# COMMISSIONI RIUNITE

## IV (Difesa)
## e IX (Trasporti, poste e telecomunicazioni)

*S O M M A R I O*

ATTI DELL'UNIONE EUROPEA:

Comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE. JOIN(2022) 49 final *(Esame e rinvio)* ..... 14

**ATTI DELL'UNIONE EUROPEA**

*Mercoledì 15 marzo 2023. — Presidenza del presidente della IX Commissione Salvatore DEIDDA. – Interviene il sottosegretario di Stato per la difesa Matteo Perego Di Cremnago.*

**La seduta comincia alle 14.25.**

**Comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE.**
**JOIN(2022) 49 final.**

*(Esame e rinvio).*

Le Commissioni iniziano l'esame del provvedimento.

Salvatore DEIDDA, *presidente*, avverte che il gruppo PD-IDP ha chiesto che la pubblicità dei lavori sia assicurata anche attraverso il sistema di ripresa audiovideo a circuito chiuso. Non essendovi obiezioni, ne dispone l'attivazione.

Monica CIABURRO (FDI), *relatrice per la IV Commissione*, riferisce che la comunicazione « La politica di ciberdifesa dell'UE », presentata dalla Commissione e dall'Alto Rappresentante il 10 novembre 2022, propone una serie d'iniziative volte alla creazione di una capacità di ciberdifesa dell'UE a tutto spettro, sulla base del mandato ricevuto dal Consiglio dell'UE, delle priorità indicate dalla Bussola Strategica dell'UE – il documento approvato nel marzo 2022 che delinea un percorso per rafforzare la politica di sicurezza e di difesa dell'UE per il prossimo decennio – delle conclusioni adottate dal Consiglio europeo lo scorso 15 dicembre, che ha chiesto la definizione di una politica forte dell'UE in materia di ciberdifesa e maggiori investimenti per la cibersicurezza e per la resilienza delle infrastrutture critiche.

Fa presente quindi che, come evidenziato anche dalla comunicazione, negli ultimi anni si è assistito ad un moltiplicarsi dei comportamenti dolosi di soggetti statali e non statali nel ciberspazio, compreso un numero crescente di attacchi informatici che hanno preso di mira infrastrutture critiche militari e civili. Anche l'aggressione militare della Russia contro l'Ucraina ha evidenziato l'urgenza per l'UE di difendere i propri interessi e valori anche nel ciberspazio. Inoltre, gli attacchi alle reti energetiche, alle infrastrutture di trasporto e di

telecomunicazioni hanno mostrato come, nel ciberspazio, i confini tra minacce condotte alla dimensione militare civile e quella civile vanno sfumandosi. La crescente interdipendenza tra le infrastrutture fisiche e digitali ha, infatti, evidenziato la possibilità che incidenti di cibersicurezza gravi possano perturbare o danneggiare le infrastrutture critiche e destabilizzare l'economia e la società europee, minacciando anche, attraverso attacchi alle infrastrutture elettorali, il corretto funzionamento delle nostre democrazie.

In tale contesto, peraltro in veloce evoluzione per la continua progressione della digitalizzazione delle nostre società, l'UE è chiamata con urgenza, anche al fine di non accumulare un crescente *gap* di vulnerabilità, ad assumere maggiori responsabilità per la propria sicurezza nell'ambito della ciberdifesa a tutto spettro, dalla ricerca, al rilevamento, alla protezione ed alla risposta ad eventuali attacchi e gli Stati membri devono impegnarsi ad aumentare gli investimenti nelle rispettive capacità di ciberdifesa. L'UE deve essere, infatti, in grado di rilevare gli attacchi nelle loro fasi iniziali. La prevenzione e il rilevamento comuni costituiscono un aspetto importante della complessiva capacità di difesa dell'Unione e i dati di rilevamento devono poter essere trasformati in *intelligence* utilizzabile, che possa servire tanto per i profili civili di cibersicurezza quanto per quelli militari di ciberdifesa.

La comunicazione evidenzia, infatti, come la cooperazione tra le cibercomunità civili e della difesa sia alla base di una complessiva migliore conoscenza situazionale comune nel ciberspazio e sia cruciale per una risposta coordinata ed efficace alle crisi. Infine, poiché le cibertecnologie presentano un forte potenziale di duplice uso, la comunicazione indica che le industrie e le attività di ricerca e sviluppo nel settore della cibersicurezza e della ciberdifesa devono poter lavorare in modo molto più sinergico di quanto fatto fino ad ora e sottolinea l'importanza di costruire moduli per una collaborazione efficace fornitori privati di fiducia, che agiscano come forza di riserva per la cibersicurezza per migliorare la risposta in caso di attacchi informatici.

