutte le istituzioni, gli organismi e le agenzie dell'UE*"[83].
Le conseguenze di un attacco informatico potrebbero avere un impatto sia sull'economia che sull'ordine sociale, per questo motivo l'azione di prevenzione e gestione dei rischi provenienti dal *cyberspace* richiedono uno sforzo congiunto sia dei governi che del settore privato e, data l'estrema interdipendenza delle reti e dei sistemi, l'intera materia dovrebbe essere gestita a livello sovranazionale.
Ciò che emerge da quanto detto sinora è che coloro che sono chiamati a garantire la sicurezza della

[81] Risoluzione del Consiglio, 2009/C 321/01, sez. 3, par. 2.
[82] "*Poiché la vasta maggioranza delle reti e dei sistemi informativi sono di proprietà privata e sono operati da privati, è essenziale coinvolgere maggiormente il settore privato nel rafforzamento della cibersicurezza. Il settore privato dovrebbe elaborare, a livello tecnico, capacità proprie di ciberresilienza e scambiare buone pratiche a livello intersettoriale. Anche il settore pubblico dovrebbe beneficiare degli strumenti messi a punto dall'industria per rispondere agli incidenti, individuare le cause e condurre indagini di polizia scientifica*". JOIN(2013) 1 final, p. 6.
[83] COM(2020) 605 final, p. 10.

nostra società devono affrontare sfide difficili, perché **una società democratica è per definizione aperta ed accessibile e per questo vulnerabile.**

Per la riuscita di qualsiasi strategia atta a migliorare le capacità di prevenzione, protezione, mitigazione, risposta e ripristino dagli attacchi, **è richiesto un elevato livello di collaborazione tra il settore pubblico e quello privato,** un flusso continuo di informazioni, investimenti in tecnologie avanzate per combattere le minacce, la predisposizione di protocolli adeguati per la mitigazione dei rischi e l'utilizzo di modelli di gestione del rischio efficaci, poiché solo attraverso le capacità combinate dei governi e dei privati possiamo proteggere le nostre società e i valori democratici su cui si esse fondano.