COMMISSIONE
EUROPEA

ALTO RAPPRESENTANTE
DELL'UNIONE PER
GLI AFFARI ESTERI E
LA POLITICA DI SICUREZZA

Bruxelles, 16.12.2020
JOIN(2020) 18 final

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

La strategia dell'UE in materia di cibersicurezza per il decennio digitale

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

La strategia dell'UE in materia di cibersicurezza per il decennio digitale

I. INTRODUZIONE: CIBERSICUREZZA DELLA TRASFORMAZIONE DIGITALE IN UN AMBIENTE CARATTERIZZATO DA MINACCE COMPLESSE

La cibersicurezza è parte integrante della sicurezza degli europei. Che si tratti di utilizzare dispositivi connessi o reti elettriche, oppure di usufruire dei servizi di banche, trasporti aerei, amministrazioni pubbliche o ospedali i cittadini devono avere la garanzia di essere protetti dalle minacce informatiche. L'economia, la democrazia e la società dell'UE dipendono, ora più che mai, da strumenti digitali e connettività sicuri e affidabili. La cibersicurezza è quindi fondamentale per creare un'Europa digitale, verde e resiliente.

I trasporti, l'energia e la sanità, le telecomunicazioni, la finanza, la sicurezza, i processi democratici, lo spazio e la difesa dipendono fortemente da sistemi informativi e di rete sempre più interconnessi. Le interdipendenze intersettoriali sono molto forti poiché, a loro volta, le reti e i sistemi informativi dipendono per il loro funzionamento da una fornitura costante di energia elettrica. I dispositivi connessi superano già il numero delle persone sul pianeta, e si prevede che il loro numero salirà a 25 miliardi entro il 2025[1]: un quarto di questi si troverà in Europa. La digitalizzazione dei modelli di lavoro è stata accelerata dalla pandemia di COVID-19, durante la quale il 40 % dei lavoratori all'interno dell'Unione è passato al telelavoro, con probabili ripercussioni permanenti sulla vita quotidiana[2]. Ciò aumenta le vulnerabilità agli attacchi informatici[3]. I dispositivi connessi vengono spesso inviati al consumatore con vulnerabilità note, il che amplia ulteriormente la superficie di attacco per le attività informatiche dolose[4]. Il panorama industriale dell'UE è sempre più digitalizzato e connesso e ciò comporta anche che gli attacchi informatici abbiano un impatto sulle industrie e gli ecosistemi di gran lunga superiore rispetto al passato.

Il panorama delle minacce è aggravato dalle tensioni geopolitiche riguardanti la rete Internet globale e aperta e il controllo delle tecnologie lungo l'intera catena di

[1] Stime dell'associazione internazionale dei gestori di telefonia mobile (GSMA); https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). L'International Data Corporation prevede 42,6 miliardi di macchine, sensori e telecamere connessi; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Secondo un'indagine condotta nel giugno 2020, il 47 % dei dirigenti aziendali ha dichiarato l'intenzione di consentire ai dipendenti di lavorare a distanza a tempo pieno anche quando diventerà nuovamente possibile ritornare sul proprio luogo di lavoro; l'82 % intendeva consentire il lavoro da remoto almeno per una parte del tempo; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Mirai, ad oggi uno dei malware più dannosi, ha creato botnet di oltre 600 000 dispositivi che hanno perturbato il funzionamento di vari siti Internet di rilievo in Europa e negli Stati Uniti.

approvvigionamento[5]. Tali tensioni si riflettono sul numero crescente di Stati nazionali che erigono frontiere digitali. Le limitazioni di Internet e su Internet minacciano il ciberspazio aperto e globale, nonché lo Stato di diritto, i diritti fondamentali, la libertà e la democrazia, ossia i valori chiave dell'UE. Il ciberspazio è sempre più sfruttato a fini politici e ideologici e la crescente polarizzazione a livello internazionale ostacola un multilateralismo efficace. Le minacce ibride combinano campagne di disinformazione con attacchi informatici alle infrastrutture, ai processi economici e alle istituzioni democratiche, e possono potenzialmente causare danni fisici, ottenere accesso illegale ai dati personali, carpire segreti industriali o di Stato, diffondere sfiducia e indebolire la coesione sociale. Queste attività mettono a repentaglio la sicurezza e la stabilità internazionali nonché i benefici che il ciberspazio offre allo sviluppo economico, sociale e politico.

Gli attacchi dolosi a infrastrutture critiche rappresentano un importante rischio globale[6]. Internet presenta un'architettura decentrata priva di struttura centrale e una governance multipartecipativa ed è riuscita a sostenere un aumento esponenziale dei volumi di traffico, pur essendo un bersaglio costante di tentativi dolosi di perturbazione[7]. Nel contempo si fa sempre più affidamento sulle funzioni principali di un'Internet globale e aperta, quale il sistema dei nomi di dominio (DNS), nonché i servizi Internet essenziali per comunicazioni e hosting, applicazioni e dati. Questi servizi sono sempre più concentrati nelle mani di poche imprese private[8], rendendo l'economia e la società europea vulnerabili a eventi geopolitici o tecnici destabilizzanti che incidono sul nucleo di Internet o su una o più di queste imprese. L'aumento dell'uso di Internet e i cambiamenti dovuti alla pandemia hanno messo ulteriormente in luce la fragilità delle catene di approvvigionamento che dipendono da questa infrastruttura digitale.

Le preoccupazioni in materia di sicurezza rappresentano un importante disincentivo all'uso di servizi online[9]**.** Circa i due quinti degli utenti UE hanno sperimentato problemi riguardanti la sicurezza e tre quinti si reputano incapaci di proteggersi di fronte alla criminalità informatica[10]. Negli ultimi tre anni, un terzo degli utenti ha ricevuto e-mail o telefonate fraudolente in cui si richiedevano dati personali; tuttavia l'83 % di questi non ha

[5] Compresi componenti elettronici, analisi dei dati, cloud, reti più veloci e più intelligenti con il 5G e oltre, crittografia, intelligenza artificiale (IA), nonché nuovi e affidabili paradigmi di calcolo e di elaborazione dati come blockchain, cloud-to-edge e calcolo quantistico.

[6] Forum economico mondiale, "Global Risks Report 2020".

[7] Secondo l'Organizzazione per la cooperazione e lo sviluppo economici la pandemia ha comportato un aumento del 60 % del traffico Internet; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. L'Organismo dei regolatori europei delle comunicazioni elettroniche e la Commissione pubblicano regolarmente relazioni sullo stato della capacità di Internet durante l'applicazione delle misure di confinamento per coronavirus. Secondo una relazione pubblicata dall'ENISA, nel terzo trimestre del 2019 si è riscontrato un aumento del 241 % del numero totale di attacchi distribuiti di negazione del servizio (DDos) rispetto al terzo trimestre del 2018. Gli attacchi DDoS stanno aumentando di intensità: il più grande attacco di sempre si è verificato nel febbraio 2020, con un traffico di picco di 2,3 terabit al secondo. Durante l'interruzione di Internet dovuta a CenturyLink, verificatasi nel mese di agosto 2020, un problema di routing nel fornitore di servizi Internet statunitense ha portato a un crollo del 3,5 % del traffico web globale; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8] Internet Society, "The Global Internet Report: Consolidation in the Internet Economy"; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/.

[9] https://data.europa.eu/euodp/it/data/dataset/S2249_92_2_499_ENG.

[10] Indice di digitalizzazione dell'economia e della società 2020; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

mai denunciato reati informatici. Un'impresa su otto è stata oggetto di attacchi informatici[11]. Oltre la metà dei personal computer aziendali e di consumo che sono stati infettati da malware una volta, vengono reinfettati entro lo stesso anno[12]. Centinaia di milioni di record di dati vengono persi ogni anno a causa di violazioni dei dati; nel 2018 il costo medio di una violazione nei confronti di una singola impresa è aumentato fino a superare i 3,5 milioni di EUR[13]. Spesso è impossibile isolare l'impatto di un attacco informatico, che può innescare reazioni a catena nell'intera economia e società ripercuotendosi su milioni di individui[14].

Le indagini su quasi tutti i tipi di reato hanno una componente digitale. Nel 2019 il numero di incidenti segnalati su base annuale è triplicato. Si stima che vi siano 700 milioni di nuovi esemplari di malware, il mezzo utilizzato più di frequente per agevolare un attacco informatico[15]. Si stima che nel 2020 il costo annuale della criminalità informatica per l'economia mondiale sia stato pari a 5 500 miliardi di EUR, il doppio rispetto al 2015[16]. Esso rappresenta il più ingente trasferimento di ricchezza economica della storia, maggiore anche di quello risultante dal commercio mondiale di sostanze stupefacenti. Per un incidente grave come l'attacco ransomware WannaCry del 2017 si stima che il costo per l'economia mondiale sia stato di oltre 6,5 miliardi di EUR[17].

I servizi digitali e il settore finanziario, unitamente al settore pubblico e manifatturiero, sono tra i bersagli più frequenti degli attacchi informatici; eppure la preparazione e la consapevolezza informatiche delle imprese e dei singoli individui rimangono scarse[18] e tra i lavoratori si riscontra una grave carenza di competenze in materia di cibersicurezza[19]. Nel 2019 si sono verificati quasi 450 incidenti connessi alla cibersicurezza che hanno coinvolto infrastrutture essenziali europee come il settore della finanza e dell'energia[20]. Le organizzazioni sanitarie e i professionisti del settore sono stati colpiti in modo particolarmente duro durante la pandemia. Poiché la tecnologia diventa inscindibile dal mondo fisico, gli attacchi informatici mettono a rischio le vite e il benessere dei soggetti più vulnerabili[21]. Oltre due terzi delle imprese, in particolare le PMI, sono considerate dei "principianti" nel campo della cibersicurezza e le imprese europee sono considerate meno

[11] Conferenza stampa di Eurostat, "ICT security measures taken by vast majority of enterprises in the EU", 6/2020 - 13 gennaio 2020. "Gli attacchi informatici alle infrastrutture essenziali sono diventati la nuova normalità in settori come l'energia, l'assistenza sanitaria e i trasporti"; WEF, "The Global Risks Report 2020".
[12] Fonte: Comparitech.
[13] "Annual Cost of a Data Breach Report", 2020 Ponemon Institute e, sulla base dell'analisi quantitativa di 524 recenti violazioni in 17 aree geografiche e 17 diversi settori: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.
[14] Relazione del Centro comune di ricerca (JRC), "Cybersecurity, our digital anchor"; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor
[15] Fonte: AV-TEST, https://www.av-test.org/en/statistics/malware/.
[16] JRC, "Cybersecurity – Our Digital Anchor".
[17] Fonte: Cyence.
[18] La consapevolezza delle imprese resta scarsa, soprattutto tra le PMI, anche in relazione al furto informatico dei segreti commerciali; PwC, "Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets", 2018.
[19] Cfr. "ENISA Threat Landscape 2020" e anche "Verizon Data Breach Investigations Report 2020"; https://enterprise.verizon.com/resources/reports/dbir/
[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.
[21] Il ransomware è stato utilizzato per accedere a ospedali e cartelle cliniche, ad esempio in Romania (giugno 2020), a Düsseldorf (settembre 2020) e Vastaamo (ottobre 2020).

preparate di quelle asiatiche e americane[22]. Si stima che circa 291 000 posti di lavoro per professionisti della cibersicurezza in Europa restino vacanti. L'assunzione e la formazione di esperti in materia di cibersicurezza richiedono tempo e questo comporta maggiori rischi di cibersicurezza per le organizzazioni[23].

L'Unione europea è priva di consapevolezza situazionale collettiva in materia di minacce informatiche. Questo perché le autorità nazionali non prevedono la raccolta e la condivisione sistematiche di informazioni, come quelle disponibili nel settore privato, che potrebbero aiutare a valutare lo stato della cibersicurezza all'interno dell'UE. Gli Stati membri segnalano solo una parte degli incidenti e la condivisione delle informazioni non è né sistematica né completa[24]; gli attacchi informatici possono essere solo una faccia degli attacchi dolosi concertati compiuti contro le società europee. Attualmente l'assistenza operativa reciproca tra gli Stati membri è limitata e non esiste alcun meccanismo operativo tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE in caso di crisi o incidenti informatici transfrontalieri su larga scala[25].

Migliorare la cibersicurezza è pertanto di fondamentale importanza affinché le persone possano fidarsi, fare uso e beneficiare delle innovazioni, della connettività e dell'automazione, come pure per salvaguardare i diritti e le libertà fondamentali, compresi i diritti alla riservatezza e alla protezione dei dati personali nonché la libertà di espressione e di informazione. La cibersicurezza è indispensabile alla connettività di rete e all'Internet globale e aperta che devono essere alla base della trasformazione dell'economia e della società negli anni 2020. La cibersicurezza contribuisce a migliorare e aumentare i posti di lavoro e a rendere i luoghi di lavoro più flessibili, i trasporti e l'agricoltura più efficienti e sostenibili e l'accesso ai servizi sanitari più semplice ed equo. Conformemente al Green Deal europeo[26], la cibersicurezza è inoltre essenziale per la transizione verso un'energia più pulita, attraverso reti transfrontaliere e contatori intelligenti, evitando inutili duplicazioni nell'archiviazione dei dati. La cibersicurezza è infine di importanza fondamentale per la sicurezza e la stabilità internazionali e per lo sviluppo delle economie, delle democrazie e delle società a livello globale. È pertanto necessario che governi, imprese e singoli individui utilizzino gli strumenti digitali in modo responsabile e attento alla sicurezza. La consapevolezza in materia di cibersicurezza e l'igiene informatica devono essere alla base della trasformazione digitale delle attività quotidiane.

