CORTE DEI CONTI EUROPEA

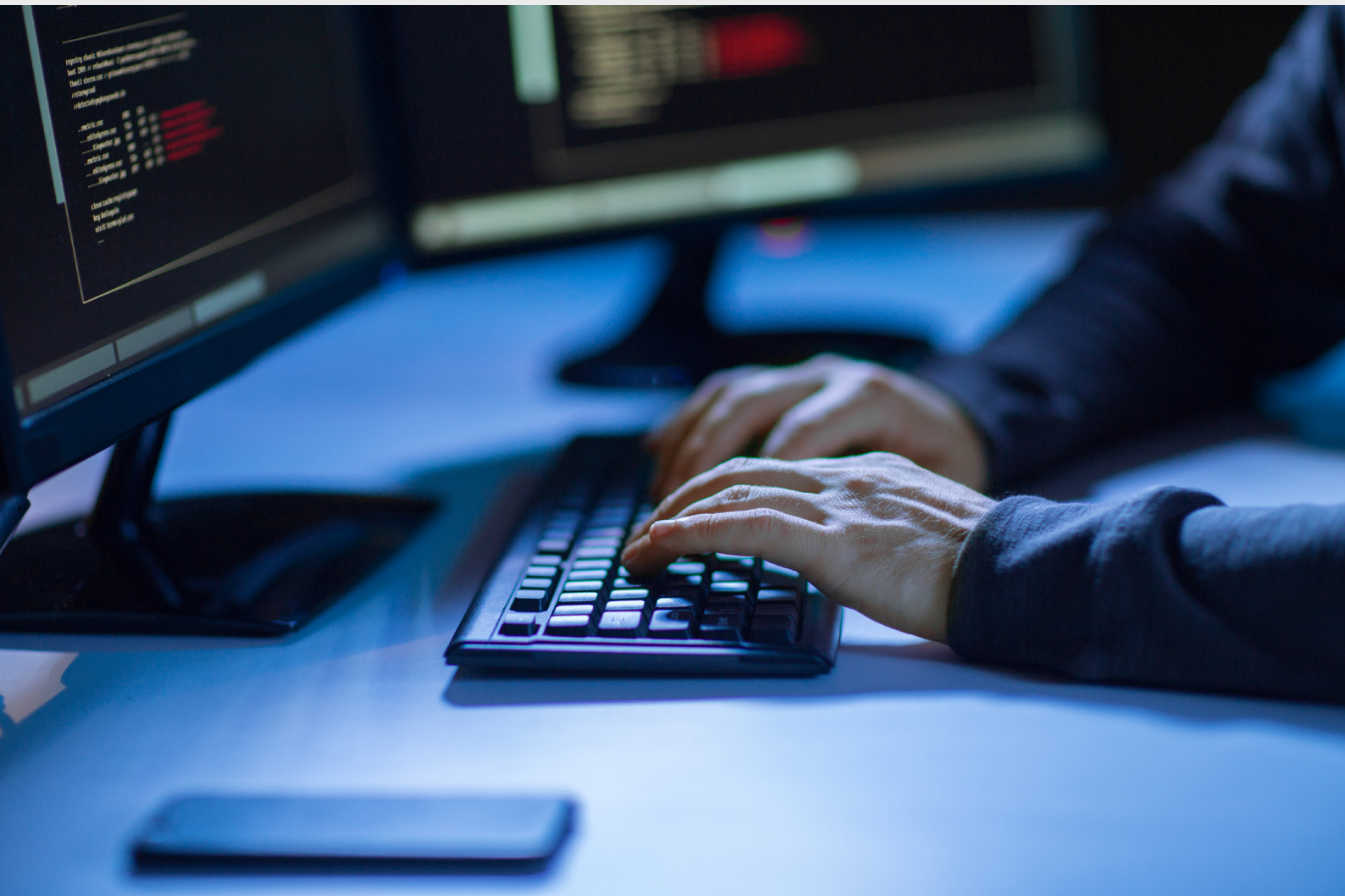
IT

2019

Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza

Documento di riflessione

Marzo 2019



Contenuto del documento

Il presente documento di riflessione, che non costituisce una relazione di audit, intende offrire una panoramica dell'articolata politica dell'UE in materia di cibersicurezza e individuare le principali sfide per una sua efficace realizzazione. Affronta i temi della sicurezza delle reti e dell'informazione, della criminalità informatica, della ciberdifesa e della disinformazione. Sarà inoltre preso in considerazione in qualsiasi attività di audit espletata in questo ambito.

L'analisi della Corte si basa su un esame documentale di informazioni pubblicamente disponibili in documenti ufficiali, documenti di sintesi e studi di terzi. L'attività sul campo è stata svolta tra aprile e settembre 2018 e si tiene conto degli sviluppi fino al dicembre 2018. Tale lavoro è stato integrato da un'indagine presso le istituzioni superiori di controllo degli Stati membri e da colloqui intrattenuti con importanti portatori di interesse delle istituzioni dell'UE e con rappresentanti del settore privato.

Le sfide individuate dagli auditor della Corte sono raggruppate in quattro grandi categorie: i) il quadro strategico; ii) il finanziamento e la spesa; iii) lo sviluppo della ciberresilienza; iv) una risposta efficace agli incidenti informatici. Resta imperativo conseguire un livello superiore di cibersicurezza nell'UE. Pertanto, alla fine di ogni capitolo si espongono varie idee come materia di ulteriore riflessione da parte dei responsabili delle politiche, dei legislatori e degli operatori del settore.

La Corte desidera esprimere la propria riconoscenza per le risposte costruttive ricevute dai servizi della Commissione, dal Servizio europeo per l'azione esterna, dal Consiglio dell'Unione europea, dall'ENISA, dall'Europol, dall'Organizzazione europea per la cibersicurezza e dalle istituzioni superiori di controllo degli Stati membri.

Indice

Sintesi

I Grazie alla tecnologia, che fa di prodotti e servizi inediti una parte integrante della nostra vita quotidiana, si sta spalancando un intero universo di nuove opportunità. Al contempo, cresce il rischio di essere vittima della criminalità o di un attacco informatici, il cui impatto socioeconomico continua a espandersi. Si concretizza quindi in un momento critico il recente impulso che l'UE ha impresso dal 2017 per accelerare gli sforzi volti a rafforzare la cibersicurezza e l'autonomia digitale.

II Il presente documento di riflessione, che non costituisce una relazione di audit e si fonda su informazioni di dominio pubblico, intende passare in rassegna una politica complessa e composita, nonché individuare le principali sfide per una sua efficace realizzazione. Esso verte sulla politica dell'UE in materia di cibersicurezza, sulla criminalità informatica e sulla ciberdifesa e illustra anche gli sforzi per combattere la disinformazione. Le sfide individuate dagli auditor della Corte sono raggruppate in quattro grandi categorie: i) il quadro normativo e strategico; ii) il finanziamento e la spesa; iii) lo sviluppo della ciberresilienza; iv) una risposta efficace agli incidenti informatici. Ciascun capitolo comprende alcuni spunti di riflessione sulle sfide presentate.

Il quadro normativo e strategico

III In assenza di obiettivi misurabili e di sufficienti dati attendibili, non è facile sviluppare un'azione in linea con le ampie finalità della strategia dell'UE in materia di cibersicurezza: divenire l'ambiente digitale più sicuro al mondo. Gli effetti sono misurati di rado e pochi settori d'intervento sono stati valutati. Una sfida importante risiede quindi nell'**assicurare un obbligo di rendiconto e una valutazione pregnanti**, muovendo verso una cultura della performance che includa pratiche di valutazione.

IV Il quadro normativo resta incompleto. **Le lacune nel diritto dell'UE, unitamente a una sua trasposizione disomogenea**, possono far sì che la normativa non esplichi appieno le sue potenzialità.

Il finanziamento e la spesa

V È difficoltoso **equiparare i livelli degli investimenti alle finalità perseguite**: ciò implica non solo incrementare gli investimenti globali nella cibersicurezza (finora modesti e frammentati nell'UE), bensì anche accrescerne l'impatto, soprattutto mettendo più a frutto i risultati della spesa per la ricerca, nonché indirizzando e finanziando in maniera efficace le *start-up*.

VI Per sapere quali lacune colmare per conseguire le finalità perseguite è essenziale che l'UE e gli Stati membri **abbiano una chiara visione d'insieme della spesa UE**. Poiché non sussiste un'apposita dotazione UE per finanziare la strategia in materia di cibersicurezza, manca un chiaro quadro degli importi investiti e della loro destinazione.

VII In un'epoca in cui le priorità politiche sono sempre più dettate da motivi di sicurezza, la **scarsa adeguatezza delle risorse assegnate alle agenzie dell'UE operanti nel settore della cibersicurezza** può precludere la realizzazione delle ambizioni dell'UE. Nell'affrontare questa sfida occorre trovare modalità per attrarre e trattenere i talenti.

Lo sviluppo della ciberresilienza

VIII Le debolezze nella governance della cibersicurezza abbondano nei settori pubblico e privato dell'intera UE e anche a livello internazionale. Ciò compromette la capacità della comunità mondiale di rispondere agli attacchi informatici e di contenerli, nonché inficia un approccio coerente sul piano UE. La sfida risiede quindi nel **rafforzare la governance della cibersicurezza**.

IX È fondamentale **accrescere le competenze e condurre un'opera di sensibilizzazione** in tutti i settori e i livelli della società, data la crescente carenza generale di competenze in materia di cibersicurezza. Le norme a livello dell'UE per la formazione, la certificazione o le valutazioni dei rischi informatici sono attualmente limitate.

X Per rafforzare la ciberresilienza globale è fondamentale un fondamento di fiducia. La Commissione stessa ha valutato che il coordinamento in genere è tuttora carente. Rimane difficile **migliorare lo scambio di informazioni e il coordinamento** tra i settori pubblico e privato.

Una risposta efficace agli incidenti informatici

XI I sistemi digitali sono divenuti così complessi che è impossibile impedire tutti gli attacchi. Per rispondere a questa sfida occorre **una rapida azione di rilevazione e risposta**. La cibersicurezza, tuttavia, non è ancora pienamente integrata nei meccanismi esistenti di coordinamento della risposta alle crisi a livello di UE, il che ne limita potenzialmente la capacità di reagire a incidenti informatici transfrontalieri su vasta scala.

XII La **protezione delle infrastrutture critiche e delle funzioni di rilevanza sociale** è fondamentale. Le potenziali interferenze nelle procedure elettorali e le campagne di disinformazione rappresentano una sfida cruciale.

XIII Le attuali sfide poste dalle minacce informatiche cui sono confrontati l'UE e il più ampio contesto mondiale necessitano di un impegno indefesso e di un'adesione piena e costante ai valori fondanti dell'UE.

Introduzione

01 Grazie alla tecnologia si sta spalancando un intero universo di nuove opportunità. Come prendono piede, prodotti e servizi inediti diventano parte integrante della nostra vita quotidiana. Tuttavia, con ogni nuovo sviluppo cresce la nostra dipendenza tecnologica e altrettanto accade anche all'importanza della cibersicurezza. Quanti più dati personali mettiamo online e quanto più siamo connessi, tanto più probabile è essere vittima di una qualche forma di criminalità o di attacco informatici.

Che cos'è la cibersicurezza?

02 Non esiste una definizione convenzionale, universalmente accettata, di "cibersicurezza"[1]. In termini ampi, essa designa il complesso di tutele e misure adottate per difendere i sistemi informativi e i relativi utenti da accessi non autorizzati, attacchi e danni al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati.

03 Nella cibersicurezza rientrano la prevenzione e l'individuazione degli incidenti informatici, la risposta agli stessi e il successivo recupero. Gli incidenti possono essere intenzionali o meno e vanno, ad esempio, dalla divulgazione accidentale di informazioni agli attacchi a imprese e infrastrutture critiche, dal furto di dati personali fino addirittura all'interferenza nei processi democratici. Tutte queste occorrenze hanno effetti dannosi di ampia portata su persone fisiche, organizzazioni e comunità.

04 Nel gergo delle politiche dell'UE, il termine "cibersicurezza" non è riferito esclusivamente alla sicurezza delle reti e dei sistemi informativi, bensì designa qualsiasi attività illecita che comporti l'impiego di tecnologie digitali nel ciberspazio. Può comprendere quindi reati informatici quali gli attacchi con virus informatici e le frodi perpetrate con mezzi di pagamento diversi dai contanti, travalicando la separazione fra sistemi e contenuti, come nel caso della diffusione online di materiale pedopornografico. Può anche riguardare campagne di disinformazione volte a influenzare il dibattito online e produrre presunte interferenze nelle consultazioni elettorali. In aggiunta, Europol nota una convergenza tra criminalità informatica e terrorismo[2].

05 Vari attori, fra cui Stati, gruppi criminali e "hacktivisti", fomentano gli incidenti informatici, spinti da ragioni diverse. Tali incidenti hanno ricadute a livello nazionale, europeo e addirittura mondiale. Spesso, però, è difficile risalire all'autore dell'attacco a causa del carattere immateriale di Internet, che perlopiù non conosce frontiere,

nonché degli strumenti e delle tattiche utilizzate (il cosiddetto “problema dell’attribuzione”).

06 I numerosi tipi di minacce per la cibersicurezza possono essere classificati in base a cosa succede ai dati (divulgazione, modifica, distruzione o accesso negato) oppure ai princìpi fondamentali di sicurezza delle informazioni che vengono violati, come illustra la seguente ***figura 1***. Nel ***riquadro 1*** sono descritti alcuni esempi di attacchi. Poiché gli attacchi ai sistemi informativi sono sempre più sofisticati, i nostri meccanismi di difesa perdono efficacia[3].

Figura 1 – Tipi di minacce e princìpi di sicurezza a rischio

Fonte: rielaborazione della Corte dei conti europea da uno studio del Parlamento europeo[4]. Lucchetto = nessun impatto per la sicurezza; punto esclamativo = sicurezza a rischio

Riquadro 1

Tipi di attacchi informatici

Ogni volta che un nuovo dispositivo si connette online o si collega ad altri dispositivi, aumenta la cosiddetta “superficie d’attacco” della cibersicurezza. La crescita esponenziale dell’Internet degli oggetti, del *cloud*, dei *big data* e della digitalizzazione dell’industria è accompagnata da un aumento dell’esposizione delle vulnerabilità, che consente ai malintenzionati di mirare a un numero sempre maggiore di vittime. È davvero difficile stare al passo con tipi di attacco così vari e sempre più sofisticati[5].

Un ***malware*** (software nocivo) è concepito per danneggiare dispositivi o reti. Può comprendere virus, *trojan*, *ransomware*, *worm*, *adware* e *spyware*. Un ***ransomware*** crittografa i dati, impedendo agli utenti di accedere ai propri *file* finché non è pagato un riscatto, generalmente in una criptovaluta, o viene eseguita un'azione. Secondo Europol, gli attacchi con *ransomware* dominano la scena e il numero di tipi diversi di *ransomware* è esploso negli anni recenti. Stanno aumentando anche gli attacchi **distribuiti di negazione del servizio** (*Distributed Denial of Service*, DDoS), che mettono fuori uso servizi o risorse inondandoli con più richieste di quante siano in grado di gestire; nel 2017 è stato confrontato a questo tipo di attacco un terzo delle organizzazioni[6].

Gli utenti possono essere indotti a eseguire inconsciamente un'azione o a divulgare informazioni riservate. Questo stratagemma, noto come **ingegneria sociale**, può essere usato per il furto di dati o lo spionaggio informatico. Vi sono diversi modi per raggiungere tale scopo, ma un metodo diffuso è il ***phishing***, in cui e-mail che sembrano provenire da fonti fidate inducono con l'inganno gli utenti a rivelare informazioni o a cliccare su collegamenti destinati a infettare i dispositivi scaricando *malware*. Oltre metà degli Stati membri ha segnalato indagini su attacchi in rete[7].

Forse i tipi di minacce più nefasti sono costituiti dalle **minacce persistenti avanzate** (*advanced persistent threats*, APT). Si tratta di attacchi sofisticati volti a monitorare nel lungo termine e rubare dati, che talvolta celano anche finalità distruttive. Lo scopo in questo caso è di passare inosservati quanto più a lungo possibile. Le APT sono spesso collegate ad attività di Stato e mirate a settori particolarmente sensibili quali tecnologia, difesa e infrastrutture critiche. Si ritiene che lo spionaggio informatico rappresenti almeno un quarto della totalità degli incidenti informatici e che comporti i costi più elevati[8].

Quanto grave è il problema?

07 Non è facile cogliere l'impatto di una insufficiente preparazione a un attacco informatico, poiché mancano dati attendibili. L'impatto economico della criminalità informatica si è quintuplicato tra il 2013 e il 2017[9], colpendo amministrazioni pubbliche e imprese, grandi e piccole indifferentemente. A fronte di questa tendenza, si prevede un aumento dei premi di assicurazione informatica dai 3 miliardi di euro del 2018 a 8,9 miliardi di euro nel 2020.

08 Sebbene l'impatto finanziario degli attacchi informatici continui ad aumentare, vi è una preoccupante disparità tra il costo di lanciare un attacco e i costi di prevenzione, indagine e riparazione. Ad esempio per perpetrare un attacco DDoS può bastare una spesa di 15 euro al mese, mentre le perdite subite dall'impresa colpita, anche per il danno reputazionale, sono nettamente superiori[10].

09 Benché l'80 % delle imprese dell'UE abbia subito almeno un incidente di cibersicurezza nel 2016[11], i rischi al riguardo sono ancora ignorati in maniera allarmante. Tra le imprese nell'UE, il 69 % ha una comprensione nulla o solo basilare della propria esposizione alle minacce informatiche[12] e il 60 % non ha mai stimato le potenziali perdite finanziarie[13]. Inoltre, stando a un sondaggio mondiale, un terzo delle organizzazioni preferirebbe pagare il riscatto chiesto dagli *hacker* che investire nella sicurezza delle informazioni[14].

10 Nel 2017 gli attacchi perpetrati a livello mondiale con il *ransomware* "Wannacry" e il *wiper* "NotPetya" hanno colpito nel loro complesso oltre 320 000 soggetti in circa 150 paesi[15]. Questi incidenti hanno provocato una sorta di presa di coscienza della minaccia posta dagli attacchi informatici, che ha impresso un nuovo impulso all'integrazione della cibersicurezza nella riflessione globale sulle politiche. Inoltre, l'86 % dei cittadini UE ritiene ora in aumento il rischio di essere vittima di un reato informatico[16].

L'azione dell'UE in materia di cibersicurezza

11 L'UE è divenuta una organizzazione con status di osservatore nella convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 2001[17] (la convenzione di Budapest). Da allora, l'UE si è avvalsa di politiche, normative e risorse finanziarie per accrescere la propria ciberresilienza. A fronte di un numero crescente di gravi attacchi e incidenti informatici, dal 2013 l'attività al riguardo si è intensificata, come illustra la ***figura 2***. Parallelamente, gli Stati membri hanno adottato (e in alcuni casi già aggiornato) le prime strategie nazionali per la cibersicurezza.

12 I principali attori dell'UE competenti per la cibersicurezza sono descritti nel ***riquadro 2*** e nell'***allegato I***.

Riquadro 2

Chi partecipa?

La **Commissione europea** si prefigge di sviluppare le capacità e la cooperazione in materia di cibersicurezza, di rafforzare il ruolo dell'UE quale attore della cibersicurezza e di integrare questo aspetto nelle altre politiche dell'UE. Le principali direzioni generali (DG) preposte alla politica in materia di cibersicurezza sono le DG **CNECT** (cibersicurezza) e **HOME** (criminalità informatica), competenti rispettivamente per il mercato unico digitale e l'Unione della sicurezza. La DG **DIGIT** è tenuta ad assicurare la sicurezza informatica dei sistemi della Commissione stessa.

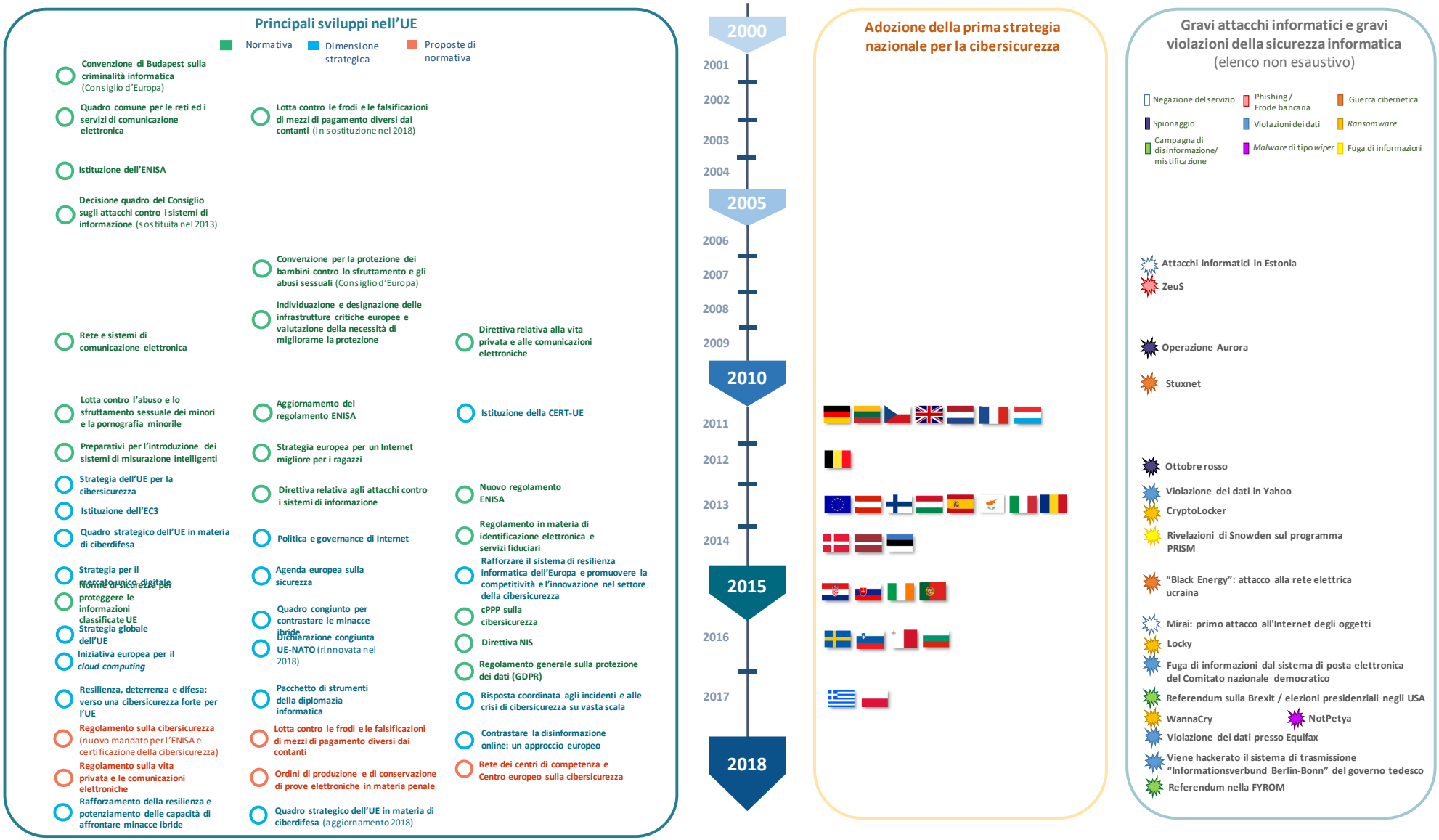
La Commissione è coadiuvata da varie agenzie UE, in particolare l'**ENISA** (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione), ossia l'agenzia dell'UE per la cibersicurezza, che costituisce principalmente un organismo consultivo destinato a contribuire allo sviluppo strategico, alla creazione delle capacità e alla sensibilizzazione. Il Centro europeo per la lotta alla criminalità informatica (**EC3**) presso Europol è stato istituito per rafforzare l'azione di contrasto dell'UE alla criminalità informatica. La Commissione ospita una squadra di pronto intervento informatico (**CERT-UE**) che assiste tutte le istituzioni, gli organismi e le agenzie dell'Unione.

