CAMERA DEI DEPUTATI SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

Doc. **XXXIV**
n. **1**

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

(istituito con la legge 3 agosto 2007, n. 124)

(composto dai deputati: *Raffaele Volpi,* Presidente, *Dieni,* Segretario, *Enrico Borghi, Vito* e *Zennaro*; e dai senatori: *Urso,* Vicepresidente, *Arrigoni, Castiello, Fazzone* e *Magorno*)

RELAZIONE

sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale

(Relatore: on. Elio VITO)

Approvata nella seduta dell'11 dicembre 2019

Trasmessa alle Presidenze il 12 dicembre 2019

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Camera dei Deputati - Senato della Repubblica

COMITATO PARLAMENTARE
PER LA SICUREZZA DELLA REPUBBLICA

IL PRESIDENTE

Signor Presidente,

nella seduta dell'11 dicembre 2019, il Comitato che presiedo ha approvato all'unanimità la "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale", a conclusione di un approfondito lavoro che si è sviluppato a partire dal 18 dicembre 2018.

Nella medesima seduta il Comitato ha, altresì, deciso - ai sensi degli articoli 35 e 37, comma 2, della legge n. 124 del 2007 - di rendere pubblica la relazione, deliberandone la presentazione al Parlamento.

Mi onoro, pertanto, di trasmettere la Relazione a Lei e al Presidente del Senato della Repubblica.

L'occasione mi è gradita per inviarLe i miei più cordiali saluti.

Raffaele Volpi

On. Roberto FICO
Presidente della Camera dei deputati

Camera dei Deputati - Senato della Repubblica

COMITATO PARLAMENTARE
PER LA SICUREZZA DELLA REPUBBLICA

IL PRESIDENTE

Signora Presidente,

nella seduta dell'11 dicembre 2019, il Comitato che presiedo ha approvato all'unanimità la "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale", a conclusione di un approfondito lavoro che si è sviluppato a partire dal 18 dicembre 2018.

Nella medesima seduta il Comitato ha, altresì, deciso - ai sensi degli articoli 35 e 37, comma 2, della legge n. 124 del 2007 - di rendere pubblica la relazione, deliberandone la presentazione al Parlamento.

Mi onoro, pertanto, di trasmettere la Relazione a Lei e al Presidente della Camera dei deputati.

L'occasione mi è gradita per rinnovarLe i miei più cordiali saluti.

Raffaele Volpi

Sen. Elisabetta ALBERTI CASELLATI
Presidente del Senato della Repubblica

PAGINA BIANCA

INDICE

PAGINA BIANCA

Finalità dell'indagine.

Il tema del rafforzamento dei livelli di sicurezza dei sistemi e delle reti di telecomunicazioni, in parallelo al crescente sviluppo delle infrastrutture di nuova generazione, è da alcuni anni al centro dell'attenzione di tutti i Paesi occidentali. Esso rappresenta del resto un terreno di confronto fra diverse, e in qualche caso contrapposte, esigenze, che fanno capo da un lato alle strutture statali e dall'altro ad aziende e singoli cittadini.

La fruizione di sempre più veloci ed efficienti modalità di collegamento e di reperimento di informazioni, garantito dalla rete internet, ha contestualmente prodotto una esposizione dei dati affidati agli archivi informatici ad attacchi e intrusioni da parte sia di organizzazioni criminali di *hackers* singoli o più spesso organizzati, sia di gruppi indirettamente riconducibili a entità statuali. Questi ultimi in particolare hanno evidenziato un crescente attivismo, correlato a diverse finalità, e spesso idoneo a mettere in pericolo la sicurezza dei dati di cittadini, di aziende e di enti e organismi pubblici.

I Paesi dell'Unione europea hanno avviato da tempo una strategia di contrasto di tali rischi, attraverso l'implementazione di strumenti normativi che peraltro solo negli ultimi anni sono divenuti concretamente operativi, anche e soprattutto in relazione all'imminente avvento delle nuove reti di 5ª generazione (5G), che, grazie al notevole incremento di velocità e potenza rispetto alla precedente, renderà potenzialmente più vulnerabile il sistema. Appare quindi inevitabile predisporre un proporzionale adeguamento degli strumenti di difesa.

Lo sviluppo tecnologico in questo settore, che in una prima fase ha visto la prevalenza degli Stati Uniti, negli anni recenti ha fatto registrare una crescita rilevante delle aziende cinesi (Huawei, ZTE), che sono oggi protagoniste significative nell'ambito della tecnologia per la realizzazione delle reti 5G. Huawei in particolare ha notevolmente potenziato la sua presenza commerciale nel nostro Paese, ed oggi è uno degli attori fondamentali per la realizzazione della rete 5G.

Contrariamente a quanto avviene per le imprese occidentali, le aziende cinesi, pur formalmente indipendenti dal potere governativo, sono tuttavia indirettamente collegate alle istituzioni del loro Paese, anche in virtù di alcune norme della legislazione interna.

Il Comitato ha affrontato il tema della sicurezza nello spazio cibernetico fin dalla XVI legislatura con un'apposita indagine al termine della quale, nella seduta del 7 luglio 2010, è stata approvata una relazione tematica *(Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, Doc. XXXIV, n. 4).

In quella sede il Comitato segnalò l'esigenza di « una pianificazione coordinata e unitaria al livello del vertice politico » al fine di difendere i sistemi strategici nazionali connessi alla rete informatica e raccomandò al Governo « di dotarsi di un impianto strategico-organizzativo che assicuri una *leadership* adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati » e di insediare a tal fine una struttura di

coordinamento presso la Presidenza del Consiglio o l'Autorità delegata.

Anche nella XVII legislatura il Comitato ha ritenuto opportuno approfondire alcuni aspetti della questione, stavolta con più specifico riferimento ai sistemi e programmi destinati alla difesa cibernetica (*Relazione sulle procedure e la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni,* Doc. XXXIV, n. 7).

Nelle conclusioni, il documento sottolineava, tra l'altro: l'esigenza di un rafforzamento dell'Ufficio centrale per la segretezza (UCSe), all'interno del DIS, al quale affidare la vigilanza operativa sulle aziende interessate e lo svolgimento di verifiche costanti e periodiche sulla sussistenza dei necessari standard di sicurezza ed affidabilità; di una individuazione delle diverse responsabilità che fanno capo alla fornitura dei *software*, all'attivazione dei virus e degli strumenti di captazione e alla corretta utilizzazione dei dati e delle informazioni in tal modo acquisite; di prevedere nell'ambito del DIS un'apposita struttura competente nella creazione di progetti sorgenti da impiegare nei sistemi di captazione da remoto in modo da avere a disposizione nell'immediato futuro prodotti certificati di origine italiana, muniti dei requisiti di qualità, sicurezza ed affidabilità; di un efficace coordinamento, da parte del DIS, della rete dei vari CERT in modo che rispondano ad una regia unitaria e coerente nella definizione dei criteri minimi di certificazione della qualità delle aziende.