La nuova strategia dell'UE in materia di cibersicurezza per il decennio digitale rappresenta una componente chiave del documento "Plasmare il futuro digitale dell'Europa"[27], del piano per la ripresa europea[28] della Commissione, della strategia per l'Unione della sicurezza 2020-2025[29], della strategia globale per la politica estera e di sicurezza dell'Unione europea[30] e

[22] PwC, "The Global State of Information Security", 2018; ESI Thoughtlab, "The Cybersecurity Imperative", 2019.
[23] Agenzia dell'Unione europea per la cibersicurezza, "Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database", dicembre 2019.
[24] Gli Stati membri sono tenuti a fornire al gruppo di cooperazione una relazione sintetica annuale sulle notifiche ricevute a norma dell'articolo 10, paragrafo 3, della direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva (UE) 2016/1148).
[25] Sono in atto procedure operative standard per la mutua assistenza tra i membri della rete di CSIRT.
[26] Il Green Deal europeo, COM(2019) 640 final.
[27] Plasmare il futuro digitale dell'Europa, COM(2020) 67 final.
[28] Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione, COM(2020) 98 final.
[29] La strategia dell'UE per l'Unione della sicurezza 2020-2025, COM(2020) 605 final.

dell'agenda strategica del Consiglio europeo 2019-2024[31]. La strategia definisce in che modo l'UE proteggerà i cittadini, le imprese e le istituzioni dalle minacce informatiche, promuoverà la cooperazione internazionale e contribuirà a garantire un'Internet globale e aperta.

II. PENSARE IN OTTICA GLOBALE, AGIRE A LIVELLO EUROPEO

La presente strategia è volta ad assicurare un'Internet globale e aperta, con forti linee guida per affrontare i rischi per la sicurezza e per i diritti e le libertà fondamentali dei cittadini europei. Sulla scorta dei progressi conseguiti con le strategie precedenti, contiene proposte concrete per l'attuazione di **tre strumenti principali – normativi, di investimento e politici –** per **tre settori di intervento dell'UE: 1) resilienza, sovranità tecnologica e leadership, 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta e 3) promozione di un ciberspazio globale e aperto.** L'UE è impegnata a sostenere questa strategia attraverso un **livello di investimenti senza precedenti nella transizione digitale dell'UE per i prossimi sette anni**, potenzialmente quadruplicando i livelli precedenti nell'ambito delle nuove politiche tecnologiche e industriali e dell'agenda per la ripresa[32].

La cibersicurezza deve essere integrata in tutti questi investimenti digitali, in particolare le tecnologie chiave come l'intelligenza artificiale (IA), la crittografia e il calcolo quantistico, utilizzando incentivi, obblighi e parametri di riferimento. Ciò può stimolare la crescita del settore europeo della cibersicurezza fornendo le certezze necessarie a facilitare la graduale eliminazione dei sistemi legacy. Il Fondo europeo per la difesa (FED) sosterrà le soluzioni europee in materia di ciberdifesa all'interno della base industriale e tecnologica europea riguardante la difesa. La cibersicurezza è inclusa negli strumenti finanziari esterni a sostegno dei nostri partner, in particolare lo strumento di vicinato, cooperazione allo sviluppo e cooperazione internazionale. La prevenzione dell'abuso tecnologico, la protezione delle infrastrutture essenziali e la garanzia dell'integrità delle catene di approvvigionamento permettono inoltre all'UE di conformarsi alle norme, alle regole e ai principi di comportamento responsabile degli Stati dell'ONU[33].

1. RESILIENZA, SOVRANITÀ TECNOLOGICA E LEADERSHIP

Le infrastrutture chiave e i servizi essenziali dell'UE sono sempre più interdipendenti e digitalizzati. Tutti gli elementi connessi a Internet nell'UE, che si tratti di automobili automatizzate, sistemi di controllo industriale o elettrodomestici, e l'intera catena di approvvigionamento che li rende disponibili, devono essere sicuri fin dalla progettazione, resilienti agli incidenti informatici e, nel caso vengano scoperte delle vulnerabilità, queste devono poter essere corrette rapidamente. Questi aspetti sono fondamentali per dare al settore pubblico e privato dell'UE la possibilità di scegliere le infrastrutture e i servizi più sicuri. Il prossimo decennio rappresenta l'opportunità per l'UE di guidare lo sviluppo di tecnologie

[30] https://eeas.europa.eu/topics/eu-global-strategy_en.
[31] https://www.consilium.europa.eu/it/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#.
[32] Gli investimenti nell'intera catena di approvvigionamento digitale, che contribuiscono alla transizione digitale o ad affrontare le sfide che ne derivano, dovrebbero ammontare almeno al 20 %, pari a 134,5 miliardi di EUR, dei 672,5 miliardi di EUR del dispositivo per la ripresa e la resilienza sotto forma di sovvenzioni e prestiti. Nell'ambito del quadro finanziario pluriennale 2021-2027 sono previsti finanziamenti dell'UE per la cibersicurezza a titolo del programma Europa digitale, nonché per la ricerca sulla cibersicurezza a titolo di Orizzonte Europa, con particolare attenzione al sostegno alle PMI, per un totale che potrebbe ammontare complessivamente a 2 miliardi di EUR, cui si aggiungeranno gli investimenti degli Stati membri e dell'industria.
[33] https://undocs.org/A/70/174.

sicure lungo l'intera catena di approvvigionamento. Garantire la resilienza e il rafforzamento delle capacità industriali e tecnologiche nel campo della cibersicurezza dovrebbe mobilitare tutti i necessari strumenti normativi, di investimento e politici. La cibersicurezza fin dalla progettazione per i processi, le operazioni e i dispositivi industriali può mitigare i rischi, ridurre potenzialmente i costi per le imprese, come pure per la società in senso lato, aumentandone pertanto la resilienza.

1.1 Infrastruttura resiliente e servizi critici

Le **norme UE in materia di sicurezza delle reti e dei sistemi informativi (NIS)** sono al centro del mercato unico per la cibersicurezza. La Commissione propone di riformare queste regole nell'ambito di una direttiva NIS riveduta per aumentare il livello di **ciberresilienza di tutti i settori pertinenti, pubblici e privati, che svolgono una funzione importante per l'economia e la società**[34]**.** La revisione è necessaria per ridurre le incoerenze nel mercato interno allineando i requisiti riguardanti l'ambito di applicazione, la sicurezza e la segnalazione degli incidenti nonché la vigilanza e l'applicazione a livello nazionale e le capacità delle autorità competenti.

La riforma della direttiva NIS fornirà le basi per norme più specifiche, necessarie anche per i settori strategicamente importanti, compresi quelli dell'energia, dei trasporti e della sanità. Al fine di garantire un approccio coerente, come annunciato nell'ambito della strategia per l'Unione della sicurezza 2020-2025, la riforma della direttiva è proposta congiuntamente a una revisione della legislazione in materia di resilienza delle infrastrutture critiche[35]. Le tecnologie nel settore dell'energia che integrano componenti digitali e la sicurezza delle catene di approvvigionamento associate sono importanti per assicurare la continuità dei servizi essenziali e il controllo strategico delle infrastrutture energetiche critiche. La Commissione proporrà pertanto l'adozione, entro la fine del 2022, di misure comprendenti un "codice di rete" che stabilisca regole per la cibersicurezza dei flussi transfrontalieri di energia elettrica. Come proposto dalla Commissione[36], il settore finanziario deve inoltre rafforzare la resilienza operativa digitale e garantire la capacità di resistere a tutti i tipi di perturbazioni e minacce legate alle TIC. Per quanto riguarda il settore dei trasporti, la Commissione ha aggiunto disposizioni in materia di cibersicurezza[37] alla legislazione dell'UE sulla sicurezza dell'aviazione e continuerà ad adoperarsi per migliorare la ciberresilienza per tutti i modi di trasporto. Rafforzare la ciberresilienza dei **processi e delle istituzioni democratiche** rappresenta un elemento fondamentale del piano di azione per la democrazia europea[38], per la salvaguardia e la promozione di elezioni libere, del dibattito democratico e della pluralità dei media. Infine, per la sicurezza delle infrastrutture e dei servizi nell'ambito del futuro programma spaziale, la Commissione continuerà ad approfondire la strategia per la

[34] [*inserire riferimento alla proposta NIS*].
[35] [inserire riferimento alla *proposta* di direttiva sulla resilienza di entità critiche].
[36] Proposta di regolamento sulla resilienza operativa digitale per il settore finanziario che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) N. 600/2014 e (UE) n. 909/2014, COM/2020/595 final.
[37] Regolamento di esecuzione (UE) 2019/1583 della Commissione.
[38] Comunicazione sul piano d'azione per la democrazia europea COM(2020) 790. In base al piano, la rete europea di cooperazione in materia elettorale e le reti elettorali degli Stati membri sosterranno l'invio di squadre congiunte di esperti per contrastare le minacce, incluse le minacce informatiche, durante i processi elettorali; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_it.

cibersicurezza di Galileo per la prossima generazione di servizi del sistema globale di navigazione satellitare e altre nuove componenti del programma spaziale[39].

1.2 Creare un ciberscudo europeo

Con il diffondersi della connettività e la crescente sofisticazione degli attacchi informatici, i centri di condivisione e di analisi delle informazioni, ovvero gli ISAC, svolgono una valida funzione, anche a livello settoriale, nel permettere lo scambio di informazioni sulle minacce informatiche tra più portatori di interessi[40]. Oltre a ciò, le reti e i sistemi informatici richiedono un monitoraggio e un'analisi costanti per rilevare intrusioni e anomalie in tempo reale. Molte imprese private, organizzazioni pubbliche e autorità nazionali hanno quindi istituito gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e centri operativi di sicurezza, ovvero i SOC.

I centri operativi di sicurezza sono di vitale importanza per la raccolta di log[41] e l'isolamento di eventi sospetti che si verificano sulle reti di comunicazione che tali centri provvedono a monitorare, un risultato a cui giungono mediante l'identificazione di segnali e modelli nonché l'estrazione di conoscenza delle minacce da grandi quantità di dati da valutare. Essi hanno contribuito all'individuazione delle attività di file eseguibili malevoli e ciò ha, a sua volta, contribuito a contenere gli attacchi informatici. Il lavoro richiesto in questi centri è molto impegnativo e frenetico ed è per questo che l'IA, in particolare le tecniche di apprendimento automatico, possono fornire un supporto inestimabile ai professionisti[42].

La Commissione propone di creare una **rete di centri operativi per la sicurezza all'interno dell'UE[43]** al fine di sostenere il miglioramento dei centri esistenti e di istituirne di nuovi. Sosterrà inoltre la formazione e lo sviluppo di competenze dei lavoratori impegnati in questi centri e, sulla base di un'analisi delle esigenze effettuata presso i portatori di interessi pertinenti e con il contributo dell'agenzia dell'Unione europea per la cibersicurezza (ENISA), potrebbe stanziare oltre 300 milioni di EUR a sostegno della cooperazione pubblico-privata e transfrontaliera al fine di creare reti nazionali e settoriali che coinvolgano anche le PMI e si basino su adeguate disposizioni in materia di governance, condivisione dei dati e sicurezza.

Gli Stati membri sono incoraggiati a co-investire in questo progetto. I centri sarebbero quindi in grado di condividere e correlare in modo più efficiente i segnali rilevati, nonché di creare una intelligence di alta qualità sulle minacce da condividere con gli ISAC e le autorità nazionali, consentendo pertanto una maggiore consapevolezza situazionale. L'obiettivo sarebbe quello di collegare, per fasi, il maggior numero possibile di centri in tutta l'UE al fine di sviluppare una conoscenza collettiva e condividere le migliori pratiche. Sarà messo a disposizione di questi centri un sostegno per migliorare la velocità di rilevamento degli incidenti, di analisi e di risposta attraverso capacità all'avanguardia di intelligenza artificiale e

[39] Ivi compresa la nuova iniziativa governativa in materia di comunicazioni satellitari (GOVSATCOM) e il sistema di sorveglianza dei detriti spaziali (SST).
[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
[41] In maniera tale che le autorità giudiziarie e di contrasto possano usarli come prove.
[42] Source: indagine del Ponemon Institute Research, "Improving the Effectiveness of the SOC", 2019; per gli studi sull'uso dell'IA nei centri operativi di sicurezza si veda ad esempio: Khraisat, A., Gondal, I., Vamplew, P. *et al.* "Survey of intrusion detection systems: techniques, datasets and challenges", *Cybersecur* 2**,** 20 (2019).
[43] Saranno sviluppati accordi più dettagliati riguardanti la governance, i principi operativi e il finanziamento di questi centri e le modalità di integrazione delle strutture già esistenti come i poli dell'innovazione digitale.

di apprendimento automatico e sarà integrato da un'infrastruttura di supercalcolo sviluppata nell'UE dall'impresa comune per il calcolo ad alte prestazioni europeo[44].