A fronte di tale quadro e delle criticità sopra evidenziate, la comunicazione in esame delinea quattro linee di azione principali: innanzi tutto, partendo dal presupposto che le azioni per la ciberdifesa sono in primo luogo una responsabilità nazione, si indica la necessita di rafforzare i meccanismi di coordinamento fra attori nazionali e dell'UE. È poi necessario predisporre un quadro di azioni volte a mettere in sicurezza l'ecosistema di ciberdifesa dell'UE; quindi promuovere un aumento degli investimenti in capacità di ciberdifesa da parte degli Stati membri ed infine, occorre sviluppare efficaci partenariati con Paesi terzi per superare le sfide comuni.

Rinvia, poi, l'illustrazione delle iniziative dettagliate alla documentazione degli uffici, soffermandosi, invece, sugli aspetti di maggiore rilevanza per ognuna delle linee di azione.

Per quanto riguarda la necessità di rafforzare i meccanismi di coordinamento fra attori nazionali e dell'UE nel settore della ciberdifesa, anche al fine di intensificare lo scambio di informazioni e la cooperazione fra le comunità militari e civili della ciberdifesa, si propone: di istituire un centro di coordinamento della ciberdifesa dell'UE che dovrebbe svolgere il ruolo di punto di raccordo per la conoscenza situazionale militare comune, coordinandosi con gli altri organi già operanti in ambiti affini a livello europeo; la creazione di una rete operativa a livello europeo dei *Computer Emergency Response Team* militari nazionali (milCERT), promuovendo altresì la cooperazione con la rete dei *Computer Security Incident Response Team* (CSIRT) civili nazionali ed inoltre la previsione di una conferenza dei comandanti per la sicurezza informatica dell'UE, che si dovrebbe riunire almeno due volte l'anno per discutere temi di interesse comune. Si prevede poi di promuovere un progetto denominato CyDef-X volto a servire come quadro di riferimento per le esercitazioni di ciberdifesa a livello UE. Inoltre segnala l'indicazione di valutare lo sviluppo ulteriore del concetto di gruppi di reazione rapida agli

incidenti informatici, sulla base del progetto *Cyber Rapid Response Teams*, già avviato in ambito PESCO.

Sul versante delle azioni che prevedono, invece, il sostegno a soggetti civili, sottolinea la possibilità di apportare modifiche al regolamento relativo al programma Europa digitale al fine di rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta; sviluppare una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia; effettuare prove presso soggetti critici al fine di rilevarne potenziali vulnerabilità.

Ulteriori modifiche legislative al programma Europa digitale, potrebbero inoltre consentire di sostenere finanziariamente a più lungo termine, e a integrazione dei finanziamenti nazionali, appalti congiunti di strumenti e infrastrutture ultrasicuri di prossima generazione.

Infine, per promuovere una maggiore sinergia tra la dimensione civile e quella militare, si prospetta la possibilità di vagliare lo sviluppo di sistemi di certificazione della cibersicurezza a livello UE per l'industria della cibersicurezza e le imprese private e di migliorare la cooperazione tra le cibercomunità della ciberdifesa e quelle di altro tipo.

Relativamente alle azioni volte a mettere in sicurezza il complesso dell'ecosistema della difesa da possibili vulnerabilità in ambito *ciber*, la comunicazione – rilevando come le Forze armate dipendano in larga misura dalle infrastrutture critiche civili per la mobilità, le comunicazioni o l'energia – indica la necessità di lavorare ulteriormente alla normazione e certificazione della cibersicurezza per mettere al riparo sia il settore civile sia quello militare. Gli Stati membri stanno, infatti, sviluppando per i rispettivi sistemi militari norme e requisiti di sicurezza propri, che non sempre tengono conto della necessità di interoperabilità né dell'esistenza di norme civili per i prodotti a duplice uso, andando quindi ad incidere negativamente sulla capacità di azione comune dell'UE nel ciberspazio e creando ostacoli all'eventuale assistenza reciproca. Inoltre, il fatto di dover rispettare norme diverse per i clienti civili e per quelli militari aumenta i costi industriali di produzione dei prodotti a duplice uso.