All'inizio della attuale legislatura – anche a seguito del grave attacco informatico che ha colpito nel novembre 2018 un fornitore di servizi di posta elettronica certificata, coinvolgendo circa 3.500 domini per un totale di oltre 500.000 utenze, di cui molte facenti capo alla pubblica amministrazione – il Copasir ha ritenuto di approfondire alcuni degli aspetti che erano stati oggetto del lavoro del precedente Comitato.

Ha quindi proceduto preliminarmente all'audizione del vicedirettore del DIS, professor Roberto Baldoni, che in qualità di responsabile del Nucleo per la sicurezza cibernetica ha delineato un quadro complessivo della strategia nazionale in tale materia. Il Comitato, anche sulla base delle informazioni acquisite nel corso di tale audizione, ha quindi deliberato – il 18 dicembre 2018 – di procedere, attraverso una serie di audizioni, ad un approfondimento del tema, per verificare: il livello di sicurezza informatica garantito ai cittadini, alle istituzioni, alle infrastrutture critiche e alle imprese di interesse strategico nazionale; il grado di implementazione degli interventi attuativi delle linee di indirizzo strategiche e operative, fissate nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico e nel relativo Piano nazionale; nonché l'efficacia delle procedure di coordinamento tra i diversi soggetti, pubblici e privati, chiamati ad attuarli.

Sono stati in primo luogo ascoltati gli organismi civili e militari cui lo Stato attribuisce competenze in materia: Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM), Agenzia per l'Italia digitale (AgID) - CERT P.A., CNAIPIC - Polizia postale, Nucleo per la sicurezza cibernetica istituito presso il DIS, Reparti

specializzati di AISI e AISE, Comando interforze operazioni cibernetiche (CIOC) della Difesa.

Sono stati poi ascoltati alcuni dei principali gruppi e aziende operanti nelle telecomunicazioni e nelle infrastrutture di rete mobile, quali: Telecom Italia, Wind Tre, Vodafone Italia, Telsy, Huawei Italia, Fastweb ed Ericsson.

Il contributo di questi soggetti è stato particolarmente utile con riferimento alle tematiche connesse all'avvento delle nuove reti 5G e alle misure di sicurezza rese necessarie dall'implementazione di tali strutture.

L'indagine è stata completata con le audizioni del Garante per la protezione dei dati personali, in relazione ai profili di tutela della privacy, e di ENI e Leonardo S.p.A. Finmeccanica, che, quali aziende di interesse strategico nazionale, hanno fornito informazioni circa i propri sistemi di sicurezza cibernetica e valutazioni relative alle prospettive connesse con l'avvento della rete 5G.

Il ciclo delle audizioni si è quindi concluso con il sottosegretario di Stato alla difesa, onorevole Angelo Tofalo.

Prima del termine dell'indagine, è stato emanato e convertito in legge il decreto-legge 21 settembre 2019, n. 105, che fornisce una risposta, sia pure ancora non completa, alle esigenze di sicurezza che il Comitato intendeva evidenziare. Molto tuttavia resta ancora da fare, ed in questo senso con le conclusioni che la presente relazione propone al Parlamento si intende offrire un contributo per integrare e migliorare la strumentazione normativa ed amministrativa di cui il nostro Paese può disporre per tutelare efficacemente la libertà, la sicurezza e la privacy dei propri cittadini, delle istituzioni e delle aziende di interesse strategico nazionale.

Il contesto normativo nazionale ed europeo.

La legge n. 133 del 2012 ha introdotto nel testo della legge n. 124 del 2007 recante « Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto », nuove specifiche competenze del Presidente del Consiglio, del Comitato interministeriale per la sicurezza della Repubblica (CISR) e del Dipartimento delle informazioni per la sicurezza (DIS) in materia di sicurezza cibernetica.

Successivamente, è stata definita per la prima volta con il decreto del Presidente del Consiglio del 24 gennaio 2013 (cosiddetto « decreto Monti ») e poi con il decreto del Presidente del Consiglio del 17 febbraio 2017 (cosiddetto « decreto Gentiloni ») l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riferimento alla protezione cibernetica e alla sicurezza informatica nazionali.

Sulla base dei due citati decreti sono stati adottati il Quadro strategico nazionale per la sicurezza dello spazio cibernetico (dicembre 2013) e il Piano nazionale per la protezione cibernetica e la sicurezza informatica (marzo 2017). Quest'ultimo individua gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre

in essere per dare concreta attuazione al Quadro strategico nazionale, alla luce degli indirizzi per la protezione cibernetica e la sicurezza informatica indicati dal Presidente del Consiglio dei ministri nella sua qualità di organo di vertice dell'architettura nazionale cibernetica.

L'organo deputato a impartire direttive al DIS e alle Agenzie al fine di rafforzare le attività informative in materia di protezione cibernetica è, dunque, il Presidente del Consiglio dei ministri, che presiede il CISR (che svolge funzioni di consulenza, « alta sorveglianza » e deliberazione). Il supporto all'attività del CISR è garantito dall'organismo collegiale di coordinamento (il cosiddetto « CISR tecnico »), presieduto dal direttore generale del DIS.

Il cuore dell'architettura nazionale a protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, è il Nucleo per la sicurezza cibernetica (NSC), istituito presso il DIS, il cui ruolo è stato ulteriormente rafforzato dal decreto Gentiloni del 2017.

Il Nucleo per la sicurezza cibernetica, istituito nel 2013, ha avuto inizialmente sede presso il Consigliere militare del Presidente del Consiglio. Con il decreto Gentiloni è stato invece insediato presso il DIS e non è più presieduto dal Consigliere militare ma da un vicedirettore generale del Dipartimento. Il direttore generale, dunque, delega specificamente a uno dei vicedirettori generali del DIS le funzioni di sovrintendenza e raccordo delle attività in materia di sicurezza cibernetica. A tale riguardo, come riporta la relazione annuale sull'attività svolta dal Comitato, approvata nella seduta del 24 gennaio 2018 (Doc. XXXIV, n. 5), « nella fase istruttoria il Comitato è intervenuto per chiedere una definizione stringente della delega, limitata agli aspetti specificamente attinenti all'ambito cibernetico – nel significato poi effettivamente recepito nel testo entrato in vigore – al fine di evitare qualsiasi possibile ambiguità interpretativa circa la portata della disposizione ».

La scelta strategica di creare una figura di vicedirettore generale del DIS con specifica delega sulla sicurezza cibernetica è riconducibile alla consapevolezza – come affermato nella sopra citata relazione del Comitato del 2010 – che « di fronte a qualsiasi attacco condotto con mezzi cibernetici, il successo è direttamente proporzionale alla velocità di applicazione delle contromisure » e che, dunque, tali contromisure debbano rientrare nell'ambito di una pianificazione a lungo termine e debbano essere predisposte « prima che avvenga l'attacco, in una prospettiva che, in ragione della dimensione globale della minaccia cibernetica e della pluralità dei soggetti che potrebbero essere coinvolti, supera i confini nazionali e va organizzata secondo logiche di sicurezza integrate e con strategie di intervento che coinvolgano tutti gli attori della sicurezza ».