Il **Servizio europeo per l'azione esterna** (SEAE) è a capo della ciberdifesa, della ciberdiplomazia e della comunicazione strategica, nonché ospita centri di analisi e *intelligence*. L'**Agenzia europea per la difesa** (AED) è preposta allo sviluppo delle capacità di ciberdifesa.

Gli **Stati membri** sono in primo luogo responsabili della propria cibersicurezza e agiscono, a livello di UE, tramite il **Consiglio**, che dispone di numerosi organi di coordinamento e di condivisione delle informazioni (fra cui il Gruppo orizzontale "Questioni riguardanti il ciberspazio"). Il **Parlamento europeo** interviene come colegislatore.

Le **organizzazioni del settore privato**, tra cui gli operatori del settore, gli organismi di governance di Internet e gli ambienti accademici, partecipano e contribuiscono allo sviluppo e all'attuazione delle politiche, anche attraverso un **partenariato pubblico-privato contrattuale** (cPPP).

Figura 2 – Accelerazione nello sviluppo delle politiche e nella normativa (al 31 dicembre 2018)



Fonte: Corte dei conti europea.

Dimensione strategica

13 L'ecosistema cibernetico dell'UE è complesso e stratificato, interessa trasversalmente vari ambiti di politica interna, come la giustizia e gli affari interni, il mercato unico digitale e le politiche in materia di ricerca. In politica estera, la cibersicurezza svolge un ruolo di primo piano nella diplomazia ed è sempre più parte dell'emergente politica di difesa dell'UE.

14 L'approccio strategico dell'UE ruota attorno alla **strategia per la cibersicurezza del 2013**[18]. Questa intende rendere l'ambiente digitale dell'UE il più sicuro al mondo, difendendo al contempo i valori e le libertà fondamentali. Si pone cinque obiettivi principali: i) accrescere la ciberresilienza; ii) ridurre la criminalità informatica; iii) sviluppare politiche e capacità di ciberdifesa; iv) sviluppare le risorse industriali e tecnologiche per la cibersicurezza; v) creare una politica internazionale relativa al ciberspazio che sia in linea con i valori fondanti dell'UE.

15 La strategia per la cibersicurezza è in correlazione con tre strategie adottate successivamente:

— l'**Agenda europea sulla sicurezza** (2015) si pone l'obiettivo di migliorare l'azione di contrasto e la risposta giudiziaria alla criminalità informatica, principalmente rinnovando e/o aggiornando le politiche e la normativa esistenti[19]. Espone anche misure per individuare gli ostacoli alle indagini penali riguardanti la criminalità informatica e per rafforzare lo sviluppo delle competenze nel settore della cibersicurezza;

— La **strategia per il mercato unico digitale**[20] (2015) intende migliorare l'accesso ai beni e ai servizi digitali creando un contesto favorevole in cui si esplichi appieno il potenziale di crescita dell'economia digitale. A tal fine, è essenziale rafforzare la sicurezza online, la fiducia e l'inclusione;

— La **strategia globale**[21] del 2016 si propone di rafforzare il ruolo dell'UE nel mondo. La cibersicurezza costituisce un pilastro centrale tramite un rinnovato impegno nelle questioni riguardanti il ciberspazio, la cooperazione con i partner chiave e la determinazione a fronteggiare le questioni suddette in tutti i settori di intervento, anche contrastando la disinformazione mediante una comunicazione strategica.

16 Negli anni recenti, in un contesto di crescente militarizzazione[22] e strumentalizzazione offensiva[23] del ciberspazio, si è giunti a considerarlo la quinta zona di confronto bellico[24]. La ciberdifesa protegge i sistemi, le reti e le infrastrutture

critiche del ciberspazio dagli attacchi militari e di altro tipo. Nel 2014 è stato adottato un **quadro strategico UE in materia di ciberdifesa**, aggiornato poi nel 2018[25]. In quest'ultimo aggiornamento sono individuate sei priorità, fra cui lo sviluppo delle capacità di ciberdifesa, nonché la protezione delle reti di comunicazione e informazione della politica di sicurezza e di difesa comune (PSDC) dell'UE. La ciberdifesa è anche parte del quadro di cooperazione strutturata permanente (PESCO) e della cooperazione UE-NATO.

17 Il **quadro congiunto per contrastare le minacce ibride** (2016), applicato nell'UE, affronta le minacce informatiche sia per le infrastrutture critiche che per gli utenti privati, evidenziando il fatto che gli attacchi informatici possono essere condotti mediante campagne di disinformazione sui *social media*[26]. Vi si rileva inoltre la necessità di una sensibilizzazione e di un rafforzamento della cooperazione tra UE e NATO, che ha trovato riscontro nelle dichiarazioni congiunte UE-NATO del 2016 e del 2018[27].

18 Nel 2017 la Commissione ha presentato un nuovo pacchetto sulla cibersicurezza, a dimostrazione della crescente urgenza di protezione digitale. Ne faceva parte una nuova comunicazione della Commissione che aggiornava la strategia del 2013 per la cibersicurezza[28], un programma per una risposta rapida e coordinata a un grave attacco e una comunicazione finalizzata a una celere attuazione della direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)[29]. Il pacchetto comprendeva inoltre una serie di proposte legislative (cfr. paragrafo ***22***).

Normativa

19 A partire dal 2002 sono stati adottati atti legislativi afferenti che presentavano gradi diversi di attinenza con la cibersicurezza.

20 Quale cardine della strategia del 2013 per la cibersicurezza, la componente giuridica portante è la **direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)**[30] del 2016, il primo atto giuridico a livello UE sulla cibersicurezza. La direttiva, che doveva essere recepita entro maggio 2018, intende conseguire un livello minimo di capacità armonizzate, imponendo agli Stati membri di adottare strategie NIS nazionali nonché di creare punti di contatto unici e gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)[31]. Stabilisce inoltre obblighi di sicurezza e di notifica per gli operatori di servizi essenziali in settori critici e per i fornitori di servizi digitali.

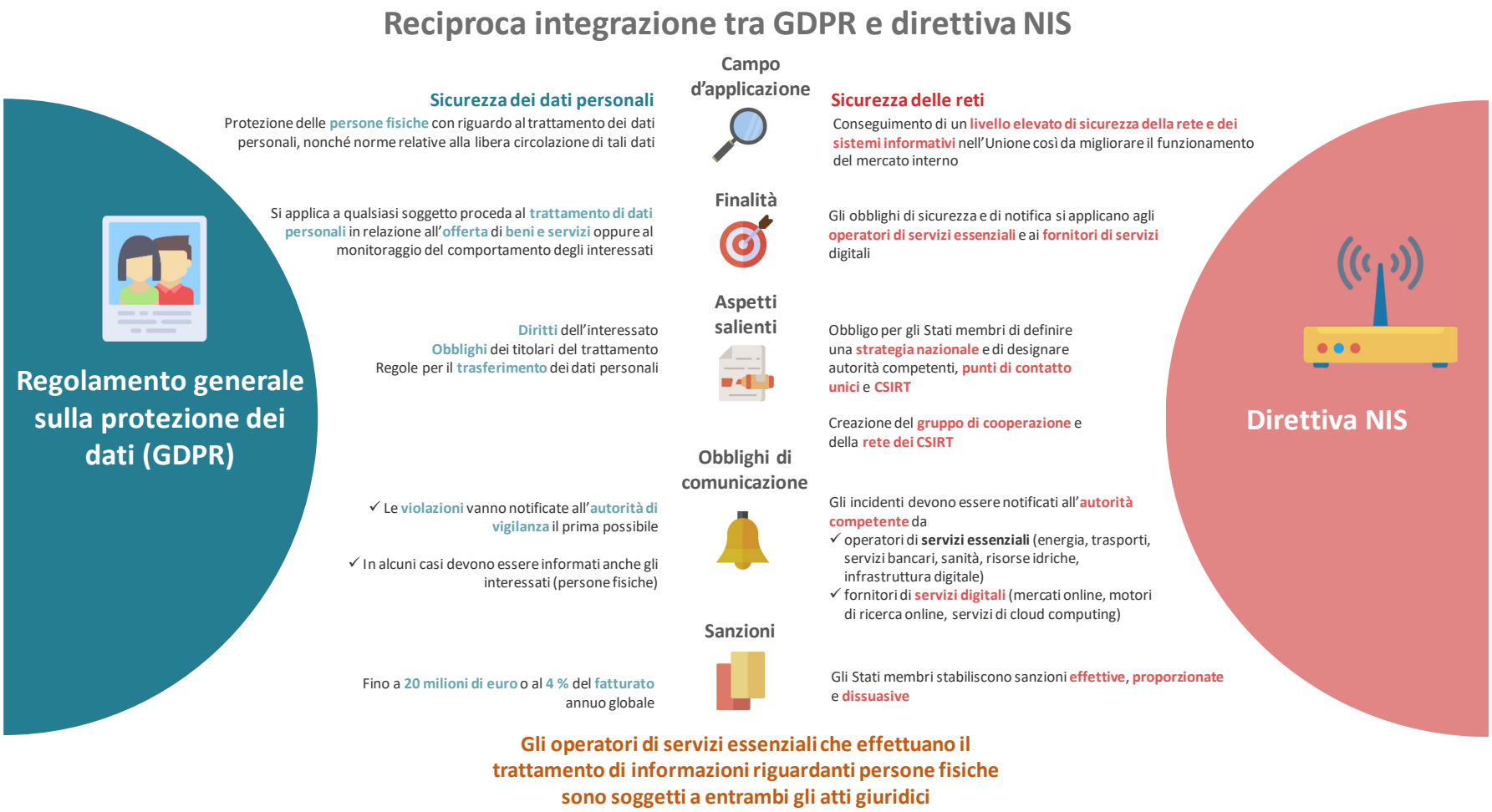
21 Parallelamente, dal maggio 2018 è applicato il **regolamento generale sulla protezione dei dati**[32] (GDPR), che era entrato in vigore nel 2016. Il suo obiettivo è proteggere i dati personali dei cittadini europei fissando regole per il trattamento e la divulgazione degli stessi. Esso riconosce alle persone interessate determinati diritti e impone obblighi ai titolari del trattamento dei dati (fornitori di servizi digitali) in merito all'utilizzo e al trasferimento delle informazioni. Dispone inoltre obblighi di notifica in caso di violazione e, in alcuni casi, commina eventuali sanzioni pecuniarie. La ***figura 3*** illustra come la direttiva NIS e il GDPR si completino a vicenda nel perseguire i rispettivi obiettivi di rafforzare la cibersicurezza e tutelare la protezione dei dati.

22 Nelle proposte legislative attualmente in discussione rientrano il regolamento sulla cibersicurezza per rafforzare l'ENISA e istituire un meccanismo di certificazione a livello UE[33], la proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche[34], nonché la proposta di direttiva in materia di prove elettroniche[35]. Fa parte del pacchetto del 2017 sulla cibersicurezza anche la proposta del 2018 riguardante il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento (di seguito denominata "rete dei centri di competenza sulla cibersicurezza e del Centro europeo di ricerca e di competenza")[36].

23 Può risultare difficile farsi un'idea della vastità del quadro strategico e legislativo afferente la cibersicurezza e del modo in cui incide sulla nostra vita quotidiana.

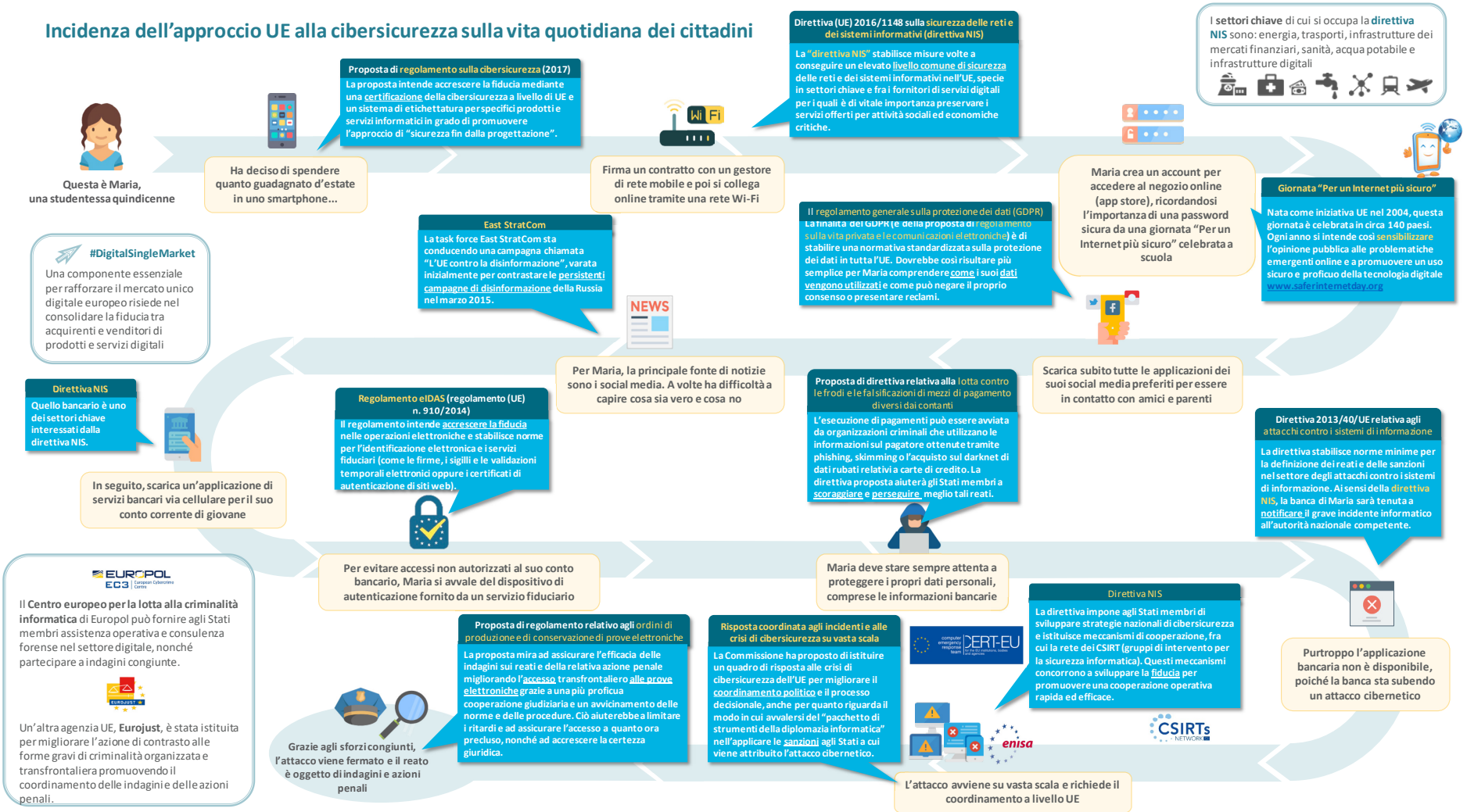
24 La ***figura 4*** intende tracciare l'interazione dei diversi atti legislativi e di altre attività con la vita di un fittizio cittadino europeo.

Figura 3 – Reciproca integrazione tra GDPR e direttiva NIS



Fonte: Corte dei conti europea.

Figura 4 – Incidenza dell'approccio UE alla cibersicurezza sulla vita quotidiana dei cittadini



Fonte: Corte dei conti europea.

Creare un quadro normativo e d'intervento

25 L'ecosistema cibernetico dell'UE è complesso e stratificato e coinvolge molti portatori d'interesse(cfr. ***allegato I***). Fare di tutte le sue disparate parti un complesso organico è una sfida non da poco. A partire dal 2013 si è agito di comune concerto per conferire una struttura coerente al settore della cibersicurezza dell'UE[37].

Sfida n. 1: una valutazione e una rendicontabilità che abbiano senso

26 Come ha rilevato la Commissione, è difficile stabilire un nesso causale tra la strategia del 2013 e gli eventuali cambiamenti occorsi. Gli obiettivi della strategia 2013 erano formulati in termini molto ampi ed esponevano più una visione che un valore-obiettivo misurabile[38]. In assenza di obiettivi misurabili, non è facile sviluppare un'azione in linea con tali ampie finalità. Il più recente quadro strategico in materia di ciberdifesa (2018) mirerà a sviluppare obiettivi che stabiliscono un livello minimo di cibersicurezza e fiducia da conseguire. Ciò però sarà limitato alla ciberdifesa; non sono stati fissati obiettivi che definiscano il livello di resilienza auspicato per l'intera UE.

27 Gli effetti sono misurati di rado e sono stati valutati pochi settori d'intervento[39]. Ciò è riconducibile in parte alla recente attuazione di molte misure (legislative o meno), che ostacola una piena valutazione del loro impatto. La sfida risiede nel definire criteri di valutazione pregnanti che possano aiutare a misurare l'impatto. Inoltre, una valutazione rigorosa non è ancora divenuta la norma per la cibersicurezza in generale. È necessario quindi passare ad una cultura della performance che includa pratiche di valutazione e una reportistica standardizzata. Il mandato attuale dell'ENISA non contempla la valutazione e il monitoraggio dello stato della cibersicurezza e del livello di preparazione dell'UE.

28 La definizione delle politiche sulla base di elementi probatori dipende dalla disponibilità di dati e statistiche sufficienti e attendibili che aiutino a monitorare e ad analizzare tendenze e bisogni. I dati attendibili sono scarsi a causa dell'assenza di un sistema di monitoraggio comune e obbligatorio. Gli indicatori spesso non sono prontamente disponibili e sono difficili da definire[40]. In alcuni ambiti, tuttavia, sono stati sviluppati parametri di misurazione specifici, come ad esempio per il ciclo programmatico dell'UE utilizzato per contrastare la criminalità organizzata e le forme gravi di criminalità.

29 Pochi Stati membri raccolgono con regolarità dati ufficiali su questioni connesse al ciberspazio, il che ostacola la comparabilità. L'UE ha fornito finora scarse indicazioni sull'esigenza di consolidare le statistiche a livello europeo[41]. Sono esigue anche le analisi indipendenti a livello di UE disponibili che coprano argomenti chiave quali[42]: l'economia della cibersicurezza, compresi gli aspetti comportamentali (disallineamento degli incentivi, asimmetrie dell'informazione); una comprensione dell'impatto dei cedimenti informatici e della criminalità informatica; macrostatistiche sulle tendenze nel ciberspazio e sfide previste; soluzioni ottimali per sventare le minacce.

30 In assenza di obiettivi specifici e data la scarsità di dati attendibili e indicatori ben definiti, la valutazione di quanto conseguito dalla strategia è stata finora di carattere qualitativo. Le relazioni sui progressi compiuti descrivono le attività svolte o le tappe intermedie raggiunte, senza una misurazione approfondita dei risultati. Non sono ancora stati stabiliti inoltre valori di partenza per la valutazione della resilienza dei sistemi. In aggiunta, data la mancanza di una definizione codificata di "criminalità informatica", è pressoché impossibile trovare indicatori europei pertinenti che aiutino il monitoraggio e la valutazione.

31 La sorveglianza indipendente sull'attuazione della politica in materia di cibersicurezza varia da uno Stato membro all'altro. Gli auditor della Corte hanno condotto un'indagine presso le istituzioni superiori di controllo nazionali sull'esperienza maturata nell'espletare audit in questo campo. Metà di tutte le istituzioni che hanno risposto[43] non aveva mai sottoposto ad audit questo settore. Nel caso di quelle che invece lo avevano fatto, gli audit vertevano principalmente su: governance delle informazioni; protezione delle infrastrutture critiche; scambio di informazioni e coordinamento tra le principali parti coinvolte; grado di preparazione agli incidenti, notifica degli stessi e risposta. Tra le tematiche meno trattate si annoverano le misure di sensibilizzazione e la carenza di competenze digitali. Le risultanze di questi audit o valutazioni non sono sempre rese pubbliche, per motivi di sicurezza nazionale. Nell'***allegato III*** figura un elenco delle relazioni di audit pubblicate dalle istituzioni superiori di controllo.

32 I principali ostacoli all'audit delle misure delle amministrazioni pubbliche in questo ambito erano ravvisati nelle limitate competenze in materia di ciberspazio (cfr. anche paragrafi ***82-90***) e nelle difficoltà a valutare i progressi compiuti in termini di cibersicurezza.

Sfida n. 2: colmare le lacune nel diritto dell'UE e sanarne il recepimento disomogeneo

33 Il ritmo con cui emergono nuove tecnologie e minacce è di gran lunga più serrato rispetto a quello con cui è definita e attuata la normativa UE. Le procedure dell'UE non sono state concepite in considerazione dell'era digitale: sviluppare procedure innovative e flessibili per assicurare un quadro strategico e giuridico che sia adatto allo scopo[44] è assolutamente prioritario[45] se si vuole prevedere e influenzare meglio il futuro.

