CAMERA DEI DEPUTATI

Doc. **XXII** n. **30**

PROPOSTA DI INCHIESTA PARLAMENTARE

D'INIZIATIVA DEI DEPUTATI

BICCHIELLI, CAVO, CESA, ALESSANDRO COLUCCI, LUPI, SEMENZATO, TIRELLI

Istituzione di una Commissione parlamentare di inchiesta sul rischio cibernetico e sull'attuazione delle strategie e delle misure di sicurezza nazionali

Presentata il 18 maggio 2023

ONOREVOLI COLLEGHI ! – I recenti avvenimenti cibernetici che hanno interessato l'Italia rendono ancora più urgente la diffusione della consapevolezza dei rischi cibernetici ai quali il nostro Paese è esposto. I noti avvenimenti, seppur non catastrofici, sono un serio campanello d'allarme in termini di sicurezza nazionale. La digitalizzazione e l'interconnessione sociale ed economica sono ormai diventate un elemento strutturale del contesto in cui viviamo. Lo scoppio della pandemia di COVID-19 ha accelerato l'adozione di tecnologie informatiche all'interno di infrastrutture critiche, dei processi produttivi e, in ultima analisi, della vita privata dei cittadini. Se da un lato l'evoluzione tecnologica determina rilevanti benefici, dall'altro introduce nuovi rischi: il cyberspazio diventa quindi il luogo dove organizzazioni ostili, talvolta anche di natura governativa, possono attuare proprie strategie di minaccia alla sicurezza nazionale dell'Italia. La massiccia campagna di attacchi informatici conferma gli effetti potenzialmente dirompenti di questi rischi, oltre all'urgenza di interventi difensivi efficaci e globali. Alla luce di questi eventi, si osserva come il cyberspazio diventi spesso strumentale al perseguimento di interessi di tipo statuale mirati all'indebolimento della sicurezza nazionale al fine di sconvolgere delicati equilibri geostrategici.

Stiamo assistendo chiaramente, nell'ultimo ventennio, a un'accelerazione straordinaria di operazioni cibernetiche con lo scopo di indebolire il sistema economico nazionale attraverso il trafugamento di « *know-how* » e competenze delle nostre imprese.

I danni causati da attacchi cibernetici sono di natura molteplice e comprendono il danno di immagine o reputazione, operativo e di disinformazione, dove per disinformazione s'intende il potere di spostare opinioni di massa e decisioni, con un

potenziale impatto politico e militare nonché strategico.

Anche il sistema finanziario risulta particolarmente esposto alla minaccia cibernetica in ragione della centralità del suo ruolo per il funzionamento di un'economia di mercato. Oltre a tale aspetto va considerato anche che l'interconnessione con altre infrastrutture critiche strategiche, tra le quali quelle energetiche e di telecomunicazione, ne estende indefinitamente i confini con chiare ricadute sulla sicurezza nazionale e con un evidente aumento della vulnerabilità complessiva del sistema economico italiano.

La sistematica esposizione a notizie manipolate o palesemente false a cui è sottoposta la popolazione può diventare veicolo di minacce alla sicurezza nazionale e, in ultima analisi, alla stessa tenuta del nostro sistema democratico.

La guerra, la pandemia e più in generale le tensioni internazionali hanno portato ad una situazione di paura e incertezza che in Europa non si vedeva da decenni.

Le principali fonti internazionali affermano che il 2021 è stato l'anno peggiore di sempre per quanto concerne le minacce *cyber* e i relativi impatti.

Come indicato nel Rapporto *Clusit* del 2022, gli attacchi informatici sono aumentati del 53 per cento (da 745 a 1.141) dal primo semestre del 2018 alla fine del 2022.

In quattro anni e mezzo la media mensile di attacchi gravi a livello globale è passata da 124 a 190, con un incremento di oltre il 65 per cento.

A crescere in questi anni, e nell'ultimo semestre in particolare, non è stato solo il numero dei *cyber* attacchi ma anche la loro gravità. Il citato Rapporto *Clusit* del 2022 infatti ha classificato come *critical* o *high* il 78 per cento degli attacchi avvenuti dal mese di gennaio 2022: vuol dire che le azioni di *cyber* criminali e malintenzionati hanno avuto ripercussioni gravi (nel 45 per cento dei casi) quando non addirittura critiche (in un caso su tre) sulla sfera economica, politica e sociale.