Un contributo alla costruzione di una politica di sicurezza nello spazio cibernetico è stato segnato, inoltre, dall'approvazione della legge di stabilità del 2016 (articolo 1, comma 965, legge 28 dicembre 2015, n. 208), che ha istituito, per l'anno 2016, un fondo « per il potenziamento degli interventi e delle dotazioni strumentali in materia di protezione cibernetica e di sicurezza informatica nazionali » con una dotazione finanziaria di 150 milioni di euro, di cui un decimo

destinato al « rafforzamento della formazione del personale del Servizio di polizia postale e delle comunicazioni, nonché all'aggiornamento della tecnologia dei macchinari e delle postazioni informatiche ».

La disciplina giuridica nazionale è stata inoltre integrata e implementata a seguito degli sviluppi normativi avvenuti a livello europeo. Nel 2013, infatti, l'Unione europea si è dotata di una Strategia comune in materia di *cybersecurity* (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)*, dalla quale è poi scaturita la direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cosiddetta direttiva NIS – *Network and Information Security)*. Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società e per l'Unione europea è essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno. Secondo l'Unione, infatti, « la portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono, inoltre, diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi (...), impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione » (paragrafo 2 della direttiva (UE) 2016/1148, cosiddetta direttiva NIS).

L'obiettivo della direttiva è, dunque, quello di migliorare le capacità degli Stati membri nella sicurezza cibernetica, di rafforzare la collaborazione in ambito europeo attraverso l'istituzione di un « Gruppo di cooperazione » (composto da rappresentanti degli Stati membri, dalla Commissione e dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, ENISA) e promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, imponendo misure di sicurezza e obblighi di notifica per gli operatori di servizi essenziali (OSE) e per i fornitori di servizi digitali (FSD).

A tal fine, ogni Stato membro ha il compito di designare uno o più autorità competenti NIS (che identificano gli OSE e gli FSD), un Punto di contatto unico (PoC) in materia di sicurezza delle reti e dei sistemi informativi (con una funzione di collegamento per la cooperazione transfrontaliera con le autorità degli altri Stati membri) e uno o più CSIRT (*Computer Security Incident Response Team)*, « anche noti come squadre di pronto intervento informatico ("CERT"), ben funzionanti e rispondenti a determinati requisiti essenziali, in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione » (paragrafo 34 della direttiva (UE) 2016/1148, cosiddetta direttiva NIS).

La direttiva NIS è stata attuata in Italia con il decreto legislativo 18 maggio 2018, n. 65, che stabilisce misure volte a conseguire un elevato livello di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo così a elevare il livello comune di

sicurezza dello spazio cibernetico europeo. In particolare, con il decreto legislativo n. 65 del 2018 è stato istituito, presso la Presidenza del Consiglio dei ministri, il CSIRT italiano – definito dalla direttiva 2016/1148 quale gruppo di intervento per la sicurezza informatica in caso di incidente – che definisce le procedure per la prevenzione e la gestione degli incidenti informatici e che garantisce la collaborazione effettiva, efficiente e sicura con la rete di CSIRT europea; sono state individuate per settore, a livello ministeriale, le cosiddette « Autorità NIS »[1] con il compito di individuare gli operatori di servizi essenziali (OSE) con sede sul territorio nazionale; è stato designato il DIS quale « Punto di contatto unico » in Italia in materia di sicurezza delle reti e dei sistemi informativi.

L'autorità di contrasto è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (Servizio di polizia postale e delle comunicazioni), al quale è attualmente attribuita la competenza ad assicurare « i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale (...), operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate » (articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito con legge 31 luglio 2005, n. 155).

Sempre secondo il decreto attuativo della direttiva NIS, gli operatori di servizi essenziali e i fornitori di servizi digitali inviano le notifiche relative a eventuali incidenti al CSIRT italiano, che informa le autorità NIS e il Punto di contatto unico (DIS).

Gli operatori di servizi essenziali, ai fini del provvedimento, sono i soggetti pubblici o privati, operanti nei settori energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, individuati dalle autorità competenti NIS. È posto a loro carico l'obbligo di individuare le misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti e, sotto il profilo procedurale, sono definite le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti, individuando altresì le condizioni e le modalità secondo le quali potranno essere coinvolti gli organismi di altri Paesi.

Il decreto del Ministro dello sviluppo economico del 15 febbraio 2019, in attuazione del DPCM 12 febbraio 2017, ha istituito il Centro di valutazione e certificazione nazionale (CVCN), presso l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità

---

(1) Il Ministero per lo sviluppo economico per il settore energia, il Ministero delle infrastrutture e dei trasporti per il settore trasporti, il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, il Ministero della salute, le Regioni e le Province autonome per l'attività di assistenza sanitaria, il Ministero dell'ambiente e della tutela del territorio e del mare, le Regioni e le Province autonome nel settore della fornitura e della distribuzione di acqua potabile.

di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

In tema di poteri speciali (cosiddetto *golden power*) inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G, è intervenuto dapprima l'articolo 1 del decreto-legge 25 marzo 2019, n. 22, che ha apportato modifiche alla disciplina su tali poteri e, successivamente, il decreto-legge 11 luglio 2019, n. 64, non convertito in legge.

Un complessivo aggiornamento della disciplina in tale materia è stato poi introdotto con il decreto-legge 21 settembre 2019, n. 105, convertito con legge 18 novembre 2019, n. 133.

Il decreto istituisce il perimetro di sicurezza nazionale cibernetica, al fine di assicurare la sicurezza di reti, sistemi informativi e servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza del Paese. L'individuazione dei soggetti inclusi nel perimetro è demandata ad un decreto del Presidente del Consiglio dei ministri, adottato su proposta del CISR.

Sempre con decreto del Presidente del Consiglio, da adottare su proposta del CISR, previo parere delle competenti Commissioni parlamentari, vengono determinate le procedure di notifica degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica e delle misure di sicurezza.

È rimessa a un regolamento, da emanarsi entro 10 mesi dalla data di entrata in vigore della legge di conversione, la definizione delle procedure, delle modalità e dei termini ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici.

Il decreto-legge interviene anche rafforzando le competenze del Centro di valutazione e certificazione nazionale (CVCN) in tema di acquisto di prodotti e servizi di tecnologie dell'informazione e della comunicazione (ICT), ove destinati a reti, sistemi informativi e sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica.