34 Nonostante l'impulso verso una maggiore coerenza, il quadro normativo per la cibersicurezza rimane incompleto (cfr. ***tabella 1*** per alcuni esempi). Frammentazione e lacune ostacolano il conseguimento degli obiettivi strategici e danno luogo a inefficienze. Fra le lacune individuate dalla Commissione nella valutazione della strategia rientravano l'Internet degli oggetti, il bilanciamento delle responsabilità tra utenti e fornitori di prodotti digitali e certi aspetti non affrontati nella direttiva NIS. Il regolamento proposto sulla cibersicurezza cerca di porvi rimedio in parte, promuovendo la sicurezza fin dalla progettazione attraverso un sistema di certificazione a livello di UE. A giudizio di alcuni portatori d'interesse, si sente ancora forte la mancanza di una politica chiaramente definita per la ciberindustria e di un approccio comune allo spionaggio informatico[46].

Tabella 1 – Lacune e recepimento disomogeneo del quadro normativo (elenco non esaustivo)

Settore d'intervento	Esempi
Mercato unico digitale	o L'attuale direttiva sulla vendita dei beni di consumo non affronta il tema della cibersicurezza. Le direttive proposte sul contenuto digitale[47] e sulle vendite online[48] mirano a colmare detta lacuna. o Vi sono quadri normativi limitati e variegati per gli obblighi di diligenza negli Stati membri, il che genera incertezza giuridica e difficoltà a esperire i mezzi di ricorso[49]. o Le politiche in materia di divulgazione delle vulnerabilità dei *software* si stanno sviluppando a ritmi diversi da uno Stato membro all'altro, senza che vi sia un quadro giuridico globale a livello dell'UE tale da consentire un approccio coordinato[50].
Rafforzamento della sicurezza delle reti e dell'informazione	o Gli Stati membri hanno la facoltà di comprendere settori omessi nella direttiva NIS[51]. I settori della ricettività, che non sono considerati, possono fornire una porta d'ingresso ad altri reati, fra cui la tratta di essere umani, il traffico di droga e l'immigrazione irregolare[52].
Lotta alla criminalità informatica	o Molti Stati membri non hanno definito le prove elettroniche nella legislazione nazionale[53] (cfr. anche paragrafo ***22***). o La vigente decisione quadro contro le frodi perpetrate tramite mezzi di pagamento diversi dai contanti non include esplicitamente gli strumenti fisici dematerializzati, come le valute virtuali, la moneta elettronica e il denaro mobile (*mobile money*), né tratta azioni come il *phishing*, lo *skimming* e il possesso e la condivisione di informazioni sul pagatore[54]. o La direttiva relativa agli attacchi contro i sistemi di informazione non si occupa direttamente dell'acquisizione illegale dei dati dall'interno (ad esempio, nel caso di spionaggio informatico), rendendo difficile l'attività di contrasto[55]. o A seguito della sentenza della Corte di giustizia dell'Unione europea sulla conservazione dei dati[56], le differenze nell'applicazione del quadro normativo tra Stati membri hanno ostacolato le attività di contrasto, dando luogo potenzialmente alla perdita di indizi investigativi e compromettendo l'efficace azione giudiziaria contro l'attività criminale online[57].

Fonte: Corte dei conti europea.

35 L'applicazione di alcuni aspetti della normativa rimane su base volontaria, sia per le autorità nazionali che per gli operatori privati. Ad esempio, nel quadro del gruppo di cooperazione, la valutazione delle strategie nazionali sulla sicurezza delle reti e dei sistemi informativi nonché dell'efficacia dei CSIRT avviene su base volontaria. Inoltre, per quanto riguarda il sistema di certificazione proposto nel regolamento sulla cibersicurezza, l'applicazione della certificazione per i prodotti e i servizi TIC sarà volontaria.

36 Nell'UE, la cibersicurezza è prerogativa degli Stati membri. Ciò nonostante, all'UE spetta un ruolo cruciale nel creare le condizioni perché le capacità degli Stati membri migliorino e perché collaborino fra loro e infondano fiducia. Tuttavia, date le ampie differenze tra Stati membri in termini di capacità e impegno[58], le informazioni sensibili (inerenti alla sicurezza nazionale) saranno ancora fornite su base volontaria.

37 Il recepimento non omogeneo del diritto dell'UE da parte degli Stati membri può generare incoerenza sotto il profilo giuridico e operativo e impedisce alla normativa di esplicare tutte le sue potenzialità. Ad esempio, gli Stati membri interpretano in modo diverso il modo in cui effettuare i controlli sulle esportazioni di prodotti a duplice uso[59]: ne consegue che talune imprese con sede nell'UE potrebbero esportare tecnologie e servizi atti a essere usati per la sorveglianza informatica e la violazione dei diritti umani mediante censura o intercettazione. Il Parlamento europeo ha espresso preoccupazione a tale proposito[60].

38 Inoltre, la tutela della vita privata e della libertà di espressione invoca una risposta legislativa mirata che consenta di trovare il necessario equilibrio tra la salvaguardia dei valori fondamentali e l'assolvimento degli obblighi inderogabili in materia di sicurezza nell'UE. Ad esempio, come assicurare la cifratura da punto a punto e, al contempo, trovare il modo migliore per sostenere l'attività di contrasto? Oppure come conseguire le finalità del GDPR e, al contempo, comprenderne le implicazioni per le informazioni pubblicamente disponibili su chi registra nomi di dominio e su titolari di blocchi di indirizzi IP? E quali sono le potenziali ricadute negative sulle indagini delle autorità di contrasto[61]?

39 La normativa da sola non garantisce la resilienza. Sebbene l'obiettivo della direttiva NIS sia di conseguire un elevato livello di sicurezza in tutta l'UE, essa mira esplicitamente a conseguire un'armonizzazione minima[62], non massima. Via via che il panorama cibernetico evolve, continueranno ad emergere lacune.

Spunti di riflessione – Quadro strategico

- Quali passi essenziali sono necessari per sospingere tanto i responsabili delle politiche quanto i legislatori verso una più profonda cultura della performance nella cibersicurezza, definendo anche la resilienza globale?

- Come può la ricerca contribuire meglio a generare i dati e le statistiche necessarie per consentire una valutazione pregnante?

- In quali modi i processi legislativi dell'UE possono essere modificati perché siano più flessibili e tengano meglio conto della velocità con cui la tecnologia e le minacce evolvono?

- In che modo lo sviluppo di parametri di misurazione (indicatori, valori-obiettivo) nel ciclo programmatico dell'UE può essere adattato, innalzato di livello e replicato per l'intero settore della cibersicurezza?

- Cosa possono apprendere reciprocamente le istituzioni superiori di controllo nazionali dagli approcci da esse adottati nell'audit delle politiche e delle misure relative alla cibersicurezza?

- Quali discordanze nel recepimento e nell'attuazione del quadro normativo dell'UE pregiudicano al momento una risposta più efficace alle lacune in materia di cibersicurezza e alla criminalità informatica e qual è il modo migliore in cui gli Stati membri e le istituzioni dell'UE potrebbero porvi rimedio?

- Quanto sono efficaci i controlli delle esportazioni dell'UE sui beni e servizi informatici nel prevenire la violazione dei diritti umani all'esterno dell'UE?

Il finanziamento e la spesa

40 L'UE aspira a creare l'ambiente online più sicuro al mondo. Per realizzare questa ambizione, tutte le parti in causa devono compiere sforzi significativi, tra cui anche assicurare un solido fondamento finanziario accuratamente gestito.

Sfida n. 3: allineare i livelli di investimento agli obiettivi

Accrescere gli investimenti

41 Si stima che, a livello mondiale, la spesa totale per la cibersicurezza si collochi allo 0,1 % del PIL. Negli Stati Uniti[63], questo valore sale allo 0,35 % (compreso il settore privato). In percentuale del PIL, la spesa del governo federale statunitense iscritta a bilancio per il 2019 ammonta allo 0,1 % circa, ossia circa 21 miliardi di dollari USA[64].

42 In confronto, la spesa nell'UE è stata modesta, frammentata e spesso non sostenuta da programmi concertati e diretti dai governi. Per quanto difficile da quantificare, la spesa del settore pubblico dell'UE per la cibersicurezza si collocherebbe, secondo le stime, tra uno e due miliardi di euro all'anno[65]. La spesa di alcuni Stati membri, in percentuale al PIL, è pari a un decimo di quella degli Stati Uniti o addirittura inferiore[66]. L'UE e i suoi Stati membri hanno bisogno di sapere quanto stanno investendo nel complesso per decidere quali lacune colmare.

43 Non è facile tracciare un quadro esaustivo, data l'assenza di dati precisi dovuta al carattere trasversale della cibersicurezza e al fatto che quest'ultima spesso non può essere distinta dalla spesa per il settore informatico in generale[67]. L'indagine della Corte ha confermato che è difficile ottenere statistiche affidabili sulla spesa sia nel settore pubblico che in quello privato. Tre quarti delle istituzioni superiori di controllo hanno dichiarato di non disporre di una visione d'insieme a livello centrale della spesa pubblica connessa alla cibersicurezza e neanche uno Stato membro ha imposto agli enti pubblici di indicare separatamente, nei rispettivi piani finanziari, la spesa per la cibersicurezza.

44 È particolarmente difficile accrescere gli investimenti pubblici e privati nelle imprese europee che si occupano di cibersicurezza. I fondi pubblici sono spesso disponibili nelle fasi iniziali, mentre diminuiscono per gli stadi della crescita e dell'espansione[68]. Esistono svariate iniziative di finanziamento dell'UE, che però non sono sfruttate, in gran parte a causa degli adempimenti burocratici implicati[69]. Nel

complesso, le imprese dell'UE che si occupano di cibersicurezza registrano una performance inferiore rispetto alle omologhe internazionali: meno numerose, l'ammontare medio dei finanziamenti che raccolgono è nettamente inferiore[70]. Per conseguire gli obiettivi dell'UE relativi alla politica digitale è quindi fondamentale assicurare un efficace indirizzamento e finanziamento delle *start-up*.

Accrescere l'impatto

45 Colmando la carenza di investimenti nel settore della cibersicurezza si dovrebbero produrre effetti utili. Ad esempio, nonostante le notevoli capacità del settore della ricerca e innovazione dell'UE, i risultati non sono oggetto di brevetti, commercializzazioni o estensioni sufficienti a contribuire al rafforzamento della resilienza, della competitività e dell'autonomia digitale[71]. Ciò risulta particolarmente evidente nel confronto con i concorrenti dell'UE a livello mondiale. I risultati sono raramente sfruttati in maniera adeguata a causa di una serie di fattori[72], tra cui:

- la mancanza di una strategia transnazionale omogenea per estendere l'approccio e fare in modo che soddisfi le esigenze digitali più ampie dell'UE per la competitività e una maggiore autonomia;
- la durata del ciclo della catena del valore, che causa la rapida obsolescenza degli strumenti;
- la scarsa sostenibilità, in quanto i progetti si concludono generalmente con lo scioglimento dell'équipe di progetto e la fine dell'assistenza fornita, anche per quanto riguarda aggiornamenti e soluzioni correttive (*patch*).

46 Con la proposta della Commissione di stabilire una rete di centri di competenza per la cibersicurezza e un centro di ricerca e di competenza si intende superare la frammentazione nel campo di ricerca della cibersicurezza e promuovere gli investimenti su vasta scala[73]. Nell'intera UE si contano in tutto circa 665 centri di competenza.

Sfida n. 4: una chiara visione d'insieme della spesa finanziata dal bilancio dell'UE

47 Una visione d'insieme della spesa è importante per la trasparenza e per un migliore coordinamento. Senza di essa, è difficile per i decisori politici vedere in che modo la spesa è allineata ai bisogni per conseguire gli obiettivi prioritari.

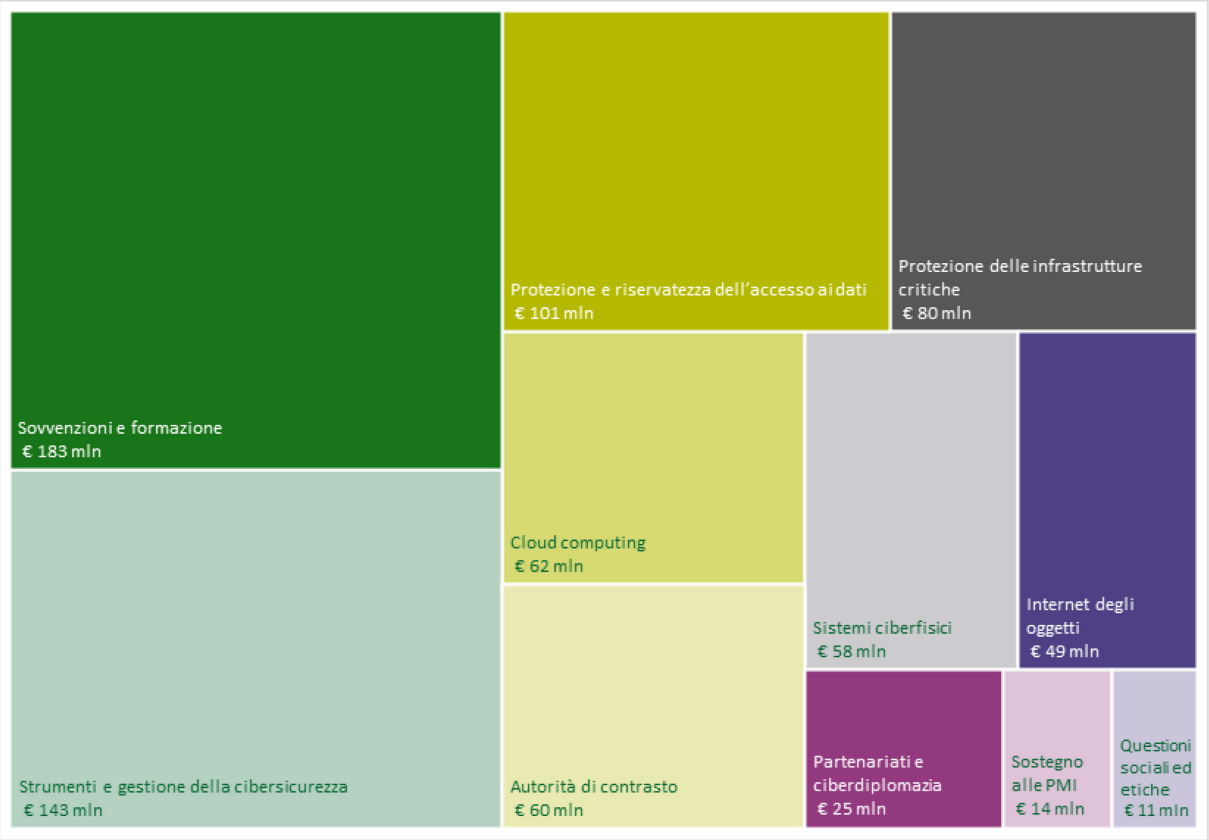
48 La strategia per la cibersicurezza non è finanziata da nessuna dotazione ad hoc. A livello UE, i fondi spesi per la cibersicurezza provengono invece dal bilancio generale dell'UE e dal cofinanziamento degli Stati membri. Dall'analisi condotta dagli auditor della Corte emerge una complessa architettura di almeno dieci diversi strumenti a valere sul bilancio generale dell'UE, ma nessuna visione chiara di quali fondi vanno dove (cfr. ***allegato II***).

49 Acquisire una chiara visione d'insieme della spesa per una questione che tocca trasversalmente molti ambiti d'intervento è dunque una grande sfida. I programmi di spesa sono gestiti da diversi servizi della Commissione, ognuno con obiettivi, regole e calendari propri. Il quadro è ulteriormente complicato se si tiene conto del cofinanziamento degli Stati membri, come nel caso del Fondo sicurezza interna – Polizia[74].

Spesa identificabile per la cibersicurezza

50 Nel periodo 2014-2018, la Commissione ha speso almeno 1,4 miliardi di euro per attuare la strategia[75], assegnandone la maggior parte a Orizzonte 2020[76]. I fondi di Orizzonte 2020 sono erogati principalmente tramite progetti nell'ambito della sfida "Società sicure" e della "Leadership nelle tecnologie abilitanti e industriali"[77]. Gli auditor della Corte hanno individuato 279 progetti appaltati in materia di cibersicurezza fino a settembre 2018, per un finanziamento UE complessivo di 786 milioni di euro[78]. La ***figura 5*** illustra la tipologia di questi progetti sulla base di tale analisi.

Figura 5 – Progetti di ricerca di Orizzonte 2020 in materia di cibersicurezza appaltati



Fonte: Corte dei conti europea.

51 Nel 2016 è stato creato un partenariato pubblico-privato contrattuale per stimolare il settore della cibersicurezza europeo. La finalità era di convogliare 450 milioni di euro del programma Orizzonte 2020 nel partenariato suddetto e di attrarre ulteriori 1,8 miliardi di euro provenienti dal settore privato entro il 2020. Nei 18 mesi fino al 31 dicembre 2017, 67,5 milioni di euro sono stati convogliati da Orizzonte 2020 nel partenariato pubblico-privato contrattuale e il settore privato ha investito un miliardo di euro[79].

52 La lotta alla cibercriminalità è sostenuta anche dal Fondo sicurezza interna – Polizia ("ISF-Polizia" o "ISF-P"). L'ISF-Polizia finanzia studi, riunioni di esperti ed attività di comunicazione; tali attività sono ammontate a quasi 62 milioni di euro tra il 2014 e il 2017. Gli Stati membri possono inoltre ricevere, in modalità di gestione concorrente, sovvenzioni per attrezzature, formazione, ricerca e raccolta dati. Dette sovvenzioni sono state sfruttate da 19 Stati membri, per un valore di 42 milioni di euro.

53 I fondi a sostegno della cooperazione giudiziaria e del funzionamento degli accordi di assistenza giudiziaria reciproca, con particolare riguardo allo scambio di dati

elettronici e di informazioni finanziarie, sono ammontati a 9 milioni di euro nel quadro del programma Giustizia gestito dalla DG JUST.

54 La direttiva NIS dispone esplicitamente che i CSIRT debbano esser dotati di risorse adeguate per svolgere in modo efficace i propri compiti[80]. Tra il 2016 e il 2018, il meccanismo per collegare l'Europa ha messo a disposizione ogni anno 13 milioni di euro, utilizzabili dagli Stati membri per sostenere l'attuazione di quanto disposto dalla direttiva. Non vi è stato alcuno studio che stabilisse i fondi effettivamente necessari alla rete dei CSIRT ed al gruppo di cooperazione per avere un impatto.

55 Svariate spese operative delle agenzie miravano specificamente ad attività per la cibersicurezza o di contrasto alla cibercriminalità. Risulta però difficile ricavare cifre esatte dalle informazioni di pubblico dominio.

56 La convenzione di Budapest (cfr. paragrafo ***11***) ha costituito la struttura portante della spesa dell'UE per la cibersicurezza esterna. Nel periodo 2014-2018, l'UE ha speso circa 50 milioni di euro per potenziare la cibersicurezza oltre i propri confini. Quasi la metà di tale ammontare è stato erogato tramite lo strumento inteso a contribuire alla stabilità e alla pace; un progetto (GLACY+, da 13,5 milioni di euro) mirava a rafforzare in tutto il mondo le capacità di elaborare ed attuare norme in materia di cibercriminalità e ad accrescere la cooperazione internazionale[81]. La spesa finanziata da altri strumenti finanziari dell'UE è stata per lo più concentrata sui Balcani occidentali[82], nonché sul vicinato europeo: ad esempio, il progetto "Cybercrime@EaP" con i paesi del partenariato orientale mira a migliorare la cooperazione internazionale in materia di cibercriminalità e prove elettroniche.

Altre spese per la cibersicurezza

57 Non è sempre possibile individuare spese specifiche per la cibersicurezza nei programmi dell'UE:

- i fondi di Orizzonte 2020 sono stati erogati anche tramite l'impresa comune ECSEL (Componenti e sistemi elettronici per la leadership europea) per i sistemi ciberfisici. Tuttavia, gli auditor della Corte non sono riusciti a stabilire cosa, fra i 27 progetti attuati tra il 2015 e il 2016 per un valore totale di 437 milioni di euro, si riferisse specificamente alla cibersicurezza;

- nell'ambito dei Fondi strutturali e di investimento europei, è disponibile un massimo di 400 milioni di euro per spese in materia di cibersicurezza e servizi fiduciari. Tale importo copre gli investimenti in sicurezza e protezione dei dati per

rafforzare l'interoperabilità e l'interconnessione delle infrastrutture digitali, l'identificazione elettronica, il rispetto della vita privata e i servizi fiduciari.

58 Nel proprio piano operativo del 2018, la Banca europea per gli investimenti ha annunciato l'intenzione di aumentare fino a 6 miliardi di euro in tre anni il finanziamento delle tecnologie a duplice uso, della cibersicurezza e della sicurezza civile[83].

Prospettive

59 La componente di cibersicurezza da 2 miliardi di euro del nuovo programma Europa digitale[84] proposto per il 2021-2027 è concepita per rafforzare il settore della cibersicurezza dell'UE e la complessiva tutela della società, anche sostenendo l'attuazione della direttiva NIS. La proposta rete di centri di competenza sulla cibersicurezza ed il proposto centro europeo di ricerca e di competenza, miranti a conseguire un approccio più razionale, dovrebbero costituire il principale meccanismo di esecuzione della spesa dell'UE nell'ambito del programma Europa digitale.

60 La spesa per la difesa a valere sul bilancio dell'UE è stata di recente aumentata tramite il programma europeo di sviluppo del settore industriale della difesa, con 500 milioni di euro da assegnare nel 2019 e nel 2020[85]. Detto programma sarà incentrato sul miglioramento del coordinamento e dell'efficienza della spesa per la difesa degli Stati membri tramite incentivi per lo sviluppo congiunto. Mira a generare investimenti, per un totale di 13 miliardi di euro, nelle capacità di difesa dopo il 2020 tramite il Fondo europeo per la difesa, alcuni dei quali coprono la ciberdifesa[86].

Sfida n. 5: assegnare risorse adeguate alle agenzie dell'UE

61 I tre principali organismi al cuore della politica di cibersicurezza dell'UE, ossia l'ENISA, l'EC3 di Europol e la CERT-UE (cfr. ***riquadro 2***), stanno avendo difficoltà legate alle risorse, in un momento di priorità politiche spinte da una accentuata richiesta di sicurezza. L'attuale ripartizione di risorse umane e finanziarie presso le agenzie dell'UE continua a rendere difficoltoso per loro il conseguimento delle aspettative[87].