Attraverso una collaborazione e una cooperazione continue, tale rete segnalerà tempestivamente eventuali incidenti di cibersicurezza alle autorità e a tutti i portatori di interessi coinvolti, compresa l'unità congiunta per il ciberspazio (cfr. sezione 2.1). **Essa rappresenterà un vero e proprio scudo di cibersicurezza per l'UE**, fornendo una solida rete di torri di controllo in grado di rilevare potenziali minacce prima che queste ultime possano causare danni su larga scala.

1.3 Un'infrastruttura di comunicazione ultra sicura

Le comunicazioni satellitari governative dell'Unione europea[45], una componente del programma spaziale, forniranno capacità di comunicazione satellitari sicure ed efficienti in termini di costi per garantire le missioni e le operazioni critiche in materia di sicurezza gestite dall'UE e dai suoi Stati membri, compresi gli attori nazionali in materia di sicurezza e le istituzioni, gli organismi e le agenzie dell'UE.

Gli Stati membri si sono impegnati a lavorare assieme alla Commissione per la realizzazione di un'infrastruttura di comunicazione quantistica sicura per l'Europa[46]. L'infrastruttura di comunicazione quantistica offrirà alle autorità pubbliche un modo nuovo per trasmettere informazioni riservate utilizzando una forma ultra sicura di crittografia a protezione dagli attacchi informatici, creata con tecnologia europea. Sarà composta di due elementi principali: reti terrestri di comunicazione in fibra esistenti, che collegano i siti strategici a livello nazionale e transfrontaliero, e satelliti spaziali collegati a copertura dell'intera UE, compresi i territori d'oltremare[47]. Tale iniziativa, volta a sviluppare e realizzare forme nuove e più sicure di crittografia, nonché a individuare nuovi modi per proteggere comunicazioni e asset di dati critici può aiutare a mantenere la sicurezza delle informazioni sensibili e quindi delle infrastrutture critiche.

In questa prospettiva, e spingendosi oltre, la Commissione esaminerà la possibile realizzazione di un sistema di connettività sicura multi-orbitale. Basandosi su GOVSATCOM e sulle infrastrutture di comunicazione quantistica, esso integrerebbe tecnologie all'avanguardia (quantistiche, 5G, IA, edge computing) che aderiscono al più restrittivo quadro di cibersicurezza al fine di supportare servizi sicuri fin dalla progettazione, come una

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

[45] GOVSATCOM è una componente del programma spaziale dell'Unione.

[46] La dichiarazione EuroQCI è stata finora firmata dalla maggior parte degli Stati membri, lo sviluppo e la realizzazione delle infrastrutture sono previsti per gli anni 2021-2027 mediante finanziamenti provenienti da Orizzonte Europa ed Europa digitale, e dall'Agenzia spaziale europea, soggetti ad adeguati meccanismi di governance; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

[47] È necessario sviluppare una componente spaziale per realizzare connessioni punto-punto a lunga distanza (>1 000 km) che non sono possibili mediante l'infrastruttura a terra. Sfruttando le proprietà nella meccanica quantistica, l'infrastruttura di comunicazione quantistica permetterà inizialmente alle parti di condividere in sicurezza chiavi segrete casuali da usare per criptare e decriptare i messaggi. Sarà anche compresa la realizzazione di un'infrastruttura di prova e di conformità per valutare la conformità dei dispositivi e dei sistemi di comunicazione quantistica europei all'infrastruttura di comunicazione quantistica e la loro certificazione e convalida prima dell'integrazione nell'infrastruttura stessa. Quest'ultima sarà studiata per supportare applicazioni aggiuntive una volta raggiunto il necessario livello di maturità tecnologica. L'attuale progetto pilota OpenQKD (https://openqkd.eu/) è un precursore di questa infrastruttura di prova e di conformità.

connettività affidabile, sicura ed efficiente in termini di costi e una comunicazione criptata per attività governative critiche.

1.4 Rendere sicura la prossima generazione di reti mobili a banda larga

I cittadini e le imprese all'interno dell'UE che utilizzano applicazioni avanzate e innovative abilitate da **5G e future generazioni di reti** dovrebbero beneficiare dei più elevati standard di sicurezza. Gli Stati membri, insieme alla Commissione e con il sostegno dell'ENISA, hanno stabilito, unitamente al pacchetto di strumenti dell'UE per il 5G[48] del gennaio 2020, un approccio alla cibersicurezza del 5G completo, obiettivo e basato sul rischio, fondato su una valutazione dei possibili piani di attenuazione e sull'individuazione delle misure più efficaci. L'UE sta inoltre consolidando le proprie capacità in materia di 5G e oltre, al fine di evitare dipendenze e promuovere una catena di approvvigionamento diversificata e sostenibile.

Nel mese di dicembre 2020 la Commissione ha pubblicato una relazione sull'impatto della raccomandazione del 26 marzo 2019 sulla cibersicurezza delle reti 5G[49]. La relazione ha rilevato i notevoli progressi conseguiti da quando è stato concordato il pacchetto di strumenti, constatando che gran parte degli Stati membri è sulla buona strada per completare a breve una parte significativa dell'attuazione del pacchetto di strumenti, anche se con alcune variazioni e lacune rimanenti, come già individuato nella relazione sullo stato di avanzamento pubblicata nel luglio 2020[50].

Nel mese di ottobre 2020 il Consiglio europeo ha richiesto all'UE e agli Stati membri "di avvalersi appieno del pacchetto di strumenti per la cibersicurezza del 5G" e di "applicare le pertinenti restrizioni ai fornitori ad alto rischio per gli asset chiave definiti critici e sensibili nelle valutazioni dei rischi coordinate a livello dell'UE, sulla base di criteri oggettivi comuni"[51].

Guardando al futuro l'UE e i suoi Stati membri dovrebbero garantire che i rischi individuati siano stati mitigati adeguatamente e in maniera coordinata, in particolare per quanto riguarda l'obiettivo di minimizzare l'esposizione a fornitori ad alto rischio e di evitare la dipendenza da tali fornitori a livello nazionale e dell'Unione, come pure che qualsiasi nuovo sviluppo o rischio significativo sia preso in considerazione. Gli Stati membri sono invitati a utilizzare pienamente il pacchetto di strumenti nei loro investimenti in materia di capacità digitali e connettività.

Sulla base della relazione sull'impatto della raccomandazione 2019, la Commissione incoraggia gli Stati membri ad accelerare i lavori finalizzati al completamento dell'attuazione delle principali misure del pacchetto di strumenti entro il secondo trimestre del 2021. Invita altresì gli Stati membri a continuare a monitorare congiuntamente lo stato di avanzamento, garantendo un ulteriore allineamento degli approcci. A livello dell'UE, saranno perseguiti tre obiettivi principali a sostegno di tale processo: garantire un'ulteriore convergenza negli approcci di attenuazione dei rischi in tutta l'UE, sostenere lo scambio continuo di conoscenze e lo sviluppo di capacità e promuovere la resilienza della catena di approvvigionamento e

[48] Comunicazione "Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE", COM(2020) 50.
[49] Relazione della Commissione sull'impatto della raccomandazione della Commissione del 26 marzo 2019 sulla cibersicurezza delle reti 5G, 15 dicembre 2020.
[50] Relazione del gruppo di cooperazione NIS sull'attuazione del pacchetto di strumenti del 24 luglio 2020.
[51] EUCO 13/20, Riunione straordinaria del Consiglio europeo (1° e 2 ottobre 2020) – Conclusioni.

altri obiettivi strategici di sicurezza dell'UE. Azioni concrete relative a questi obiettivi chiave sono stabilite nell'apposita appendice della presente comunicazione.

La Commissione continuerà a lavorare in stretta collaborazione con gli Stati membri per realizzare questi obiettivi e azioni con il sostegno dell'ENISA (cfr. allegato).

L'approccio del pacchetto di strumenti dell'UE per il 5G ha tuttavia suscitato l'interesse di paesi terzi che stanno sviluppando approcci per la sicurezza le loro reti di comunicazione. I servizi della Commissione, unitamente al Servizio europeo per l'azione esterna e alla rete di delegazioni dell'UE, sono pronti a fornire alle autorità di tutto il mondo, su richiesta, ulteriori informazioni in merito al loro approccio completo, obiettivo e basato sul rischio.

1.5 Un'Internet delle cose sicura

Ogni dispositivo connesso presenta vulnerabilità che possono essere sfruttate con ramificazioni potenzialmente estese. Le regole del mercato interno prevedono garanzie contro prodotti e servizi ritenuti insicuri. La Commissione si sta già adoperando per garantire **soluzioni trasparenti in materia di sicurezza e la certificazione a norma del regolamento sulla cibersicurezza**, e per incentivare prodotti e servizi sicuri senza scendere a compromessi sulle prestazioni[52]. Il primo programma di lavoro progressivo dell'Unione sarà adottato dalla Commissione nel primo trimestre del 2021 (da aggiornare almeno ogni tre anni) per permettere all'industria, alle autorità nazionali e agli enti di normazione di prepararsi in anticipo in vista di futuri sistemi europei di certificazione della cibersicurezza[53]. Con la diffusione dell'Internet delle cose, è necessario rafforzare le norme applicabili, sia per garantire la resilienza complessiva che per aumentare la cibersicurezza.

La Commissione terrà conto di un approccio completo, comprendente possibili **nuove norme orizzontali volte a migliorare la cibersicurezza di tutti i prodotti connessi e servizi associati presenti nel mercato interno**[54]. Tali norme potrebbero includere un **nuovo dovere di diligenza da parte dei produttori di dispositivi connessi** volto ad affrontare le vulnerabilità del software, compresa la prosecuzione degli aggiornamenti software e di sicurezza, nonché la garanzia, alla fine del ciclo di vita, della cancellazione dei dati personali e di altri dati sensibili. Tali norme rafforzerebbero l'iniziativa riguardante "il diritto alla riparazione di software obsoleti" introdotta dal piano d'azione per l'economia circolare e integrerebbero le misure in corso riguardanti tipi specifici di prodotto, quali i requisiti obbligatori da proporre per l'accesso al mercato di determinati prodotti wireless (attraverso l'adozione di un atto delegato a norma della direttiva sulle apparecchiature radio[55]). Le stesse rafforzerebbero anche l'obiettivo di attuare norme in materia di cibersicurezza per i veicoli a

[52] Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza"). Il regolamento sulla cibersicurezza promuove la certificazione delle TIC a livello dell'UE mediante un quadro europeo di certificazione della cibersicurezza per l'introduzione di sistemi volontari europei di certificazione della cibersicurezza, al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC nell'Unione, oltre che per ridurre la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione. Nel contempo le società di "rating" della cibersicurezza tendono ad avere sede al di fuori dell'UE con una trasparenza e un controllo limitati; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

[53] A norma dell'articolo 47, paragrafo 5, del regolamento sulla cibersicurezza.

[54] Le conclusioni del Consiglio invitano ad adottare misure orizzontali in materia di cibersicurezza dei dispositivi connessi; 13629/20, 2 dicembre 2020.

[55] Direttiva 2014/53/UE.

motore per tutti i nuovi tipi di veicolo, a decorrere dal luglio 2022[56]. Tali norme si baserebbero inoltre sulla proposta di revisione delle norme generali di sicurezza dei prodotti, che non affrontano direttamente gli aspetti della cibersicurezza[57].

1.6 Maggiore sicurezza Internet a livello globale

Una serie di protocolli principali e infrastrutture di sostegno assicurano la funzionalità e l'integrità di Internet in tutto il mondo[58]. Tale serie comprende il sistema dei nomi di dominio (DNS) e il relativo sistema gerarchico e decentrato di zone, a partire, in cima alla gerarchia, dalla zona root e dai tredici server root DNS[59] da cui dipende il World Wide Web. La Commissione intende sviluppare **un piano di emergenza, sostenuto da finanziamenti dell'UE, per affrontare scenari estremi che compromettono l'integrità e la disponibilità del sistema root DNS globale**. Collaborando con l'ENISA, gli Stati membri, i due operatori dei server root DNS dell'UE[60] e la comunità multipartecipativa, la Commissione valuterà il ruolo di questi operatori nel garantire che Internet resti globalmente accessibile in qualsiasi circostanza.

Per poter accedere a una risorsa in un particolare nome di dominio su Internet, la richiesta di un "client" (tipicamente attraverso un identificatore uniforme di risorse o URL) deve essere tradotta o "risolta" in un indirizzo IP, facendo riferimento a server DNS. Tuttavia le persone e le organizzazioni all'interno dell'UE si affidano sempre di più a un numero limitato di risolutori DNS pubblici gestiti da entità di paesi terzi. Questo consolidamento della risoluzione DNS nelle mani di poche società[61] rende il processo stesso di risoluzione vulnerabile in caso di eventi significativi che interessino un provider importante e rende più difficile per le autorità dell'UE affrontare possibili attacchi informatici dolosi e gravi incidenti geopolitici e tecnici[62].

Per ridurre i problemi di sicurezza legati alla concentrazione del mercato, la Commissione incoraggerà i portatori di interessi pertinenti, tra cui le imprese dell'UE, i fornitori di servizi Internet e i fornitori di browser, ad adottare una strategia di diversificazione della risoluzione DNS. La Commissione intende inoltre contribuire a rendere sicura la connettività Internet sostenendo lo sviluppo di un **servizio pubblico europeo di risoluzione DNS**. L'iniziativa "DNS4EU" offrirà un servizio alternativo ed europeo per accedere all'Internet globale.