Per quanto riguarda le procedure di segnalazione degli incidenti su reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica, i soggetti coinvolti devono notificare l'incidente al CSIRT italiano, che a sua volta informa tempestivamente il DIS. Le misure di sicurezza devono assicurare elevati livelli di prevenzione e salvaguardia di reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

In tema di poteri speciali, la normativa prevede che essi siano esercitati previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, effettuata dal CVCN e dal Centro di valutazione del Ministero della difesa. Con specifico riferimento ai settori della difesa e della sicurezza nazionale, e alle

attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, il decreto-legge, oltre a prolungare da 15 a 45 giorni il termine – che decorre dalla notifica da parte dell'impresa della informativa dell'operazione di acquisto avviata nei confronti di aziende italiane – per l'esercizio dei poteri speciali da parte del Governo, con contestuale arricchimento dell'informativa resa dalle imprese detentrici degli *asset* strategici, modifica la disciplina dei poteri speciali in tema di tecnologie 5G, e individua i criteri per determinare se un investimento estero è suscettibile di incidere sulla sicurezza o sull'ordine pubblico.

Viene in particolare rafforzato ed ampliato l'ambito di ricorso ai poteri speciali nel caso in cui l'acquirente di partecipazioni rilevanti sia un soggetto esterno all'Unione europea, e sottoposta all'obbligo di notifica anche l'acquisizione a qualsiasi titolo, in luogo del solo acquisto, di beni o servizi relativi alle reti 5G, quando posta in essere da soggetti esterni all'Unione europea.

Viene altresì regolata l'ipotesi di intervento di emergenza in casi di rischio grave o di crisi di natura cibernetica. Si prevede infatti che il Presidente del Consiglio – su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR) – possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati. Entro 30 giorni, il Presidente del Consiglio è tenuto ad informare il Comitato parlamentare per la sicurezza della Repubblica delle misure disposte.

Da ultimo, in ambito Unione europea, è utile segnalare la *Relazione sulla valutazione coordinata a livello di UE dei rischi per la cybersicurezza delle reti di quinta generazione (5G)*, del 9 ottobre 2019. Il documento, che si colloca nel filone degli atti volti a garantire un elevato livello di cybersicurezza delle reti 5G in tutta l'UE, ed è stato predisposto dal Gruppo di cooperazione istituito dalla direttiva NIS, si basa sui risultati delle valutazioni nazionali dei rischi per la cybersicurezza, effettuate da tutti gli Stati membri dell'UE, e individua le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità (di natura tecnica e di altro tipo), nonché diversi rischi strategici.

La Relazione, in particolare, sottolinea i potenziali scenari di rischio connessi alla implementazione delle nuove reti:

maggiore esposizione agli attacchi e aumento del numero dei potenziali punti di accesso per gli autori di tali attacchi. Dato che le reti 5G si basano sempre più su *software*, stanno assumendo importanza i rischi legati a gravi lacune a livello di sicurezza, come quelle derivanti da processi inadeguati di sviluppo del *software* da parte dei fornitori. Ciò potrebbe anche consentire agli autori delle minacce di inserire malevolmente *backdoor* più difficilmente individuabili nei prodotti;

maggiore sensibilità di alcune apparecchiature e funzioni di rete, quali le stazioni base o le principali funzioni di gestione tecnica delle reti;

maggiore esposizione ai rischi legati alla dipendenza degli operatori di reti mobili dai fornitori, che aumenterà anche il numero

dei percorsi di attacco sfruttabili dagli autori delle minacce (ivi compresi gli stati non membri dell'UE) ed esacerberà la potenziale gravità dell'impatto di tali attacchi;

aumento dei rischi derivanti da una forte dipendenza da un unico fornitore, che accresce l'esposizione al rischio derivante da un'eventuale interruzione dell'approvvigionamento dovuta, ad esempio, a un insuccesso commerciale, e alle sue conseguenze. Tale dipendenza aumenta inoltre il potenziale impatto delle debolezze o delle vulnerabilità nonché la possibilità che queste vengano sfruttate dagli autori di minacce, in particolare quando la dipendenza riguarda un fornitore che presenta un elevato grado di rischio;

sviluppo delle minacce alla disponibilità e all'integrità delle reti, che diventeranno importanti problemi in materia di sicurezza, in aggiunta alle minacce alla riservatezza e alla tutela della privacy. La conversione delle reti 5G nella colonna portante di numerose applicazioni informatiche critiche farà sì che l'integrità e la disponibilità di tali reti diventino rilevanti problemi in materia di sicurezza nazionale e una sfida di primo piano per la sicurezza a livello di UE.

A fronte di tali rilevanti scenari di rischio, la Relazione considera necessario rafforzare il paradigma di sicurezza, e a tal fine richiede un riesame dell'attuale quadro politico e di sicurezza applicabile al settore e al suo ecosistema, ed impone agli Stati membri di adottare le necessarie misure di attenuazione.

La Relazione fissa al 31 dicembre 2019 il termine entro il quale il gruppo di cooperazione dovrebbe concordare una serie di misure di attenuazione per far fronte ai rischi per la cybersicurezza individuata a livello nazionale e dell'Unione.

Entro il 1º ottobre 2020 gli Stati membri, in cooperazione con la Commissione, dovrebbero quindi valutare gli effetti della raccomandazione per determinare se vi sia bisogno di ulteriori interventi, tenendo conto dell'esito della valutazione europea coordinata dei rischi e dell'efficacia delle misure.

Vanno infine segnalate le conclusioni del recente Consiglio dell'Unione europea Trasporti, telecomunicazioni ed energia, svoltosi il 3 e 4 dicembre 2019, e la Dichiarazione di Londra approvata dal Vertice dei Capi di Stato e di Governo della NATO, anch'esso svoltosi il 3 e il 4 dicembre 2019.

Il Consiglio della UE, sul tema dei rischi connessi alle reti 5G, evidenzia la necessità di considerare fra i fattori di rischio per la sicurezza non solo i profili attinenti la tecnologia ma altresì quelli derivanti da fattori extra-tecnici, e collegati alle politiche e ai sistemi legali vigenti nei Paesi terzi, con i quali vengano instaurati rapporti per la fornitura di servizi e prodotti.

Nella Dichiarazione di Londra, i Paesi della NATO si impegnano, tra l'altro, a garantire la sicurezza delle comunicazioni, anche con riferimento alle reti 5G, rilevando l'esigenza di poter fare affidamento su sistemi informatici sicuri e resilienti.

Valutazioni e proposte del Comitato.

Cenni sullo stato della minaccia.

Il crescente pericolo per le infrastrutture strategiche del nostro Paese, derivante dalla minaccia cyber, rappresenta un dato di sicuro allarme, che ha trovato conferma anche nel corso delle numerose audizioni svolte dal Comitato nel corso del 2019.

Le statistiche sugli attacchi evidenziano un incremento costante – sebbene non siano ovviamente ancora disponibili i dati definitivi per l'anno in corso – non solo sul piano quantitativo ma anche sul versante della capacità innovativa di cui gli autori di tali iniziative danno continue dimostrazioni.

Le modalità di dissimulazione degli attacchi sono sempre più efficaci, e fra queste si segnala l'utilizzo di apposite piattaforme tecnologiche, prese temporaneamente in affitto, che rendono ovviamente molto complicata l'individuazione originaria degli attacchi stessi.