62 Le richieste di risorse aggiuntive presentate dalle agenzie per soddisfare la crescente domanda non sono state pienamente soddisfatte, e ciò potrebbe aver ostacolato il (puntuale) conseguimento degli obiettivi strategici. Ad esempio:

- la limitatezza delle risorse è stato uno dei fattori che ha impedito all'ENISA di conseguire appieno i propri obiettivi nel 2017[88]. Nel pacchetto del 2017, sono state proposte risorse aggiuntive per tener conto del nuovo mandato dell'ENISA;

- presso l'EC3 di Europol, l'afflusso di analisti e di investimenti in capacità di TIC non ha tenuto il passo della domanda[89]. Inoltre, la task force di azione congiunta contro la criminalità informatica (J-CAT) dell'EC3 di Europol è composta di esperti degli Stati membri e di paesi non-UE che hanno il compito di coadiuvare le indagini condotte con metodi di *intelligence*. Ma i costi sono in larga parte sostenuti dagli Stati che inviano gli esperti, e ciò disincentiva l'invio di un numero maggiore. Tramite alcuni finanziamenti di Europol o del ciclo programmatico dell'UE è stato ideato un invio temporaneo, sulla base dei casi, onde permettere la partecipazione di più paesi.

63 Alcune limitazioni sono autoinflitte. Molti di coloro che lavorano presso la CERT-UE e l'ENISA sono agenti contrattuali, le cui procedure di assunzione sono in genere lente. Altre difficoltà, come quella ad attrarre e mantenere le persone di talento, derivano dall'incapacità delle agenzie di competere con gli stipendi offerti dal settore privato, oppure sono dovute a magre prospettive di carriera. L'ENISA ha perciò esternalizzato molte delle proprie attività tra il 2014 e il 2016[90].

64 Le carenze di personale e dei necessari strumenti possono comportare notevoli rischi, specie riguardo alla raccolta di *intelligence* sulle minacce. Il volume di dati da fonti aperte e chiuse continua ad aumentare e rischia di sopraffare la capacità degli analisti di effettuare adeguate analisi delle minacce. Senza le giuste capacità e i giusti strumenti per integrare con successo e correlare tali dati, non si riuscirà in modo efficace a tradurli in *intelligence* delle minacce che possa essere condivisa ed analizzata in tutta l'UE[91].

Spunti di riflessione – Finanziamenti e spesa

- In che modo la Commissione e i legislatori possono razionalizzare la spesa UE per la cibersicurezza e allinearla in modo più esplicito a obiettivi chiaramente definiti?

- Come si può ovviare alla carenza di risorse presso le agenzie dell'UE in modo generale, tenendo conto delle esigenze e delle finalità dell'Unione?

- Quali misure vengono individuate a livello dell'UE e degli Stati membri per ridurre gli ostacoli che impediscono alle PMI di reperire capitali d'investimento per espandere le proprie attività?

- Quali risultati concreti e continui stanno producendo i fondi di Orizzonte 2020 per generare soluzioni in tema di cibersicurezza?

- In che misura le attività UE di potenziamento delle capacità stanno potenziando le capacità oltre i confini della stessa in linea con i valori dell'UE?

Costruire una società resiliente agli attacchi e agli incidenti informatici

65 La governance della cibersicurezza concerne la gestione delle minacce e dei rischi, il potenziamento delle capacità e della consapevolezza, nonché il coordinamento e la condivisione delle informazioni basati sulla fiducia.

Sfida n. 6: potenziare la governance e gli standard

La governance della sicurezza delle informazioni

66 La governance della sicurezza delle informazioni consiste nel porre in atto strutture e politiche che assicurino la riservatezza, l'integrità e la disponibilità dei dati. Non si tratta solo di una questione tecnica; sono necessari una leadership efficace, processi solidi e strategie allineate con gli obiettivi organizzativi[92]. Un suo sottoinsieme è la governance della cibersicurezza, che riguarda tutti i tipi di minacce informatiche, compresi attacchi, violazioni o incidenti mirati e sofisticati difficili da individuare o gestire.

67 I modelli di governance della cibersicurezza differiscono da uno Stato membro all'altro, e nell'ambito di detti modelli la responsabilità per la cibersicurezza è spesso suddivisa tra molte entità. Queste differenze potrebbero ostacolare la collaborazione necessaria per rispondere ad incidenti transfrontalieri di grande scala e per scambiare *intelligence* sulle minacce a livello nazionale, per non dire dell'UE. Dall'indagine condotta dalla Corte presso le istituzioni superiori di controllo nazionali è emerso che le debolezze nei meccanismi di governance e nella gestione dei rischi delle autorità pubbliche erano percepite come i rischi più elevati.

68 Sebbene le conseguenze per le organizzazioni del settore privato possano essere gravi, le debolezze nella cibergovernance sono moltissime. Quasi nove organizzazioni su dieci affermano che la propria funzione della cibersicurezza non risponde pienamente ai bisogni[93] e che gli addetti alla cibersicurezza sono spesso lontani di almeno due livelli dall'organo direttivo[94].

69 Le direttive dell'UE in materia di diritto societario non stabiliscono obblighi specifici circa l'informativa sui rischi informatici. Negli Stati Uniti, la *Securities and Exchange Commission* ha di recente emanato orientamenti non vincolanti per assistere

le imprese pubbliche a predisporre informative sui rischi e sugli incidenti relativi alla cibersicurezza[95]. Il comitato congiunto[96] delle autorità europee di vigilanza (AEV) ha segnalato il crescere dei rischi informatici, esortando le istituzioni finanziarie a migliorare sistemi informatici fragili e ad esplorare i rischi intrinseci per la sicurezza delle informazioni, la connettività e l'esternalizzazione[97].

70 Potenziare la governance della sicurezza delle informazioni delle PMI è particolarmente difficile, poiché il più delle volte le PMI non sono in grado di porre in atto i sistemi appropriati. Le PMI non dispongono di idonee linee-guida sull'applicazione dei requisiti in materia di sicurezza delle informazioni e di privacy e sulla mitigazione dei rischi tecnologici[98]. Comprendere meglio le esigenze delle PMI e fornire gli incentivi ed il sostegno necessari costituiscono dunque delle sfide cruciali.

71 La mancanza di un quadro di governance coerente per la cibersicurezza a livello internazionale compromette la capacità della comunità internazionale di rispondere agli attacchi informatici e di limitarli. È quindi importante creare un consenso su tale quadro di governance che rifletta al meglio gli interessi ed i valori dell'UE[99]. I tentativi di fissare norme internazionali vincolanti sul ciberspazio stanno risultando sempre più vani, come si è visto per il mancato consenso, all'interno del gruppo di esperti governativi delle Nazioni Unite sulla sicurezza delle informazioni, sulle modalità con cui il diritto internazionale dovrebbe applicarsi alle risposte degli Stati agli incidenti.

72 Per potenziare il proprio programma in materia di governance del ciberspazio, l'UE ha inoltre formalizzato sei ciberpartenariati per istituire periodici dialoghi strategici miranti a sviluppare fiducia e aree comuni di collaborazione[100]. Gli esiti sono eterogenei, ma, complessivamente, nel campo internazionale, l'UE non può ancora esser considerata un "principale attore della cibersicurezza", sebbene abbia innalzato il proprio profilo[101].

La sicurezza delle informazioni presso le istituzioni dell'UE

73 Ciascuna istituzione dell'UE dispone di proprie norme di governance della sicurezza delle informazioni. Un accordo interistituzionale prevede che la Commissione fornisca assistenza in materia di sicurezza delle informazioni alle altre istituzioni ed agenzie. Le istituzioni e gli organismi dell'UE hanno riconosciuto la necessità di sviluppare in modo coerente le proprie capacità cibernetiche e i propri approcci alla gestione dei rischi. La Commissione, il Consiglio e il SEAE presenteranno nel 2020 al Gruppo orizzontale "Questioni riguardanti il ciberspazio" una relazione sulla governance e sui progressi compiuti nel chiarire e armonizzare la governance della cibersicurezza presso le istituzioni e le agenzie dell'UE[102].

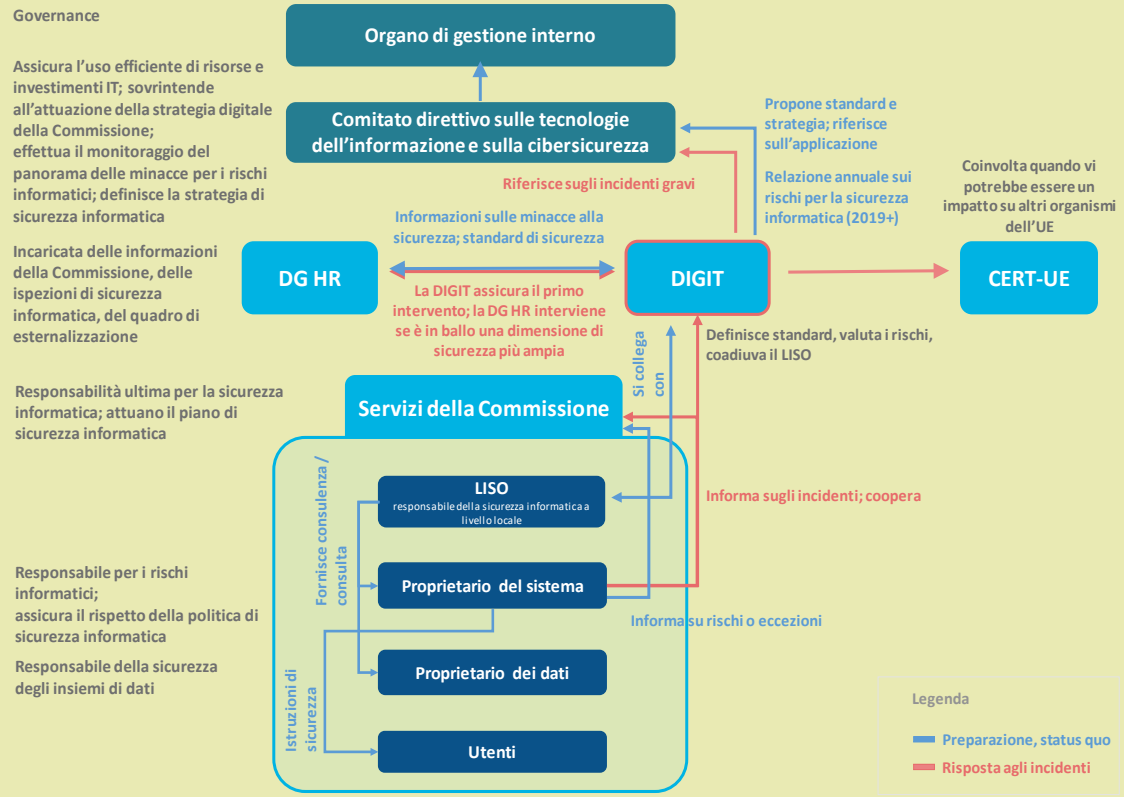
74 All'interno della Commissione, la direzione generale dell'Informatica (DIGIT) è responsabile della sicurezza delle infrastrutture e dei servizi informatici (cfr. ***riquadro 3***). I principali obiettivi di sicurezza informatica della strategia digitale della Commissione sono: incorporare la sicurezza informatica nei processi di gestione; fornire infrastrutture e resilienza efficaci e ottimali sotto il profilo dei costi; ampliare la portata dell'individuazione degli incidenti e della risposta agli stessi; integrare la governance informatica e quella della sicurezza[103]. La Commissione, nei termini del contratto concluso con il proprio fornitore, fa sì che quasi tutto il software sia oggetto di manutenzione attiva e che venga usato solo software per il quale sia disponibile l'assistenza tecnica del produttore[104].

75 L'importanza di proteggere le istituzioni si estende anche alle missioni di PSDC dell'UE e alle strutture dell'UE nel mondo. Una delle priorità del quadro strategico UE in materia di ciberdifesa (aggiornamento del 2018) è il rafforzamento della protezione dei sistemi di comunicazione e informazione PSDC utilizzati da entità dell'UE. In seno al SEAE, è stato creato un comitato di governance informatica, che si è riunito per la prima volta nel giugno 2017[105].

Riquadro 3

Proteggere i sistemi informativi della Commissione

I circa 1 300 sistemi e 50 000 dispositivi della Commissione sono continuamente bersagliati da ciberattacchi. Come illustrato nel grafico che segue, la responsabilità per le tecnologie dell'informazione è decentrata. La sicurezza delle informazioni e quella informatica sono basate su un piano di sicurezza informatica comune predisposto dalla DIGIT. Il Comitato direttivo sulle tecnologie dell'informazione e sulla cibersicurezza (*Information Technology and Cybersecurity Board*) funge *de facto* da responsabile-capo della sicurezza delle informazioni della Commissione e collega il lato operativo della sicurezza informatica con l'alta direzione della Commissione, rappresentata dall'organo di gestione interno.



Fonte: Corte dei conti europea, sulla base delle decisioni della Commissione[106].

Il compito principale della DG Risorse umane e sicurezza (DG HR) consiste nel proteggere il personale, le informazioni e i beni della Commissione. Detta direzione generale conduce inoltre indagini su incidenti che hanno una dimensione di sicurezza più ampia rispetto a quella relativa alle sole tecnologie dell'informazione, nell'ambito quindi delle proprie attività di controspionaggio e di lotta al terrorismo.

La DIGIT è responsabile della sicurezza informatica ed ospita la squadra di pronto intervento informatico CERT-UE. Creata nel 2011, la CERT-UE ha una dotazione finanziaria annua di circa 2,5 milioni di euro e impiega circa 30 effettivi. Assicura il primo intervento per qualunque incidente relativo alla sicurezza delle informazioni riguardante più istituzioni, ma non opera ancora 24 ore su 24 e 7 giorni su 7. Ospita una piattaforma

di condivisione delle informazioni. Nel 2018, la CERT-UE ha firmato un memorandum d'intesa non vincolante con l'ENISA, il Centro europeo per la lotta alla criminalità informatica (EC3) e l'Agenzia europea per la difesa per potenziare la collaborazione e il coordinamento. Ha concluso inoltre un accordo tecnico con la capacità NATO di risposta ai ciberincidenti (NCIRC).

Valutazioni delle minacce e dei rischi

76 Tanto per le organizzazioni pubbliche quanto per quelle private, le valutazioni ben fondate e continue delle minacce e dei rischi costituiscono strumenti importanti. Tuttavia, non vi è un approccio standard alla classificazione e alla mappatura delle ciberminacce o alla valutazione dei rischi: in altre parole, il contenuto delle singole valutazioni varia considerevolmente e ciò è problematico per un approccio alla cibersicurezza coerente per tutta l'UE[107]. Inoltre, spesso dette valutazioni sono fondate sulle medesime fonti, o anche su altre valutazioni delle minacce; il risultato è un riecheggiare delle stesse conclusioni ripetute[108], con il rischio che non si presti sufficiente attenzione ad altre minacce. Ciò è aggravato da un persistente riluttanza a condividere le informazioni e a segnalare tutti gli incidenti.

77 La cellula per l'analisi delle minacce ibride[109] integrata nel SEAE è stata creata per migliorare la conoscenza situazionale e supportare la presa di decisioni tramite la condivisione di analisi, ma deve ampliare le proprie competenze, comprese quelle nel campo della cibersicurezza. In parallelo, la CERT-UE fornisce alle istituzioni, agli organismi e alle agenzie dell'UE relazioni e *briefing* concernenti le ciberminacce che li riguardano.

78 L'ENISA ha osservato in passato che molti Stati membri hanno una comprensione qualitativa delle minacce e che vi è l'esigenza di una maggiore modellizzazione delle ciberminacce[110]. Il monitoraggio della capacità di analisi strategica rafforzerà la comprensione complessiva. Tuttavia, le valutazioni delle minacce potrebbero coprire non solo le minacce tecnologiche, ma anche quelle socio-politiche ed economiche, al fine di garantire una visione più completa, nonché i fattori di minaccia e i moventi degli attori.

Incentivi

79 Le organizzazioni sono ancora troppo poco incentivate, giuridicamente ed economicamente, a notificare e condividere le informazioni sugli incidenti. Temendo un danno reputazionale, molte organizzazioni preferiscono tuttora trattare i

ciberattacchi in modo discreto oppure pagare gli autori degli stessi. Resta da vedere quanto sarà efficace la direttiva NIS nell'elevare il livello delle notifiche. La Commissione si attende che i miglioramenti si materializzino primariamente a livello nazionale, ma il proposto regolamento dell'UE sulla cibersicurezza aggiungerà una prospettiva valida per tutta l'UE[111].

80 Incorporando alcuni standard nei loro appalti, le autorità pubbliche hanno una notevole influenza sui fornitori in qualità di acquirenti di prodotti e servizi digitali tramite appalto pubblico, nonché in qualità di finanziatori di ricerche e programmi (ad esempio, richiedendo l'adozione di alcuni standard tecnici, come il protocollo Internet IPv6, per contribuire alla lotta contro la cibercriminalità). Attualmente, però, non vi è alcun quadro per appalti congiunti per le infrastrutture di cibersicurezza[112]. La Commissione può fare molto in proposito. Il programma Europa digitale proposto per il prossimo quadro finanziario pluriennale mira ad ovviare al fatto che gli investimenti del settore pubblico nell'acquisto delle più recenti tecnologie di cibersicurezza sono stati finora limitati.

81 Tramite i propri poteri normativi, la Commissione può far sì che vengano sviluppati gli standard giusti e che vengano adottati in modo generalizzato, al fine di potenziare la sicurezza. La Commissione e Europol lavorano con organismi di governance della rete Internet quali l'ICANN (cfr. paragrafo ***38***) e il RIPE-NCC[113]; ciò è essenziale per porre in essere la giusta architettura di lotta alla cibercriminalità al fine di coadiuvare le autorità di contrasto e quelle giudiziarie.

Sfida n. 7: sviluppo delle competenze e sensibilizzazione

82 L'ENISA ha sottolineato che gli utenti svolgono un ruolo cruciale contro i ciberattacchi e che il potenziamento delle competenze, dell'istruzione e della consapevolezza è essenziale per costruire una società ciber-resiliente[114]. Sia al lavoro che a casa, singoli individui che ben riescono a cogliere i segnali di allarme e possiedono le giuste tecniche possono rallentare o prevenire gli attacchi.

83 Particolare preoccupazione desta la crescente asimmetria tra le conoscenze necessarie per commettere un atto di criminalità informatica o a lanciare un ciberattacco e le competenze necessarie per difendersene. Il modello di attività criminale come servizio ha abbassato le barriere d'ingresso al mercato della cibercriminalità: individui che non posseggono le conoscenze tecniche per costruire *botnet*, kit per *exploit* o pacchetti di *ransomware* possono adesso affittarli.

Formazione, competenze e sviluppo delle capacità

84 Nel mondo vi è una crescente penuria di competenze in materia di cibersicurezza; il divario in termini di forza lavoro è cresciuto del 20 % dal 2015[115]. I tradizionali canali di assunzione non soddisfano la domanda, comprese le posizioni manageriali e interdisciplinari[116]. Quasi il 90 % della forza lavoro mondiale addetta alla cibersicurezza è costituito da uomini; la persistente mancanza di diversità di genere restringe ulteriormente il serbatoio di talenti cui attingere[117]. Per di più, nelle università le materie connesse alla cibersicurezza sono sottorappresentate nei programmi di studio non tecnici.

85 Sono necessarie formazione e istruzione per tutti: funzionari pubblici, funzionari delle autorità di contrasto, autorità giudiziarie, forze armate e educatori. Ad esempio, i tribunali devono essere in grado di affrontare le particolarità tecniche, che mutano rapidamente, della cibercriminalità e delle vittime di quest'ultima[118]; non esistono al momento standard di formazione e certificazione applicabili a tutta l'UE[119]. Presso le istituzioni dell'UE, è importante ottenere la giusta combinazione di competenze. Altrimenti, le istituzioni potrebbero non essere in grado di definire in modo appropriato l'ambito, di individuare i giusti partner e le esigenze di sicurezza o potrebbero non disporre della capacità di gestire programmi. Ciò, a sua volta, potrebbe nuocere all'efficacia dei programmi dell'UE o alla definizione delle politiche.

86 Sebbene i responsabili delle politiche di istruzione a livello UE siano gli Stati membri, numerose attività di formazione (cfr. ***tabella 2***) ed esercitazioni (cfr. ***riquadro 4***) stanno già avendo luogo. L'UE può contribuire a inserire standard validi per tutta l'UE nei curriculum di apprendimento per tutte le pertinenti discipline[120]. Nell'area della scienza forense digitale, ad esempio, sono necessari standard di formazione comuni per facilitare il percorso verso l'ammissibilità delle prove negli Stati membri. Stante la natura transfrontaliera della cibercriminalità, più di una giurisdizione può essere coinvolta, il che richiede formazione a livello UE. Ciononostante, CEPOL, l'Agenzia dell'UE per la formazione delle autorità di contrasto, ha osservato che più di due terzi degli Stati membri non forniscono formazione periodica su queste materie ai funzionari di dette autorità[121]. L'UE potrebbe inoltre individuare modi per porre in sinergia l'istruzione e la formazione tra le sfere civile e militare[122]. Ciò detto, l'ENISA ha riscontrato che, sebbene le attuali opportunità di formazione nei settori critici siano ampie, non coprono sufficientemente la resilienza delle infrastrutture critiche[123].

Tabella 2 – Alcune delle iniziative UE di formazione in materia di cibersicurezza e cibercriminalità

Progetti dell'Agenzia europea per la difesa, ad esempio sostegno alle esercitazioni da parte del settore privato e il progetto Poligoni virtuali.	Rete dell'Accademia europea per la sicurezza e la difesa (che fornisce formazione civile-militare), compresa la piattaforma informatica in materia di istruzione, formazione, valutazione ed esercitazioni	Formazione dell'ENISA, che offre programmi formativi laddove il mercato commerciale potrebbe non farlo
Programmi di formazione di Europol, CEPOL e ECTEG[124], tra cui il modello di governance della formazione e il quadro delle competenze formative (compresa la certificazione)	Rete dei centri di competenza e Centro europeo di ricerca e di competenza sulla cibersicurezza (proposti)	Misure sulla cifratura proposte nell'undicesima relazione sui progressi compiuti verso un'Unione della sicurezza
Cooperazione UE-NATO su formazione e istruzione in materia di ciberdifesa	Programma Erasmus militare	Rete europea di formazione giudiziaria

Fonte: Corte dei conti europea.