---

[56] A seguito del regolamento UNECE adottato nel giugno 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[57] Revisione delle attuali norme relative alla sicurezza generale dei prodotti (direttiva 2001/95/CE); sono previste anche proposte di norme modificate relative alla responsabilità dei produttori in campo digitale nell'ambito di applicazione del quadro normativo UE in materia di responsabilità.

[58] "Il nucleo pubblico dell'Internet aperta, vale a dire i suoi protocolli e le sue infrastrutture principali, che costituiscono un bene pubblico globale, consente la funzionalità essenziale di Internet nel suo complesso e ne supporta il normale funzionamento. L'ENISA dovrebbe sostenere la sicurezza del nucleo pubblico dell'Internet aperta e la stabilità del suo funzionamento, compresi, solo a titolo di esempio, i protocolli chiave (in particolare DNS, BGP e IPv6), il funzionamento del sistema dei nomi di dominio (come il funzionamento di tutti i domini di primo livello) e il funzionamento della zona root."; considerando 23 del regolamento sulla cibersicurezza.

[59] https://www.iana.org/domains/root/servers.

[60] I server i.root gestiti da Netnod in Svezia e i server k.root gestiti da RIPE NCC nei Paesi Bassi.

[61] "Consolidation in the DNS resolver market – how much, how fast how dangerous?" (), "Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services" ( ).

[62] È inoltre dimostrato che i dati DNS possono essere utilizzati a fini di profilazione, con un impatto sui diritti alla riservatezza e alla protezione dei dati.

DNS4EU sarà trasparente, conforme alle più recenti norme e regole in materia di sicurezza, protezione dei dati e riservatezza per impostazione predefinita e fin dalla progettazione, e sarà parte integrante dell'alleanza industriale europea per i dati e il cloud[63].

In collaborazione con gli Stati membri e l'industria, la Commissione **accelererà inoltre l'adozione di norme Internet chiave tra cui l'IPv6[64] e di norme di sicurezza Internet consolidate, nonché di buone pratiche per la sicurezza DNS, del routing e della posta elettronica[65]**, non escludendo misure regolamentari, come una clausola di decadenza europea per l'IPv4, per orientare il mercato in caso di progressi insufficienti in direzione dell'adozione. L'UE dovrebbe promuovere (ad esempio nell'ambito della strategia UE-Africa[66]) l'attuazione di queste norme nei paesi partner come supporto allo sviluppo dell'Internet globale e aperta e per contrastare i modelli chiusi e basati sul controllo di Internet. In ultima analisi, la Commissione prenderà in considerazione la necessità di un meccanismo per il monitoraggio e la raccolta in maniera più sistematica di dati aggregati sul traffico Internet e per la consulenza su potenziali perturbazioni[67].

1.7 Presenza rafforzata lungo la catena di approvvigionamento tecnologico

Con il sostegno finanziario programmato per la trasformazione digitale cibersicura nel quadro finanziario pluriennale 2021-2027, l'UE ha l'opportunità unica di mettere in comune i propri asset per promuovere la propria strategia industriale[68] e la propria leadership in materia di tecnologie digitali e cibersicurezza lungo la catena di approvvigionamento digitale (comprendente dati e cloud, tecnologie dei processori di nuova generazione, connettività ultra sicura e reti 6G), in linea con i propri valori e priorità. L'intervento del settore pubblico dovrebbe fare affidamento sugli strumenti forniti dal quadro normativo degli appalti pubblici dell'UE, nonché sugli importanti progetti di comune interesse europeo. Esso può inoltre sbloccare investimenti privati attraverso partenariati pubblico-privati (anche sulla base dell'esperienza del partenariato pubblico-privato contrattuale sulla cibersicurezza e la sua attuazione attraverso l'Organizzazione europea per la cibersicurezza), capitali di rischio a sostegno delle PMI o alleanze industriali e strategie sulle capacità tecnologiche.

Particolare attenzione sarà dedicata anche allo strumento di sostegno tecnico[69] e all'uso ottimale dei più recenti strumenti di cibersicurezza da parte delle PMI, specialmente quelli che non rientrano nell'ambito di applicazione della direttiva NIS riveduta, anche attraverso attività dedicate, nell'ambito dei poli dell'innovazione digitale del programma Europa digitale. L'obiettivo è di stimolare investimenti analoghi da parte degli Stati membri, cui dovrebbe corrispondere un contributo analogo da parte dell'industria, nell'ambito di un partenariato gestito in collaborazione con gli Stati membri stessi in relazione alla proposta di

[63] Dichiarazione comune: "Building the next generation cloud for businesses and the public sector in the EU"; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe.
[64] L'utilizzo dell'IPv6 è ora più avanzato per via del grave esaurimento dell'offerta e dell'aumento dei costi degli indirizzi IPv4. L'impiego dell'IPv6 è tuttavia disomogeneo all'interno dell'UE.
[65] Tali norme includono DNSSEC, HTTPS, DNS su HTTPS (DoH), DNS su TLS (DoT), SPF, DKIM, /DMARC, STARTTLS, DANE e norme e buone pratiche relative al routing, come ad esempio norme convenute di comune accordo sulla sicurezza del routing (Mutually Agreed Norms for Routing Security - MANRS).
[66] Comunicazione congiunta "Verso una strategia globale per l'Africa", JOIN(2020) 4 final, del 9 marzo 2020.
[67] Tale "osservatorio di Internet" potrebbe rientrare nell'ambito delle attività del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza; Proposta di regolamento 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.
[68] Comunicazione su una nuova strategia industriale per l'Europa, COM(2020) 102 final.
[69] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2020:0409:FIN.

un **centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e rete di centri di coordinamento (CCCN)**. Il CCCN dovrebbe sia svolgere un ruolo chiave, con il contributo dell'industria e delle comunità accademiche, nello sviluppo della sovranità tecnologica dell'UE in materia di cibersicurezza e nella costruzione di capacità per garantire la sicurezza di infrastrutture sensibili come il 5G, sia ridurre la dipendenza da altre parti del mondo per le tecnologie più importanti.

La Commissione intende sostenere, potenzialmente con il CCCN, lo sviluppo di un programma di master dedicato sulla cibersicurezza, e contribuire dopo il 2020 a una tabella di marcia comune europea di ricerca e innovazione in materia di cibersicurezza. Gli investimenti attraverso il CCCN si baserebbero anche sulla cooperazione nella ricerca e nello sviluppo da parte di reti di centri di eccellenza per la cibersicurezza, che riuniscono i migliori team di ricerca europei e l'industria, al fine di progettare e attuare programmi di ricerca comuni, in linea con la tabella di marcia dell'Organizzazione europea per la cibersicurezza[70]. La Commissione continuerà a fare affidamento sul lavoro di ricerca svolto dall'ENISA e da Europol e continuerà anche a sostenere, nell'ambito di Orizzonte Europa, i singoli innovatori di Internet che sviluppano tecnologie di comunicazione sicure e che rafforzano la tutela della vita privata basate su software e hardware open source, come avviene attualmente nell'ambito dell'iniziativa "Internet di prossima generazione".

1.8 Una forza lavoro dell'UE dotata di competenze informatiche

Gli sforzi dell'UE per migliorare le competenze della forza lavoro, per attrarre e trattenere i migliori talenti in materia di cibersicurezza e per investire nella ricerca e nell'innovazione di livello mondiale, costituiscono una componente importante della protezione contro le minacce informatiche in generale. Questo settore presenta un grande potenziale, per cui occorre dedicare particolare attenzione a sviluppare, attrarre e trattenere talenti maggiormente diversificati. Il piano d'azione riveduto per l'istruzione digitale promuoverà le attività di sensibilizzazione in materia di cibersicurezza tra le persone, specialmente i bambini e i giovani, e tra le organizzazioni, in particolare le PMI[71]. Incoraggerà inoltre la partecipazione femminile nell'ambito dell'istruzione in campo scientifico, tecnologico, ingegneristico e matematico, della riqualificazione professionale nel settore delle TIC o del miglioramento delle competenze nel settore digitale. Inoltre la Commissione, assieme all'Ufficio dell'Unione europea per la proprietà intellettuale presso Europol, all'ENISA, agli Stati membri e al settore privato, svilupperà strumenti di sensibilizzazione e orientamenti per aumentare la resilienza delle imprese dell'UE **nei confronti dei furti di proprietà intellettuale favoriti dall'informatica**[72].

L'istruzione, compresa l'istruzione e formazione professionale, le attività di sensibilizzazione e le esercitazioni, dovrebbero aumentare ulteriormente la cibersicurezza e le competenze in materia di ciberdifesa a livello dell'UE. A questo proposito, gli attori pertinenti dell'UE, quali l'ENISA, l'Agenzia europea per la difesa (AED) e l'Accademia europea per la sicurezza e la difesa (AESD)[73] dovrebbero trovare sinergie tra le rispettive attività.

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_it.
[72] https://ec.europa.eu/commission/presscorner/detail/it/IP_20_2187.
[73] Attraverso la piattaforma informatica in materia di istruzione, formazione, valutazione ed esercitazioni (ETEE).

Iniziative strategiche

L'UE dovrebbe garantire:

- l'adozione della direttiva NIS riveduta;
- misure di regolamentazione per un'Internet delle cose sicura;
- attraverso gli investimenti del CCCN nella cibersicurezza (in particolare mediante il programma Europa digitale, Orizzonte Europa e il dispositivo per la ripresa), la realizzazione di investimenti pubblici e privati, nel periodo 2021-2027, per un valore fino a 4,5 miliardi di EUR;
- una rete UE di centri operativi di sicurezza abilitati all'IA e un'infrastruttura di comunicazione ultra sicura che sfrutti le tecnologie quantistiche;
- l'adozione diffusa delle tecnologie di cibersicurezza attraverso un supporto dedicato alle PMI nell'ambito dei centri di innovazione digitale;
- lo sviluppo di un servizio di risoluzione DNS dell'UE quale alternativa aperta e sicura di accesso a Internet per i cittadini, le imprese e l'amministrazione pubblica dell'UE; e
- il completamento dell'attuazione del pacchetto di strumenti per il 5G entro il secondo trimestre del 2021 (cfr. allegato).

2. SVILUPPARE CAPACITÀ OPERATIVE DI PREVENZIONE, DISSUASIONE E RISPOSTA

Gli incidenti informatici, siano essi accidentali o frutto dell'azione deliberata di criminali, attori statali e non statali, possono causare danni enormi. La loro portata e complessità, che spesso comporta lo sfruttamento di servizi, hardware e software di terzi per compromettere un obiettivo finale, rendono il contesto delle minacce collettive dell'UE difficile da contrastare senza una sistematica e completa condivisione delle informazioni e cooperazione per una risposta collettiva. **Attraverso la piena attuazione degli strumenti normativi, la mobilitazione e la cooperazione**, l'UE mira a sostenere gli Stati membri nella difesa dei loro cittadini, nonché dei loro interessi economici e di sicurezza nazionale, nel pieno rispetto dei diritti e delle libertà fondamentali e dello Stato di diritto. Diverse comunità, formate da reti, istituzioni, organismi e agenzie dell'UE, nonché autorità degli Stati membri, hanno la responsabilità di prevenire, scoraggiare, dissuadere e rispondere alle minacce informatiche, utilizzando i rispettivi strumenti e iniziative[74]. Tali comunità comprendono: i) autorità NIS, quali i CSIRT, e gli organismi di reazione alle catastrofi; ii) autorità giudiziarie e di contrasto; iii) la diplomazia informatica; e iv) la ciberdifesa.

[74] Tra cui il sostegno dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) alla cooperazione operativa e gestione delle crisi; la rete di CSIRT; la rete delle organizzazioni di collegamento per le crisi informatiche (CyCLONE, che diventerà EU-CyCLONE come proposto nella direttiva NIS riveduta); il gruppo di cooperazione NIS; "rescEU"; il Centro europeo per la lotta alla criminalità informatica e la task force di azione congiunta contro la criminalità informatica di Europol e il protocollo di risposta alle emergenze delle autorità di contrasto; il Centro UE di situazione e di intelligence (INTCEN) e il pacchetto di strumenti della diplomazia informatica; la capacità unica di analisi dell'intelligence (SIAC); i progetti informatici nell'ambito della cooperazione strutturata permanente (PESCO), in particolare i "gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza" (CRRT).

2.1 Un'unità congiunta per il ciberspazio

Un'unità congiunta per il ciberspazio avrebbe la funzione di piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cibersicurezza all'interno dell'UE, con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera.

L'unità congiunta per il ciberspazio rappresenterebbe un importante passo avanti per il completamento del **quadro europeo di gestione delle crisi informatiche**. Come indicato negli orientamenti politici della presidente della Commissione[75], l'unità dovrebbe consentire agli Stati membri e alle istituzioni, agli organismi e alle agenzie dell'UE di utilizzare appieno le strutture, le risorse e le capacità esistenti, nonché promuovere il principio della "**necessità di condividere**". Essa fornirebbe i mezzi per consolidare i progressi compiuti finora nell'attuazione della raccomandazione del 2017 riguardante una risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala ("programma")[76] e fornirebbe anche l'opportunità di rinforzare ulteriormente la cooperazione riguardo all'architettura del programma e di sfruttare i progressi compiuti, in particolare all'interno del gruppo di cooperazione NIS e la rete CyCLONe.

