SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

Doc. XXIV
n. 35

RISOLUZIONE DELLA 4ª COMMISSIONE PERMANENTE

(Difesa)

d'iniziativa del senatore ORTIS

approvata il 7 aprile 2021

---

ai sensi dell'articolo 50, comma 2, del Regolamento, a conclusione dell'esame dell'affare assegnato sui profili della sicurezza cibernetica attinenti alla difesa nazionale

---

TIPOGRAFIA DEL SENATO

La Commissione,

a conclusione dell'esame, ai sensi dell'articolo 50, comma 2, del Regolamento, dell'affare assegnato sui profili della sicurezza cibernetica attinenti alla difesa nazionale;

a seguito di un'attività istruttoria nel cui ambito si sono svolte le audizioni del generale di divisione Calogero Massara, vice comandante del Comando per le operazioni in rete (COR); di Laura Carpini, capo Unità per le politiche e la sicurezza dello spazio cibernetico del Ministero degli affari esteri e della cooperazione internazionale (MAECI); di Fabio Rugge, capo dell'Osservatorio dell'Istituto per gli studi di politica internazionale (ISPI) sulla sicurezza cibernetica; del colonnello Giovanni Reccia, già comandante del Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza; di Gabriele Faggioli, presidente dell'Associazione italiana per la sicurezza informatica; di Antonio Missiroli, vice segretario NATO con delega per le sfide emergenti alla sicurezza; di Roberto Baldoni, vice direttore del Dipartimento delle informazioni per la sicurezza (DIS); di Nunzia Ciardi, direttrice del servizio della Polizia postale della Polizia di Stato; del generale di brigata Marco Mochi, capo del III Reparto « Telematica » dell'Arma dei carabinieri; della professoressa Paola Severino; di Paolo Prinetto, direttore del Laboratorio nazionale *cyber security*; di Antimo Ponticiello, Direttore generale per lo studente, l'integrazione e la partecipazione del Ministero dell'istruzione; del generale Claudio Graziano, presidente del Comitato militare dell'Unione europea; di Eva Spina, Dirigente generale del Ministero dello sviluppo economico e dei rappresentanti delle società Leonardo, Fincantieri, Telsy, Telecom Italia, Elettronica, Intesa Sanpaolo, ENI, ENEL, SNAM ed *Engineering* Ingegneria informatica;

considerato che:

da tempo le relazioni sulla politica dell'informazione per la sicurezza pongono particolare attenzione sulla minaccia *cyber*, che è in continua evoluzione, capace di adattarsi all'innovazione tecnologica e di sfruttarne gli sviluppi. Le caratteristiche più significative di tale dominio sono l'ubiquità e l'asimmetria della minaccia, la velocità di trasmissione, l'assenza di confini geografici e politici, la difficoltà di individuare chi conduce l'attacco. Il rapido progresso nel settore informatico, sebbene da un lato sia ormai un irrinunciabile punto di forza per ogni Paese, dall'altro espone al potenziale rischio da attività malevola condotta nello spazio cibernetico, che sfrutta sia le vulnerabilità di cui possono essere affetti gli strumenti informatici in uso, sia la limitata sensibilità degli utenti, spesso inconsapevoli del rischio o poco inclini ad adottare le misure minime di sicurezza. Nel prossimo futuro, peraltro, non è difficile prevedere un'ulteriore espo-

nenziale estensione del dominio cibernetico e, quindi, delle possibilità di attacchi (anche in seguito alla diffusione, tra l'altro, delle criptovalute, o del cosiddetto « *internet* delle cose », dell'intelligenza artificiale, eccetera);