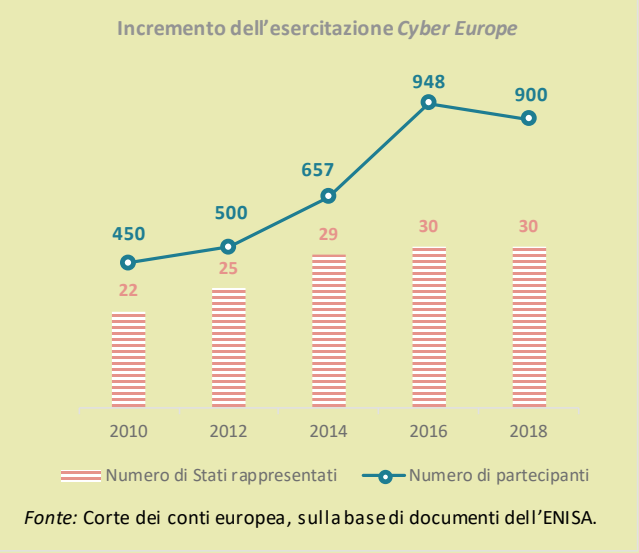
87 L'UE ha inviato esperti di lotta al terrorismo e di sicurezza in 17 delegazioni, per ribadire il nesso tra la sicurezza interna e la sicurezza esterna dell'UE[125]. Nonostante vincoli di risorse, maggiori ciber-conoscenze hanno potuto contribuire a porre in atto i giusti progetti, nonché ad individuare sinergie con altri programmi o fonti di finanziamento[126]. Esse potrebbero inoltre elevare il profilo della cibersicurezza nel dialogo politico, sebbene quest'ultima dovrà concorrere con molte altre priorità, come le migrazioni, la criminalità organizzata o il ritorno dei combattenti (*foreign fighters*) nel paese d'origine.

Riquadro 4

Esercitazioni

Le esercitazioni sono elementi importanti della ciber-istruzione e ciber-formazione: offrono opportunità impareggiabili per potenziare la preparazione testando le capacità, generando risposte a scenari di vita reale e costruendo reti di relazioni di lavoro. Dal 2010, la loro frequenza è nettamente aumentata.

I partecipanti vi prendono parte sul posto o a distanza. Vi sono valutazioni post-esercitazione per individuare gli insegnamenti appresi, sebbene questi ultimi forse non filtrino pienamente tra i livelli strategico/politico, operativo e tecnico[127].



Fonte: Corte dei conti europea, sulla base di documenti dell'ENISA.

Le esercitazioni-faro dell'UE e della NATO – la "Cyber Europe" (operativa) che ha luogo ogni due anni e la "Locked Shields" (tecnica) che ha luogo ogni anno – attraggono oltre 1 000 partecipanti da circa 30 Stati che vi prendono parte. Entrambe le esercitazioni sono incentrate sulla protezione ed il mantenimento delle infrastrutture critiche in scenari di attacco simulato. Dette esercitazioni sono notevolmente cresciute di spessore e adesso comprendono entrambe elementi di natura mediatica, giuridica e finanziaria per migliorare la conoscenza situazionale degli operatori. Le esercitazioni parallele e coordinate PACE (strategiche) testano l'interazione tra UE e NATO in uno scenario di crisi ibrida.

Non si tratta delle sole esercitazioni internazionali. L'ENISA organizza ogni anno la *European Cyber Security Challenge*, evento durante il quale le squadre competono per risolvere problemi relativi alla sicurezza, come la sicurezza delle reti e dei telefoni cellulari, enigmi di crittografia, *reverse engineering*, questioni di etica e di scienze forensi. La prima esercitazione di livello ministeriale, EU CYBRID, ha avuto luogo nel settembre 2017 ed è stata incentrata sulla presa di decisioni strategiche. Nel 2018, è stata varata, sotto l'egida della NATO, l'esercitazione "Crossed Swords", per migliorare gli elementi di attacco dell'esercitazione "Locked Shields" della NATO. La NATO organizza inoltre le esercitazioni "Cyber Coalition".

Una delle sfide più importanti è assicurare il coinvolgimento attivo di tutti gli importanti portatori d'interessi, nonché il coordinamento di tutte le esercitazioni, per evitare duplicazioni e condividere in modo efficiente gli insegnamenti appresi.

Consapevolezza

88 I cittadini sono spesso vettori degli attacchi e della diffusione di disinformazione, poiché è probabile che siano esposti, senza saperlo, a vulnerabilità in dispositivi e software poco costosi e a larga distribuzione, oppure che siano vittime di ingegneria sociale. La sensibilizzazione è dunque essenziale per costruire un'efficace ciberresilienza; eppure, non è per niente un compito facile, poiché è difficile per i non-esperti comprendere la complessità della cibersicurezza ed i rischi associati.

89 Il "Mese europeo della sensibilizzazione in tema di cibersicurezza" (ECSM), evento annuale, e la giornata "Per un internet più sicuro" sono esempi di sensibilizzazione. Sette Stati che non fanno parte dell'UE hanno adesso aderito all'ECSM[128]. La campagna *Say No!* di Europol mira a ridurre il rischio che i bambini cadano vittime della coercizione ed estorsione sessuali online. Ridurre detto rischio è importante perché, al momento attuale, poche vittime di attacchi informano la polizia di questi reati[129]. La Commissione riconosce che la strategia in tema di cibersicurezza è stata solo "parzialmente efficace" nel sensibilizzare i cittadini e le imprese[130]. Ciò è dovuto all'entità del compito, alla limitatezza delle risorse, all'impegno non omogeneo degli Stati membri e a un'assenza di prove scientifiche su come sensibilizzare e misurare la consapevolezza nel migliore dei modi.

90 La sfida, per la Commissione e per le agenzie competenti, è fare in modo che le misure di sensibilizzazione siano ben mirate, pubblicizzate e inclusive, seguano il panorama delle minacce ed evitino effetti non intenzionali quali la "*security fatigue*"[131]. Inoltre, la Commissione e le agenzie competenti dovrebbero sviluppare metodi valutativi e parametri di misurazione per valutare l'efficacia di dette misure. Ciò dovrebbe applicarsi in egual misura in seno alle stesse istituzioni dell'UE, dove la cultura della consapevolezza deve essere migliorata[132].

Sfida n. 8: uno scambio di informazioni e un coordinamento migliori

91 La cibersicurezza necessita della cooperazione tra il settore pubblico e quello privato, specie in termini di condivisione delle informazioni e di scambio delle buone pratiche. La fiducia è essenziale a tutti i livelli per creare l'ambiente giusto per la condivisione transfrontaliera di informazioni sensibili. Uno scarso coordinamento porta alla frammentazione, alla duplicazione degli sforzi e a una dispersione di competenze. Un efficace coordinamento può avere come risultato successi tangibili, come la chiusura di alcuni mercati del *dark web*[133]. Nonostante i progressi compiuti negli ultimi

anni, i livelli di fiducia sono ancora "insufficienti"[134] a livello UE e in alcuni Stati membri[135].

Coordinamento tra le istituzioni dell'UE e con gli Stati membri

92 Una delle finalità della strategia dell'UE in materia di cibersicurezza, e delle strutture di cooperazione introdotte con la direttiva NIS, era quella di rafforzare la fiducia tra i portatori d'interesse. Nel documento di valutazione di detta strategia si riconosceva che erano state poste le fondamenta di una cooperazione strategica ed operativa a livello UE[136]. Ciononostante, il coordinamento in generale è "insufficiente"[137]. La difficoltà consiste nel far sì che lo scambio di informazioni non sia solo sensato, ma permetta anche una visione completa del quadro complessivo. Raggiungere una comprensione comune sulla base di una terminologia accettata è un fattore importante a questo proposito (cfr. ***riquadro 5***).

93 Nella valutazione relativa all'ENISA, tuttavia, si osserva che l'approccio dell'UE alla cibersicurezza non è stato coordinato a sufficienza, risultando in mancate sinergie tra le attività dell'ENISA e quelle di altri portatori d'interessi. I meccanismi di cooperazione sono ancora relativamente immaturi[138]; il proposto regolamento sulla cibersicurezza intende ovviarvi potenziando il ruolo di coordinamento dell'ENISA. Il desiderio di rafforzare la cooperazione è stato il motivo per il quale è stato firmato, nel 2018, il memorandum d'intesa tra l'ENISA, l'AED, l'EC3 di Europol e la CERT-UE[139]. Nei prossimi anni, una delle priorità della Commissione sarà garantire un adeguato allineamento tra iniziative strategiche, bisogni e programmi d'investimento, al fine di superare la frammentazione e generare sinergie[140].

94 Le funzioni di coordinamento sono integrate in seno ai vari organismi istituzionali. La task force sull'Unione della sicurezza è stata creata per svolgere un ruolo centrale nel coordinare le diverse direzioni generali della Commissione al fine di sostenere l'agenda della Commissione relativa all'Unione della sicurezza[141]. Il sottogruppo di lavoro sulla cibersicurezza della task force è presieduto dalla DG CNECT.

95 Presso il Consiglio, la cibersicurezza è gestita dal Gruppo orizzontale "Questioni riguardanti il ciberspazio", che coordina questioni strategiche e orizzontali ed aiuta a preparare le esercitazioni e a valutarne i risultati. Opera a stretto contatto con il comitato politico e di sicurezza, che dispone di un ruolo decisionale centrale in relazione a eventuali misure di ciberdiplomazia ("diplomazia informatica"); si veda il ***riquadro 6*** nella sezione che segue. Poiché la cibersicurezza è una tematica trasversale, coordinare tutti gli interessi in causa non è semplice: non meno di 24 gruppi di lavoro e

organismi preparatori si sono di recente occupati di questioni riguardanti il ciberspazio[142].

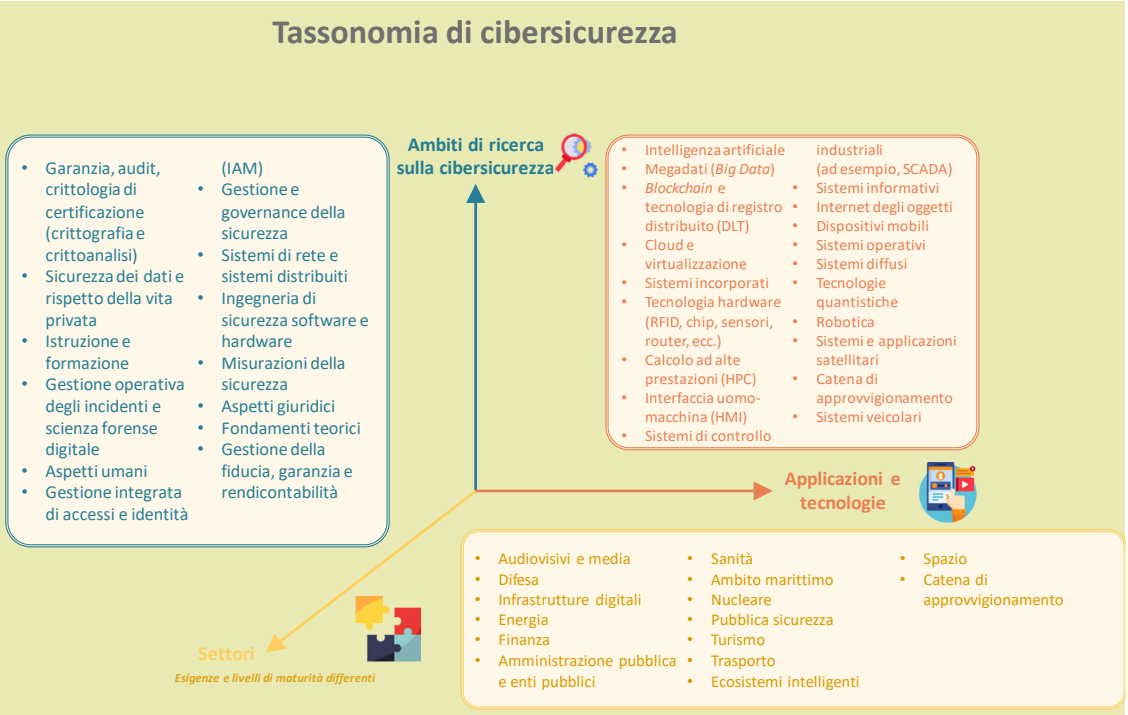
96 Le due proposte legislative sul potenziamento dell'ENISA (2017) e sull'istituzione di una rete di centri di competenza sulla cibersicurezza e di un centro europeo di ricerca e di competenza sulla cibersicurezza (2018) sono specificamente concepite per ovviare alla frammentazione e alla duplicazione degli sforzi. Un fattore che ha spinto a proporre la creazione dei centri di competenza sulla cibersicurezza e del centro europeo di ricerca e di competenza sulla cibersicurezza è stata la necessità di colmare il divario che le strutture di cooperazione previste dalla direttiva NIS non colmano, poiché non erano state concepite per sostenere lo sviluppo di soluzioni all'avanguardia (*cutting edge*).

Riquadro 5

Tentativi di parlare la stessa ciber-lingua: *coerenza tecnologica*

La chiarezza terminologica migliora la conoscenza situazionale ed il coordinamento[143] e contribuisce a stabilire con esattezza cosa costituisca una minaccia e un rischio.

Il Centro comune di ricerca (JRC) della Commissione ha recentemente messo a punto una tassonomia di ricerca rivista, tratta da diversi standard internazionali[144]. L'intento è che essa divenga un punto di riferimento che gli enti di ricerca di tutta Europa utilizzeranno come repertorio.



Fonte: Corte dei conti europea, sulla base di documentazione della Commissione europea.

Fino a poco tempo fa, le istituzioni e le agenzie dell'UE non avevano definizioni comuni. Ciò sta cambiando. Nel quadro del proprio programma, il gruppo di cooperazione NIS ha elaborato una tassonomia degli incidenti, al fine di facilitare una efficiente collaborazione transfrontaliera.

Cooperazione e scambio di informazioni con il settore privato

97 La cooperazione tra le autorità pubbliche ed il settore privato è essenziale per il rafforzamento dei livelli complessivi di cibersicurezza. Nonostante ciò, nella propria valutazione 2017 della strategia di cibersicurezza la Commissione ha rilevato che lo scambio di informazioni tra i portatori d'interesse privati e tra i settori pubblico e privato era "ancora non ottimale", data la "mancanza di meccanismi di segnalazione affidabili e di incentivi per condividere le informazioni"[145], e che ciò ostacolava il conseguimento delle finalità strategiche. La Commissione ha inoltre constatato la mancanza di un meccanismo di cooperazione efficiente con il quale gli Stati membri possano collaborare per rafforzare strategicamente capacità industriali durevoli su vasta scala[146].

98 I centri di condivisione e di analisi delle informazioni (ISAC) sono organizzazioni istituite per fornire piattaforme e risorse per facilitare la condivisione di informazioni tra i settori pubblico e privato, nonché per raccogliere informazioni sulle ciberminacce.

Mirano a costruire la fiducia tramite condivisione di esperienze, conoscenze e analisi, specie in merito alle cause profonde, agli incidenti e alle minacce. Esistono già ISAC nazionali e settoriali in molti Stati membri, ma a livello europeo sono ancora relativamente poco numerosi[147]. Tuttavia, incontrano numerose difficoltà (limiti di risorse, difficoltà a valutare i propri successi, a porre in essere le strutture giuste per coinvolgere sia il settore pubblico che quello privato, a coinvolgere le autorità di contrasto) che dovranno essere superate affinché gli ISAC possano contribuire ad attuare la direttiva NIS e a costruire capacità di sicurezza ad un livello europeo[148].

99 La stretta cooperazione con il settore privato è particolarmente importante per combattere la cibercriminalità complessa, ma la sua efficienza non è omogenea tra gli Stati membri e dipende dal livello di fiducia[149]. L'EC3 di Europol, tuttavia, ha creato una serie di gruppi consultivi con operatori del settore privato, istituzioni e agenzie dell'UE e altre organizzazioni internazionali al fine di migliorare la collaborazione tramite attività di rete, condivisione di *intelligence* strategica e cooperazione. Detti gruppi lavorano a piani allineati con gli obiettivi del ciclo programmatico dell'UE[150]. L'utilizzo a fini criminali delle tecnologie di cifratura è un altro campo carico di problematiche che richiedono maggiore cooperazione con il settore privato. L'EC3 di Europol sta attualmente vagliando diverse opzioni per ospitare presso la J-CAT (cfr. paragrafo ***62***), a breve termine e per casi specifici, delegazioni di esperti del settore privato e del mondo universitario.

100 Le comunità e civili e della difesa, sia pubbliche che private, risentono dell'assenza di meccanismi di cooperazione efficienti. Fra gli ambiti che pongono problematiche comuni figurano crittografia, sistemi integrati sicuri, individuazione di *malware*, tecniche di simulazione, protezione delle reti e dei sistemi di comunicazione, tecnologie di autenticazione. Promuovere la cooperazione tra civili e militari e sostenere la ricerca e le tecnologie (specie aiutando le PMI) sono due delle priorità del quadro strategico UE in materia di ciberdifesa (aggiornato al 2018).

Spunti di riflessione – Costruire la resilienza

- Come può essere trovato un adeguato equilibrio a livello UE tra, da un lato, l'esigenza di incorporare la politica di cibersicurezza nelle altre politiche e di assicurare un coordinamento efficiente tra i vari attori e, dall'altro, la dispersione delle responsabilità?
- Quanto ben preparate sono le istituzioni ed agenzie dell'UE per il prossimo attacco massiccio che verrà lanciato direttamente contro di loro?
- In che modo è possibile rendere più attraenti per le persone di talento le agenzie dell'UE competenti in materia di cibersicurezza?
- Quali ulteriori misure sono necessarie per garantire per le istituzioni ed agenzie dell'UE una capacità tale da consentire un quadro di valutazione dei rischi e delle minacce coerente?
- In che modo le autorità di vigilanza europee (l'Autorità bancaria europea, l'Autorità europea degli strumenti finanziari e dei mercati e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali) stanno affrontando le ciber-vulnerabilità insite nel settore finanziario e quali insegnamenti possono esser tratti da questo settore a beneficio di altri settori?
- Con la generale carenza di competenze, in che modo l'assistenza tecnica dell'UE alle autorità pubbliche può essere utilizzata al meglio per avere il massimo impatto complessivo nel migliorare la ciberresilienza?
- Come possono l'UE e gli Stati membri assicurare una presenza sensata nei dibattiti internazionali per dar forma alla governance e a standard del ciberspazio e promuovere i valori dell'UE?
- Quali misure di sensibilizzazione a livello UE e di Stati membri (compresi gli sforzi di prevenzione) fanno realmente la differenza e cosa può fare l'UE per innalzarle di livello?
- Di quale ruolo dispone l'UE nel contribuire al conseguimento della diversità di genere nel campo della cibersicurezza?
- In che modo l'UE e gli Stati membri possono potenziare le sinergie tra le comunità civili e di difesa, in linea con il quadro strategico in materia di ciberdifesa (aggiornamento del 2018)?

Rispondere in modo efficace agli incidenti informatici

101 Ideare una risposta efficace ai ciberattacchi è cruciale per fermare la loro progressione il prima possibile. È particolarmente importante che i settori critici, gli Stati membri e le istituzioni dell'UE siano in grado di rispondere in modo celere e coordinato. Una rapida individuazione è essenziale a tal fine.

Sfida n. 9: individuazione e risposta efficaci

Individuazione e notifica

102 Gli strumenti di individuazione comunemente usati aiutano ogni giorno a sconfiggere la maggior parte degli attacchi[151]. Ciononostante, i sistemi digitali sono divenuti così complessi che è impossibile sventarli tutti. Gli attacchi sono talmente sofisticati che spesso si riesce a individuarli solo dopo lunghi periodi di tempo. Gli esperti affermano, dunque, che bisognerebbe concentrarsi sull'individuazione e sulla difesa rapide[152]. Invece, alcuni strumenti di individuazione, quali l'automazione, l'apprendimento automatico (*machine learning*) e l'analisi comportamentale, che mirano a ridurre i rischi e ad analizzare ed apprendere dal comportamento dei sistemi, vengono poco usati, in percentuale, dalle imprese[153]. Ciò è in parte dovuto alla generazione di falsi positivi, per cui attività che non presentano minacce vengono scambiate per attività potenzialmente dannose.

103 Una volta individuata ed analizzata una violazione della sicurezza, è necessario notificarla e segnalarla celermente, in modo che le entità pubbliche e private possano agire in modo preventivo e che le autorità competenti possano aiutare le vittime. Molte organizzazioni sono riluttanti a riconoscere che è avvenuto un ciberincidente e a segnalarlo[154]. Il coinvolgimento, sin dalle prime fasi, delle autorità di contrasto nella risposta iniziale ai presunti ciber-reati è essenziale, così come lo è lo scambio di informazioni con i CSIRT.

104 La precedente mancanza di requisiti UE comuni in tema di notifica degli incidenti rischiava di ritardare la comunicazione delle violazioni della sicurezza e di ostacolare la risposta alle stesse; con l'approvazione della direttiva NIS (cfr. paragrafo ***20***) si è cercato di porvi rimedio. In seguito agli attacchi Wannacry del 2017, la Commissione ha concluso che il sistema della rete di CSIRT "non era ancora

pienamente operativo"[155]. Mentre l'attuazione della direttiva prosegue, resta da vedere se gli orientamenti predisposti dal Gruppo di cooperazione NIS riusciranno a far superare la riluttanza a segnalare gli incidenti[156].

105 A norma della vigente normativa UE, i fornitori di servizi essenziali in alcuni settori sono soggetti a molteplici obblighi di notifica (inclusa quella nei confronti dei consumatori); ciò potrebbe nuocere all'efficienza del processo. Ad esempio, gli operatori nei settori finanziario e bancario sono soggetti a diversi criteri, norme, soglie e tempi di notifica nell'ambito del regolamento generale sulla protezione dei dati, della direttiva NIS, della direttiva sui servizi di pagamento, delle norme sulla BCE/MVU, di quelle su TARGET2 e dell'eIDAS[157]. È quindi importante razionalizzare questi obblighi, poiché tale eterogeneità, oltre a costituire un onere amministrativo non necessario, potrebbe avere come risultato una segnalazione frammentaria.