Ciò potrebbe colmare **due grandi lacune** che attualmente aumentano le vulnerabilità e creano inefficienze nella risposta alle minacce e agli incidenti transfrontalieri che interessano l'Unione. In primo luogo, le **comunità** civili, diplomatiche, delle forze dell'ordine e della difesa in materia di cibersicurezza non dispongono ancora di uno spazio comune per incoraggiare una cooperazione strutturata e facilitare la cooperazione operativa e tecnica. In secondo luogo, i portatori di interessi in materia di cibersicurezza non sono ancora stati in grado di sfruttare appieno il **potenziale** della cooperazione operativa e dell'assistenza reciproca all'interno delle reti e delle comunità già esistenti. A questo si aggiunge l'assenza di una piattaforma che consenta la cooperazione operativa con il settore privato. L'unità dovrebbe migliorare e accelerare il coordinamento, e permettere all'UE di far fronte e rispondere a incidenti e crisi informatiche su larga scala.

L'unità congiunta per il ciberspazio non sarà un organismo aggiuntivo e autonomo, né influirà sulle competenze e i poteri delle autorità nazionali di cibersicurezza o dei partecipanti dell'UE. L'unità agirebbe piuttosto come punto d'appoggio dove i partecipanti possono avvalersi del supporto e delle competenze reciproche, soprattutto nel caso in cui le varie cibercomunità debbano lavorare a stretto contatto. Al tempo stesso i recenti avvenimenti dimostrano la necessità per l'UE di intensificare il suo livello di ambizione e preparazione per affrontare il panorama e le realtà delle minacce informatiche. Nell'ambito del loro contributo all'unità congiunta per il ciberspazio, gli attori dell'UE (la Commissione e le agenzie e gli organismi dell'UE) saranno quindi pronti ad aumentare in maniera sostanziale le loro risorse e capacità in modo da accrescere la loro preparazione e resilienza.

L'unità congiunta per il ciberspazio risponderebbe a tre obiettivi principali. In primo luogo, garantirebbe la **preparazione** di tutte le comunità di cibersicurezza; in secondo luogo, attraverso la condivisione delle informazioni, fornirebbe una **consapevolezza** situazionale

[75] "Un'Unione più ambiziosa. Il mio programma per l'Europa", orientamenti politici per la prossima Commissione europea 2019-2024 della candidata alla carica di presidente della Commissione europea Ursula von der Leyen.
[76] Raccomandazione sul programma C(2017) 6100 final, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

continua e condivisa; in terzo luogo, rafforzerebbe la **risposta** coordinata e la ripresa. Per raggiungere questi obiettivi, l'unità dovrebbe basarsi su **blocchi e obiettivi** ben definiti, quali la garanzia di una **condivisione sicura e rapida delle informazioni**, il miglioramento della **cooperazione** tra i partecipanti, compresa l'interazione tra gli Stati membri e le pertinenti entità dell'UE, la creazione di **partenariati strutturati con una base industriale di fiducia** e la facilitazione di un approccio coordinato alla **cooperazione con i partner esterni**. A tal fine, sulla base di una mappatura delle capacità disponibili a livello nazionale e comunitario, l'unità potrebbe facilitare lo sviluppo di un quadro di cooperazione.

Affinché l'unità congiunta per il ciberspazio diventi il cuore della cooperazione operativa dell'UE in materia di cibersicurezza, la Commissione collaborerà con gli Stati membri e con le istituzioni, gli organismi e le agenzie dell'UE pertinenti, tra cui ENISA, CERT-EU ed Europol, per promuovere un **approccio incrementale e inclusivo**, nel pieno rispetto delle competenze e dei mandati di tutti i soggetti coinvolti. In linea con tale approccio, l'unità potrebbe contribuire ad un'ulteriore cooperazione tra i costituenti di una specifica cibercomunità, laddove tali costituenti lo ritengano necessario.

Per la creazione dell'unità congiunta per il ciberspazio sono proposte quattro fasi principali:

- *definizione*, mappando le capacità disponibili a livello nazionale e dell'UE;
- *preparazione*, istituendo un quadro per la cooperazione e l'assistenza strutturate;
- *realizzazione*, attuando il quadro di riferimento attingendo alle risorse fornite dai partecipanti in modo da rendere operativa l'unità congiunta per il ciberspazio;
- *espansione*, rafforzando la capacità di risposta coordinata con il contributo dell'industria e dei partner.

Basandosi sui risultati della consultazione avuta con gli Stati membri, le istituzioni, gli organismi e le agenzie dell'UE[77], la Commissione, con il coinvolgimento dell'alto rappresentante e in linea con le sue competenze, presenterà, entro febbraio 2021, la procedura, le tappe e le scadenze per **la definizione, la preparazione, la realizzazione e l'espansione dell'unità congiunta per il ciberspazio**.

2.2 Contrastare la criminalità informatica

La nostra dipendenza dagli strumenti online ha aumentato in modo esponenziale la superficie di attacco per la criminalità informatica portando a una situazione in cui le indagini su quasi tutti i tipi di crimine presentano una componente digitale. Inoltre parti fondamentali della nostra società sono minacciate dagli attori informatici e da coloro che utilizzano strumenti informatici per pianificare e perpetrare le loro azioni illegali. Vi sono quindi stretti legami con la politica di sicurezza generale dell'UE, come si evince dagli elementi informatici della strategia dell'UE per l'Unione della sicurezza 2020 e dal programma di lotta al terrorismo dell'UE[78].

[77] Consultazione degli Stati membri (anche durante l'esercitazione Blue OLEx20 che ha riunito i responsabili delle autorità nazionali di cibersicurezza), le istituzioni, gli organismi e le agenzie dell'UE condotta tra luglio e novembre 2020.
[78] Comunicazione "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond", 9.12.2020, COM(2020) 795 final.

Contrastare efficacemente la criminalità informatica è fondamentale per garantire la sicurezza informatica: la dissuasione non può essere ottenuta mediante la sola resilienza, ma richiede anche l'individuazione e il perseguimento dei trasgressori. Si rende quindi necessario promuovere la cooperazione e lo scambio tra gli attori impegnati nella cibersicurezza e le forze dell'ordine. A livello dell'UE, pertanto, Europol ed ENISA hanno già instaurato una forte cooperazione, organizzando conferenze e workshop congiunti e fornendo relazioni congiunte alla Commissione, agli Stati membri e ai portatori di interessi sulle minacce alla sicurezza informatica e sulle sfide tecnologiche. La Commissione continuerà a sostenere questo approccio integrato al fine di garantire una risposta coerente ed efficace basata su un quadro di informazioni completo.

Come elemento importante di tale risposta, l'UE e le autorità nazionali devono ampliare e migliorare la capacità delle forze dell'ordine di indagare sulla criminalità informatica, rispettando pienamente i diritti fondamentali e perseguendo il necessario equilibrio tra i vari diritti e interessi. L'UE dovrebbe essere in grado di contrastare la criminalità informatica attuando pienamente una legislazione adatta allo scopo, con particolare attenzione alla lotta contro l'abuso sessuale online dei minori e alle indagini digitali, compresa la criminalità nella "dark net". Le forze dell'ordine devono essere adeguatamente equipaggiate per le indagini digitali e la Commissione attuerà pertanto un piano d'azione per migliorare la capacità digitale degli organismi di contrasto, fornendo loro le competenze e gli strumenti necessari. Parallelamente Europol svilupperà ulteriormente il suo ruolo di centro di competenza a sostegno delle autorità di contrasto nazionali preposte alla lotta contro reati dipendenti e favoriti dall'informatica, contribuendo alla definizione di norme forensi comuni (attraverso il laboratorio e il polo per l'innovazione di Europol). Tutte queste attività richiedono un'adeguata adozione da parte degli Stati membri, i quali sono incoraggiati ad avvalersi dei programmi nazionali del Fondo sicurezza interna e a proporre progetti in risposta agli inviti a presentare proposte nell'ambito dello strumento tematico.

La Commissione si avvarrà di tutti i mezzi appropriati, comprese le procedure d'infrazione, per garantire che la direttiva del 2013 relativa agli attacchi contro i sistemi di informazione[79] sia pienamente recepita e attuata, compresa la fornitura di statistiche da parte degli Stati membri. Essa provvederà a prevenire al meglio l'abuso dei nomi di dominio, anche per quanto riguarda la distribuzione di contenuti illegali, e a perseguire la disponibilità di dati di registrazione accurati continuando a collaborare con l'Internet Corporation for Assigned Names and Numbers (ICANN) e con altri soggetti interessati al sistema di governance di Internet, in particolare attraverso il gruppo di lavoro sulla sicurezza pubblica del Comitato consultivo governativo dell'ICANN. La proposta inserita nella direttiva NIS riveduta prevede di conseguenza il mantenimento di database accurati e completi dei nomi di dominio e dei dati di registrazione, ovvero "dati WHOIS", permettendo l'accesso legale a tali dati quale componente fondamentale per garantire la sicurezza, la stabilità e la resilienza del DNS.

La Commissione continuerà inoltre a adoperarsi per fornire canali appropriati e chiarire le regole per ottenere un accesso transfrontaliero alle prove elettroniche ai fini delle indagini penali (necessario per l'85 % delle indagini, con il 65 % delle richieste totali che vanno a provider con sede in un'altra giurisdizione), facilitando l'adozione e la successiva attuazione

[79] Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione.

del "pacchetto sulle prove elettroniche" e di misure pratiche[80]. La rapida adozione da parte del Parlamento europeo e del Consiglio delle proposte relative alle prove elettroniche è fondamentale per fornire agli operatori uno strumento efficace. Le prove elettroniche devono essere leggibili, pertanto la Commissione continuerà a impegnarsi per sostenere la capacità di contrasto nelle indagini digitali, anche per quanto riguarda la crittografia nell'ambito delle indagini penali, pur preservando pienamente la sua funzione di protezione dei diritti fondamentali e della cibersicurezza.

2.3 Pacchetto di strumenti della diplomazia informatica dell'UE

L'UE sta utilizzando un **pacchetto di strumenti della diplomazia informatica**[81] per prevenire, scoraggiare, dissuadere e rispondere alle attività informatiche dolose. Dopo l'introduzione, nel mese di maggio 2019[82], del quadro giuridico riguardante misure restrittive mirate contro gli attacchi informatici, l'UE ha imposto, nel luglio 2020, misure restrittive a sei soggetti e tre entità responsabili o coinvolte in attacchi informatici che hanno colpito l'UE e i suoi Stati membri, nell'ambito di tale regime[83]. Nel mese di ottobre 2020 due altri soggetti e un organismo sono stati inseriti nell'elenco[84]. Le attività informatiche dolose, comprese quelle i cui effetti non si manifestano immediatamente, dovrebbero essere contrastate mediante una risposta diplomatica comune efficace e globale dell'UE, utilizzando l'intera gamma di misure disponibili a livello dell'Unione.

Una risposta diplomatica comune rapida ed efficace dell'UE richiede una consapevolezza situazionale solida e condivisa, come pure la capacità di elaborare rapidamente una posizione comune dell'UE. L'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza promuoverà e faciliterà l'istituzione di un **gruppo di lavoro di intelligence informatica degli Stati membri dell'UE**, all'interno del Centro UE di situazione e di intelligence (INTCEN), per far progredire la cooperazione in materia di intelligence strategica sulle minacce e sulle attività informatiche. Questo lavoro andrà a sostenere ulteriormente la consapevolezza situazionale dell'UE e la capacità decisionale per una

[80] COM(2018) 225 e 226; C(2020) 2779 final. In particolare il progetto SIRIUS ha recentemente ricevuto un finanziamento aggiuntivo nell'ambito dello strumento di partenariato al fine di migliorare i canali per ottenere un accesso transfrontaliero legale alle prove elettroniche per le indagini penali (necessario per l'85 % delle indagini sui reati gravi, con il 65 % delle richieste totali che vanno a provider con sede in un'altra giurisdizione), e stabilire regole compatibili a livello internazionale.

[81] https://www.consilium.europa.eu/it/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[82] Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 129I del 17.5.2019, pag. 13); e regolamento (UE) 2019/796 del Consiglio,
del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 129I del 17.5.2019, pag. 1).

[83] Decisione (PESC) 2020/1127 del Consiglio, del 30 luglio 2020, che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (ST/9564/2020/INIT) (GU L 246 del 30.7.2020, pag. 12); e regolamento di esecuzione (UE) 2020/1125 del Consiglio, del 30 luglio 2020, che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (ST/9568/2020/INIT) (GU L 246 del 30.7.2020, pag. 4).

[84] Decisione (PESC) 2020/1537 del Consiglio, del 22 ottobre 2020, che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 351I del 22.10.2020, pag. 5); e regolamento di esecuzione (UE) 2020/1536 del Consiglio, del 22 ottobre 2020, che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 351I del 22.10.2020, pag. 1).

risposta diplomatica congiunta. Il gruppo di lavoro deve interagire con le strutture esistenti[85], comprese, se necessario, quelle che si occupano della più ampia minaccia di interferenze ibride e straniere, al fine di raccogliere e valutare la consapevolezza situazionale.