Tra le iniziative volte a far fronte a tali profili problematici in tema di cibersicurezza e interoperabilità, merita segnalare la proposta di sviluppare raccomandazioni non giuridicamente vincolanti per la comunità della Difesa, ispirate alle disposizioni della direttiva NIS2, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (misure che non si applicano al settore della Difesa), e quella di promuovere raccomandazioni sui requisiti di interoperabilità per la ciberdifesa dell'UE per facilitare le attività di collaborazione ed eventualmente condurre ad iniziative di sviluppo e approvvigionamento congiunte.

Per quanto riguarda l'ultimo profilo di competenza, quello relativo alla cooperazione con i Paesi *partner*, la comunicazione evidenzia l'importanza della cooperazione con quegli Stati che condividono gli stessi princìpi e valori, al fine di instaurare partenariati per gestire le sfide comuni nell'ambito della ciberdifesa che siano reciprocamente vantaggiosi.

Conclude richiamando l'esigenza – assai chiara nel testo della comunicazione – che occorre rafforzare, in via prioritaria, il partenariato strategico con l'Alleanza atlantica, sia nel settore della ciberdifesa sia in quello della cibersicurezza, nell'ambito dei quali sono necessari ulteriori sforzi per lo sviluppo di soluzioni condivise in relazione a sfide e minacce comuni e la cooperazione con gli Stati Uniti e i Paesi candidati all'adesione, fornendo in particolare sostegno a questi ultimi per lo sviluppo delle loro capacità di ciberdifesa, anche nel nuovo contesto determinato dall'aggressione militare della Russia nei confronti dell'Ucraina.

Erik Umberto PRETTO (LEGA), *relatore per la IX Commissione*, venendo ai profili di competenza della IX Commissione, gli preme innanzitutto evidenziare, nell'ambito della comunicazione, l'obiettivo di mobilitare investimenti nelle capacità europee di ciberdifesa, al fine di ovviarne le attuali vulnerabilità.

La comunicazione evidenzia le seguenti criticità: *a)* l'industria dell'UE della difesa, per quanto riguarda in particolare la ciberdifesa, si affida sostanzialmente a soluzioni civili e a mercati esterni; *b)* sebbene il mercato dei prodotti civili per l'informazione e la cibersicurezza sia in rapida crescita, esistono requisiti militari specifici che non sono soddisfatti dai normali prodotti civili; *c)* parti importanti dell'*hardware* e del *software* attualmente utilizzati per la ciberdifesa non sono prodotte nell'UE, il che crea dipendenze a livello industriale e tecnologico, suscettibili di produrre vulnerabilità importanti; *d)* la situazione di frammentazione della base industriale e tecnologica di difesa dell'UE, per la quale la maggior parte delle imprese che si occupano di cibersicurezza nell'UE sono piccole e medie imprese, ne riduce la sua competitività a livello globale.

Per ovviare alle suddette criticità, la Commissione intende promuovere la valorizzazione delle sinergie tra imprese civili e del settore della difesa ed avviare un dialogo con il settore al fine di sviluppare l'industria dell'UE della ciberdifesa, coinvolgendo opportunamente l'Agenzia europea per la difesa.

A tale fine, nell'immediato, la comunicazione indica la necessità di avviare innanzitutto una mappatura accurata delle capacità produttive dell'UE nel settore della difesa, al fine di individuare con precisione le carenze e gli ambiti nei quali è necessario un potenziamento, ed indica che le dipendenze critiche nel settore informatico potrebbero essere superate anche mediante il nuovo Fondo per la sovranità europea annunciato dalla presidente von der Leyen nel discorso sullo stato dell'Unione di settembre 2022.

Allo stesso tempo la comunicazione ricorda che il quadro dell'UE in materia di controllo degli investimenti esteri diretti continuerà a essere utilizzato per attenuare i rischi di acquisizioni di tecnologie o soluzioni europee che presentano rischi in materia di difesa e sicurezza.

La comunicazione rileva, inoltre, che il livello di partecipazione degli Stati membri a progetti di collaborazione per lo sviluppo della ciberdifesa rimane ad oggi insufficiente e dovrebbe essere aumentato per massimizzarne l'impatto a livello UE.