Altro strumento fondamentale è rappresentato dalla rete TOR (*The Onion Router*), che consente di effettuare attività illecite o intrusioni mantenendo l'anonimato, grazie al meccanismo per cui il *software* offensivo viene scomposto in pacchetti, che per raggiungere l'obiettivo finale seguono percorsi diversi, attraverso una serie di piattaforme, rendendo di fatto quasi impossibile l'individuazione della fonte.

Un esempio significativo, ricordato nel corso delle audizioni, è il cosiddetto « Wanna Cry », un virus capace di attaccare criptando le chiavi di accesso del sistema infettato, per poi far seguire la richiesta di un riscatto al fine di poter recuperare il proprio patrimonio di dati. Nel corso del 2017 il virus, diffuso in numerosi Paesi del mondo, ha colpito oltre centomila postazioni informatiche, molte delle quali operanti presso pubbliche amministrazioni, come ospedali, università, aziende di trasporti e del settore tecnologico.

Un attacco di rilievo, risalente al 2009, ma la cui notizia è stata rilanciata nel 2019 da organi di stampa americani, sarebbe stato portato attraverso l'installazione di *backdoor* su apparecchi forniti dall'azienda cinese Huawei a Vodafone Italia, in grado di effettuare accessi non autorizzati all'infrastruttura e quindi alle informazioni veicolate. Nel corso dell'audizione i rappresentanti di Vodafone Italia hanno precisato che le *backdoor*, predisposte ai fini di garantire l'assistenza in caso di malfunzionamento degli apparati, avevano in effetti fatto registrare alcune vulnerabilità. I tecnici dell'azienda sono riusciti, dopo alcune difficoltà iniziali, a porre rimedio al problema, prima che potessero determinarsi rischi per i dati e le informazioni transitate sui sistemi. Rischi che comunque, secondo quanto riferito dagli stessi dirigenti di Vodafone Italia, sarebbero stati di entità limitata. Secondo i rappresentanti di Huawei Italia, l'importanza della vicenda è stata eccessivamente enfatizzata dai mezzi di informazione, non essendosi in realtà trattato di una *backdoor*, ma di una procedura ordinariamente utilizzata per consentire gli interventi da remoto, che era rimasta erroneamente attiva.

La vicenda, per quanto ridimensionata secondo quanto sostenuto dalle aziende, ha posto in evidenza la permeabilità dei sistemi, e la loro possibile infiltrazione.

I rischi provenienti da Paesi terzi.

L'incidente cui si è fatto cenno rientra nella più ampia questione collegata alla crescente presenza sul mercato internazionale di aziende aventi la propria sede principale in Paesi esterni all'Europa e al mondo occidentale. Fra queste, rilevano in particolare alcune aziende cinesi, fornitrici di servizi e apparecchiature nel mercato italiano ed europeo, di cui non è certa la piena autonomia rispetto alle autorità governative del proprio Paese.

A tale proposito, i rappresentanti di Huawei Italia hanno sottolineato che l'azienda italiana è soggetto autonomo, sebbene ovviamente collegato, rispetto alla società principale, e che deve necessariamente rispettare la legislazione italiana. Con riguardo ai rischi per la sicurezza delle reti, hanno inoltre rilevato che l'eventuale debolezza del sistema risiede non nella rete predisposta dal fornitore, quanto dalla eventuale insufficienza degli elementi di protezione dei dati, e che in ogni caso all'azienda non è mai stata segnalata, nei 170 Paesi in cui essa opera, alcuna attività di spionaggio o di controllo da parte di soggetti esterni. Quanto ai rapporti con le autorità cinesi, hanno poi dichiarato che non sussisterebbe una normativa interna che autorizzi entità, agenzie o strutture del Governo a indurre i produttori alla installazione di apparati *software* o *hardware*.

Su questo aspetto, il Comitato ha tuttavia ricevuto valutazioni di segno diverso da parte dei responsabili delle Agenzie. In particolare, è stato posto in rilievo che in Cina gli organi dello Stato e le stesse strutture di *intelligence* possono fare pieno affidamento sulla collaborazione di cittadini e imprese, e ciò sulla base di specifiche disposizioni legislative. La *National Security Law* obbliga, in via generale, cittadini e organizzazioni a fornire supporto e assistenza alle autorità di pubblica sicurezza militari e alle agenzie di *intelligence*. Inoltre, con riferimento alla normativa sulle attività informatiche, la *Cyber Security Law* prevede che gli operatori di rete debbano fornire supporto agli organi di polizia e alle agenzie di *intelligence* nella salvaguardia della sicurezza e degli interessi nazionali.

Sulla base di tali elementi informativi, il Comitato non può pertanto che ritenere in gran parte fondate le preoccupazioni circa l'ingresso delle aziende cinesi nelle attività di installazione, configurazione e mantenimento delle infrastrutture delle reti 5G. Conseguentemente, oltre a ritenere necessario un innalzamento degli standard di sicurezza idonei per accedere alla implementazione di tali infrastrutture, rileva che si dovrebbe valutare anche l'ipotesi, ove necessario per tutelare la sicurezza nazionale, di escludere le predette aziende dalla attività di fornitura di tecnologia per le reti 5G.

La posizione degli USA e degli altri Paesi.

Gli Stati Uniti, nel maggio del 2019, hanno disposto, per motivi di sicurezza nazionale, il divieto per Huawei di acquistare tecnologia statunitense se non previa autorizzazione, nonché di vendere e installare le proprie infrastrutture sul territorio americano. Una linea di restrizione verso il coinvolgimento di aziende cinesi nella implementazione del 5G è stata anche adottata da Australia, Nuova Zelanda e Giappone, mentre la maggior parte dei Paesi europei finora ha scelto di rafforzare le misure di sicurezza cibernetica senza imporre limitazioni alla presenza di tali soggetti (con la parziale eccezione di Polonia e Romania, che hanno sottoscritto dichiarazioni congiunte con gli Stati Uniti su questa materia).

Ciò anche in relazione alla notevole e radicata presenza di Huawei e ZTE, che tra l'altro hanno già partecipato con successo a gare per l'implementazione di strutture destinate alle reti di nuova generazione e collaborano con quasi tutti i principali operatori di telecomunicazioni. Tali risultati sono anche determinati dalla posizione dominante e dai connessi profitti di cui questi operatori godono in Cina, che permettono di praticare offerte molto competitive nei mercati occidentali.