Per rafforzare la sua capacità di prevenire, scoraggiare, dissuadere e rispondere a comportamenti dolosi nel cyberspazio, l'alto rappresentante, con il coinvolgimento della Commissione in linea con le sue competenze, presenterà una proposta affinché l'UE definisca ulteriormente la sua **posizione in materia di dissuasione informatica**. Sulla base del lavoro svolto finora nell'ambito del pacchetto di strumenti della diplomazia informatica, la posizione dovrebbe contribuire a un comportamento responsabile degli Stati e alla cooperazione nel ciberspazio e dovrebbe impartire un orientamento specifico alle azioni di contrasto degli attacchi informatici che hanno gli effetti più significativi, in particolare quelli che riguardano le nostre infrastrutture critiche, le istituzioni e i processi democratici[86], nonché gli attacchi alla catena di approvvigionamento e i furti di proprietà intellettuale favoriti dall'informatica. La posizione dovrebbe delineare il modo in cui l'UE e gli Stati membri potrebbero sfruttare i loro strumenti di comunicazione politica, economica, diplomatica, legale e strategica contro le attività informatiche dolose, nonché affrontare il modo in cui l'UE e gli Stati membri potrebbero far progredire la loro capacità di attribuire le attività informatiche dolose. Inoltre, unitamente al Consiglio e alla Commissione, l'alto rappresentante intende esaminare **ulteriori misure nell'ambito del pacchetto di strumenti della diplomazia informatica**, compresa la possibilità di ulteriori opzioni per misure restrittive, nonché valutando il **voto a maggioranza qualificata (VMQ) per l'inserimento negli elenchi nell'ambito del regime di sanzioni orizzontali contro gli attacchi informatici**. L'UE dovrebbe intraprendere ulteriori sforzi per **rafforzare la cooperazione con i partner internazionali**, compresa la NATO, per migliorare la comprensione condivisa del panorama delle minacce, sviluppare meccanismi di cooperazione e individuare risposte diplomatiche cooperative.

L'alto rappresentante, con il coinvolgimento della Commissione, proporrà inoltre un aggiornamento delle **linee guida di attuazione del pacchetto di strumenti della diplomazia informatica**[87], anche al fine di aumentare l'efficienza del processo decisionale, e continuerà a organizzare regolarmente esercitazioni e valutazioni sul pacchetto di strumenti della diplomazia informatica stesso. L'UE dovrebbe inoltre **integrare ulteriormente il pacchetto di strumenti della diplomazia informatica nei meccanismi di crisi dell'UE**, ricercare sinergie con gli sforzi volti a contrastare le minacce ibride, la disinformazione e le interferenze straniere nell'ambito del quadro congiunto per contrastare le minacce ibride[88] e del piano d'azione per la democrazia europea. In questo contesto, l'UE dovrebbe riflettere a proposito dell'integrazione tra il pacchetto di strumenti della diplomazia informatica e il possibile utilizzo dell'articolo 42, paragrafo 7, TUE e dell'articolo 222 TFUE[89].

2.4 Promuovere le capacità di ciberdifesa

L'UE e gli Stati membri devono aumentare la loro capacità di prevenire e rispondere alle minacce informatiche, in linea con il livello di ambizione dell'UE derivante dalla strategia

[85] Come la capacità unica di analisi dell'intelligence (SIAC) dell'UE e, ove necessario, i relativi progetti sviluppati nell'ambito della PESCO, così come il sistema di allarme rapido del 2018 (RAS) creato a supporto dell'approccio generale dell'UE per contrastare la disinformazione.
[86] In particolare cercando sinergie con le iniziative nell'ambito del piano d'azione per la democrazia europea.
[87] 13007/17.
[88] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.
[89] Rispettivamente la clausola di difesa reciproca, la clausola di solidarietà.

globale dell'UE per il 2016[90]. A questo scopo, l'alto rappresentante, in collaborazione con la Commissione, presenterà una **revisione del quadro strategico in materia di ciberdifesa** al fine di migliorare ulteriormente il coordinamento e la cooperazione tra attori dell'UE[91], come pure con gli Stati membri e tra di essi, anche per quanto riguarda le missioni e le operazioni della politica di sicurezza e di difesa comune (PSDC). Il quadro strategico in materia di ciberdifesa dovrebbe fornire informazioni per la futura "bussola strategica"[92] assicurando che la sicurezza informatica e la ciberdifesa siano ulteriormente integrate nel più ampio programma di sicurezza e difesa.

Nel 2018 l'UE ha individuato il ciberspazio come un dominio operativo[93]. Un documento di prossima pubblicazione **"Visione e strategia militari sul ciberspazio come dominio operativo"** del Comitato militare dovrebbe definire ulteriormente in che modo il ciberspazio come dominio operativo permetta le missioni e le operazioni militari della PSDC dell'UE. La **rete CERT militare**[94], che sarà istituita dall'Agenzia europea per la difesa (AED), contribuirà ulteriormente ad aumentare in modo significativo la cooperazione tra gli Stati membri. Inoltre, per garantire la cibersicurezza delle infrastrutture spaziali critiche sotto la responsabilità del programma spaziale, l'Agenzia europea per il programma spaziale e in particolare il Centro di monitoraggio della sicurezza Galileo saranno rafforzati e il loro mandato sarà esteso ad altre risorse critiche del programma spaziale.

L'UE e gli Stati membri dovrebbero dare ulteriore impulso allo **sviluppo di capacità di ciberdifesa all'avanguardia** attraverso varie politiche e strumenti dell'UE, in particolare il quadro strategico dell'UE in materia di ciberdifesa e, se del caso, basandosi sul lavoro dell'AED. Ciò richiede una forte enfasi sullo sviluppo e sull'utilizzo di tecnologie chiave come l'IA, la crittografia e il calcolo quantistico. In linea con le priorità di sviluppo delle capacità dell'UE per il 2018[95] e sulla base dei risultati della prima relazione completa di revisione coordinata annuale sulla difesa (CARD)[96], l'UE dovrebbe promuovere ulteriormente la cooperazione tra gli Stati membri **in materia di ricerca, innovazione e sviluppo delle capacità nel campo della ciberdifesa** incoraggiando gli Stati membri a

[90] Conclusioni del Consiglio (14149/16) sull'attuazione della strategia globale dell'UE nel settore della sicurezza e della difesa.
[91] In particolare il SEAE, compreso lo Stato maggiore dell'UE (EUMS), l'Accademia europea per la sicurezza e la difesa (AESD), la Commissione, e le agenzie dell'UE, segnatamente l'Agenzia europea per la difesa (AED).
[92] Conclusioni del Consiglio sulla sicurezza e la difesa del 17 giugno 2020 (8910/20).
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/it/pdf.
[94] La creazione di una rete CERT militare dell'UE risponde a un obiettivo identificato nel quadro strategico dell'UE in materia di ciberdifesa del 2018 e mira a promuovere l'interazione attiva e lo scambio di informazioni tra le CERT militari degli Stati membri dell'UE.
[95] Nel giugno 2018 gli Stati membri hanno convenuto, in seno al comitato direttivo dell'AED, di guidare la cooperazione in materia di difesa a livello dell'UE.
[96] Approvata dai ministri della Difesa all'interno del comitato direttivo dell'AED nel novembre 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).

sfruttare appieno il potenziale della **cooperazione strutturata permanente (PESCO)**[97] e del **Fondo europeo per la difesa (FED)**[98].

Il prossimo **piano d'azione della Commissione sulle sinergie tra l'industria civile, della difesa e dello spazio**, che sarà presentato nel primo trimestre del 2021, comprenderà azioni per sostenere ulteriormente le sinergie a livello di programmi, tecnologie, innovazione e start-up, in linea con la governance dei rispettivi programmi[99].

Dovrebbero essere inoltre sviluppate pertinenti sinergie e interfacce tra le iniziative di ciberdifesa portate avanti in altri contesti, compresi i progetti di collaborazione in materia informatica[100] degli Stati membri nell'ambito della PESCO, nonché con le strutture di cibersicurezza dell'UE, per sostenere la condivisione delle informazioni e il sostegno reciproco.

Iniziative strategiche

L'UE dovrebbe:

- completare il quadro europeo per la gestione delle crisi di cibersicurezza e determinare la procedura, le tappe e le scadenze per la creazione dell'unità congiunta per il ciberspazio;
- proseguire l'attuazione dell'agenda sulla criminalità informatica nell'ambito della strategia dell'UE per l'Unione della sicurezza;
- promuovere e facilitare l'istituzione di un gruppo di lavoro di intelligence informatica degli Stati membri all'interno del Centro UE di situazione e di intelligence (INTCEN);
- promuovere la posizione di dissuasione informatica dell'UE per prevenire, scoraggiare, dissuadere e rispondere alle attività informatiche dolose;
- rivedere il quadro strategico dell'UE in materia di ciberdifesa;
- facilitare lo sviluppo di una "visione e strategia militari dell'UE sul ciberspazio come dominio operativo" per le missioni e le operazioni militari della PSDC;
- sostenere sinergie tra l'industria civile, della difesa e dello spazio; e
- rinforzare la cibersicurezza delle infrastrutture spaziali critiche nell'ambito del programma spaziale.

[97] Sono attualmente in corso vari progetti PESCO legati al ciberspazio, segnatamente la piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti informatici, i gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza, l'accademia e polo di innovazione dell'UE nel settore dell'informatica e il centro di coordinamento del settore informatico e dell'informazione.

[98] Nell'ambito del Fondo europeo per la difesa, la Commissione ha già individuato opportunità per potenziali azioni collaborative di ricerca e sviluppo nel campo della ciberdifesa, volte a rafforzare la cooperazione, la capacità di innovazione e la competitività dell'industria della difesa.

[99] Quali Orizzonte Europa, Europa digitale e il FED.

[100] https://pesco.europa.eu/.

3. PROMUOVERE UN CIBERSPAZIO GLOBALE E APERTO

L'UE dovrebbe continuare a collaborare con i partner internazionali per promuovere un modello politico e una visione del ciberspazio fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici che generino sviluppo sociale, economico e politico a livello globale e contribuiscano a un'Unione della sicurezza. La cooperazione internazionale è essenziale per mantenere un ciberspazio globale, aperto, stabile e sicuro. A tal fine l'UE dovrebbe continuare a lavorare con i paesi terzi, le organizzazioni internazionali e la comunità multipartecipativa per sviluppare e attuare una politica internazionale in materia di ciberspazio coerente e olistica tenendo conto della crescente interconnessione tra gli aspetti economici delle nuove tecnologie, la sicurezza interna e le politiche estere, di sicurezza e di difesa. L'UE, in quanto forte blocco economico e commerciale fondato sui valori democratici fondamentali, sul rispetto dello Stato di diritto e dei diritti fondamentali, è anche in una posizione privilegiata per guidare la definizione e la promozione di norme e standard internazionali.

3.1. Leadership dell'UE in materia di standard, norme e quadri nel ciberspazio

Potenziare la normazione internazionale

Per promuovere e difendere la sua visione del ciberspazio a livello internazionale, l'UE deve **intensificare il suo impegno e la sua leadership nei processi di normazione internazionale, nonché rafforzare la sua rappresentanza negli organismi di normazione internazionali ed europei e in altre organizzazioni per lo sviluppo di norme**[101]. Poiché le tecnologie digitali si stanno sviluppando a ritmo serrato, le norme internazionali sono sempre più importanti per integrare gli sforzi normativi tradizionali in settori quali l'IA, il cloud, il calcolo quantistico e la comunicazione quantistica. La normazione internazionale è sempre più utilizzata dai paesi terzi per far progredire la loro agenda politica e ideologica, che spesso non corrisponde ai valori dell'UE. Vi è inoltre un rischio crescente di quadri concorrenti per la normazione internazionale, che porta alla frammentazione.

La formulazione di norme internazionali nei settori delle tecnologie emergenti e dell'architettura di base di Internet in linea con i valori dell'UE è essenziale per garantire che Internet rimanga globale e aperta, che le tecnologie siano antropocentriche, attente alla riservatezza, e che il loro uso sia legale, sicuro ed etico. Nell'ambito della sua prossima strategia di normazione, l'UE dovrebbe definire i suoi **obiettivi per la normazione internazionale** e condurre un'azione proattiva e coordinata per promuoverli a livello internazionale. Si dovrebbe cercare una cooperazione più forte e una condivisione degli oneri con i partner che condividono le stesse idee e con i portatori di interessi europei.

Promuovere comportamenti responsabili degli Stati nel ciberspazio

L'UE continua a collaborare con i partner internazionali per far progredire e promuovere un ciberspazio globale, aperto, stabile e sicuro in cui il **diritto internazionale, in particolare la Carta delle Nazioni Unite (ONU)[102], sia rispettato** come pure siano rispettate **le norme, le**

[101] Ad esempio International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardization (CENELEC), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP) e Institute of Electrical and Electronics Engineers (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.

regole e i principi volontari non vincolanti di un comportamento responsabile degli Stati[103]. Con il deterioramento di un efficace dibattito multilaterale sulla sicurezza internazionale nel ciberspazio, è evidente la necessità che l'UE e gli Stati membri assumano una posizione maggiormente proattiva nelle discussioni in seno all'ONU e in altre sedi internazionali pertinenti. L'UE è nella posizione migliore per **promuovere, coordinare e consolidare le posizioni degli Stati membri** presso le **sedi internazionali** e dovrebbe **sviluppare una posizione dell'Unione sull'applicazione del diritto internazionale nel ciberspazio**. L'alto rappresentante, unitamente agli Stati membri, mira inoltre a portare avanti la loro proposta inclusiva e basata sul consenso per un impegno politico su un **programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio (PoA)**[104] in seno all'ONU. Sulla base della normativa esistente, approvata dall'Assemblea generale dell'ONU[105], il programma d'azione offre una piattaforma per la cooperazione e lo scambio delle migliori pratiche all'interno dell'ONU e propone di istituire un meccanismo per attuare le norme sul comportamento responsabile degli Stati, nonché promuovere lo sviluppo delle capacità. Inoltre l'alto rappresentante mira a rafforzare e incoraggiare l'attuazione di **misure di rafforzamento della fiducia** tra gli Stati, compresa la condivisione delle migliori pratiche a livello regionale e multilaterale e il contributo alla cooperazione interregionale.