la recente emergenza epidemiologia da COVID-19 ha poi dimostrato che un uso maggiore degli strumenti informatici e delle connessioni in rete amplifica le occasioni di attacco. Come si legge nella relazione sulla politica dell'informazione per la sicurezza 2020, infatti: « la pandemia è stata un evento determinante anche in termini di impatto sulla società, sulle tecnologie in uso alla popolazione, sulla digitalizzazione di attività e servizi nonché sul conseguente ampliarsi della superficie di rischio cibernetico per l'individuo e per l'intero Sistema Paese. Hanno quindi acquisito maggiore attualità e concretezza le minacce alla sicurezza e al funzionamento delle reti e degli impianti, nonché alla continuità degli approvvigionamenti. Nel complesso si è evidenziato come gli attori ostili abbiano sfruttato, nel periodo pandemico, il massiccio ricorso al lavoro agile e la conseguente accessibilità da *internet*, tramite collegamenti VPN (*Virtual Private Network*), di risorse digitali di Ministeri, aziende di profilo strategico e infrastrutture critiche, divenuti ancor più bersaglio di campagne ostili di matrice statuale, criminale o hacktivista »;

per quanto riguarda le linee di tendenza quantitative e qualitative della minaccia, la stessa relazione dà conto di un generale incremento delle aggressioni (+20 per cento), che, quanto alla tipologia di *target* « hanno riguardato per lo più, a conferma di una tendenza già rilevata negli ultimi anni, sistemi IT di soggetti pubblici (83 per cento, in aumento di 10 punti percentuali rispetto al 2019). Tra questi ultimi, quelli maggiormente interessati dagli eventi risultano le Amministrazioni locali (48 per cento, valore in aumento di oltre 30 punti percentuali rispetto all'anno precedente), unitamente ai Ministeri titolari di funzioni critiche (+2 per cento nel confronto anno su anno). Le azioni digitali ostili perpetrate nei confronti dei soggetti privati hanno interessato prevalentemente il settore bancario (11 per cento, in aumento di 4 punti percentuali rispetto al 2019), quello farmaceutico/sanitario (7 per cento, in sensibile incremento rispetto allo scorso anno) e dei servizi IT (11 per cento, dato pressoché stabile) »;

in base alle caratteristiche e al grado di offensività, gli attacchi informatici vengono tipicamente divisi in diverse tipologie, all'interno delle due grandi categorie della sicurezza cibernetica e della difesa cibernetica. La prima riguarda in generale la sicurezza delle infrastrutture, di interesse nazionale o comunque strategiche, pubbliche o private, che possono essere oggetto di attacchi e intrusioni esterni o soggetti a incidenti. Per difesa cibernetica, invece, si intende lo spettro delle competenze dello Stato di natura prettamente militare. Proprio le caratteristiche della minaccia, però, rendono spesso arduo operare nette distinzioni tra sicurezza interna e sicurezza esterna, così come tra i profili civili e quelli più propriamente militari. Se in altri domini il carattere militare della minaccia è facilmente distinguibile, nel dominio cibernetico, viste le sue caratteristiche ibride, tale distinzione è meno agevole. Gli effetti di un attacco informatico possono del resto essere devastanti, anche maggiori di quelli di un attacco convenzionale, e possono danneggiare o paralizzare il funzionamento di organi

vitali dello Stato, ma anche impedire il corretto funzionamento di infrastrutture critiche (ad esempio nei settori dell'energia, dei trasporti, delle cure mediche, della produzione di beni essenziali);

alle Forze armate è in ogni caso affidato il compito di proteggere il Paese da intrusioni esterne, anche laddove dirette a obiettivi civili. Come si legge nel Libro bianco per la sicurezza internazionale e la difesa del 2015, infatti, la Difesa ha il compito di sviluppare « in piena armonia con la strategia nazionale sulla protezione informatica, le possibilità di difesa contro attacchi di natura cibernetica che dovessero eccedere le capacità predisposte dalle agenzie civili »;