Risposta coordinata

106 Lo sviluppo di un quadro europeo di cooperazione in caso di crisi di cibersicurezza è ancora in corso. Il relativo "programma"[158] (cfr. paragrafo ***18***) è stato dunque introdotto per inserire una prospettiva di cibersicurezza nel meccanismo integrato di risposta politica alle crisi (IPCR), migliorare la conoscenza situazionale ed assicurare una migliore integrazione con gli altri meccanismi UE di gestione delle crisi[159]. Il suddetto programma coinvolge istituzioni, agenzie e Stati membri dell'UE. Integrare senza soluzione di continuità tutti questi meccanismi di risposta alle crisi è difficoltoso[160]. Anche l'attuale mancanza di una rete comune di comunicazione sicura tra le istituzioni dell'UE costituisce una importante carenza[161].

107 La capacità dell'UE di rispondere a ciberattacchi a livello operativo e politico in caso di incidente trasfrontaliero di vasta scala è stata ritenuta "limitata", in parte perché la cibersicurezza non è ancora integrata negli esistenti meccanismi di coordinamento della risposta alle crisi a livello UE[162]. La direttiva NIS non ha affrontato tale problema.

108 La riforma dell'ENISA proposta di recente, che prevedeva un più esteso ruolo operativo nella gestione degli incidenti di cibersicurezza su vasta scala, non è stata sostenuta dagli Stati membri; questi ultimi preferiscono che il ruolo dell'Agenzia sia di sostegno e affiancamento alla loro azione operativa[163]. Vi sono già molte CERT/CSIRT a livello di Stati membri, ma le loro capacità variano considerevolmente. Ciò costituisce un ostacolo ad un'efficace cooperazione transfrontaliera per le risposte agli incidenti di grande entità[164].

109 Gli auditor della Corte hanno cercato di effettuare una mappatura dei diversi ruoli assegnati ai vari attori individuati nel suddetto programma, ma vi erano lacune che dovranno essere colmate man mano che l'attuazione prosegue. Un ambito inizialmente poco considerato era il far rispettare la normativa, sebbene il protocollo UE di risposta alle emergenze per i servizi di contrasto avesse preso effetto nel dicembre 2018[165]. Far sì che il programma sia pratico e tutte le parti sappiano cosa fare è essenziale affinché abbia successo; a tal fine, negli anni a venire saranno necessari test estesi.

110 La risposta efficace consiste in qualcosa di più che limitare i danni; anche l'assegnazione della responsabilità per gli attacchi è cruciale. Tracciare e individuare gli autori, soprattutto in caso di attacco ibrido, può essere molto difficile, dato il crescente abuso di strumenti di anonimizzazione, criptovalute e cifratura. Tale stato di cose è noto come problema dell'attribuzione della responsabilità. Risolvere detto problema non è solo una questione tecnica; si tratta anche di una sfida per la giustizia penale. Le differenze di ordinamento e di procedura tra un paese e l'altro possono ostacolare le indagini penali ed il perseguimento dei presunti autori. Risolvere il problema dell'attribuzione della responsabilità necessiterà di uno scambio operativo di informazioni più formalizzato, tramite procedure più chiare, ad esempio con Europol o con la rete giudiziaria europea per la criminalità informatica di Eurojust.

111 A livello politico, il pacchetto di strumenti della diplomazia informatica (cfr. ***riquadro 6***) è stato sviluppato al fine di sostenere la risoluzione pacifica delle controversie internazionali nel ciberspazio. La creazione di squadre di risposta rapida ai ciberincidenti e l'iniziativa per l'assistenza reciproca in materia di cibersicurezza sono due progetti, attualmente in corso di sviluppo nel quadro della PESCO, che promuovono una potenziata condivisione delle informazioni[166].

Riquadro 6

Il pacchetto di strumenti della diplomazia informatica

La risposta diplomatica comune dell'UE alle attività informatiche dolose[167], ossia il "pacchetto di strumenti della diplomazia informatica", è scaturita dalle conclusioni del Consiglio del 2015 sulla diplomazia informatica[168]. La diplomazia informatica (o ciberdiplomazia) mira a sviluppare ed attuare un approccio comune e completo al ciberspazio, basato sui valori dell'UE, lo Stato di diritto, il potenziamento delle capacità e i partenariati, la promozione del modello multi-attore della governance di Internet, la riduzione delle minacce di cibersicurezza e l'incremento della stabilità nelle relazioni internazionali.

Tale pacchetto permette all'UE ed ai suoi Stati membri di mettere in atto una risposta diplomatica comune alle attività informatiche dolose facendo pieno uso delle misure previste dalla politica estera e di sicurezza comune. Dette misure possono essere preventive (ad esempio, sensibilizzazione, potenziamento delle capacità), di cooperazione, di stabilizzazione e restrittive (ad esempio, divieti di viaggio, embargo di armi, congelamento di fondi), oppure di sostegno alle risposte degli Stati membri[169]. L'idea è che un'ulteriore cooperazione per ridurre le minacce e la chiara indicazione delle probabili conseguenze di una risposta comune possa (potenzialmente) dissuadere comportamenti aggressivi.

Un'eventuale risposta comune dell'UE alle attività informatiche dolose sarà "proporzionata ad ambito di applicazione, portata, durata, intensità, complessità, sofisticatezza e impatto dell'attività informatica".

Affinché il "pacchetto di strumenti" abbia successo, occorre che i seguenti elementi raggiungano livelli soddisfacenti: l'interconnessione con il programma e con l'IPCR (cfr. paragrafo ***106***), il grado con il quale la conoscenza situazionale viene determinata tramite una rapida e costante condivisione di informazioni (compreso in tema di attribuzione di responsabilità)[170] ed, infine, una cooperazione efficace. Cruciale per un riuscito impiego del pacchetto è anche una comunicazione efficace e coordinata. Fino ad oggi, il pacchetto è stato usato due volte: per iniziare un dialogo con gli Stati Uniti dopo l'attacco *Wannacry*[171] e per redigere conclusioni del Consiglio che condannavano l'uso malevolo delle tecnologie di informazione e comunicazione[172]. Gli sforzi per rendere operativo il pacchetto sono in corso; rimane da vedere quanto efficaci saranno nel conseguire gli obiettivi stabiliti.

Sfida n. 10: proteggere le infrastrutture critiche e le funzioni sociali

Proteggere le infrastrutture

112 Una buona parte delle infrastrutture critiche dell'UE è gestita tramite sistemi di controllo industriali (ICS)[173]. Molti di tali sistemi sono stati concepiti come sistemi a sé stanti, dotati di limitata connettività con il mondo esterno. Quando alcune componenti degli ICS sono state connesse a Internet, questi sono divenuti maggiormente vulnerabili ad interferenze esterne. Effettuare manutenzione e installare *patch* sui sistemi esistenti potrebbe non esser più possibile, ma ammodernarli non è né veloce né economico. Gli sforzi di potenziamento della sicurezza delle infrastrutture critiche devono quindi includere l'ammodernamento degli ICS.

113 Visto che le imprese sono sempre più digitalizzate (fenomeno comunemente noto come "Industria 4.0"), l'impatto di un incidente di grande entità in un settore industriale potrebbe produrre effetti a catena altrove. L'ENISA ha osservato che è importante effettuare una mappatura dell'impatto della mutua dipendenza dei settori critici[174]. Ciò è essenziale per comprendere la potenziale diffusione di un incidente ed è il presupposto di risposte ben coordinate.

114 La direttiva NIS mira a potenziare lo stato di preparazione in settori importanti responsabili delle infrastrutture critiche. Tuttavia, non tutti i settori sono coperti (cfr. ***tabella 1***)[175], il che "riduce l'efficacia della strategia"[176]; desta particolare preoccupazione a riguardo la protezione dell'integrità democratica delle elezioni da interferenze nelle infrastrutture elettorali e dalla disinformazione (cfr. ***riquadro 7***). Oltre ad un riesame della normativa esistente, dunque, una sfida importante sarà stabilire in che modo coinvolgere questi settori in risposte efficaci ad incidenti di grande entità.

115 Le vulnerabilità nelle infrastrutture critiche non si arrestano ai confini dell'Europa. Una particolare sfida per la Commissione consiste nell'esortare i paesi candidati ad adottare i medesimi standard degli Stati membri, ad esempio in ambiti quali la normativa in tema di cibersicurezza o la protezione delle infrastrutture critiche.

Riquadro 7

Proteggere funzioni sociali critiche: *lottare contro le interferenze nelle elezioni*

Nel maggio 2019, circa 400 milioni di elettori si recheranno alle urne per le elezioni del Parlamento europeo, le prime che hanno luogo da quando vige il GDPR. Queste elezioni sono precedute da scandali concernenti l'uso illecito di dati personali per operazioni di *micro-targeting* politico e da campagne coordinate di disinformazione (*fake news*) senza precedenti. La Commissione ha messo in guardia da possibili ciber-interferenze in queste elezioni[177]; combatterle richiederà un approccio esteso a tutta la pubblica amministrazione e a tutta la società.

Infrastrutture elettorali

Organizzare elezioni è complesso, ed assicurare la loro protezione ed integrità spetta agli Stati membri. Le interferenze nelle elezioni e nelle infrastrutture elettorali potrebbero avere come scopo quello di influenzare le preferenze di voto, il risultato dello stesso processo elettorale, compresa l'effettiva votazione, nonché lo scrutinio e la comunicazione dei voti. Per le elezioni del Parlamento europeo, la protezione del cosiddetto "ultimo miglio" (la comunicazione dei risultati dalle capitali nazionali a

Bruxelles) è una sfida particolarmente critica, dato che non esiste nessun approccio di sicurezza comune e che nessun approccio è stato testato a tal fine[178].

Il recente pacchetto elettorale della Commissione comprende misure per potenziare la cibersicurezza elettorale, come la nomina di punti di contatto nazionali per coordinare e scambiare informazioni nei giorni precedenti le elezioni. La condivisione di migliori pratiche e di insegnamenti appresi riveste particolare importanza[179].

I sistemi elettorali non sono ritenuti parte delle infrastrutture critiche[180] e non sono coperti dalla direttiva NIS. Ciononostante, il gruppo di cooperazione NIS ha elaborato orientamenti pratici sulla sicurezza delle tecnologie elettorali, al fine di coadiuvare le autorità pubbliche. I punti di contatto nazionali dovrebbero riunirsi nei primi mesi del 2019[181]. Gli Stati membri sono inoltre invitati a svolgere valutazioni dei rischi di ciberminacce per i rispettivi processi elettorali.

Disinformazione

La disinformazione è un elemento sempre più importante degli attacchi ibridi che comprendono i ciberattacchi e l'intrusione abusiva (*hacking*) nelle reti. Detti attacchi possono essere utilizzati per spaccare la società, coltivare lo scetticismo e minare la fiducia nei processi democratici o in altri temi (ad esempio, campagne contro la vaccinazione, cambiamenti climatici). La disinformazione, cresciuta di scala, in velocità e in portata, costituisce una vera minaccia di sicurezza per l'UE.

L'UE ha adottato una serie di misure per ovviare alla disinformazione. Dal 2015, è stata istituita presso il SEAE la task force "East StratCom" per contrastare le campagne di disinformazione condotte dalla Russia[182]. Gli esperti hanno lodato le attività della task force riguardanti la promozione delle politiche dell'UE, il sostegno ai media indipendenti nei paesi del vicinato e la previsione, tracciatura e contrasto della disinformazione[183]. Ciononostante, le risorse della task force sono limitate se comparate all'entità e alla complessità delle campagne di disinformazione[184]. È necessaria un'interazione maggiormente sistematica con le esistenti strutture dell'UE, nonché una migliore cooperazione in materia di comunicazione strategica[185]. Un nuovo piano d'azione[186] è stato approvato dal Consiglio europeo nel dicembre 2018.

Più di recente, la Commissione, sulla scia della propria comunicazione dell'aprile 2018 sul contrasto alla disinformazione online[187], ha redatto un codice di condotta[188] non vincolante ed autoregolamentato, basato sugli esistenti strumenti d'intervento, al quale hanno aderito le piattaforme online e il settore pubblicitario[189]. Comprende azioni quali contribuire a incrementare l'attendibilità dei contenuti e sostenere gli sforzi per accrescere l'alfabetizzazione mediatica e in materia di notizie. È stata inoltre varata una rete europea indipendente di verificatori (*fact-checkers*).

La Commissione ha affermato che, se il codice di condotta non verrà rispettato, potrebbero seguire ulteriori misure di regolamentazione. Sarà cruciale determinare

l'efficacia delle misure, ed in particolare decidere come misurare i miglioramenti in termini di fiducia, trasparenza e rendicontabilità.

Un'altra sfida consisterà nel trovare modi di migliorare l'individuazione, l'analisi e la denuncia della disinformazione[190]. Sono altresì necessari un monitoraggio ed un'analisi attivi e strategici delle fonti di dati di libero accesso[191]. I tentativi di ottenere una migliore comprensione dell'ambiente delle minacce dovrebbero inoltre coprire le tendenze emergenti, quali i *deepfake* (video falsi creati con l'aiuto dell'intelligenza artificiale e dell'apprendimento profondo (*deep machine learning*)), nonché gli strumenti necessari per individuarli.

Rafforzare l'autonomia

116 L'UE è un importatore netto di prodotti e servizi di cibersicurezza; ciò accresce il rischio di dipendenza tecnologica dagli operatori non-UE, nonché la vulnerabilità nei loro confronti[192]. In particolare, tale stato di cose indebolisce la sicurezza delle infrastrutture critiche dell'UE, che è inoltre sostenuta da complesse reti di approvvigionamento globali. Detto rischio è ulteriormente esacerbato quando operatori non-UE acquistano società europee di cibersicurezza. Spetta agli Stati membri svolgere un controllo degli investimenti diretti esteri ed attualmente non vi è alcun meccanismo di controllo a livello UE[193].

117 Una maggiore autonomia strategica è un obiettivo enunciato sia nella strategia globale dell'UE in materia di politica estera e di sicurezza sia nella comunicazione del 2017 su *Resilienza, deterrenza e difesa*[194]. Ovviare alla miriade di problematiche e sfide illustrate nel presente documento di riflessione contribuirà a potenziare questa desiderata autonomia. Nessuna singola misura vi riuscirà da sola.

Spunti di riflessione – Una risposta efficace

- In che modo la direttiva NIS ha migliorato la notifica dei ciberincidenti nei settori critici e negli altri settori?
- In che misura le istituzioni dell'UE stanno internalizzando il coordinamento della risposta alle crisi in caso di grave ciberincidente?
- In che modo la ciberdiplomazia può svolgere un ruolo più incisivo nelle azioni esterne dell'UE?
- Le attuali strutture e azioni dell'UE di contrasto alla disinformazione sono proporzionate alla dimensione e alla complessità del problema?

Osservazioni conclusive

118 Negli ultimi anni, l'UE e gli Stati che ne fanno parte hanno portato alla ribalta la cibersicurezza per migliorare la ciberresilienza complessiva. Tuttavia, conseguire un più elevato livello di cibersicurezza nell'UE continua ad essere un'impresa monumentale. Nel presente documento di riflessione, la Corte ha cercato di evidenziare alcune delle principali problematiche e sfide per l'ambizione che l'UE ha di diventare l'ambiente digitale più sicuro del mondo.

119 Dall'analisi svolta risulta che è necessario passare ad una cultura della performance, che integri pratiche di valutazione, per assicurare una **rendicontabilità e** una **valutazione** che abbiano senso. **Permangono** alcune **lacune nella normativa e le norme esistenti non sono recepite in modo uniforme dagli Stati membri** Ciò può rendere difficile il dispiegamento del pieno potenziale della normativa. Un'altra problematica individuata concerne l'**allineamento tra i livelli di investimento e gli obiettivi strategici**: è necessario incrementare i livelli d'investimento e l'impatto degli stessi. Ciò risulta più arduo quando l'UE e i suoi Stati membri non dispongono di una **chiara visione d'insieme della spesa UE** in cibersicurezza. Vi sono anche indizi di **scarsa adeguatezza delle risorse assegnate alle agenzie dell'UE operanti nei settori rilevanti per la cibersicurezza**; dette agenzie hanno anche difficoltà ad attrarre e trattenere persone di talento.

120 Gli studi disponibili concludono che **la governance della cibersicurezza può essere rafforzata** per incrementare la capacità della comunità globale di rispondere ai ciberattacchi e agli incidenti. Al tempo stesso, impedire tutti gli attacchi è impossibile. Pertanto una **rapida azione di individuazione e risposta** e la **protezione delle infrastrutture critiche e delle funzioni sociali**, insieme a un migliore **scambio di informazioni e** a un miglior **coordinamento** tra il settore pubblico e quello privato rappresentano sfide cruciali da vincere. Infine, la crescente carenza globale di competenze in materia di cibersicurezza significa che anche **l'accrescimento delle competenze e la sensibilizzazione** in tutti i settori e livelli della società rappresenta una sfida vitale.

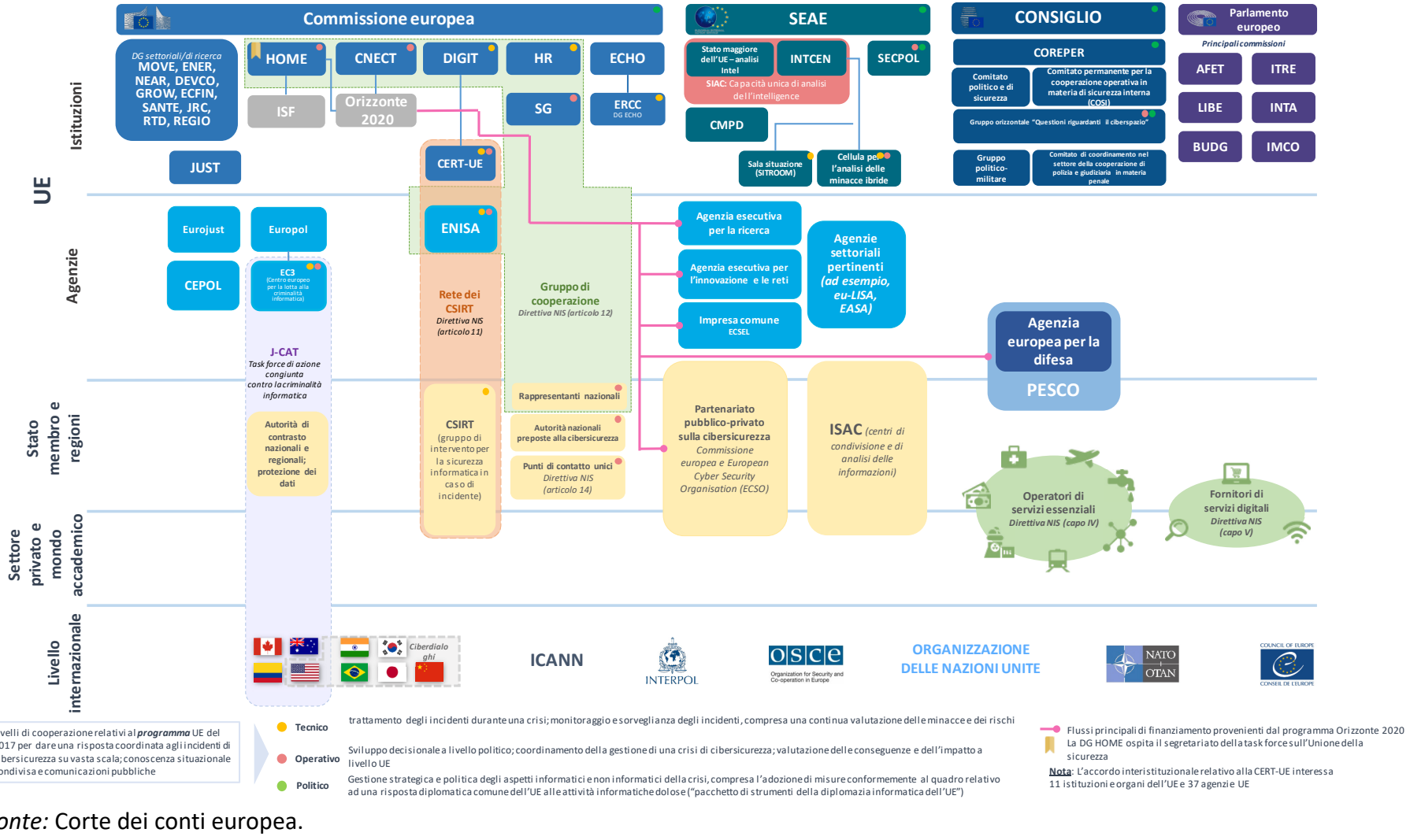
121 Queste sfide poste dalle minacce informatiche cui sono confrontati l'UE e il più ampio contesto mondiale necessitano di un impegno indefesso e di un'adesione piena e costante ai valori dell'UE.

Il presente documento di riflessione è stato adottato dalla Sezione III nella riunione del 14 febbraio 2019.