A questo proposito, alcune aziende hanno sottolineato, nel corso delle audizioni, il problema costituito dalla strategia praticata dalle aziende cinesi, che si configura come una sorta di *dumping*, attraverso offerte che in qualche caso giungono a presentare prezzi sensibilmente inferiori rispetto a quelli proposti dai concorrenti europei (questo aspetto potrebbe essere adeguatamente valutato dai competenti organi europei e internazionali). È chiaro come fenomeni di questo tipo siano riconducibili alle asimmetrie normative e organizzative che caratterizzano questo tipo di confronto, laddove gli standard nazionali ed europei concernenti salari, condizioni di lavoro e sicurezza dei dipendenti, non sono evidentemente paragonabili a quelli vigenti nella realtà cinese. Problema ovviamente riscontrabile in tutti i settori del commercio, ma particolarmente avvertito nell'ambito della produzione di apparati e strutture ad elevato contenuto tecnologico.

Appare certamente difficile, in una realtà caratterizzata dalle leggi del mercato e della libera concorrenza, prevedere interventi autoritativi che potrebbero mettere a rischio la stessa realizzabilità di progetti ritenuti essenziali per lo sviluppo delle nuove tecnologie. Del resto, lo stesso Governo americano, a seguito delle numerose problematiche paventate dalle aziende nazionali in conseguenza del predetto divieto, ha più volte rinviato la piena attuazione del provvedimento stesso (da ultimo, l'entrata in vigore del divieto è stata prorogata al febbraio 2020).

Per queste medesime ragioni, né gli organi della UE, né i principali Paesi europei hanno finora adottato provvedimenti di divieto o limitazione alle attività degli operatori cinesi, pur nella consapevolezza dei possibili rischi che potrebbero derivarne.

Lo stesso Governo italiano ha assunto una posizione sostanzialmente allineata a quella dei principali partner europei. Il Presidente del Consiglio ha in proposito rilevato che le preoccupazioni manife-

state soprattutto dagli Stati Uniti – secondo cui l'espansionismo economico cinese sarebbe frutto di iniziative non solo delle aziende, ma di un disegno collettivo nazionale volto a conquistare il primato nel mondo occidentale nel settore *high tech* – sono certamente meritevoli di essere tenute in considerazione, come pure lo è la rilevanza della legislazione interna cinese in materia di sicurezza nazionale, con i relativi obblighi per le aziende. A fronte di tale contesto, il nostro Paese deve pertanto porre in essere tutte le misure di sicurezza preventiva che possano limitare i rischi derivanti dalla presenza di tali aziende nel nostro sistema, con particolare riferimento allo sviluppo delle reti 5G. In tal senso, il Governo ritiene fondamentale l'attuazione delle misure contenute nel decreto-legge istitutivo del Perimetro di sicurezza nazionale cibernetica e di quelle concernenti il Centro di valutazione e certificazione nazionale (CVCN). Tuttavia, il Presidente del Consiglio ha sottolineato come decisioni che limitino la presenza di tali aziende dal mercato nazionale non sarebbero coerenti con i principi economici e commerciali praticati nel nostro Paese e nel mondo occidentale, come del resto dimostra l'orientamento di quasi tutti i Paesi europei, che hanno scelto anch'essi di rafforzare le misure di sicurezza e di vigilanza, senza imporre esclusioni o limitazioni all'ingresso di soggetti extraeuropei nello sviluppo e nella fornitura di prodotti e servizi relativi alle reti 5G.

In particolare, si possono segnalare a titolo di esempio le esperienze di due fra i principali Paesi europei.

Nel Regno Unito, nel dicembre 2018 è stato creato un comitato di analisi delle minacce di Stato, il *Joint State Threat Analysis*, integrato da rappresentanti del Governo e dalle agenzie di *intelligence*. Si tratta di una iniziativa che conferma l'attenzione e il monitoraggio su questo tema e sui rischi potenziali che ne possono derivare, ma che peraltro non ha comportato al momento alcuna decisione limitativa nei confronti delle aziende in questione.

La Germania, nel dicembre 2018, ha adottato misure di protezione dell'economia attraverso l'implementazione, a cura della comunità *intelligence* e delle forze di polizia, di due progetti connessi con il sistema di monitoraggio degli investimenti esteri. Il primo progetto, denominato « Iniziativa per la protezione del *business* », è coordinato dal Ministero dell'interno, mentre il secondo, coordinato dal Ministero dell'economia, è dedicato allo *screening* degli investimenti diretti esteri. Sono state inoltre assunte iniziative per modificare la normativa interna, al fine di abbassare la quota, fissata al 25 per cento, di acquisizioni dall'estero di società che operano in settori strategici.

La rilevanza del problema è stata, peraltro, recentemente confermata in occasione del Consiglio dell'Unione europea Trasporti, telecomunicazioni ed energia del 3-4 dicembre 2019, che nelle conclusioni sul tema del 5G ha, tra l'altro, sottolineato come i Paesi membri debbano considerare fra i fattori di rischio per la sicurezza non solo i profili attinenti la tecnologia ma altresì quelli derivanti dalle politiche e dagli ordinamenti legislativi vigenti nei Paesi terzi dai quali vengono acquisiti prodotti e servizi.

In proposito, il Comitato ritiene di sottolineare che le pur significative esigenze commerciali e di mercato, che assumono un ruolo fondamentale in una economia aperta, non possono prevalere su quelle che attengono alla sicurezza nazionale, ove queste siano messe in pericolo. Non si ritiene pertanto di condividere le valutazioni espresse da molti degli operatori ascoltati in audizione, secondo i quali i rapporti e la interconnessione con le aziende cinesi sarebbero ormai tali da non consentire interventi limitativi della presenza di queste ultime nell'assetto delle infrastrutture di rete del nostro Paese, e ciò anche con riferimento alla rete 5G.

A parere del Comitato, il Governo e gli organi competenti in materia dovrebbero considerare molto seriamente, anche sulla base di quanto prevede la recente disciplina dettata dal decreto-legge n. 105/2019, la possibilità di limitare i rischi per le nostre infrastrutture di rete, anche attraverso provvedimenti nei confronti di operatori i cui legami, più o meno indiretti, con gli organi di governo del loro Paese appaiono evidenti. A tali organi potrebbero infatti potenzialmente essere veicolate informazioni e dati sensibili riconducibili a cittadini, enti e aziende italiani.

In tal senso, su sollecitazione dei membri del Comitato, i rappresentanti di una delle aziende audite hanno affermato che nel caso si dovesse giungere a un divieto per le aziende cinesi, simile a quello adottato dagli Stati Uniti, sarebbe comunque possibile procedere alla implementazione delle infrastrutture e degli apparati collegati al 5G, con costi complessivi approssimativamente quantificati in circa 600 milioni di euro, senza peraltro che ciò comporti particolari ritardi nello sviluppo della nuova tecnologia.

La tutela dei dati personali.

Uno dei temi su cui si è soffermato il Garante per la tutela dei dati personali, nel corso della sua audizione, è rappresentato dalla prassi del massiccio prelievo di dati da parte delle grandi piattaforme che operano in rete, che li utilizzano per la 'profilazione' degli utenti, a scopi prevalentemente, ma non esclusivamente, commerciali.