le componenti di natura più prettamente militare si inquadrano in una più ampia strategia nazionale per la sicurezza cibernetica, la cui architettura si è andata componendo grazie a una serie di interventi normativi, in particolare a partire dal 2013. In quell'anno, con il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013 (cosiddetto « decreto Monti »), il nostro Paese ha definito le diverse competenze tra i vari attori istituzionali convolti nella gestione, a livello nazionale e della *cyber security*. Il 17 febbraio 2017 è stata adottata, con decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, pubblicato nella *Gazzetta Ufficiale* 13 aprile 2017, n. 87, la direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, che ha sostituito le norme del 2013, con l'obiettivo di assicurare un maggiore coordinamento tra le diverse strutture istituzionali. Nel maggio del 2018, con il decreto legislativo 18 maggio 2018, n. 65 (di recepimento della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, cosiddetta « direttiva NIS ») sono stati delineati ulteriori interventi di rafforzamento del sistema di sicurezza cibernetica del Paese. Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 (cosiddetto *Cybersecurity Act*), ha poi introdotto una certificazione europea della sicurezza cibernetica di *hardware* e *software*, trasponendo in campo informatico gli *standard* di sicurezza già applicati per i prodotti fisici prodotti e commercializzati nell'Unione europea. Il citato regolamento ha anche rafforzato le competenze dell'Agenzia europea per la cibersicurezza (ENISA);

sulla base di questa normativa, la responsabilità della politica generale del Governo nel campo della sicurezza cibernetica viene attribuita al Presidente del Consiglio dei ministri, che provvede al coordinamento delle politiche per la sicurezza cibernetica, impartisce le direttive e, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce le disposizioni per l'organizzazione e il funzionamento del sistema. Dal punto di vista operativo al centro del sistema di controllo è il Dipartimento delle informazioni per la sicurezza (DIS), al cui interno è collocato il Nucleo per la sicurezza cibernetica, cui spetta la gestione delle crisi cibernetiche e il raccordo tra le diverse componenti del sistema. Al Ministero dello sviluppo economico spetta invece il compito di svolgere le attività di valutazione e certificazione per la verifica dell'affidabilità della componentistica in uso alla pubblica amministrazione;

dal 2018 è stato anche istituito un *Computer Security Incident Response Team* (CSIRT), con compiti di natura tecnica, per supportare la pubblica amministrazione e altri utenti, definendo le procedure per la prevenzione e la gestione degli incidenti informatici, oltre che la collaborazione con le analoghe strutture degli altri Paesi;

il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, ha poi istituito il perimetro di sicurezza nazionale cibernetica, con il fine di assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche e dei soggetti privati, da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato. A seguire sono stati approvati i criteri per l'individuazione dei soggetti pubblici e privati da includere nel perimetro e poi l'elenco (non pubblico) di più di cento soggetti, che erogano servizi essenziali nell'ambito delle infrastrutture nazionali. Nel gennaio di quest'anno è divenuto poi operativo il sistema che fa capo al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, chiamato a effettuare verifiche e valutazioni dei beni, dei sistemi e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (ICT) che i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica intendono acquisire qualora, tramite questi ultimi, vengano erogati e garantiti servizi essenziali;

rilevato che:

il campo cibernetico è stato da tempo individuato come teatro di possibili scontri militari ed è di conseguenza qualificato, in ambito sia NATO che dell'Unione europea, come il « quinto dominio di scontro », oltre a quelli tradizionali della terra, dell'aria, del mare e dello spazio. In ambito militare la minaccia cibernetica è attuale e immanente, considerando che, come ricordato dal generale Graziano nel corso della sua audizione, « circa il 70 per cento degli equipaggiamenti e dei sistemi d'arma ha componenti tecnologiche che potrebbero essere degradate o inabilitate da attacchi cibernetici ». Di conseguenza « è indispensabile agire subito. Le minacce di conflitti tradizionali sono potenziali, mentre il confronto cibernetico è fattuale, avviene ogni giorno: si deve essere in grado di rispondere ora, non domani ». Inoltre, nel dominio cibernetico non è possibile ricorrere a strumenti di difesa tipici dei domini tradizionali, come la deterrenza. Considerato che gli attacchi possono essere sferrati con strutture e risorse anche molto contenute, occorre puntare tutto sulla difesa e sulla resilienza, anche attraverso sistemi di *fallback* analogici – ove applicabili – da utilizzare in caso di necessità. Gli Stati sono peraltro connessi tra loro da una fitta rete di scambi informatici, per cui « la debolezza di un Paese è la debolezza di tutti ». È quindi necessario sviluppare un quadro normativo, a livello internazionale, che disciplini l'individuazione dei soggetti responsabili degli attacchi, la loro eventuale riconducibilità ad attori statuali, il sistema sanzionatorio, la proporzionalità della difesa e la legittimità della difesa preventiva;