Per la Corte dei conti europea

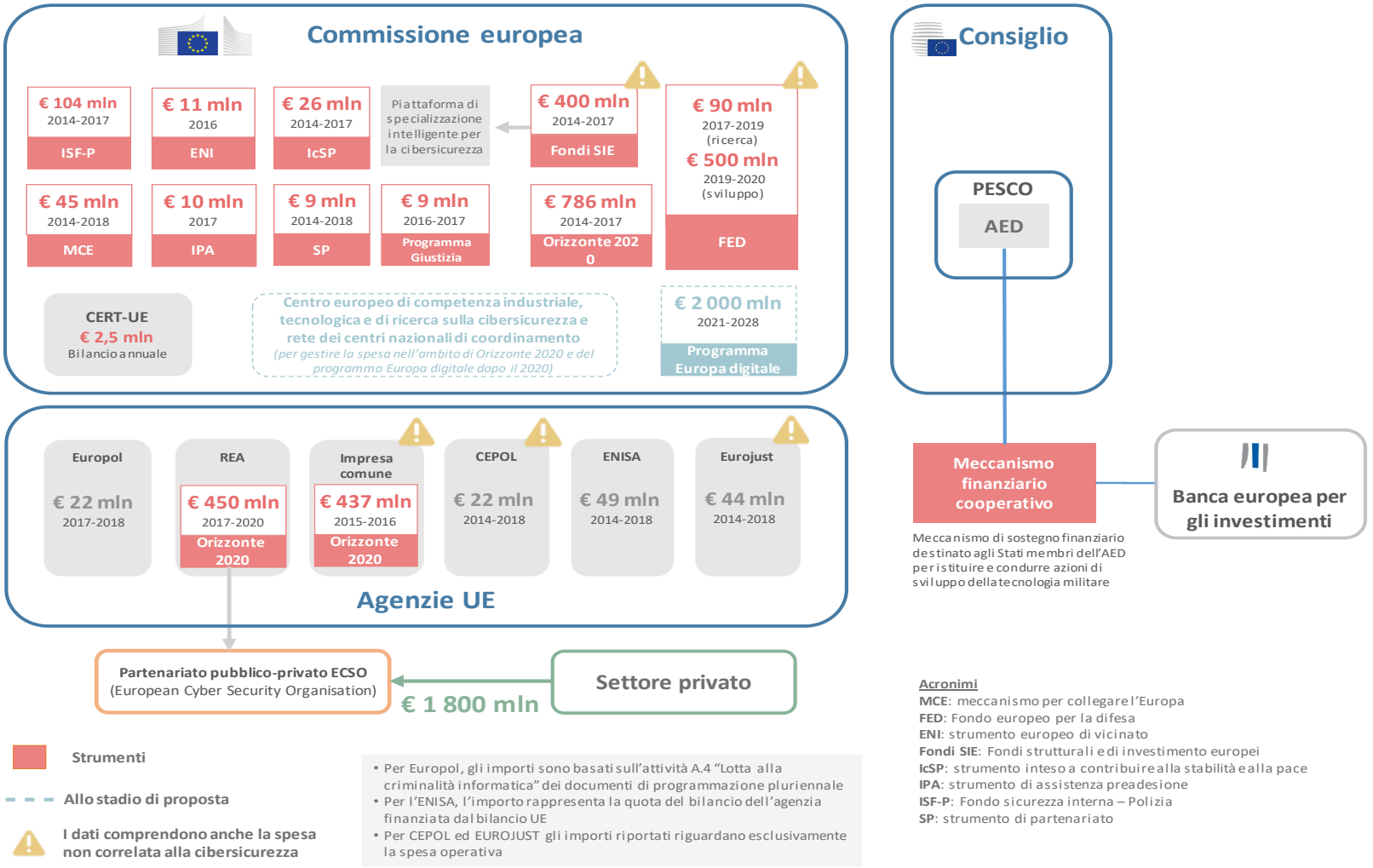
Klaus-Heiner Lehne
Presidente

Allegato I — Un panorama complesso e stratificato, con molti attori



Fonte: Corte dei conti europea.

Allegato II — Spesa dell'UE per la cibersicurezza dal 2014



Fonte: Corte dei conti europea, sulla base di documenti della Commissione europea e delle agenzie dell'UE.

Allegato III — Relazioni delle istituzioni superiori di controllo degli Stati membri dell'UE

Tipo	Titolo (con link)	Anno	Stato membro
Audit di conformità	Nota di valutazione del controllo interno	2014	FR
	Relazione di certificazione dei conti del regime generale di previdenza sociale (difesa, esteri)	2016	FR
	Certificazione dei conti dello Stato	2016	FR
	Assicurare la sicurezza e la preservazione delle banche dati nazionali estoni di importanza critica	Finalizzato nel 2018 / non ancora pubblicato	EE
	Efficacia dei controlli interni nella protezione dei dati personali nelle banche dati nazionali	2008	EE
Controlli di gestione (rapporto benefici/costi)	Report to the Public Accounts Committee on mitigation of cyber attacks	2013	DK
	Information security in the civil public administration (RiR 2014:23)	2014	SE
	Report on the government's processing of confidential data on persons and companies	2014	DK
	Update on the National Cyber Security Programme	2014	UK
	Relazione alla commissione Bilancio del Parlamento federale tedesco presentata in virtù del § 88, paragrafo 2, del Codice del bilancio federale (BHO) – Consolidamento IT, Governo federale	2015	DE
	Report on access to IT systems that support the provision of essential services to Danish society	2015	DK
	Plaine de France, Autorità di pianificazione pubblica	2015	FR
	"The cyber security environment in Lithuania" testo completo in lingua lituana sintesi tradotta in lingua inglese	2015	LT
	Svolgimento dei compiti di cibersisurezza da parte degli organismi pubblici in Polonia (in lingua polacca)	2015	PL
	Cybercrime – police and prosecutors can be more efficient (RiR 2015:21)	2015	SE
	Digital Skills Gap in Government (Sondaggio)	2015	UK
	Relazione al Parlamento federale dal titolo: "Perception des droits de succession par le SPF Finances"	2016	BE
	Report on management of IT security in systems outsourced to external suppliers	2016	DK
	Relazione di audit dell'attività creditizia dell'Istituto di credito ufficiale, esercizio 2016	2016	ES
	Steering of the Government Security Network	2016	FI
	Assicurare la sicurezza dei sistemi IT usati per compiti pubblici	2016	PL
	Prevenzione e lotta contro il ciberbullismo tra minori e giovani	2016	PL

Tipo	Titolo (con link)	Anno	Stato membro
	Information security work at nine agencies – un altro audit sulla sicurezza delle informazioni presso lo Stato svedese. (RiR 2016:8)	2016	SE
	Protecting Information across government	2016	UK
	Report on the protection of IT systems and health data in three Danish regions	2017	DK
	Nota sulle risultanze dell'audit cooperativo internazionale "Efficacia dei controlli interni ai fini della protezione dei dati personali nelle banche dati nazionali"	2017	EE
	Cyber protection arrangements	2017	FI
	Steering of the operational reliability of electronic services	2017	FI
	Rete delle *Chambres d'agriculture* (sintesi)	2017	FR
	Rapport d'observations definitives sur la gestion de la chambre de commerce et d'industrie de Vaucluse (redatto dalla *Chambre régionale des comptes Provence-Alpes-Côte d'Azur*)	2017	FR
	Assicurare la sicurezza e la preservazione delle banche dati nazionali estoni di importanza critica	Finalizzato nel 2018 / non ancora pubblicato	EE
	"Sviluppo delle infrastrutture elettroniche di comunicazione dello Stato" testo completo in lingua lituana sintesi tradotta in lingua inglese	2017	LT
	Information Technology Audit: Cyber Security across Government Entities	2017	MT
	Il sistema dei registri nazionali: sicurezza, performance ed usabilità	2017	PL
	WannaCry cyber attack and the NHS	2017	UK
	Online Fraud	2017	UK
	Report on protection against ransomware attacks	2018	DK
	Centre hospitalier d'Arpajon (redatto dalla *Chambre régionale des comptes Île-de-France*)	2018	FR
	"Gestione delle risorse informative statali critiche"	2018	LT
	"Ciber-reati"	2019	LT
	Sicurezza delle informazioni in Polonia	2019	PL
Altro	Banca dati degli organismi pubblici	n.d.	BE
	Questionario sulla politica in tema di sicurezza e di analisi dei rischi (in corso)	n.d.	BE

Acronimi e abbreviazioni

AED: Agenzia europea per la difesa

AEV: autorità europea di vigilanza

CERT -UE: squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee

Corte: Corte dei conti europea

cPPP: partenariato pubblico-privato contrattuale

CSIRT: gruppo di intervento per la sicurezza informatica in caso di incidente

DDoS: attacco distribuito di negazione del servizio

DG CNECT: direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie

DG HOME: direzione generale della Migrazione e degli affari interni

DG JUST: direzione generale della Giustizia e dei consumatori

DIGIT: direzione generale dell'Informatica

Direttiva NIS: direttiva sulla sicurezza delle reti e dell'informazione

EC3: Centro europeo per la lotta alla criminalità informatica (presso Europol)

ECSEL: componenti e sistemi elettronici per la leadership europea

ECSM: mese europeo della sensibilizzazione in tema di cibersicurezza

ECSO: organizzazione europea per la cibersicurezza

ENISA: Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione

Fondi SIE: Fondi strutturali e di investimento europei

GDPR: regolamento generale sulla protezione dei dati

HWPCI: Gruppo orizzontale "Questioni riguardanti il ciberspazio"

IDE: investimento diretto estero

ISF – Polizia: Fondo sicurezza interna – Polizia

ISSB: Comitato direttivo per la sicurezza dell'informazione

JRC: Centro comune di ricerca

LISO: responsabile della sicurezza informatica a livello locale

NAO: *National Audit Office* (istituzione superiore di controllo nazionale)

NCIRC: capacità di reazione della NATO in caso di incidente informatico

PED: programma Europa digitale

PESCO: cooperazione strutturata permanente

PMI: piccole e medie imprese

PSDC: politica di sicurezza e di difesa comune

SCI: sistemi di controllo industriali

SEAE: Servizio europeo per l'azione esterna

UE: Unione europea

Glossario

Adware*: *malware che mostra banner pubblicitari o finestre *pop-up* che includono linee di codice per tracciare il comportamento online delle vittime.

Attacco distribuito di negazione del servizio (DDoS): ciberattacco che impedisce agli utenti che ne hanno titolo di accedere ad un servizio o ad una risorsa online, inondandolo/a con un numero di richieste superiore a quelle che può gestire.

Ciberattacco: tentativo di compromettere o distruggere la riservatezza, l'integrità e la disponibilità dei dati o di un sistema computerizzato attraverso il ciberspazio.

Cibercriminalità: varie attività criminali che coinvolgono computer e sistemi informatici, o come strumento o come bersaglio primario. Fra dette attività figurano: reati tradizionali (ad esempio, frode, falsificazione e furto di identità); reati connessi ai contenuti (ad esempio, distribuzione online di materiale pedopornografico o incitamento all'odio razziale); reati propri ai sistemi computerizzati e informativi (ad esempio, attacchi contro sistemi informativi, attacchi mirati alla negazione del servizio e *malware*).

Ciberdifesa: sottoinsieme della cibersicurezza; mira a difendere il ciberspazio tramite mezzi militari ed altri mezzi, al fine di conseguire obiettivi strategico-militari.

Ciberincidente o incidente informatico: evento che danneggia o minaccia, direttamente o indirettamente, la resilienza e la sicurezza di un sistema informatizzato e dei dati da questo trattati, immagazzinati o trasmessi.

Ciberresilienza: capacità di prevenire, prepararsi a, sopportare e rimettersi a seguito di ciberattacchi o ciberincidenti.

Cibersicurezza: il complesso di tutele e misure adottate per difendere i sistemi informativi e i relativi dati da accessi non autorizzati, attacchi e danni al fine di assicurare la riservatezza, l'integrità e la disponibilità di tali sistemi e dati.

Ciberspazio: ambiente mondiale immateriale nel quale si verificano le comunicazioni online tra persone, software e servizi tramite reti di computer e dispositivi tecnologici.

Cifratura: trasformazione di informazioni leggibili in codice illeggibile, al fine di proteggerle. Per poter leggere le informazioni, l'utente deve avere accesso ad una chiave o a una password segreta.

Contenuto digitale: qualunque dato (testi, suono, immagini o video) immagazzinato in formato digitale.

Criptovaluta: bene digitale emesso e scambiato usando tecniche di cifratura, in modo indipendente da una banca centrale. Viene accettato come mezzo di pagamento dai membri di una comunità virtuale.

Dati di accesso: informazioni sull'attività di autenticazione (*log-in*) e di disconnessione (*log-out*) che un utente compie per accedere ad un servizio; tali informazioni comprendono l'orario, la data e l'indirizzo IP.

Dati personali: informazioni relative ad un individuo identificabile.

Disinformazione: informazioni che è possibile identificare come false o informazioni fuorvianti concepite, presentate e diffuse a scopo di lucro o per ingannare intenzionalmente il pubblico, e che possono arrecare un pregiudizio pubblico.

Disponibilità: garanzia di accesso tempestivo e attendibile alle informazioni e relativo impiego.

Ecosistema cibernetico: insieme complesso di dispositivi, dati, reti, persone, processi ed organizzazioni interagenti, assieme all'ambiente dei processi e delle tecnologie che influenzano e sostengono queste interazioni.

Gestione della vulnerabilità: parte integrante della sicurezza informatica e della sicurezza delle reti, che mira a mitigare in modo proattivo o a prevenire lo sfruttamento di vulnerabilità del sistema o del software tramite la loro individuazione, classificazione e eliminazione.

Hacktivista: individuo o gruppo di individui che accede senza autorizzazione a sistemi informativi o reti al fine di promuovere fini sociali o politici.

Infrastruttura critica: risorse, servizi e strutture fisici la cui interruzione o distruzione avrebbe un impatto grave sul funzionamento dell'economia e della società.

Infrastruttura elettorale: comprende i sistemi informatici e le banche dati per le campagne, le informazioni sensibili sui candidati, la registrazione dei votanti e i sistemi di gestione.

Ingegneria sociale: nella sicurezza delle informazioni, manipolazione psicologica per indurre con l'inganno le vittime a intraprendere un'azione o a divulgare informazioni riservate.

Installazione di *patch*: introduzione di un insieme di modifiche al software, al fine di aggiornarlo, di correggere errori, di migliorarlo; comprende l'eliminazione di vulnerabilità relative alla sicurezza.

Integrità: la tutela dalla modifica impropria delle informazioni o dalla loro distruzione, a garanzia della loro autenticità.

Internet degli oggetti: rete di oggetti quotidiani dotati di sistemi elettronici, software e sensori in modo da poter comunicare e scambiare dati via Internet.

Kit per *exploit*: un tipo di insieme di strumenti che i cibercriminali utilizzano per sfruttare vulnerabilità in reti e sistemi informativi in modo da installare *malware* o svolgere altre attività dolose.

***Malware*:** software scritto con intento malevolo (detto anche "software malevolo", "software dannoso" o "software doloso"); programma informatico concepito per danneggiare un computer, un server o una rete.

Minaccia ibrida: intento ostile espresso da parte di avversari mediante l'impiego contemporaneo di tecniche di guerra convenzionale e non convenzionale (ossia mezzi militari, politici, economici e tecnologici) al fine di perseguire con la forza i loro obiettivi.

Modello di attività criminale come servizio (Caas): modello di business criminale che muove l'economia digitale sommersa, fornendo un'ampia gamma di servizi e di strumenti che consente a cibercriminali non specializzati, di basso livello, di commettere atti di cibercriminalità.

Nuvola informatica (*cloud computing*): prestazione, su richiesta, di risorse informatiche (quali archiviazione, potenza di calcolo o capacità di condivisione dei dati) attraverso Internet, tramite *hosting* su server remoti.

***Phishing*:** invio di messaggi di posta elettronica che paiono provenire da un mittente fidato allo scopo di ingannare i destinatari e far sì che clicchino su link malevoli o condividano informazioni personali.

***Ransomware*:** *malware* che impedisce l'accesso delle vittime a un sistema informativo computerizzato o che rende illeggibili i file, in genere mediante cifratura. L'autore dell'attacco poi di solito ricatta la vittima, richiedendo il pagamento di un riscatto per ripristinare l'accesso.

Reato dipendente dall'informatica: reato che può essere commesso unicamente usando dispositivi informatici.

Reato favorito dall'informatica: reato tradizionale commesso su scala più ampia utilizzando sistemi informatici.

Rete zombie (*botnet*): rete di computer infettati da *malware* e controllati a distanza, senza che gli utenti ne siano consapevoli, per inviare messaggi di posta elettronica indesiderati, sottrarre informazioni o lanciare ciberattacchi coordinati.

Riservatezza: protezione delle informazioni, dei dati o dei beni da accessi o divulgazione non autorizzati.

Servizio fiduciario: servizio che rafforza la validità giuridica di una transazione elettronica, come firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato e autenticazione di siti Internet.

Sicurezza delle informazioni: insieme di processi e strumenti che tutelano i dati fisici e digitali dall'accesso, utilizzo, divulgazione, interruzione, modifica, registrazione o distruzione non autorizzati.

Sicurezza delle reti: sottoinsieme della cibersicurezza che protegge i dati inviati tramite dispositivi sulla stessa rete, per impedire che le informazioni vengano intercettate o modificate.

Sistema *legacy* un sistema, un'applicazione o un linguaggio di programmazione obsoleto o non aggiornato che è ancora in uso, ma per il quale gli aggiornamenti e l'assistenza tecnica del venditore, compresa l'assistenza relativa alla sicurezza, potrebbero non essere disponibili.

***Skimming*:** furto dei dati della carta di credito o di debito quando vengono inseriti online.

Vettorializzazione del testo: conversione di parole, frasi o interi documenti in vettori numerici che possono essere utilizzati da algoritmi di apprendimento automatico (*machine-learning*).

***Wiper*:** tipo di *malware* concepito per cancellare tutto il contenuto del disco duro del computer infettato.

[1] Nella proposta di regolamento dell'UE sulla cibersicurezza, questa è stata definita come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, i loro utenti e le persone interessate dalle minacce informatiche". Il regolamento dovrebbe essere adottato dal Parlamento europeo e dal Consiglio agli inizi del 2019.

[2] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2017*.

[3] European Cyber Security Organisation (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, giugno 2016.

[4] Parlamento europeo, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, studio per la commissione LIBE, settembre 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18 gennaio 2018.

[6] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*.

[7] Europol, *già citato*, 2018.

[8] European Centre for International Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper n. 2/18, febbraio 2018.

[9] Commissione europea, discorso del Presidente sullo Stato dell'Unione 2017.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, comunicato stampa, 25 aprile 2018.

[11] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2017*.

[12] Scheda informativa della Commissione europea sulla cibersicurezza, settembre 2017.

[13] Nei costi rientrano: mancati introiti; costi per la riparazione dei sistemi danneggiati; potenziali responsabilità per informazioni o beni rubati; incentivi versati per mantenere la clientela; premi assicurativi maggiorati; maggiori costi di protezione (nuovi sistemi, assunzioni, corsi di formazione); potenziale liquidazione di spese per la messa a norma o la composizione di controversie.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] Il *ransomware* "Wannacry" ha sfruttato vulnerabilità del protocollo di Microsoft Windows consentendo l'appropriazione a distanza di qualsiasi computer. Una volta scoperta la vulnerabilità, la Microsoft ha diffuso una *patch*. Ciò nonostante, centinaia di migliaia di computer non erano stati ancora aggiornati e molti di questi sono stati in seguito infettati. Fonte: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19 dicembre 2017.

[16] Commissione europea, *Europeans' attitudes towards cybersecurity*, Eurobarometro, numero speciale 464a, settembre 2017. A inizio 2019 dovrebbe essere pubblicata un'indagine di follow-up.

[17] La convenzione di Budapest, un orientamento internazionale vincolante per i paesi che legiferano contro la criminalità informatica, fornisce un quadro di riferimento per la

cooperazione tra le parti nazionali. L'UE è attualmente rappresentata da Commissione, Consiglio dell'Unione europea, Europol, ENISA e Eurojust.

[18] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza:un ciberspazio aperto e sicuro*, JOIN(2013) 1 *final*, 7 febbraio 2013.

[19] Commissione europea, *Agenda europea sulla sicurezza*, COM(2015) 185 *final* del 28 aprile 2015.

[20] Commissione europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 *final* del 6 maggio 2015.

[21] SEAE, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, giugno 2016.

[22] Centro per gli studi politici europei, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, novembre 2018.

[23] Il *malware* utilizzato per sferrare l'attacco "Wannacry", attribuito alla Corea del Nord da Stati Uniti, Regno Unito e Australia, è stato sviluppato in origine e tesaurizzato dall'Agenzia statunitense per la sicurezza nazionale al fine di sfruttare le vulnerabilità di Windows. Fonte: A. Greenberg, già citato, WIRED, 19 dicembre 2017. All'indomani degli attacchi, Microsoft ha condannato la tesaurizzazione delle vulnerabilità dei software da parte dei governi e ha ribadito la necessità di una Convenzione di Ginevra digitale, che ha sollecitato.

[24] In aggiunta a terra, mare, aria e spazio.

[25] Quadro strategico dell'UE in materia di ciberdifesa (aggiornato nel 2018), 14413/18, 19 novembre 2018.

[26] Commssione europea/Servizio europeo per l'azione esterna, *Quadro congiunto per contrastare le minacce ibride – La risposta dell'Unione europea*, JOIN(2016) 18 *final*, 6 aprile 2016.

[27] Dichiarazione congiunta del Presidente del Consiglio europeo, del Presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico, 8 luglio 2016 e 10 luglio 2018.

[28] Commissione europea/Servizio europeo per l'azione esterna, *Resilienza, deterrenza e difesa:verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 *final*, 13 settembre 2017.

[29] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

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

[31] Questi sono integrati in strutture di cooperazione stabilite dalla direttiva, la rete dei CSIRT (una rete costituita dai CSIRT designati dagli Stati membri dell'UE e dalla CERT-UE; l'ENISA ospita il segretariato) e nel gruppo di cooperazione (che assiste e facilita la cooperazione strategica e lo scambio di informazioni tra Stati membri; la Commissione ne ospita il segretariato).

[32] 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) (GU L 119 del 4.5.2016, pag. 1).

[33] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")*, COM(2017) 477 *final*/3 del 13 settembre 2017.

[34] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 *final* del 17 aprile 2018.

[35] Commissione europea, *Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, COM(2018) 226 *final* del 17 aprile 2018.

[36] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento*, COM(2018) 630 *final* del 12 settembre 2018.

[37] H. Carrapico and A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, vol. 55, n. 6, 2017.

[38] Commissione europea, già citato, SWD(2017) 295 *final* del 13 settembre 2017.

[39] Servizio Ricerca del Parlamento europeo, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, dicembre 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27 novembre 2014.

[41] Un'eccezione è rappresentata dall'articolo 14 ("Monitoraggio e statistiche") della direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio

[42] Comitato economico e sociale europeo, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, marzo 2018. Task force CEPS-ECRI, Cybersecurity in Finance: Getting the policy mix right!, giugno 2018.

[43] All'indagine della Corte hanno risposto 24 istituzioni superiori di controllo su 28.

[44] Ossia basato su princìpi e quanto più neutro possibile sotto il profilo tecnologico.

[45] Meccanismo di consulenza scientifica della Commissione europea, Scientific Opinion 2/2017, 24 marzo 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, settembre 2018. European Centre for Political Economy, già citato, Occasional Paper No 2/18, febbraio 2018.

[47] Commissione europea, *Proposta di direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale*, COM(2015) 634 *final* del 9 dicembre 2015.

[48] Commissione europea, *Proposta di direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di vendita online e di altri tipi di vendita a distanza di beni*, COM(2017) 635 *final* del 9 dicembre 2015.

[49] Cyber Security Council dei Paesi Bassi, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, giugno 2018.

[51] Commissione europea, *Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*, COM(2017) 476 *final* del 4 ottobre 2017.

[52] Europol, già citato, 2017.