È stato in proposito citato il caso di Cambridge Analytica, società britannica di consulenza, accusata nel 2018 di avere raccolto, senza consenso degli interessati, attraverso *account* del *social network* Facebook, un elevato numero di dati personali, da utilizzare poi per finalità di propaganda politica.

Il Garante ha anche sottolineato di ritenere opportuna una iniziativa dell'Unione Europea, intesa a escludere che i dati personali detenuti da aziende e da piattaforme cinesi, operanti in rete, possano essere oggetto di prelievo da parte di organismi governativi.

A tale proposito, un caso recentemente emerso riguarda il *social network* cinese Tik Tok, che conta circa 500 milioni di abbonati, ed è utilizzato in larga parte da giovani al di sotto dei 18 anni. Anche in questo caso, si segnalano i rischi derivanti dai possibili utilizzi dei dati raccolti mediante l'attività di profilazione degli utenti, attraverso

la raccolta dei dati presenti negli *account,* al fine di personalizzare i contenuti dell'applicazione.

Tali attività hanno già comportato per l'azienda una multa da 5,7 milioni di dollari, comminata nel febbraio 2019 dall'Agenzia governativa americana per la tutela dei consumatori, per avere raccolto i dati personali di minori di 13 anni senza il consenso dei genitori.

A seguito di denunce da parte di alcuni parlamentari americani, il Governo degli Stati Uniti ha recentemente aperto una indagine, volta ad accertare se l'azienda, attraverso la raccolta di dati personali, possa non solo mettere a rischio la privacy dei cittadini americani, ma rappresentare un pericolo per la sicurezza nazionale, in relazione al fatto che la società è tenuta a rispettare le leggi cinesi, anche con riferimento ai rapporti con il Governo e gli altri organi statuali.

Su tali aspetti, il Comitato ritiene necessario che sia in sede europea sia a livello nazionale vengano assunte iniziative idonee a garantire il rispetto e la tutela dei dati personali, disciplinando con rigore le attività consentite alle piattaforme e ai *social network* nei riguardi degli *account* degli utenti. In tal senso, dovrebbe essere sostenuta la proposta del Garante – rilanciata proprio a seguito dell'indagine avviata dal Governo americano – volta a definire, in sede europea, un accordo per gli scambi di dati a scopo commerciale con la Cina, in analogia a quelli già conclusi con Stati Uniti e Giappone.

Standard di sicurezza dei prodotti.

Fra le esigenze rilevate nel corso delle audizioni, condivise dal Comitato, va segnalata quella relativa alla opportunità di innalzare il livello di sicurezza cibernetica già al momento della definizione dei contratti di acquisto dei prodotti e dei servizi, destinati alla pubblica amministrazione, attraverso la Consip. I rappresentanti di Telecom Italia su questo aspetto hanno rilevato che l'acquisizione di prodotti e servizi con gara Consip, che prevede soltanto il criterio del massimo ribasso economico e non fa specifico riferimento ai requisiti di sicurezza, pone oggettivamente un problema cui occorre trovare adeguate soluzioni. A tale esigenza ha dato una risposta la nuova disciplina introdotta con il citato decreto-legge n. 105 del 2019, che attribuisce al CVCN compiti di verifica sulla sicurezza dei prodotti e dei servizi connessi alle telecomunicazioni.

Assume rilievo in tale ambito, con particolare riferimento alle reti 5G, l'impatto della metodologia di verifica del rischio e di certificazione, che, a parere di molti degli operatori auditi, dovrebbe tenere conto delle esigenze delle imprese e pertanto conciliare efficacia e tempestività.

A questo ordine di problemi dovrebbe almeno in parte rispondere il Centro di valutazione e certificazione nazionale - CVCN (le cui competenze sono state estese e rafforzate con il decreto-legge n. 105/2019), a cui il Comitato ritiene pertanto necessario venga assicurata piena e tempestiva operatività.

A tali profili problematici si ricollega il tema della manutenzione e degli aggiornamenti dei prodotti, che in questo campo sono necessari

per incorporare la continua evoluzione della tecnologia. Tali attività vengono svolte nella maggior parte dei casi da remoto, direttamente dal produttore. Ovviamente, soprattutto se l'azienda ha sede in Paesi considerati a rischio per gli standard di sicurezza europei, ne derivano potenziali pericoli per la sicurezza dei servizi e prodotti coinvolti.

Modalità ed evoluzione delle azioni ostili.

Per quanto concerne le statistiche sugli attacchi cyber, nelle audizioni dei reparti specializzati delle Agenzie e in quella del vicedirettore del DIS, professor Roberto Baldoni, responsabile del Nucleo per la sicurezza cibernetica, sono state fornite al Comitato informazioni dettagliate sia circa i dati quantitativi che sugli obiettivi colpiti. Si tratta peraltro di informazioni coperte da segreto, e pertanto in questa sede si potrà fare riferimento alle informazioni contenute nella Relazione sulla politica dell'informazione per la sicurezza, presentata al Parlamento nel febbraio del 2019. Da tali dati, emerge un numero complessivo di azioni ostili riferite al 2018 più che quintuplicato rispetto all'anno precedente (anche grazie alle accresciute capacità di rilevamento), che hanno colpito soprattutto i sistemi informatici di pubbliche amministrazioni centrali e locali (72 per cento del totale). Nei confronti dei soggetti pubblici si rileva un incremento pari al 561 per cento rispetto all'anno precedente. Sensibile l'aumento di attacchi contro reti ministeriali (24 per cento delle azioni ostili) e contro infrastrutture IT riconducibili ad enti locali (39 per cento del totale). Gli attacchi in danno di soggetti privati sono più che triplicati, e hanno colpito soprattutto i settori energetico, delle telecomunicazioni e dei trasporti.

Agli attacchi portati da *hacker*, o da gruppi organizzati e strutturati (quali ad esempio Anonymous Italia e AntiSec ITA), si sono da tempo aggiunti quelli derivanti da soggetti che, sia pure senza poterne attribuire con certezza la provenienza, appaiono riconducibili ad attori statuali individuabili, per i quali tali iniziative rappresentano uno degli strumenti cui fare ricorso per perseguire obiettivi strategici. Tali attività si inseriscono pienamente nel quadro della cosiddetta minaccia ibrida, considerata quale impiego combinato di strumenti convenzionali e non, i cui effetti risultano notevolmente rafforzati proprio in seguito ai processi di digitalizzazione che hanno interessato larghi settori della vita sociale ed economica.

Minacce in ambito economico-finanziario.

Non possono inoltre essere sottovalutati gli obiettivi di tipo economico-commerciale spesso perseguiti dalle predette iniziative, che nascondono in certi casi intenti predatori nei confronti di aziende o *asset* nazionali da parte di soggetti statuali. Attività sulle quali i reparti specializzati del Comparto hanno in più occasioni riferito al Comitato.

Anche sotto questo profilo, l'implementazione delle reti 5G non può che destare preoccupazione e, come testimoniato in molte delle

audizioni svolte, imporre l'adozione di misure di prevenzione efficaci e tempestive nei confronti delle possibili minacce derivanti da tale sviluppo delle strutture informatiche nazionali.