Il resoconto sull'attività della Polizia postale e delle comunicazioni e dei Centri operativi per la sicurezza cibernetica evidenzia come, nel corso del 2022, siano stati registrati in Italia 12.947 attacchi rivolti verso infrastrutture critiche, istituzioni, aziende e privati, con un incremento percentuale del 138 per cento rispetto al 2021.

È di estrema importanza inquadrare il rischio *cyber* nella giusta prospettiva, non solo quella del singolo attacco che va a creare disservizi o colpire economicamente una singola realtà, ma quella invece di un potenziale rischio per il sistema Paese. In quest'ottica è possibile individuare due macro-rischi principali, uno avente a che fare con la sicurezza delle infrastrutture critiche nazionali, l'altro con la tenuta economica del Paese nel medio-lungo termine.

La sicurezza delle infrastrutture critiche è tema centrale nel dibattito odierno, dal loro corretto funzionamento dipende l'operatività del Paese stesso e la pervasività della digitalizzazione le rende *target* possibili e di valore per attacchi informatici.

La tenuta economica del Paese nel medio-lungo termine deve essere valutata con visione ampia e con lungimiranza partendo dagli attacchi che colpiscono le aziende del nostro Paese. Un attacco contro un'impresa italiana non va a danneggiare solamente la stessa in termini economici, ma si può tradurre in perdite di fatturato e quindi di introiti per lo Stato, perdita di posti di lavoro e, in caso di furto di proprietà intellettuale, anche perdita di competitività sul mercato, che nel lungo termine e nel contesto più ampio di tutto il territorio italiano porterebbe ad un serio rischio per la sicurezza nazionale.

Risulta inoltre di primaria importanza la sinergia e il rafforzamento della strategia per il *cloud* nazionale, anche per la pubblica amministrazione, al fine di accelerare i processi di sicurezza e resilienza del Paese e per ridurre la dipendenza da *provider* esteri, in particolare al di fuori dell'Unione europea, rispetto a tale tipologia di tecnologia abilitante.

È dunque fondamentale che il legislatore possa informarsi tempestivamente su tali argomenti ed essere aggiornato per poter guidare la formulazione di soluzioni a protezione dell'interesse nazionale.

I vari governi negli ultimi anni hanno varato norme significative, spesso recependole dall'Unione europea, altre volte elaborandole in proprio. E così sono stati introdotti il regolamento generale sulla protezione dei dati (GDPR), di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, il decreto legislativo 18 maggio 2018, n. 65 (attuativo della direttiva (UE) 2016/1148, cosiddetta « direttiva NIS – *Directive on security of network and information systems* »), il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (che ha istituito il perimetro di sicurezza nazionale cibernetica), i piani triennali per l'informatica nella pubblica amministrazione (tra cui il più recente, riferito al triennio 2022-2024, risale al 27 febbraio 2023), il decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92 (relativo al perimetro cibernetico, al Centro di valutazione e certificazione nazionale e ad altre questioni) e infine la recente direttiva NIS2 (direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022). Il panorama normativo si va ampliando e articolando, eppure assistiamo quasi quotidianamente ad azioni illegali, che definiamo genericamente come violazioni della sicurezza informatica, spesso nei confronti dello Stato, nelle sue numerose espressioni, dall'apparato militare a quello sanitario, senza trascurare la pubblica amministrazione in genere, le agenzie di *intelligence* e le forze di sicurezza e difesa.

Nonostante la cybersicurezza nazionale si sia recentemente arricchita di un nuovo strumento mediante la costituzione dell'Agenzia per la cybersicurezza nazionale (istituita con il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109), alla quale è stato affidato il ruolo di implementare la resilienza del Paese nel dominio cibernetico, colmando un'importante lacuna che l'Italia scontava da decenni, essa tuttavia necessita di ulteriori interventi a supporto.