in seno all'Alleanza Atlantica, l'approccio nei confronti della minaccia *cyber* si è evoluto in modo significativo negli ultimi anni, dal punto di vista sia dell'inquadramento della minaccia che delle strategie e delle capacità operative. L'impegno della NATO si concentra sullo sviluppo di capacità in chiave difensiva, ai sensi dell'articolo 3 del Trattato Nord Atlantico. Si è inoltre riconosciuto che un attacco cibernetico può arrivare a causare danni paragonabili a quelli di un attacco armato e quindi può attivare la clausola della difesa collettiva, ai sensi dell'articolo 5 del Trattato Nord Atlantico. Dopo la prima *Policy on Cyber Defence* (adottata nel 2008), le politiche NATO in materia hanno segnato un deciso passo in avanti;

nel 2016 è stato adottato un *Cyber Defence Pledge*, che ha istituito una piattaforma comune tra i Paesi membri per migliorare le capacità nazionali di risposta, con impegni da realizzare progressivamente. Nel 2019 è stato approvato il *Report on Enhancing NATO's Response to Hybrid Threats*, che delinea una serie di priorità in materia. Nel 2020 i Paesi membri hanno riaffermato l'impegno a utilizzare lo spettro completo delle loro capacità, quindi anche aeree, marittime, terrestri e spaziali, per contrastare un attacco *cyber*. Notevoli sono stati gli sviluppi anche dal punto di vista organizzativo e operativo. La NATO ha adottato politiche e piani d'azione, istituendo comitati, agenzie e centri operativi per integrare il dominio cibernetico nelle operazioni e nello sviluppo delle capacità militari dei Paesi membri. In tale contesto la NATO ha sviluppato un progetto per rendere disponibile una capacità di contro-offensiva *cyber* come strumento di risposta in soccorso agli Alleati (ai sensi dell'articolo 5), basato sulle singole capacità nazionali alleate (« *Roadmap to implement cyberspace as a domain of operations* »). Ne discende, pertanto, la necessità di un maggiore coordinamento non solo sullo sviluppo delle singole capacità, ma anche un sistema condiviso più ampio, che comprenda anche il complesso processo di attribuzione di responsabilità di un attacco *cyber*. È quindi opportuno che il nostro Paese partecipi attivamente a tale progetto, non solo per una questione di credibilità internazionale, ma soprattutto per acquisire informazioni essenziali per massimizzare le proprie risorse nel dominio strategico. Nello stesso disegno, dopo l'istituzione del *Cyber Defence Committee*, responsabile per la *governance* politica della difesa cibernetica, nel 2019, all'interno del Comando operativo di Mons, in Belgio, è stato creato un *Cyberspace Operations Centre*, responsabile delle operazioni in questo dominio a supporto dei comandi operativi;

la difesa cibernetica rientra anche negli strumenti di programmazione dello sviluppo capacitivo, a cominciare dal *Nato Defence Planning Process*, con cui gli Stati membri concordano gli obiettivi delle rispettive Forze armate, anche per contribuire agli impegni di difesa comune. Allo stato attuale la difesa cibernetica è a supporto dei comandi operativi « tradizionali », ma è aperta la possibilità che in futuro venga costituito un comando autonomo. Sotto il profilo informativo la *Nato Communication and Information Agency* gestisce alcune reti alleate, agendo in diretta relazione con il *Nato Computer Incident Response Capability*, la struttura che coordina lo scambio di informazioni tecniche sulle minacce ed è incaricata di fornire la prima risposta in caso di attacchi. Sul piano della