È quindi prioritario rafforzare la cooperazione e l'interoperabilità in materia di ciberdifesa sviluppando capacità congiunte e aumentando gli investimenti in ricerca e sviluppo, collaborando tramite le piattaforme di cooperazione e i meccanismi di finanziamento disponibili a livello di UE, quali la cooperazione strutturata permanente (PESCO) e il Fondo europeo per la difesa, il programma di ricerca e sviluppo Orizzonte Europa e il programma Europa digitale.

La comunicazione prevede poi un'iniziativa volta a delineare scenari di rischio per le infrastrutture critiche rilevanti per la comunicazione e la mobilità militari, concentrandosi innanzitutto nei settori dell'energia, delle telecomunicazioni, dei trasporti e dello spazio, comprese le infrastrutture fisse e mobili, i satelliti, i cavi sottomarini, l'instradamento in Internet.

La questione dell'infrastruttura critica marittima, compresa la protezione dei cavi sottomarini su cui transitano i dati, sarà ulteriormente affrontata nel contesto dell'imminente revisione della strategia per la sicurezza marittima dell'UE e del relativo piano d'azione, mentre ulteriori misure destinate a migliorare la solidità e la ciberresilienza delle infrastrutture spaziali e dei servizi collegati dovrebbero essere delineate nella strategia spaziale dell'UE per la sicurezza e la difesa la cui presentazione è prevista dalla bussola strategica.

Infine, si indica la necessita di rafforzare la cooperazione tra gli organismi di normazione civili e militari per la definizione di norme armonizzate per i prodotti a duplice uso, valutando in particolare la possibilità di istituire un comune sistema europeo di certificazione per le imprese che forniscono servizi all'industria della difesa.

La comunicazione invita gli Stati membri a prendere in considerazione l'elaborazione – nell'ambito del processo di revisione coordinata annuale sulla difesa (la cosiddetta CARD) – di una serie di impegni volontari per lo sviluppo di capacità nazio-

nali di ciberdifesa e di capacità multinazionali al di là dei progetti di ciberdifesa della PESCO esistenti.

Nell'ultimo rapporto sulla CARD, presentato dall'Agenzia per la difesa europea il 2 dicembre 2022, si evidenzia infatti che il settore cyberspazio è uno dei domini operativi della difesa che riceve minori investimenti da parte del complesso degli Stati membri dell'UE, con 9,8 miliardi di euro di investimenti previsti nel periodo 2019-2025, pari al circa il 3 per cento degli investimenti complessivi per l'intero periodo per il complesso degli altri domini operativi.

Da ultimo, particolare rilievo assume la constatazione di una carenza di competenze informatiche, che l'Organizzazione europea per la cibersicurezza ha stimato di 500.000 addetti al 2022, e la contestuale prefigurazione di un'accademia dell'UE delle competenze informatiche, che dovrebbe avere l'obiettivo di aumentare il numero di operatori professionali formati in cibersicurezza, e invita gli Stati membri a sviluppare programmi di istruzione specifici nel settore della ciberdifesa, coinvolgendo istituzioni accademiche e di istruzione superiore (civili e militari).

Il sottosegretario di Stato Matteo PEREGO DI CREMNAGO ringrazia i relatori per l'esauriente illustrazione della comunicazione e, a dimostrazione dell'attualità della minaccia cibernetica, aggiunge che il conflitto in Ucraina è stato preceduto da un imponente attacco *ciber*. Considera fondamentale la sensibilità dell'Unione europea per il rafforzamento dei sistemi di protezione nell'ambito delle reti informatiche e sottolinea come, in ambito Difesa, il COR sia l'organo deputato a garantire, con visione « unitaria », coerente ed in sicurezza, la gestione tecnico-operativa dei sistemi *Information and Communication Technology* (ICT) oltre ad essere preposto alla condotta delle *Cyber Network Operation*.

Pertanto, dopo avere rimarcato la forte compenetrazione tra gli aspetti militari e quelli civili della sicurezza delle comunicazioni, ribadisce l'esigenza che l'Unione europea riesca a dotarsi di una sovranità tecnologica in questo settore, evitando così di continuare a rimanere esposta alle minacce cibernetiche e sottolinea come il documento in esame consideri non più rinviabile la decisione di rafforzare le nostre reti.