La proposta di istituire una Commissione di inchiesta si focalizza sulla sicurezza informatica e sul rischio di natura *cyber*, con l'obiettivo d'investigare e studiare il fenomeno al fine di attuare tutte le misure necessarie per contrastare e gestire il rischio, nonché offrire supporto della Strategia nazionale di cybersicurezza, presentata a Palazzo Chigi nel mese di maggio 2022.

Il citato decreto-legge n. 82 del 2021 infatti attua una riorganizzazione dell'architettura nazionale della cybersicurezza nazionale, articolata su quattro pilastri:

l'Agenzia per la cybersicurezza nazionale, con competenze in ambito di cybersicurezza e resilienza;

l'attività di prevenzione e di contrasto della criminalità informatica, realizzata da una serie di corpi e servizi della Polizia di Stato, del Dipartimento di pubblica sicurezza, del Ministero dell'interno, dell'Arma dei carabinieri e del Corpo della Guardia di finanza;

l'attività di difesa e della sicurezza dello Stato, con il ruolo del Ministero della difesa nell'ambito della definizione e del coordinamento della politica militare, della *governance* e delle capacità militari in ambito cibernetico;

l'attività di ricerca e di elaborazione informativa, per la tutela degli interessi politici, militari, economici, scientifici e industriali dell'Italia, affidata al comparto « *intelligence* ».

L'obiettivo della Commissione di inchiesta è quello di creare tavoli di lavoro e di dialogo con tutti gli *stakeholder* istituzionali e rappresentanti del settore privato (ad esempio rappresentanti delle Forze armate, della sanità, della pubblica amministrazione, delle piccole e medie imprese, dei gestori di infrastrutture strategiche, degli operatori economico-finanziari, eccetera), permettendo così di sviluppare strategie comuni in un'ottica di cooperazione tra il sistema economico pubblico e quello privato e rafforzare gli strumenti di protezione e difesa in ambito cibernetico. In quest'ottica, pertanto, l'istituzione di una Commissione parlamentare di inchiesta risulterebbe uno strumento utile a disposizione dell'organo legislativo, poiché consen-

tirebbe, con analisi puntuali e con attività dedicate, di operare sulla situazione presente, sulla congruità degli strumenti normativi, stimolando lo spirito di coesione e di approfondire e comprendere fenomeni complessi e interconnessi in un settore di per sé ibrido e multidisciplinare, al fine di definire un quadro di riferimento utile per eventuali e auspicabili interventi normativi di portata strategica.

PROPOSTA DI INCHIESTA PARLAMENTARE

—

Art. 1.

(Istituzione e durata della Commissione)

1. È istituita, ai sensi dell'articolo 82 della Costituzione, per la durata della XIX legislatura, una Commissione parlamentare di inchiesta sul rischio cibernetico e sull'attuazione delle strategie e delle misure di sicurezza nazionali, di seguito denominata « Commissione ».

Art. 2.

(Compiti della Commissione)

1. La Commissione, fatte salve le competenze dell'autorità giudiziaria, ha il compito di:

a) approfondire la conoscenza dei fatti e dei fenomeni connessi alla sicurezza cibernetica, in particolare per quanto riguarda la protezione dei dati personali e la sicurezza informatica dei sistemi di informazione e delle infrastrutture critiche, strategiche ed essenziali del Paese;

b) indagare sull'esistenza di eventuali responsabilità di soggetti pubblici e privati in merito a operazioni cibernetiche malevole;

c) monitorare gli investimenti volti al potenziamento dei sistemi d'arma relativi alla guerra cibernetica e dei sistemi a uso sia civile sia militare, da parte di Stati stranieri e di soggetti nazionali;

d) esaminare l'adeguatezza e la compiutezza della disciplina delle responsabilità e delle competenze dei diversi livelli istituzionali;

e) verificare l'attuazione, l'efficacia e l'adeguatezza della normativa nazionale in materia di sicurezza informatica, in particolare per quanto riguarda la sua applicazione alla sicurezza delle reti delle infrastrutture critiche;