formazione il *Cooperative Cyber Defence Center of Excellence*, situato in Estonia, prepara studi e *report*, organizzando esercitazioni periodiche. Considerate le caratteristiche del dominio *cyber*, risultano essenziali le collaborazioni con il settore della ricerca e dell'industria, che si sviluppano nell'ambito della *Nato Industry Cyber Partnership*. Da ultimo, il rapporto NATO 2030: *United for a New Era* individua sette priorità in materia di minacce *cyber* e ibride: dall'implementazione degli impegni già assunti al rafforzamento delle consultazioni di cui all'articolo 4 del Trattato Nord Atlantico, alla maggiore cooperazione civile e militare. Oltre che quella con altre organizzazioni (dall'Organizzazione delle Nazioni Unite-ONU all'Organizzazione per la sicurezza e la cooperazione in Europa-OSCE) e con Paesi terzi, la NATO vanta una significativa cooperazione con l'Unione europea. Nella dichiarazione congiunta del 2016, la *cyber* difesa è indicata tra le sette aree prioritarie di cooperazione, comprendendo scambio di informazioni, di *standard* e di politiche, oltre che di attività comuni di addestramento;

per ciò che riguarda l'Unione europea, in ambito strettamente militare il documento più articolato è il Quadro strategico dell'UE in materia di ciberdifesa (novembre 2018). Il documento si pone l'obiettivo di sviluppare la politica di difesa comune nel dominio cibernetico, attraverso sei priorità:

a) sostegno alle capacità di sviluppo della difesa cibernetica;

b) rafforzamento della comunicazione e informazione in ambito di politica di sicurezza e di difesa comune (PSDC);

c) promozione della cooperazione civile e militare;

d) ricerca e tecnologia;

e) miglioramento di formazione, istruzione ed esercitazioni;

f) potenziamento della cooperazione con i *partner* internazionali, a cominciare dalla NATO;

in linea con questo quadro strategico, la difesa cibernetica è presente in tutte le iniziative di difesa comune. Tra i progetti approvati dal 2019 nell'ambito della cooperazione strutturata permanente (PESCO), almeno quattro sono espressamente rivolti ad aumentare le capacità di difesa cibernetica dell'Unione europea, mirando a rafforzare la cooperazione tra gli Stati membri, mediante la creazione di strutture di formazione, di gruppi di intervento o di piattaforme per risposte rapide: il Centro di coordinamento nel settore informatico e dell'informazione (progetto guidato dalla Germania), l'Accademia e il polo di innovazione dell'Unione europea nel settore dell'informatica (guidato dal Portogallo), la Piattaforma per la condivisione di informazioni in materia di minaccia informatica e di risposta agli incidenti informatici (guidato dalla Grecia, cui partecipa anche l'Italia) e il progetto sui gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza (guidato dalla Lituania, cui partecipa anche l'Italia). Quest'ultimo rientra anche tra i 26 progetti che il Consiglio dell'Unione europea del 20 novembre scorso ha ritenuto in grado di produrre risultati concreti entro il 2026;

sotto il profilo del sostegno finanziario, il Programma europeo di sviluppo del settore industriale della difesa (EDIDP) ha già finanziato, tra il 2019 e il 2020, una serie di progetti in materia di difesa cibernetica. Un ulteriore incremento dei finanziamenti è previsto nel prossimo futuro, con l'entrata in funzione del Fondo europeo per la difesa (EDF), nell'ambito del quadro finanziario pluriennale 2021-2027;