[53] Consiglio dell'Unione europea, *Relazione finale del settimo ciclo di valutazioni reciproche "Attuazione pratica e funzionamento delle politiche europee in materia di prevenzione e lotta alla criminalità informatica"*, 12711/1/17 REV 1, 9 ottobre 2017.

[54] Commissione europea, *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment*, SWD/2017/0298 *final* del 13 settembre 2017. Nel dicembre 2018 è stato raggiunto un accordo politico sulla nuova normativa, che dovrebbe essere adottata agli inizi del 2019.

[55] Europol, già citato, 2017.

[56] C-362/14: Maximillian Schrems/Data Protection Commissioner (Irlanda), 6 ottobre 2015.

[57] Europol/Eurojust, *Common challenges in combatting cybercrime*, documento 7021/17 del 13 marzo 2017.

[58] Commissione europea, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 *final* del 13 settembre 2017.

[59] Servizio Ricerca del Parlamento europeo, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, *PE589.832*.

[60] Risoluzione del Parlamento europeo, *Diritti umani e tecnologia: impatto dei sistemi di sorveglianza e di individuazione delle intrusioni sui diritti umani nei paesi terzi*, (2014/2232(INI)), 8 settembre 2015. I beni e servizi a duplice uso, tra cui software e tecnologia, possono trovare un'applicazione civile e militare.

[61] Le informazioni di dominio pubblico sono memorizzate nella banca dati WHOIS, gestita dalla Internet Corporation for Assigned Names and Numbers (ICANN). L'ICANN cura il sistema dei nomi di dominio. L'uso improprio dei nomi di dominio agevola la criminalità informatica.

[62] Articolo 3 della direttiva NIS, già citata.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10 settembre 2015.

[64] The White House, *Cybersecurity spending fiscal year 2019*.

[65] Commissione europea, *Commission Staff Working Document: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'*, SWD(2018) 305 *final* del 6 giugno 2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, dicembre 2016.

[67] Commissione europea, già citato, COM(2018) 630 *final* del 12 settembre 2018.

[68] Servizio Ricerca del Parlamento europeo – Unità Prospettiva scientifica, *Achieving a sovereign and trustworthy ICT industry in the EU*, dicembre 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31 luglio 2017.

[70] Servizio Ricerca del Parlamento europeo – Unità Prospettiva scientifica, già citato, dicembre 2017.

[71] Già citato.

[72] Commissione europea, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 *final* (parte 1/4) del 12 settembre 2018.

[73] Commissione europea, già citato, COM(2018) 630 *final* del 12 settembre 2018.

[74] Relazione speciale n. 13/2018 della Corte dei conti europea, intitolata: "Lotta alla radicalizzazione che sfocia in atti terroristici".

[75] Le cifre riportate in questa sezione sono tratte da documenti della Commissione di pubblico dominio, eccetto per i 42 milioni di euro di cui al paragrafo ***51***, dei quali la Corte è stata informata direttamente dalla Commissione.

[76] Orizzonte 2020 è il programma da 80 miliardi di euro di ricerca e innovazione dell'UE e sostiene l'Unione dell'innovazione, che mira ad assicurare la competitività globale dell'UE.

[77] Orizzonte 2020, sfida per la società n. 7: "Società sicure – proteggere la libertà e la sicurezza dell'Europa e dei suoi cittadini".

[78] Gli auditor della Corte hanno analizzato i progetti di Orizzonte 2020 tramite l'insieme di dati CORDIS. Hanno effettuato una vettorializzazione del testo della descrizione di ciascun progetto, utilizzando la tassonomia di cibersicurezza del JRC (cfr. ***riquadro 5***), al fine di individuare progetti che erano verosimilmente connessi alla cibersicurezza. Hanno poi controllato manualmente i risultati e li hanno analizzati.

[79] European Cyber Security Organisation, *ECS cPPP Progress Monitoring Report 2016-2017*, 29 ottobre 2018.

[80] Articolo 9, paragrafo 2, della direttiva NIS, già citata.

[81] L'azione globale contro la cibercriminalità plus (GLACY+) è un progetto congiunto con in Consiglio d'Europa. Sostiene 12 paesi in Africa, nella regione Asia-Pacifico, in America Latina e nei Caraibi, i quali a loro volta fungono da poli di condivisione delle esperienze nell'ambito delle rispettive regioni.

[82] Il Centro europeo di strategia politica (EPSC), il think-tank della Commissione, ha osservato che vi è il rischio che sorga un "buco nero digitale" se il divario tra l'UE ed i paesi vicini dei Balcani occidentali continuerà a crescere. Paesi come la Cina e la Russia stanno investendo somme notevoli nella regione, dove si rischia che l'UE in quanto ciber-attore risulti marginalizzata. Fonte: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17 maggio 2018.

[83] Banca europea per gli investimenti, *The EIB Group Operating Framework and Operational Plan 2018*, 12 dicembre 2017. Al momento della stesura del presente documento non erano disponibili ulteriori informazioni.

[84] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il programma Europa digitale per il periodo 2021-2027*, COM(2018) 434 *final* del 6 giugno 2018.

[85] Commissione europea, *Regolamento (UE) 2018/1092 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che istituisce il programma europeo di sviluppo del settore industriale della difesa, volto a sostenere la competitività e la capacità di innovazione dell'industria della difesa dell'Unione* (GU L 200 del 7.8.2018, pag. 30). In aggiunta, nel 2017 è stata istituita un'azione preparatoria sulla ricerca in materia di difesa, finanziata da Orizzonte 2020 e ammontante in totale a 90 milioni di euro per il 2017-2019. Non è chiaro se questo importo includa spese in materia di cibersicurezza.

[86] La Corte prevede di pubblicare nel 2019 un distinto documento di riflessione sulla difesa dell'UE.

[87] L'EC3 di Europol, l'ENISA, il SEAE, l'Agenzia europea per la difesa e la CERT-UE contano, insieme, 159 effettivi. Questo totale non include il personale addetto alla cibersicurezza presso la Commissione europea o negli Stati membri. Fonte: Centro per gli studi politici europei, documento già citato, novembre 2018.

[88] Cfr. *ENISA evaluation*, 2017.

[89] Nel proprio piano pluriennale 2018-2020, Europol ha richiesto un aumento annuo del proprio organico di 70 agenti temporanei; tuttavia, per il 2018 ne sono stati approvati solo 26. Nella bozza del prossimo piano pluriennale per il 2019-2021, Europol ha previsto un modesto incremento, ipotizzando che una più grande richiesta di risorse non sarebbe stata approvata. Fonte: *Consultation on draft Multiannual Programming 2019-2021*, presentato al gruppo di controllo parlamentare congiunto, A 000834, 1° febbraio 2018.

[90] Cfr. *ENISA evaluation*, 2017. Tra il 2014 e il 2016, circa l'80 % del bilancio operativo dell'ENISA è stato usato per appaltare studi.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, dicembre 2017.

[92] ISACA (precedentemente nota come "Information Systems Audit and Control Association"), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2ª edizione, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, pag 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth?Understanding the true costs and impact of cybersecurity programs*, luglio 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21 febbraio 2018.

[96] Un forum per la cooperazione tra l'Autorità bancaria europea, l'Autorità europea degli strumenti finanziari e dei mercati e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali.

[97] Autorità europea degli strumenti finanziari e dei mercati, *Joint Committee report on risks and vulnerabilities in the EU financial system*, aprile 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, dicembre 2015.

[99] Riferendosi agli Stati membri dell'UE, il meccanismo di consulenza scientifica della Commissione ha osservato il sostanziale ed univoco livello di consenso su princìpi e valori fondamentali, nonché un interesse strategico condiviso che può essere al cuore di una efficace governance della cibersicurezza nell'UE. Fonte: Commissione europea, Gruppo ad alto livello di consulenti scientifici, Parere scientifico 2/2017, 24 marzo 2017.

[100] Con Stati Uniti, Cina, Giappone, Corea del Sud, India e Brasile.

[101] T. Renard e A. Barrinha, *"The EU as a partner in cyber diplomacy and defence"*, in Accademia europea per la sicurezza e la difesa, *Handbook on cyber security*, 23 novembre 2018, capitolo 3.4.

[102] Consiglio dell'Unione europea, *Piano d'azione per l'attuazione delle conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio:"Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"*, 15748/17 del 12 dicembre 2017.

[103] Commissione europea, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 *final*, 21 novembre 2018.

[104] Risposta della commissaria Gabriel all'interrogazione parlamentare scritta E-004294-17 del 28 giugno 2017.

[105] Consiglio dell'Unione europea, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, documento 15870/17 del 19 dicembre 2017.

[106] Le decisioni (UE, Euratom) 2015/443, 2015/444 e 2017/46 disciplinano la sicurezza dei sistemi di comunicazione e informazione della Commissione. La decisione della Commissione

C(2018) 7706 del 21 novembre 2018 istituisce un Comitato direttivo sulle tecnologie dell'informazione e sulla cibersicurezza (*Information Technology and Cybersecurity Board*) risultante dalla fusione del precedente comitato per le tecnologie dell'informazione (*IT Board*) e del precedente Comitato direttivo per la sicurezza dei sistemi informativi (*Information System Security Steering Board*).

[107] Comitato economico e sociale europeo, *documento già citato*, marzo 2018.

[108] Parlamento europeo, *documento già citato*, settembre 2015.

[109] La "cellula dell'UE per l'analisi delle minacce ibride" è stata creata nel 2016 in seno al Centro UE di situazione e di *intelligence* del SEAE. Riceve ed analizza informazioni, sia classificate che da fonti pubbliche, provenienti da vari soggetti e riguardanti le minacce ibride.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, novembre 2013.

[111] Commissione europea, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 *final* (Parte 1/6), 13 settembre 2017.

[112] Commissione europea, già citato, SWD(2018) 403 *final* del 12 settembre 2018.

[113] Si tratta del centro di coordinamento di rete RIPE (*Résaux IP Européens*), ossia del registro regionale di Internet per l'Europa, che sovraintende all'assegnazione e alla registrazione delle risorse di numeri Internet.

[114] ENISA, *EISAS Large-Scale Pilot – Collaborative Awareness Raising for EU Citizens & SMEs*, novembre 2012.

[115] Center for Cyber Safety and Education, in partenariato con Booz Allen Hamilton, Alta Associates e Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Comitato economico e sociale europeo, *documento già citato*, marzo 2018.

[117] Camera dei Lord, Camera dei Comuni, *Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*, 16 luglio 2018.

[118] Europol/Eurojust, *Common challenges in combatting cybercrime*, documento 7021/17 del 13 marzo 2017.

[119] Europol/Eurojust, già citato, documento7021/17 del 13 marzo 2017.

[120] Commissione europea, già citato, SWD(2018) 403 *final* del 12 settembre 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, 20 novembre 2018.

[122] Ad esempio, la cooperazione tra il SEAE, gli Stati membri, le agenzie e gli organismi quali CEPOL, ECTEG o AESD.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, dicembre 2017.

[124] Gruppo europeo di formazione e istruzione in materia di criminalità informatica.

[125] Commissione europea, "Tredicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza", COM(2018) 46 *final* del 24 gennaio 2018.

[126] Sulla base delle osservazioni contenute nella Relazione speciale n. 14/2018, già citata.

[127] Risoluzione del Parlamento europeo del 13 giugno 2018 sulla ciberdifesa (2018/2004(INI)). Consiglio dell'Unione europea, già citato, documento 15870/17 del 19 dicembre 2017.

[128] Svizzera, Macedonia del Nord, Ucraina, Bosnia-Erzegovina, Kosovo (tale designazione non pregiudica le posizioni riguardo allo status ed è in linea con la risoluzione 1244 (1999) dell'UNSC e con il parere della CIG sulla dichiarazione di indipendenza del Kosovo), Turchia e Stati Uniti.

[129] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*.

[130] Commissione europea, già citato, SWD(2017) 295 *final* del 13 settembre 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman e S. Furman, *Security Fatigue*, "IT Professional", vol. 18, n. 5, 2016, pagg. 26-32. Cfr. anche questa pagina del sito del National Institute of Standards and Technology (NIST).

[132] Commissione europea/Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Comunicazione congiunta al Parlamento europeo e al Consiglio,*Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride*, JOIN (2018) 16 *final* del 13 giugno 2018.

[133] Ad esempio, la chiusura di AlphaBay e di Hansa a seguito di operazioni congiunte dirette dall'FBI e dalla polizia olandese con l'assistenza di Europol. Si trattava dei più grandi mercati per la commercializzazione di beni illeciti quali medicinali, armi da fuoco e strumenti di criminalità informatica, come il *malware*. Fonte: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, comunicato stampa del 29 maggio 2018.

[134] Commissione europea, già citato, SWD(2018) 403 *final* del 12 settembre 2018.

[135] Consiglio dell'Unione europea, già citato, documento 12711/1/17 REV 1 del 9 ottobre 2017.

[136] Commissione europea, già citato, SWD(2017) 295 *final* del 13 settembre 2017.

[137] Commissione europea/Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Comunicazione congiunta al Parlamento europeo e al Consiglio, già citata, JOIN(2018) 16 *final* del 13 giugno 2018.

[138] Commissione europea, SWD(2017) 500 *final* del 13 settembre 2017.

[139] *Memorandum d'intesa tra l'ENISA, l'AED, l'EC3 di Europol e la CERT-UE*, 23 maggio 2018.

[140] Commissione europea, bando di gara *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27 ottobre 2017.

[141] Jean-Claude Juncker, *Mission letter for the Commissioner for the Security Union*, 2 agosto 2016. La difesa non rientra nel mandato della task force.

[142] Consiglio dell'Unione europea, *EU cybersecurity roadmap*, documento 8901/17 dell'11 maggio 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues, 5ª edizione*, novembre 2017.

[144] JRC Technical Reports, *European Cybersecurity Centres of Expertise Map: Definitions and Taxonomy. Impact Assessment* sulle proposte concernenti il centro europeo di ricerca e di competenza sulla cibersicurezza e la rete di centri nazionali di coordinamento, SWD(2018) 403 *final* del 12 settembre 2018.

[145] Commissione europea, già citato, SWD(2017) 295 *final* del 13 settembre 2017.

[146] Commissione europea, già citato, SWD(2018) 403 *final* del 12 settembre 2018.

[147] Ad esempio, l'ISAC delle istituzioni finanziarie europee include rappresentanti del settore finanziario, delle CERT nazionali, delle autorità di contrasto, dell'ENISA, dell'Europol, della Banca centrale europea, del Consiglio europeo per i pagamenti e della Commissione europea.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14 febbraio 2018.

[149] Consiglio dell'Unione europea, già citato, documento 12711/1/17 REV 1 del 9 ottobre 2017.

[150] https://www.europol.europa.eu/empact.

[151] Da uno studio condotto nel 2018 da Accenture in 15 paesi è emerso che l'87 % dei ciberattacchi mirati venivano sventati; cfr. *Gaining Ground on the Cyber Attacker – 2018 State of Cyber Resilience*, 10 aprile 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Oxford University Politics Blog, 14 settembre 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14 luglio 2017.

[154] Comitato economico e sociale europeo, *già citato*, marzo 2018.

[155] Commissione europea, *Ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza*, COM(2017) 354 *final* del 29 giugno 2017.

[156] Cfr. le varie pubblicazioni del Gruppo di cooperazione NIS.

[157] PSD2: seconda direttiva sui servizi di pagamento; BCE/MVU: Banca centrale europea/Meccanismo di vigilanza unico; TARGET2: sistema di trasferimento espresso transeuropeo automatizzato di regolamento lordo in tempo reale (seconda generazione); eIDAS: regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Fonte: Task force CEPS-ECRI, documento già citato, giugno 2018.

[158] Commissione europea, *Raccomandazione della Commissione del 13.9.2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala*, C(2017) 6100 *final* del 13 settembre 2017.

[159] Commissione europea, già citato, SWD(2017) 295 *final* del 13 settembre 2017. Vi sono numerosi meccanismi di gestione delle crisi, tra i quali il meccanismo integrato di risposta politica alle crisi (IPCR), il meccanismo di risposta alle crisi della Commissione (Argus), il

meccanismo di risposta alle crisi del SEAE, il meccanismo di protezione civile dell'UE e il protocollo UE di risposta alle emergenze per i servizi di contrasto.

[160] Inoltre, ciò potrebbe anche indurre ad invocare l'articolo 42, paragrafo 7, del Trattato sull'Unione europea (clausola di assistenza reciproca) o l'articolo 222 del Trattato sul funzionamento dell'Unione europea (clausola di solidarietà).

[161] Commissione europea/Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Comunicazione congiunta al Parlamento europeo e al Consiglio, già citata, JOIN(2018) 16 *final* del 13 giugno 2018. Nel dicembre 2018, i media hanno segnalato presunti atti di pirateria informatica ai danni della COREU, la rete di comunicazioni diplomatiche del SEAE (fonte: New York Times, *, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*, 18 dicembre 2018. La questione è attualmente oggetto di indagine.

[162] Anche la cooperazione in materia di allarmi preventivi e assistenza reciproca necessita di essere ulteriormente sviluppata; cfr. *Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, documento 10086/18 del 26 giugno 2018.

[163] Servizio Ricerca del Parlamento europeo, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, settembre 2018.

[164] Comitato economico e sociale europeo, *documento già citato*, marzo 2018.

[165] Consiglio dell'Unione europea, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, documento 14893/18 del dicembre 2018.

[166] "Gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza"; "piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti informatici". Fonte: Consiglio dell'Unione europea, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19 novembre 2018.

[167] Consiglio dell'Unione europea, Progetto di conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica"), documento 9916/17 del 7 giugno 2017.

[168] Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla diplomazia informatica*, documento 6122/15 dell'11 febbraio 2015.

[169] Consiglio dell'Unione europea, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, documento 13007/17.

[170] Attribuire la responsabilità di un incidente rimane una decisione politica sovrana degli Stati membri e non tutte le misure del pacchetto necessitano che essa venga attribuita.

[171] L'utilizzo del pacchetto non ha condotto ad un'azione comune; singoli Stati membri hanno adottato la posizione degli Stati Uniti.

[172] Consiglio dell'Unione europea, *Conclusioni del Consiglio sulle attività informatiche dolose*, documento 7925/18 del 16 aprile 2018.

[173] Sistemi computerizzati usati per controllare i processi in vari settori, quali il settore dei servizi di pubblica utilità, il settore manifatturiero chimico e industriale, quello della trasformazione degli alimenti, quello dei sistemi e dei poli di trasporto e quello dei servizi logistici.

[174] ENISA, già citato, dicembre 2017.

[175] Ad esempio, amministrazione pubblica, industrie chimiche e nucleari, settore manifatturiero, lavorazione degli alimenti, turismo, logistica e protezione civile.

[176] Commissione europea, già citato, SWD(2017) 295 *final* del 13 settembre 2017.

[177] Discorso della commissaria Jourová alla sessione plenaria del Parlamento europeo, *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign*, 14 novembre 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23 maggio 2018.

[179] L. Past, "Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses", in: Commissione europea, Centro europeo di strategia politica, *Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts*, 2018.

[180] Secondo la direttiva 2008/114/CE del Consiglio relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

[181] Commissione europea, Raccomandazione della Commissione del 12.9.2018 relativa alle reti di cooperazione in materia elettorale, alla trasparenza online, alla protezione dagli incidenti di cibersicurezza e alla lotta contro le campagne di disinformazione nel contesto delle elezioni del Parlamento europeo, C(2018) 5949 *final* del 12 settembre 2018.

[182] Conclusioni del Consiglio europeo, documento EUCO 11/15 del 20 marzo 2015. Da allora si sono aggiunte altre due task force, una per i Balcani occidentali e l'altra per il vicinato meridionale.

[183] Una relazione dell'Atlantic Council esortava l'UE ad obbligare tutti gli Stati membri ad inviare esperti nazionali alla task force. Cfr. D. Fried e A. Polyakova, *Democratic Defense Against Disinformation*, 5 marzo 2018.

[184] In origine non disponeva di una propria dotazione finanziaria; nel 2018 le sono stati assegnati 1,1 milioni di euro dal Parlamento europeo per una azione preparatoria "StratCom Plus".

[185] E. Brattberg, T. Maurer, Carnegie Endowment for International Peace, già citato, 23 maggio 2018.

[186] Commissione europea, Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, *Piano d'azione contro la disinformazione*, JOIN(2018) 36 *final*. Detto piano è incentrato sugli aspetti seguenti: migliorare le capacità delle istituzioni dell'UE di individuare, analizzare e denunciare la disinformazione; potenziare risposte coordinate e comuni alla disinformazione; mobilitare il settore privato; sostenere azioni di sensibilizzazione e rafforzare la resilienza sociale.

[187] Commissione europea, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 *final* del 26 aprile 2018.

[188] Da non confondersi con il codice di condotta per contrastare l'illecito incitamento all'odio online.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, aprile 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* aprile 2018.

[191] C. Frutos López, *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, in Centro europeo di strategia politica, già citato, 2018.

[192] Commissione europea, già citato, SWD(2018) 403 *final* del 12 settembre 2018.

[193] La proposta di regolamento (COM(2017) 487 *final*, del 13 settembre 2017) sul controllo degli investimenti esteri diretti, presentata nel settembre 2017, segue attualmente la procedura legislativa. Riguarda in modo specifico le tecnologie critiche, fra le quali figurano l'intelligenza artificiale, la cibersicurezza e le applicazioni a duplice uso.

[194] Commissione europea/Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Comunicazione congiunta al Parlamento europeo e al Consiglio, già citata, JOIN(2017) 450 *final* del 13 settembre 2017.

Équipe della Corte dei conti europea

Il presente documento di riflessione, intitolato *Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza*, è stato adottato dalla Sezione di audit III della Corte (competente per l'audit della spesa per azioni esterne, sicurezza e giustizia), presieduta da Bettina Jakobsen, Membro della Corte. I lavori sono stati diretti da Baudilio Tomé Muguruza, Membro della Corte, coadiuvato da: Daniel Costa de Magalhaes, capo di Gabinetto, e Ignacio Garcia de Parada, attaché di Gabinetto; Alejandro Ballester-Gallardo, primo manager; Michiel Sweerts, capoincarico; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha, auditor, e Johannes Bolkart, tirocinante. Hannah Critoph ha fornito l'assistenza linguistica.

Da sinistra a destra: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

CORTE
DEI CONTI
EUROPEA

Ufficio delle pubblicazioni

CORTE DEI CONTI EUROPEA
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Modulo di contatto: eca.europa.eu/it/Pages/ContactForm.aspx
Sito Internet: eca.europa.eu
Twitter: @EUAuditors