f) individuare eventuali carenze e criticità della normativa vigente in materia di sicurezza informatica e di messa in sicurezza dei sistemi e delle infrastrutture critiche anche valutando, a tale fine, gli effetti dell'evoluzione normativa;

g) individuare gli ostacoli alla piena operatività degli organi amministrativi e tecnici, all'adozione di misure di prevenzione e di contrasto dei fenomeni di criminalità cibernetica, al potenziamento della collaborazione internazionale in materia di sicurezza cibernetica e al potenziamento della collaborazione tra pubblico e privato;

h) accertare il livello di controllo, di capacità di intervento e di prevenzione dei soggetti pubblici e privati tenuti al rispetto delle norme vigenti;

i) indicare gli interventi anche di carattere normativo, amministrativo e regolamentare sui temi della difesa cibernetica e della resilienza cibernetica, ritenuti più opportuni al fine di realizzare la più adeguata ed efficace strategia per combattere i rischi derivanti da attacchi alla rete informatica, verificando nel contempo l'impatto delle innovazioni intervenute in materia sulle pubbliche amministrazioni e sulle imprese inserite nel perimetro di sicurezza nazionale, nonché su tutte le altre amministrazioni e imprese, comprese le piccole e medie imprese;

l) effettuare una ricognizione completa delle risorse effettivamente disponibili per garantire una reale sicurezza alle strutture informatiche nazionali e locali;

m) indicare le iniziative ritenute più opportune per la formazione in ambito scolastico e universitario, al fine di creare una diffusa consapevolezza in materia di sicurezza informatica e di rischio cibernetico e di preparare operatori esperti sui temi della difesa cibernetica e della resilienza cibernetica;

n) accertare il livello di controllo e la capacità di intervento e di azione da parte delle istituzioni centrali, del settore della difesa, degli organismi di informazione per la sicurezza e delle società private in me-

rito alle capacità di resistenza ad attacchi informatici;

o) monitorare la capacità di deterrenza in ambito cibernetico nel settore pubblico e privato e promuovere l'introduzione di eventuali misure di rafforzamento;

p) svolgere approfondimenti in ordine al quadro giuridico e strategico di riferimento, con particolare riguardo alla vigente normativa dell'Unione europea e internazionale applicabile in materia, compresi la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, resa esecutiva ai sensi della legge 18 marzo 2008, n. 48, e il relativo Secondo protocollo addizionale sul rafforzamento della cooperazione e la divulgazione delle prove elettroniche, fatto a Strasburgo il 12 maggio 2022, anche al fine di individuare l'esigenza di eventuali interventi normativi in materia;

q) valutare le strategie e le capacità di deterrenza nazionali da parte delle pubbliche amministrazioni competenti in materia.

2. La Commissione riferisce alla Camera dei deputati ogniqualvolta lo ritenga necessario. Alla fine dei propri lavori presenta una relazione sull'attività svolta e sui risultati dell'inchiesta.

Art. 3.

(Composizione della Commissione)

1. La Commissione è composta da diciotto deputati, nominati dal Presidente della Camera dei deputati, in proporzione al numero dei componenti dei gruppi parlamentari, comunque assicurando la presenza di almeno un deputato per ciascun gruppo. I componenti sono nominati tenendo conto anche della specificità dei compiti assegnati alla Commissione.

2. Il Presidente della Camera dei deputati, entro dieci giorni dalla nomina dei suoi componenti, convoca la Commissione per la costituzione dell'ufficio di presidenza.

3. La Commissione, nella prima seduta, elegge il presidente, due vicepresidenti e due segretari. Si applicano le disposizioni dell'articolo 20, commi 2, 3 e 4, del Regolamento della Camera dei deputati.

Art. 4.

(Poteri e limiti della Commissione)

1. La Commissione procede alle indagini e agli esami con gli stessi poteri e le stesse limitazioni dell'autorità giudiziaria. La Commissione non può adottare provvedimenti attinenti alla libertà e alla segretezza della corrispondenza e di ogni altra forma di comunicazione nonché alla libertà personale, fatto salvo l'accompagnamento coattivo di cui all'articolo 133 del codice di procedura penale.