la capacità di risposta ad attacchi *cyber* è ricompresa anche tra le undici priorità individuate nel Piano di sviluppo delle capacità *(Capacity Development Plan),* documento redatto dall'Agenzia europea per la difesa (EDA) che individua, sulla base delle indicazioni degli Stati membri, e con il supporto del Comitato militare e dello Stato maggiore dell'Unione europea, le capacità militari da sviluppare in seno all'Unione europea. In ambito EDA operano diversi gruppi di esperti con il compito di mappare le aree di ricerca ritenute essenziali e di individuare i fattori tecnici ritenuti necessari per l'autonomia dell'Unione europea (tra cui un sistema di crittografia condivisa, lo sviluppo di tecniche di simulazione e visualizzazione, l'aggiornamento di tecnologie di autenticazione, eccetera);

lo scorso 22 marzo il Consiglio dell'Unione europea ha anche approvato le conclusioni sulla strategia europea per la cibersicurezza che contiene indicazioni anche per i profili della difesa cibernetica. Il Consiglio infatti, in attesa della proposta di revisione del quadro strategico in materia, « si impegna a proseguire gli sforzi per rafforzare le dimensioni di cibersicurezza e ciberdifesa al fine di garantirne la piena integrazione nel più ampio settore della sicurezza e della difesa, in particolare nel contesto dei lavori sulla Bussola strategica ». Il Consiglio ha anche espresso apprezzamento per l'attività dell'Agenzia europea per la difesa, volta a promuovere la cooperazione tra le strutture con certificazione di resistenza al fuoco (CERT) militari a livello nazionale e ha ribadito di sostenere « gli sforzi compiuti per consolidare le sinergie civili-militari e il coordinamento in materia di ciberdifesa e cibersicurezza, compresi gli aspetti connessi allo spazio, anche attraverso i progetti specifici della PESCO »;

in linea con le direttrici di sviluppo in ambito NATO e Unione europea, anche il nostro Paese sta da tempo rafforzando le proprie capacità militari nel campo cibernetico. Come si legge nel Libro bianco per la sicurezza internazionale e la difesa del 2015, lo spazio cibernetico è un dominio « che dovrà essere presidiato e difeso », anche perché gli attacchi alle reti informatiche possono produrre « effetti sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali »;

il Quadro strategico nazionale per la sicurezza dello spazio cibernetico (2013) assegna del resto al Ministero della difesa una serie di compiti di grande rilevanza, che vanno al di là di una prospettiva strettamente militare. Oltre a definire e coordinare la politica militare, la *governance* e le capacità militari nell'ambiente cibernetico, la Difesa è in primo luogo chiamata a pianificare e condurre le operazioni nello spazio cibernetico, per contrastare le azioni avversarie contro sistemi e strutture della difesa. A tal fine negozia le intese internazionali in materia e coordina le proprie attività con quelle della NATO, dell'Unione europea e degli altri alleati. Il Ministero contribuisce anche al flusso informativo a supporto delle opera-

zioni cibernetiche, anche oltre i confini nazionali, e concorre alla prevenzione e al contrasto delle attività terroristiche. Esso poi « concorre alla prevenzione e al contrasto degli attacchi ai sistemi di comunicazione e informazione di rilevanza strategica per gli interessi nazionali ». La Difesa, inoltre, « assicura la formazione e l'addestramento del proprio personale e mette a disposizione i propri centri di formazione in favore delle altre Amministrazioni »;

in attuazione di questo Quadro, il Piano nazionale per la protezione cibernetica e la sicurezza (2017) prevede, tra i suoi diversi indirizzi operativi, lo « sviluppo delle capacità operative fondamentali, idonee ad espletare i compiti della Difesa nell'ambiente cibernetico ». Nell'ambito di questo indirizzo, l'obiettivo è duplice: da un lato « potenziare le strutture preposte alla difesa dello spazio cibernetico ed avere cura che gli assetti che le compongono raggiungano e mantengano nel tempo i necessari livelli di efficacia ed efficienza », dall'altro « sviluppare strutture di Comando e Controllo in grado di pianificare e condurre operazioni militari nello spazio cibernetico in maniera efficace » (compito adempiuto con l'istituzione del Comando per le operazioni in rete–COR);