A tale proposito, il Comitato valuta positivamente la disciplina introdotta con il decreto-legge n. 21 del 2019, in primo luogo per la definizione del Perimetro di sicurezza nazionale cibernetica, con l'articolazione delle finalità e delle modalità di individuazione dei soggetti pubblici e privati che ne fanno parte e, in secondo luogo, con riguardo al rafforzamento dei poteri speciali in capo al Governo, attivabili nei confronti dei soggetti che possono operare nel nostro Paese nell'ambito delle attività di infrastrutturazione e supporto alle reti in questione.

Come pure va considerato senz'altro opportuno il recente decreto (DPCM 8 agosto 2019) organizzativo del CSIRT *(Computer Security Incident Response Team),* collocato presso il DIS, che assume funzioni rilevanti nella gestione degli incidenti informatici e andrà a rafforzare le strutture già operative nell'ambito della Architettura nazionale cyber, integrando le competenze già attribuite ai due CERT (nazionale e pubblica amministrazione).

In proposito, appare fondamentale che il nuovo organismo, una volta pienamente operativo, possa garantire efficacia e tempestività nelle risposte agli attacchi, considerato che nella maggior parte dei casi la riduzione del danno e la protezione dei dati sono strettamente connessi alla durata e alla pervasività delle azioni offensive.

Il Comitato auspica peraltro che la concreta attivazione di tale organismo possa avvenire in tempi rapidi, proprio per la assoluta rilevanza dei compiti ad esso affidati.

*Formazione e specializzazione del personale dell'*Intelligence.

Tra gli aspetti delle politiche di sicurezza cibernetica cui molti degli auditi (Telecom Italia e Leonardo tra gli altri) hanno fatto cenno, va menzionato il tema delle risorse umane. In questo campo si sconta un divario significativo fra i Paesi europei e realtà quali Stati Uniti, Russia, India, che hanno investito massicciamente sul reclutamento e la formazione di personale specializzato, generalmente molto giovane e quindi in grado di sviluppare e accrescere nel tempo le proprie competenze. Il problema coinvolge ovviamente anche il comparto *Intelligence* del nostro Paese, che ha avviato negli anni scorsi iniziative volte proprio a colmare almeno in parte le carenze riscontrate, attraverso la realizzazione di corsi specializzati per la cybersicurezza, differenziati secondo le competenze e le esigenze delle Agenzie. Tuttavia, il personale formato e reso operativo nel Comparto trova spesso opportunità professionali più remunerative presso aziende private, e questo determina un oggettivo indebolimento del patrimonio di competenze delle Agenzie. Il problema, a parere del Comitato, dovrebbe essere attentamente valutato, anche in termini di possibili investimenti aggiuntivi finalizzati a questo specifico obiettivo, in considerazione della rilevanza strategica che la sicurezza cibernetica,

nei suoi vari aspetti, ha ormai assunto per i cittadini e per l'intero sistema Paese.

Sviluppi della strategia di difesa cibernetica europea e nazionale.

Con riferimento alla recente Relazione dell'Unione europea del 9 ottobre 2019 (cui si è accennato nel capitolo sul quadro normativo), la quale prevede che entro il 31 dicembre 2019 vengano emanate ulteriori misure volte all'attenuazione dei rischi per la cybersicurezza, individuati a livello nazionale e dell'Unione, e che entro il 1º ottobre 2020 gli Stati valutino se vi sia necessità di apportare nuovi interventi in tale ambito, il Comitato auspica che il nostro Paese partecipi attivamente a questa fase di verifica, anche in relazione al presumibile impatto, sugli attuali standard di sicurezza, della implementazione della tecnologia 5G.

Si ritiene nel contempo di sollecitare una riflessione in seno agli organismi europei sulla opportunità di rafforzare la strategia di difesa cibernetica comune, positivamente avviata con il varo della direttiva NIS, anche valutando possibili adeguamenti della normativa da essa introdotta.

In relazione al tema dei possibili interventi sulla normativa nazionale, il Comitato ritiene di segnalare, in primo luogo, l'esigenza messa in rilievo dal CNAIPIC (cui anche altri soggetti hanno accennato), circa la individuazione di figure di reato adeguate a fronteggiare il crescente fenomeno degli attacchi a infrastrutture critiche economiche del Paese. Una evoluzione della legislazione in tale settore appare opportuna, anche individuando nuove specifiche fattispecie di reato, ove si consideri che gli atti di criminalità cibernetica finanziaria sono allo stato attuale perseguibili facendo ricorso a fattispecie generiche (quali in particolare l'articolo 640 del codice penale), e comunque non aderenti ai contenuti e alle modalità operative che caratterizzano tali attività criminose.

In secondo luogo, si ritiene opportuna una attenta riflessione circa il tema della cosiddetta 'guerra ibrida'. Come già si è detto, le iniziative ostili da parte di attori esterni contro infrastrutture nazionali si sono notevolmente sviluppate. Allo stato attuale, le uniche risposte ad attacchi di tipo cibernetico portati su obiettivi di rilevanza strategica nazionale sono quelle di tipo reattivo/difensivo, volte cioè a contrastare e ridurre gli effetti dell'offensiva, mettendo in sicurezza le strutture colpite. Non è invece prevista la cosiddetta risposta 'proattiva', che preveda cioè anche un'attività offensiva nei confronti del soggetto attaccante, in quanto nel nostro ordinamento non è ancora contemplata una regolamentazione autorizzatoria analoga a quella prevista per i conflitti di tipo convenzionale.

La questione non è del resto risolvibile senza tenere conto del contesto e delle alleanze internazionali, con particolare riferimento alla NATO che, nella sua dottrina più recente, ha individuato in questo campo due categorie di interventi: *defensive cyber operation* e *offensive cyber operation*. Per queste ultime sono ancora oggetto di discussione, peraltro, i criteri regolatori e la relativa disciplina.

In proposito, va ricordata la recente Risoluzione approvata dall'Assemblea della NATO (n. 459 del 4 dicembre 2019), che esorta i Governi e i Parlamenti dei Paesi dell'Alleanza nord-atlantica « a onorare gli impegni nazionali in materia cibernetica assunti nell'ambito del Processo NATO di pianificazione della Difesa e dell'Impegno NATO per la Difesa Cibernetica, nonché ad adottare una dottrina NATO sullo spazio cibernetico entro la fine del 2020 ».

Il tema va pertanto considerato in continua evoluzione, ma proprio per la crescente pericolosità di questo tipo di minaccia, sembra opportuno che il legislatore possa quantomeno avviare una riflessione sulla ipotesi di introdurre nel nostro ordinamento strumenti normativi, anche sotto il profilo autorizzatorio, che possano sostenere e supportare l'azione degli organismi che presiedono alla tutela della sicurezza informatica e cibernetica del nostro Paese.

PAGINA BIANCA

PAGINA BIANCA

180340087180