2. Ferme restando le competenze dell'autorità giudiziaria, per le audizioni svolte a testimonianza davanti alla Commissione si applicano le disposizioni degli articoli 366 e 372 del codice penale.

3. Alla Commissione, limitatamente all'oggetto delle indagini di sua competenza, non può essere opposto il segreto d'ufficio né il segreto professionale. Per il segreto di Stato si applica quanto previsto dalla legge 3 agosto 2007, n. 124. È sempre opponibile il segreto tra difensore e parte processuale nell'ambito del mandato.

Art. 5.

(Acquisizione di atti e documenti)

1. Nelle materie di propria competenza la Commissione può acquisire, anche in deroga al divieto di cui all'articolo 329 del codice di procedura penale, copia di atti e documenti relativi a procedimenti o inchieste in corso presso l'autorità giudiziaria o altri organi inquirenti, nonché copia di atti relativi a indagini e inchieste parlamentari, anche se coperti dal segreto. L'autorità giudiziaria provvede tempestivamente e può ritardare la trasmissione con decreto motivato, che ha efficacia per sei mesi e può essere rinnovato, solo per ragioni attinenti a indagini in corso. Quando tali ragioni

vengono meno, l'autorità giudiziaria provvede senza ritardo a trasmettere quanto richiesto.

2. La Commissione garantisce il mantenimento del regime di segretezza sugli atti e i documenti acquisiti ai sensi del comma 1, fino a quando gli stessi sono coperti da segreto.

3. La Commissione può ottenere altresì, da parte degli organi e degli uffici della pubblica amministrazione, copia di atti e documenti da essi custoditi, prodotti o comunque acquisiti, nelle materie attinenti all'inchiesta.

4. Fermo restando quanto previsto dal comma 2, la Commissione stabilisce quali atti e documenti non devono essere divulgati, anche in relazione a esigenze connesse ad altre istruttorie o inchieste in corso. Devono in ogni caso essere coperti dal segreto gli atti e i documenti attinenti a procedimenti giudiziari nella fase delle indagini preliminari.

5. Qualora gli atti o i documenti attinenti all'oggetto dell'inchiesta siano stati assoggettati al vincolo del segreto da parte delle competenti Commissioni parlamentari di inchiesta, tale segreto non può essere opposto alla Commissione.

Art. 6.

(Obbligo del segreto)

1. I componenti della Commissione, il personale addetto alla stessa e ogni altra persona che collabora con la Commissione o compie o concorre a compiere atti di inchiesta, oppure ne viene a conoscenza per ragioni di ufficio o di servizio, sono obbligati al segreto per tutto quanto riguarda gli atti e i documenti di cui all'articolo 5, commi 2 e 4.

2. La violazione del segreto è punita ai sensi delle leggi vigenti.

Art. 7.

(Organizzazione interna)

1. Le sedute della Commissione sono pubbliche, salvo che la Commissione stessa deliberi di riunirsi in seduta segreta.

2. L'attività e il funzionamento della Commissione sono disciplinati da un regolamento interno approvato dalla Commissione stessa prima dell'inizio dei lavori. Ciascun componente può proporre la modifica delle norme regolamentari.

3. La Commissione può avvalersi dell'opera di consulenti e tecnici a titolo gratuito nonché di tutte le collaborazioni ritenute necessarie. La scelta è operata dal presidente, sentita la Commissione.

4. Per lo svolgimento delle sue funzioni la Commissione fruisce di personale, locali e strumenti operativi messi a disposizione dal Presidente della Camera dei deputati.

5. Le spese per il funzionamento della Commissione sono stabilite nel limite massimo di 75.000 euro per l'anno 2023 e per ciascuno degli anni successivi e sono poste a carico del bilancio interno della Camera dei deputati. Il Presidente della Camera dei deputati può autorizzare annualmente un incremento delle spese di cui al primo periodo, comunque in misura non superiore al 30 per cento, a seguito di richiesta formulata dal presidente della Commissione per motivate esigenze connesse allo svolgimento dell'inchiesta.

6. La Commissione cura l'informatizzazione dei documenti acquisiti e prodotti nel corso della sua attività.

PAGINA BIANCA

190220037700