tali prospettive strategiche hanno evidentemente dirette ricadute per quanto riguarda la programmazione degli investimenti e dello sviluppo capacitivo. Come si legge nel Documento programmatico pluriennale della difesa per il triennio 2020-2022, le « sfide legate alla dimensione cibernetica hanno assunto una decisa rilevanza geopolitica e geostrategica, determinata dalla sua peculiare trasversalità, in quanto potenziale canale di propagazione e amplificazione degli altri tipi di minaccia. La dimensione cibernetica dei conflitti si è aggiunta, infatti, a quella tradizionale, rendendola ancora più pericolosa ed estendendola anche al dominio cognitivo. [...] In tale contesto, il cyberspazio rappresenta un significativo fattore abilitante che amplifica le potenzialità della minaccia ibrida e costituisce un ideale campo d'azione e di proselitismo per l'estremismo violento. Parimenti, la possibilità di accesso a tecnologie avanzate, da parte di un bacino sempre più ampio di utenti, pone i nostri potenziali avversari in grado di accedere a strumenti, relativamente economici e facilmente reperibili ». Tutto ciò richiede non solo scelte finanziarie conseguenti, ma anche politiche industriali adeguate, necessarie per restare al passo con l'evoluzione tecnologica e mantenere il tradizionale vantaggio tecnologico della Difesa. In questo senso è anche necessaria l'introduzione della « *security by design* », quale prerequisito obbligatorio nello sviluppo delle applicazioni e dei sistemi;

il processo di rafforzamento della componente *cyber* implica anche un adeguamento delle strutture organizzative. Da questo punto di vista si segnala l'istituzione, nel marzo del 2020, del Comando per le operazioni in rete (COR), evoluzione e rafforzamento della struttura precedente (Comando interforze per le operazioni cibernetiche-CIOC). Il nuovo Comando è posto alle dirette dipendenze del Capo di Stato maggiore della difesa, con la missione di « garantire, con visione unitaria e coerente, la condotta delle operazioni nel dominio cibernetico e la gestione tecnico-operativa in sicurezza di tutti i sistemi di ICT/C4 della Difesa ». Con il COR, la Difesa intende riordinare e razionalizzare il settore, per assicurare la direzione, il

coordinamento e il controllo unitario nella gestione, in sicurezza, dei sistemi ICT, nonché l'adozione di un approccio « cooperativo » e interforze nel dominio cibernetico e un adeguato sviluppo capacitivo, favorendo investimenti e formazione. Il COR gestisce anche, in modo accentrato, l'evoluzione e la manutenzione della Rete integrata della difesa (RID), l'*intranet* dell'area di vertice interforze (DIFENET) e sta attivando un servizio di accesso autonomo alla rete *internet*, per tutte le Forze armate. Il COR esprime anche una capacità di pianificazione, conduzione e realizzazione dell'intera gamma delle « operazioni militari » nel dominio cibernetico, con capacità di contrasto e di neutralizzazione delle minacce portate alle reti, ai sistemi e ai servizi della Difesa, sia sul territorio nazionale che nei teatri operativi, interfacciandosi con il Centro *intelligence* interforze, per il necessario supporto informativo;

apprezzato che:

come affermato dal Ministro della difesa Guerini nel corso dell'audizione svolta lo scorso 9 marzo presso le Commissioni Difesa di Camera e Senato, uno dei tre settori in cui il dicastero intende contribuire al Piano nazionale di ripresa e resilienza è proprio « la difesa dello spazio cibernetico, ormai parte del dominio delle operazioni militari ». In questo settore, infatti, il Ministero intende sviluppare « nuovi progetti rivolti, da un lato, ad ampliare e irrobustire le capacità di gestione e protezione dei dati, dall'altro a potenziare le capacità di difesa e resilienza innalzando i livelli di sicurezza nel contrasto alle minacce informatiche e digitali, anche a protezione delle infrastrutture critiche del Paese »;