L'aumento della connettività globale non dovrebbe portare alla censura, alla sorveglianza di massa, alla violazione della riservatezza dei dati e alla repressione contro la società civile, il mondo accademico e i cittadini. L'UE dovrebbe continuare a guidare la protezione e la promozione dei **diritti umani e delle libertà fondamentali** online. A tal fine l'UE dovrebbe promuovere una maggiore conformità al diritto e alle norme internazionali in materia di diritti umani[106] e rendere operativo il suo piano d'azione sui diritti umani e la democrazia 2020-2024[107], nonché sviluppare gli orientamenti in materia di diritti umani per la libertà di espressione online e offline[108], **offrendo un nuovo impulso all'applicazione pratica degli strumenti dell'UE**. L'UE dovrebbe impegnarsi a fondo per **proteggere i difensori dei diritti umani, la società civile e il mondo accademico impegnati in ambiti quali la cibersicurezza, la riservatezza dei dati, la sorveglianza e la censura online**. A tal fine l'UE dovrebbe fornire ulteriori orientamenti pratici, promuovere le migliori pratiche e intensificare gli sforzi per prevenire l'uso improprio delle tecnologie emergenti, in particolare attraverso l'uso di misure diplomatiche, ove necessario, e il controllo delle esportazioni di tali tecnologie. L'UE dovrebbe inoltre continuare a lottare per la protezione dei membri più vulnerabili della società online, elaborando una legislazione per proteggere meglio i bambini contro l'abuso e lo sfruttamento sessuale dei minori e una strategia sui diritti dei minori.

---

[103] Come risulta dalle relazioni pertinenti dei gruppi di esperti governativi sugli sviluppi nel settore dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale (UNGGE), approvate dall'Assemblea generale delle Nazioni Unite, in particolare le relazioni del 2015, 2013 e 2010.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

[105] Come risulta dalle relazioni pertinenti del gruppo di esperti governativi sugli sviluppi nel settore dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale, approvate dall'Assemblea generale delle Nazioni Unite, in particolare le relazioni del 2015, 2013 e 2010.

[106] In particolare la Carta delle Nazioni Unite e la Dichiarazione universale dei diritti dell'uomo.

[107] https://www.consilium.europa.eu/en/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/.

[108] https://www.consilium.europa.eu/media/28348/142549.pdf.

La convenzione di Budapest sulla criminalità informatica

L'UE continua a sostenere i paesi terzi che desiderano aderire alla **convenzione di Budapest sulla criminalità informatica del Consiglio d'Europa** e si adopera per completare il **secondo protocollo aggiuntivo alla convenzione di Budapest** che comprende misure e salvaguardie volte a migliorare la cooperazione internazionale tra le forze dell'ordine e le autorità giudiziarie, nonché tra le autorità e i fornitori di servizi di altri paesi e per i quali la Commissione partecipa ai negoziati a nome dell'UE[109]. L'attuale iniziativa per un nuovo strumento giuridico sulla criminalità informatica a livello delle Nazioni Unite rischia di amplificare le divisioni e di rallentare le necessarie riforme nazionali e i relativi sforzi di sviluppo delle capacità, ostacolando potenzialmente un'efficace cooperazione internazionale contro la criminalità informatica: l'UE non vede la necessità di un nuovo strumento giuridico sulla criminalità informatica a livello delle Nazioni Unite. L'UE continua ad impegnarsi negli **scambi multilaterali sulla criminalità informatica** per garantire il rispetto dei diritti umani e delle libertà fondamentali, attraverso l'inclusione, la trasparenza e tenendo conto delle competenze disponibili, con l'obiettivo di fornire un valore aggiunto per tutti.

3.2 Cooperazione con i partner e la comunità multipartecipativa

L'UE dovrebbe **rafforzare ed espandere i propri dialoghi in materia di ciberspazio con i paesi terzi** per promuovere i suoi valori e la sua visione del ciberspazio, condividendo le migliori pratiche e cercando di cooperare in modo più efficace. L'UE dovrebbe inoltre avviare **scambi strutturati con organizzazioni regionali** come l'Unione africana, il Forum regionale dell'ASEAN, l'Organizzazione degli Stati americani e l'Organizzazione per la sicurezza e la cooperazione in Europa. Al tempo stesso l'UE dovrebbe cercare di trovare un terreno comune, ove possibile e opportuno, con altri partner sulla base di questioni di interesse comune. Lavorando con le delegazioni dell'UE e, se del caso, con le ambasciate degli Stati membri in tutto il mondo, l'UE dovrebbe formare una **rete informale della diplomazia informatica dell'UE** per promuovere la visione europea del ciberspazio, scambiare informazioni e coordinarsi regolarmente sugli sviluppi nel ciberspazio[110].

Sulla base delle dichiarazioni congiunte dell'8 luglio 2016[111] e del 10 luglio 2018[112], l'UE dovrebbe continuare a far progredire la **cooperazione UE-NATO**, in particolare per quanto riguarda i requisiti di interoperabilità della ciberdifesa. In questo contesto l'UE dovrebbe perseguire ulteriormente l'affiliazione delle pertinenti strutture PSDC alla rete delle missioni federate della NATO, consentendo l'interoperabilità della rete con la NATO e i partner, quando necessario. Inoltre la cooperazione tra l'UE e la NATO in materia di istruzione, formazione ed esercitazioni dovrebbe essere ulteriormente esplorata, anche cercando sinergie tra l'Accademia europea per la sicurezza e la difesa e il Centro di eccellenza della NATO per la ciberdifesa cooperativa.

In linea con i suoi valori, l'UE sostiene e promuove con forza il **modello multipartecipativo per la governance di Internet**. Nessuna singola entità, governo o organizzazione internazionale dovrebbe cercare di controllare Internet. L'UE dovrebbe continuare a

[109] Decisione del Consiglio del giugno 2019 (rif. 9116/19).
[110] Se del caso, potrebbe anche far leva sulle attività della rete informale della diplomazia digitale dell'UE che comprende i ministeri degli Esteri degli Stati membri.
[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/.

impegnarsi nelle sedi pertinenti[113] per rafforzare la cooperazione e garantire la protezione dei diritti e delle libertà fondamentali, in particolare il diritto alla dignità, alla riservatezza e alla libertà di espressione e di informazione. Per sviluppare una cooperazione multipartecipativa sulle questioni di cibersicurezza, la Commissione e l'alto rappresentante, in linea con le rispettive competenze, mirano a rafforzare gli **scambi regolari e strutturati con i portatori di interessi**, compreso il settore privato, il mondo accademico e la società civile, sottolineando che la natura interconnessa del ciberspazio richiede che tutti i portatori di interessi si scambino informazioni e si assumano le proprie responsabilità specifiche per mantenere un ciberspazio globale, aperto, stabile e sicuro. Questi sforzi forniranno un prezioso contributo per potenziali azioni chiave a livello dell'UE.

3.3. Consolidare le capacità globali per aumentare la resilienza globale

Al fine di garantire che tutti i paesi siano in grado di raccogliere i benefici sociali, economici e politici di Internet e dell'uso delle tecnologie, l'UE continua a sostenere i suoi partner per aumentare la loro ciberresilienza e le loro capacità di indagare sulla criminalità informatica e di perseguirla, nonché di affrontare le minacce informatiche. Al fine di garantire la coerenza complessiva, l'UE dovrebbe sviluppare un'**agenda dell'UE per lo sviluppo delle capacità informatiche esterne** al fine di orientare questi sforzi in linea con i suoi orientamenti per lo sviluppo delle capacità informatiche esterne[114] e con l'Agenda 2030 per lo sviluppo sostenibile[115]. Il programma dovrebbe sfruttare le competenze degli Stati membri e delle istituzioni, degli organismi e delle agenzie e iniziative pertinenti dell'UE, compresa la rete dell'UE per lo sviluppo delle capacità informatiche[116], in linea con i loro rispettivi mandati. Deve essere creato un **comitato dell'UE per lo sviluppo delle capacità informatiche** al fine di comprendere i pertinenti portatori di interessi dell'UE e monitorare i progressi compiuti, oltre a individuare ulteriori sinergie e potenziali lacune. Esso può inoltre sostenere una migliore cooperazione con gli Stati membri, nonché con i partner del settore pubblico e privato e altri organismi internazionali pertinenti per garantire il coordinamento degli sforzi ed evitare duplicazioni.

Lo **sviluppo delle capacità informatiche dell'UE** dovrebbe continuare a concentrarsi sui Balcani occidentali e sui paesi vicini dell'UE, nonché sui paesi partner che stanno vivendo un rapido sviluppo digitale. Gli sforzi dell'UE dovrebbero sostenere lo sviluppo della legislazione e delle politiche dei paesi partner in linea con le norme e le politiche della diplomazia informatica dell'UE. In questo contesto gli sforzi dell'UE per lo sviluppo delle capacità nel campo della digitalizzazione dovrebbero includere la cibersicurezza come caratteristica standard. A tal fine l'UE dovrebbe sviluppare un programma di formazione dedicato al personale dell'UE responsabile dell'attuazione degli sforzi dell'UE in materia di sviluppo delle capacità digitali e capacità informatiche esterne. L'UE dovrebbe inoltre assistere questi Paesi nell'affrontare la crescente sfida delle attività informatiche dolose che danneggiano lo sviluppo delle loro società e **l'integrità e la sicurezza dei sistemi democratici**, in linea con gli sforzi compiuti nell'ambito del piano d'azione per la democrazia europea. L'apprendimento tra pari tra gli Stati membri dell'UE, le agenzie UE competenti e i paesi terzi potrebbe essere particolarmente utile a questo proposito.

[113] Come la Internet Corporation for Assigned Names and Numbers (ICANN) e l'Internet Governance Forum (IGF).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

Infine, nell'ambito del patto sulla dimensione civile della PSDC del 2018[117], le missioni civili della PSDC possono anche contribuire alla più ampia risposta dell'UE per affrontare le sfide della cibersicurezza, in particolare rafforzando lo Stato di diritto all'interno dei paesi partner, nonché le capacità delle forze dell'ordine e delle amministrazioni civili dei paesi partner.

Iniziative strategiche

L'UE dovrebbe:

- definire una serie di obiettivi nei processi di normazione internazionale e promuoverli a livello internazionale;
- promuovere la sicurezza e la stabilità internazionali nel ciberspazio, in particolare attraverso la proposta dell'UE e dei suoi Stati membri di un programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio (PoA) in seno alle Nazioni Unite;
- offrire orientamenti pratici sull'applicazione dei diritti umani e delle libertà fondamentali nel ciberspazio;
- proteggere maggiormente i minori dall'abuso e dallo sfruttamento sessuale, nonché sviluppare una strategia sui diritti dei minori;
- rafforzare e promuovere la convenzione di Budapest sulla criminalità informatica, anche attraverso il lavoro sul secondo protocollo aggiuntivo alla convenzione di Budapest;
- estendere il dialogo dell'UE in materia di ciberspazio con paesi terzi, organizzazioni internazionali e regionali, anche attraverso una rete informale della diplomazia informatica dell'UE;
- consolidare gli scambi con la comunità multipartecipativa, in particolare attraverso scambi regolari e strutturati con il settore privato, il mondo accademico e la società civile; e
- proporre un'agenda dell'UE per lo sviluppo delle capacità informatiche esterne e un comitato per lo sviluppo delle capacità informatiche dell'UE.

III. LA CIBERSICUREZZA NELLE ISTITUZIONI, NEGLI ORGANISMI E NELLE AGENZIE DELL'UE

Dato il loro alto profilo politico, le loro missioni critiche per coordinare questioni altamente sensibili e il loro ruolo nella gestione di ingenti somme di denaro pubblico, **le istituzioni, gli organismi e le agenzie dell'UE sono regolarmente bersaglio di attacchi informatici**, in particolare di spionaggio informatico. Tuttavia il livello di ciberresilienza e la capacità di individuare e contrastare attività informatiche dolose varia in modo significativo tra queste entità in termini di maturità. È quindi necessario migliorare il livello generale di cibersicurezza mediante regole coerenti e omogenee.

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/it/pdf

Nel settore della sicurezza dell'informazione, sono stati compiuti progressi verso una maggiore coerenza delle **regole per la protezione delle informazioni classificate UE e delle informazioni sensibili non classificate**. L'interoperabilità dei sistemi di informazioni classificate rimane tuttavia limitata, impedendo un trasferimento fluido delle informazioni tra le diverse entità. Si dovrebbero compiere ulteriori progressi per consentire un approccio interistituzionale al trattamento delle informazioni classificate dell'UE e delle informazioni sensibili non classificate, che potrebbe anche fungere da modello per l'interoperabilità tra gli Stati membri. Occorre inoltre stabilire una base di riferimento per semplificare le procedure con gli Stati membri. L'UE dovrebbe inoltre sviluppare ulteriormente la propria capacità di comunicare in maniera sicura con i partner pertinenti basandosi, per quanto possibile, sui meccanismi e sulle procedure esistenti.