Marco PELLEGRINI (M5S) apprezza la sottolineatura del relatore Pretto sulla ristrettezza di risorse finanziarie dedicate al dominio ciberspazio della Difesa nell'ambito della cosiddetta CARD (il processo di revisione coordinata annuale sulla difesa). Evidenzia come tali ridotti investimenti possano avere ripercussioni negative sia sul versante militare che su quello civile e condivide la considerazione del rappresentante del Governo riguardo la situazione di disagio che discende dalla dipendenza da Paesi extraeuropei dei principali *software* e *hardware*. Conclude aggiungendo che un piano di investimenti accurato dovrebbe, comunque, essere successivo a una accurata mappatura delle capacità tecnologiche in modo da evitare inutili sprechi di risorse.

Giulia PASTORELLA (A-IV-RE), dopo aver premesso che tutti i gruppi parlamentari concordano evidentemente sulla necessità ed urgenza della comunicazione in esame, sottolinea quattro punti.

Sulla situazione italiana, quanto alla relazione tra settore civile e militare, si chiede che impatto possa avere il cambio di *leadership* dell'Agenzia per la cybersicurezza nazionale (ACN), con la sostituzione di Roberto Baldoni, e se ci fossero delle criticità nel funzionamento dell'ACN che abbiano giustificato tale decisione, in particolare per il ruolo dell'agenzia sia nelle certificazioni che nell'assistenza alle imprese.

Per quanto riguarda sempre il settore civile e la gestione degli investimenti ad esso dedicati, ricorda che il programma Industria 4.0 prevedeva che i beni legati alla *cybersecurity* fossero passibili di iperammortamento e superammortamento. Visto che il Governo appare abbastanza aperto sulla possibilità di una revisione della normativa citata, consiglia di porre attenzione a tali potenzialità.

Sul codice degli appalti, uno dei suggerimenti che il suo gruppo aveva dato era di specificare una norma particolare per i prodotti digitali non *standard* che avessero componenti di *cybersecurity*, introducendo una soglia di valutazione del punteggio della qualità rispetto al prezzo, per evitare di utilizzare, in un settore così delicato, esclusivamente il criterio del minor prezzo.

Infine, afferma che il concetto di sovranità tecnologica fa sempre un po' paura a chi ha una formazione liberale. Argomenta comunque che le certificazioni di parti terze sono esattamente l'opposto della sovranità tecnologica: qualunque soluzione certificata deve poter operare sul mercato. Vi sono oggi tante normative europee che vanno nella direzione della certificazione come strumento per assicurare degli *standard* e dunque verso un'apertura al mercato, mentre il Governo appare più orientato verso lo sviluppo di « campioni locali ». Dichiara che occorre riconciliare questi due approcci e che la certificazione è complementare allo sviluppo di soluzioni proprie, perché nel frattempo vi è il bisogno concreto di proteggersi.

Flavio TOSI (FI-PPE) dichiara di condividere la parte finale dell'intervento della collega Pastorella. Afferma che è un fatto assodato che i sistemi i più efficienti di cibersicurezza sono oggi prodotti fuori dall'Unione europea, negli USA in modo particolare, e che le nostre istituzioni militari e civili si appoggiano dunque a *software* di Paesi stranieri. È giusto pensare alla sovranità, conclude, ma vi è un problema di urgenza e di affidabilità dei prodotti.

Antonino IARIA (M5S) rileva che il discorso tanto decantato della sovranità digitale comincia a mostrare delle crepe, come dimostrato dagli interventi sia di maggioranza che di opposizione. Offre dunque un consiglio politico: è necessario, afferma, approfondire le questioni prima di trasformare gli *slogan* in realtà.

Il sottosegretario di Stato Matteo PEREGO DI CREMNAGO evidenzia come il cambio al vertice dell'Agenzia per la cybersicurezza nazionale sia stato motivato da questioni di carattere tecnico e non politico, rimarcando la necessità di armonizzare le competenze tra l'ACN e i vari soggetti che operano nell'ambito della sicurezza cibernetica.

Ribadisce, quindi, che la sicurezza cibernetica non può essere garantita qualora mancasse la capacità di produrre *software* in maniera autonoma e richiama, al riguardo, un recente incidente che ha comportato l'apertura di oltre 20.000 *backdoor*.

Marco PELLEGRINI (M5S) chiede di intervenire per puntualizzare come, a suo avviso, le ragioni che hanno determinato la nomina del nuovo Direttore dell'Agenzia per la cybersicurezza nazionale siano di carattere politico e non tecnico, come riportato anche dalle agenzie stampa.

Salvatore DEIDDA, *presidente*, nessun altro chiedendo di intervenire, rinvia quindi il seguito dell'esame ad altra seduta.

**La seduta termina alle 15.**