rilevato infine che dalle audizioni svolte sono emerse ulteriori sollecitazioni, non direttamente rivolte al settore della difesa, come ad esempio quelle di:

stimolare tutte le possibili sinergie tra pubbliche amministrazioni e settore privato nell'ambito della ricerca, della formazione e dello sviluppo di sistemi;

rafforzare i percorsi formativi legati alla cibersicurezza, nei diversi ordini e gradi del sistema scolastico, nonché nella formazione universitaria e post-universitaria, sia per diffondere una maggiore consapevolezza del tema per i cittadini-utenti, sia nell'ottica delle rilevanti prospettive occupazionali del settore;

intensificare le campagne formative e informative sui temi della *cyber* sicurezza, sia per la generalità dei cittadini, che per il personale delle pubbliche amministrazioni e del settore privato;

impegna il Governo a:

rafforzare gli investimenti nel comparto cibernetico, in particolare per quanto riguarda la ricerca, anche per aumentare l'autonomia strategica del Paese e il suo ruolo nel contesto internazionale, sostenendo le collaborazioni tra l'Amministrazione della difesa, le università e l'industria e anche valutando interventi fiscali per favorire gli adeguamenti in tema di sicurezza cibernetica;

potenziare le capacità nazionali di difesa cibernetica, in considerazione dello sviluppo crescente di strumenti ICT in ambito militare e al loro utilizzo, anche travisato, in situazioni di conflittualità tra Stati;

aggiornare, laddove necessario, il quadro giuridico per la partecipazione del nostro Paese a operazioni militari che utilizzino sistemi cibernetici, adeguando la catena di comando per l'avvio di tali operazioni, in particolare se svolte in contesti multilaterali, tenendo conto delle caratteristiche di questi attacchi, in particolare la loro velocità;

favorire lo scambio di informazioni e la collaborazione a livello internazionale, anche in un'ottica di prevenzione e deterrenza e sotto il profilo giudiziario;

proseguire l'impegno a rafforzare la sicurezza delle dotazioni informatiche, assumendo il principio di « *security by design* » quale prerequisito obbligatorio, fin dalla fase della ricerca e della progettazione, nello sviluppo delle applicazioni e dei sistemi di interesse strategico per il Paese, introducendo particolari prescrizioni a carico dei produttori di dispostivi tecnologici che consentano di mantenerne la sicurezza per tutto il ciclo di vita, con adeguati *standard*, per quanti gestiscono infrastrutture interconnesse con quelle dei grandi operatori e per tutta la *supply chain* degli operatori di servizi strategici;

rafforzare la componente *cyber* nei percorsi formativi destinati al personale, anche civile, della Difesa, e in generale della pubblica amministrazione;

promuovere ogni iniziativa, anche legislativa, per massimizzare l'azione di contrasto alla disinformazione, spesso operata come vera e propria minaccia ibrida alla sicurezza nazionale;

promuovere l'attiva partecipazione del nostro Paese alle diverse iniziative dell'Unione europea nel settore della difesa cibernetica, a cominciare dalla cooperazione strutturata permanente (PESCO) e dalla revisione coordinata annuale sulla difesa (CARD);

adoperarsi affinché nell'implementazione del Fondo europeo per la difesa sia dato opportuno rilievo ai progetti relativi alla difesa cibernetica e rafforzare, a livello sia finanziario che politico, la partecipazione delle aziende italiane del comparto ai diversi strumenti finanziari di sostegno, sia nella fase della ricerca che in quella dello sviluppo dei prodotti;

promuovere e aderire a iniziative comuni in ambito di Alleanza Atlantica al fine di rendere disponibili, su iniziativa nazionale, proprie capacità di contrasto e contro-offensiva rispetto alle minacce cibernetiche, favorendo al contempo la cooperazione tra NATO e Unione europea.

€ 1,00