Come annunciato nella strategia per l'Unione della sicurezza, la Commissione presenterà quindi proposte di **norme comuni vincolanti sulla sicurezza dell'informazione e di norme comuni vincolanti sulla cibersicurezza per tutte le istituzioni, gli organismi e le agenzie dell'UE nel 2021**, sulla base delle discussioni interistituzionali in corso nell'UE sulla cibersicurezza[118].

Le tendenze attuali e future in materia di telelavoro richiederanno anche ulteriori investimenti in attrezzature, infrastrutture e strumenti sicuri che consentano di lavorare a distanza su file sensibili e classificati.

Inoltre il panorama sempre più ostile delle minacce informatiche, nonché la crescente incidenza di attacchi informatici più sofisticati che interessano le istituzioni, gli organismi e le agenzie dell'UE determina la necessità di aumentare gli investimenti per raggiungere un elevato livello di maturità informatica. È in fase di istituzione un programma di sensibilizzazione informatica per tutte le istituzioni, gli organismi e le agenzie dell'UE, al fine di aumentare la consapevolezza e l'igiene informatica del personale e di sostenere una cultura comune in materia di cibersicurezza.

È necessario **rafforzare il CERT-UE con un meccanismo di finanziamento migliorato** per aumentare la sua capacità di aiutare le istituzioni, gli organismi e le agenzie dell'UE ad applicare le nuove regole in materia di sicurezza informatica e a migliorare la loro ciberresilienza. Per raggiungere tali obiettivi si dovrà rafforzare anche il mandato del CERT-UE per fornirlo di mezzi stabili.

Iniziative strategiche

1. Regolamento sulla sicurezza dell'informazione nelle istituzioni, negli organismi e nelle agenzie dell'UE
2. Regolamento su norme comuni in materia di cibersicurezza per le istituzioni, gli organismi e le agenzie dell'UE
3. Una nuova base giuridica per il CERT-UE al fine di consolidarne mandato e finanziamenti.

[118] Un regolare dibattito interistituzionale dell'UE sulla sicurezza informatica si inserisce nel più ampio scambio sulle opportunità e sulle sfide della trasformazione digitale per le istituzioni dell'UE.

IV. CONCLUSIONI

L'attuazione concertata della presente strategia contribuirà a un decennio digitale sicuro dal punto di vista della cibersicurezza per l'UE, alla realizzazione di un'Unione della sicurezza e al rafforzamento della posizione dell'UE a livello globale.

L'UE dovrebbe orientare standard e norme per soluzioni di livello mondiale e norme di cibersicurezza per i servizi essenziali e le infrastrutture critiche, così come lo sviluppo e l'applicazione di nuove tecnologie. Ogni organizzazione e ogni individuo che utilizza Internet fa parte della soluzione per garantire una trasformazione digitale caratterizzata dalla cibersicurezza.

La Commissione e l'alto rappresentante, in linea con le rispettive competenze, monitoreranno i progressi compiuti nell'ambito della presente strategia e svilupperanno criteri di valutazione. All'interno di tale monitoraggio dovrebbero confluire le relazioni dell'ENISA e le relazioni periodiche della Commissione sull'Unione della sicurezza. I risultati contribuiranno ai prossimi obiettivi del decennio digitale[119]. In linea con le loro rispettive competenze, la Commissione e l'alto rappresentante continueranno a collaborare con gli Stati membri per individuare misure pratiche di collegamento delle quattro comunità di cibersicurezza nell'UE ovvero la resilienza delle infrastrutture critiche e del mercato interno, la giustizia e le forze dell'ordine, la diplomazia informatica e la ciberdifesa, laddove necessario. La Commissione e l'alto rappresentante continueranno inoltre a impegnarsi con la comunità multipartecipativa, sottolineando la necessità che tutti coloro che utilizzano Internet facciano la loro parte per mantenere un ciberspazio globale, aperto, stabile e sicuro, dove tutti possano vivere in sicurezza la propria vita digitale.

[119] Come annunciato nel programma di lavoro della Commissione per il 2021.

Appendice: prossimi passi per la cibersicurezza delle reti 5G

Sulla base dei risultati della revisione della raccomandazione della Commissione sulla cibersicurezza delle reti 5G[120], le prossime fasi del lavoro coordinato a livello dell'UE dovrebbero concentrarsi su tre obiettivi chiave e sulle principali azioni a breve e medio termine indicate nella tabella sottostante, che dovranno essere attuate dalle autorità degli Stati membri, dalla Commissione e dall'ENISA.

La prima priorità per la prossima fase è quella di **completare l'attuazione del pacchetto di strumenti a livello nazionale, nonché di affrontare le questioni evidenziate nella relazione sullo stato di avanzamento del luglio 2020**. In questo contesto, alcune misure strategiche del pacchetto di strumenti beneficerebbero di un **maggiore lavoro di coordinamento o scambio di informazioni** all'interno del gruppo di lavoro NIS, come già rilevato nella relazione sullo stato di avanzamento, che potrebbe potenzialmente portare allo sviluppo di **buone pratiche o di orientamenti**. Per quanto riguarda le misure tecniche, l'ENISA potrebbe fornire ulteriore supporto, basandosi sul lavoro già svolto e approfondendo alcuni argomenti, oltre a **sviluppare una panoramica completa di tutti gli orientamenti pertinenti riguardanti i requisiti di cibersicurezza del 5G per gli operatori di reti mobili**.

In secondo luogo, gli Stati membri hanno sottolineato l'importanza di stare al passo con gli sviluppi attraverso il **monitoraggio continuo dell'evoluzione della tecnologia, dell'architettura 5G, delle minacce e dei casi d'uso e delle applicazioni del 5G, come pure dei fattori esterni**, al fine di poter **individuare e affrontare rischi nuovi o emergenti**. È inoltre opportuno approfondire ulteriormente alcuni aspetti dell'analisi iniziale dei rischi, in particolare per garantire che essa tenga conto dell'intero ecosistema del 5G, comprese tutte le parti pertinenti dell'infrastruttura di rete e della catena di approvvigionamento 5G. Sebbene il pacchetto di strumenti sia stato progettato come uno strumento flessibile e adattabile, a medio termine si potrebbero, se necessario, adottare misure per ampliarlo o modificarlo, affinché resti completo e aggiornato.

In terzo luogo, si dovrebbero continuare a intraprendere **azioni a livello dell'UE** volte a sostenere e completare gli obiettivi del pacchetto di strumenti al fine di integrarli pienamente nelle pertinenti politiche dell'Unione e della Commissione, in particolare dando seguito alle azioni annunciate dalla Commissione nella sua comunicazione sul pacchetto di strumenti del 29 gennaio 2020[121] per una vasta gamma di ambiti (ad esempio finanziamenti dell'UE per le reti 5G sicure, investimenti in tecnologie 5G e post-5G, strumenti di difesa commerciale e concorrenza per evitare distorsioni nel mercato dell'approvvigionamento del 5G, ecc.).

Ove opportuno, i principali attori dovrebbero concordare agli inizi del 2021, regimi dettagliati e tappe per le principali azioni stabilite qui di seguito.

Obiettivo chiave 1: garantire approcci nazionali convergenti per un'efficace attenuazione dei rischi in tutta l'UE		
Ambiti	**Principali azioni nel breve e medio termine**	**Attori**

[120] Relazione della Commissione sull'impatto della raccomandazione 2019/534 della Commissione, del 26 marzo 2019, sulla cibersicurezza delle reti 5G.

[121] Comunicazione COM(2020) 50 della Commissione "Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE", del 29 gennaio 2020.

		principali
Attuazione del pacchetto di strumenti da parte degli Stati membri	Completare l'attuazione delle misure raccomandate nelle conclusioni del pacchetto di strumenti entro il secondo trimestre del 2021, con bilanci e aggiornamenti periodici all'interno del gruppo di lavoro NIS.	Autorità degli Stati membri
Scambio di informazioni e migliori pratiche sulle misure strategiche relative ai fornitori	Intensificare gli scambi di informazioni e considerare possibili migliori pratiche, in particolare riguardo a quanto segue: - restrizioni applicate ai fornitori ad alto rischio (SM03), nonché misure sulla fornitura di servizi gestiti (SM04); - sicurezza e resilienza della catena di approvvigionamento, in particolare dando seguito all'indagine condotta dal BEREC riguardo ai SM05-SM06.	Autorità degli Stati membri, Commissione
Sviluppo delle capacità e orientamenti sulle misure tecniche	Svolgere approfondimenti tecnici e sviluppare orientamenti e strumenti comuni, tra cui: - una matrice completa e dinamica dei controlli di sicurezza e migliori pratiche in materia di sicurezza del 5G; orientamenti a sostegno dell'attuazione di misure tecniche selezionate dal pacchetto di strumenti.	ENISA, autorità degli Stati membri
Obiettivo chiave 2: sostenere lo scambio continuo di conoscenze e lo sviluppo delle capacità		
Ambiti	**Principali azioni nel breve e medio termine**	**Attori principali**
Sviluppo continuo delle conoscenze	Organizzare attività di sviluppo delle conoscenze sulla tecnologia e sulle sfide correlate (architetture aperte, caratteristiche del 5G, ad es. virtualizzazione, containerizzazione, slicing, ecc.), evoluzioni del panorama delle minacce, incidenti nella vita reale, ecc.	ENISA, autorità degli Stati membri, altri portatori di interessi
Valutazioni dei rischi	Aggiornamento e scambio di informazioni sulle valutazioni aggiornate dei rischi a livello nazionale	Autorità degli Stati membri, Commissione, ENISA
Progetti comuni finanziati dall'UE a sostegno dell'attuazione del pacchetto di strumenti	Fornire sostegno finanziario ai progetti che contribuiscono all'attuazione del pacchetto di strumenti utilizzando i finanziamenti dell'UE, in particolare nell'ambito del programma Europa digitale (ad esempio progetti di sviluppo delle capacità per le autorità nazionali, banchi di prova o altre capacità avanzate, ecc.)	Autorità degli Stati membri, Commissione
Cooperazione tra i portatori di interessi	Promuovere la collaborazione e la cooperazione tra autorità nazionali impegnate nella cibersicurezza del 5G (ad esempio gruppo di cooperazione NIS, autorità responsabili della cibersicurezza, autorità di regolamentazione delle telecomunicazioni) e con portatori privati di interessi	Autorità degli Stati membri, Commissione, ENISA
Obiettivo chiave 3: promuovere la resilienza della catena di approvvigionamento e altri obiettivi strategici di sicurezza dell'UE		
Ambiti	**Principali azioni nel breve e medio termine**	**Attori principali**
Normazione	Definire e attuare un piano di azione concreto al fine di aumentare la rappresentanza dell'UE negli organismi di normazione nell'ambito delle prossime fasi del lavoro del	Autorità degli Stati membri

	sottogruppo NIS sulla normazione, al fine di raggiungere specifici obiettivi di sicurezza, compresa la promozione di interfacce interoperabili per facilitare la diversificazione dei fornitori.	
Resilienza della catena di approvvigionamento	- Condurre un'analisi approfondita dell'ecosistema 5G e della catena di approvvigionamento per meglio individuare e monitorare gli asset chiave e le potenziali dipendenze critiche. - Assicurare che il funzionamento del mercato e della catena di approvvigionamento del 5G sia in linea con le regole e gli obiettivi dell'UE in materia di commercio e di concorrenza, come definito nella comunicazione della Commissione del 29 gennaio, e che il monitoraggio degli IED sia applicato agli sviluppi degli investimenti che possono influire sulla catena del valore del 5G, tenendo conto degli obiettivi del pacchetto di strumenti. - Monitorare le tendenze di mercato esistenti e previste, valutando i rischi e le opportunità nel campo della Open RAN, in particolare attraverso uno studio indipendente.	Autorità degli Stati membri, Commissione
Certificazione	Avviare i preparativi dei pertinenti sistemi di certificazione dei candidati per i principali componenti del 5G e i processi dei fornitori, al fine di contribuire ad affrontare alcuni rischi legati alle vulnerabilità tecniche, come definito nei piani di attenuazione dei rischi del pacchetto di strumenti.	Commissione, ENISA, autorità nazionali, altri portatori di interessi
Capacità dell'UE e dispiegamenti sicuri delle reti	- Investire nella ricerca e innovazione e nelle capacità, in particolare mediante l'adozione di reti intelligenti e partenariati di servizi. - Attuare condizioni di sicurezza pertinenti per i programmi di finanziamento e gli strumenti finanziari (interni ed esterni) dell'UE, come annunciato nella comunicazione della Commissione del 29 gennaio.	Stati membri, Commissione, portatori di interessi dell'industria del 5G
Dimensione esterna	Rispondere favorevolmente alle richieste di paesi terzi che vorrebbero comprendere e potenzialmente utilizzare l'approccio del pacchetto di strumenti sviluppato dall'UE.	Stati membri, Commissione SEAE, delegazioni UE