ATTI PARLAMENTARI

XVII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **XVII**
n. **21**

DOCUMENTO APPROVATO DALLA IV COMMISSIONE PERMANENTE (DIFESA)

nella seduta del 21 dicembre 2017

A CONCLUSIONE DELL'INDAGINE CONOSCITIVA

deliberata nella seduta del 26 gennaio 2016

SULLA SICUREZZA E LA DIFESA NELLO SPAZIO CIBERNETICO

(Articolo 144, comma 3, del Regolamento della Camera dei deputati)

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

I N D I C E

1. SCOPO E SVILUPPO DELL'INDAGINE

La globalizzazione – il fenomeno forse più significativo del nostro tempo – è stata resa possibile anche e soprattutto dalla creazione dello "spazio cibernetico", ossia di una nuova dimensione nella quale gli esseri umani, e nel prossimo futuro verosimilmente anche le intelligenze artificiali, possono agire e interagire a distanza. Tale dimensione è generata dalla ramificatissima rete di infrastrutture materiali di collegamento e di comunicazione che, attraverso la tecnologia informatica, mettono in contatto tra loro un crescente numero di esseri umani e permettono loro di attivare e controllare da ubicazioni remote macchine e apparati in tutto il mondo. Questo "spazio" è generato dall'insieme di infrastrutture informatiche interconnesse, comprensivo di *hardware*, *software* e dati, nonché delle relazioni logiche tra di essi. Tale insieme comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete; può essere definito l'"ecosistema" risultante dall'interazione di persone, programmi informatici (*software*) e servizi su internet per mezzo di tecnologie, dispositivi e reti a esso connesse.

In quanto luogo di interazioni umane, al pari dello spazio fisico, lo spazio cibernetico può essere teatro anche di atti ostili (truffa, spionaggio, bullismo, diffamazione, danneggiamento, etc.). Azioni offensive nello spazio cibernetico, come nello spazio fisico, possono essere compiute da individui isolati come pure da gruppi o da organizzazioni di qualsiasi tipo, compresi gli Stati. Analogamente, obiettivi delle azioni offensive possono essere sia gli individui sia le organizzazioni, compresi gli Stati.

L'azione offensiva può essere minacciata o realizzata da uno Stato contro uno Stato per uno qualsiasi degli scopi tradizionalmente perseguiti con il ricorso alla guerra e allo strumento militare. Quando l'attacco è portato attraverso lo spazio cibernetico, si parla di "guerra cibernetica" (*cyber-warfare*) e correlativamente di "difesa cibernetica" (*cyber-defence*).

La guerra e la difesa cibernetiche tra Stati sono ad oggi, a parte alcune avvisaglie, uno scenario soltanto possibile, al pari della guerra nucleare. Come tuttavia evidenziato da un numero crescente di analisi strategiche, lo spazio cibernetico è il nuovo fondamentale campo di battaglia e di competizione geopolitica dell'umanità. Le prossime guerre tra gli Stati non saranno certamente condotte soltanto con i tradizionali strumenti di offesa e di difesa via terra, mare e aria, ma saranno accompagnate e probabilmente iniziate – e in qualche caso vinte – con attacchi perpetrati attraverso lo spazio cibernetico. Questi sono infatti suscettibili di infliggere al nemico danni gravissimi, con effetti sulla società che gli esperti considerano paragonabili a quelli di armi convenzionali.

È noto agli analisti che alcuni Stati stanno da tempo sviluppando capacità di offensiva cibernetica, nell'ambito delle rispettive Forze armate o di strutture parastatali, in una logica – è da sperare – di mera deterrenza. Diversi governi si sono dotati delle capacità necessarie per penetrare le reti nazionali degli altri Stati (in uso sia alle autorità pubbliche sia ai privati) a fini di spionaggio o per mappare i sistemi potenzialmente oggetto di un futuro attacco. È altresì concreto il rischio che alcuni Paesi mobilitino la propria industria nazionale al fine di alterare componenti *hardware* da essa prodotte e vendute all'estero, acquisendo così la capacità di superare in maniera pressoché irrilevabile ogni difesa posta in essere dall'utilizzatore dell'assetto finito.

Nel contempo, nello spazio cibernetico operano attori – innanzitutto le organizzazioni terroristiche – che, pur senza essere Stati, sono in grado di minacciare seriamente la sicurezza degli Stati e di intere comunità nazionali. Infatti la tecnologia, e ancor più la tecnologia informatica, rende oggi possibile a un numero limitato di persone con adeguate conoscenze specialistiche di arrecare ad ampie comunità – potenzialmente anche all'intera comunità di uno Stato – danni enormi agendo da grande distanza e in totale anonimato. L'asimmetricità è una caratteristica saliente della minaccia cibernetica.

La difesa delle reti implica lo sviluppo di un'efficiente e continua capacità di monitoraggio e di analisi degli attacchi. I pericoli esistenti nello spazio cibernetico sono straordinariamente vari, in quanto straordinariamente varie sono la tipologia di attori che operano in tale spazio e le attività

umane che vi si svolgono. Per questa ragione, l'ordinamento non affida a un soggetto esclusivo la responsabilità della protezione dello spazio cibernetico nazionale, ma la ripartisce tra più soggetti istituzionali, secondo i rispettivi ambiti di competenza, concentrando tuttavia le funzioni di indirizzo politico e di coordinamento strategico in un unico organismo – il Comitato interministeriale per la sicurezza della Repubblica (CISR), organo deputato alla gestione delle emergenze afferenti alla sicurezza nazionale (art. 7-*bis*, comma 5, del decreto-legge n. 174 del 2015) – e delineando nell'insieme un'architettura che organizza e mette a sistema i molteplici attori operanti nel campo della sicurezza dello spazio cibernetico, tra i quali un ruolo di primo piano è svolto dal Dipartimento delle informazioni per la sicurezza (DIS).

Le Forze armate sono uno di questi attori. Consapevoli del pericolo, esse si sono da tempo attivate per sviluppare, in piena armonia con la strategia nazionale sulla protezione informatica, un sistema di difesa contro gli attacchi di natura cibernetica sferrati avverso le proprie infrastrutture e nel contempo hanno costituito un organismo per le operazioni nella rete: il Comando interforze per le operazioni cibernetiche (CIOC).

Rispetto alla serietà e gravità degli scenari che emergono nelle analisi internazionali e nazionali, la riflessione sul tema appare in Italia ancora troppo circoscritta all'ambito specialistico. È necessario invece che la consapevolezza di tali scenari si diffonda nella società, in modo che questa abbia chiara cognizione dell'evoluzione delle prospettive di rischio.

La Commissione Difesa della Camera dei deputati ha deliberato lo svolgimento dell'indagine conoscitiva appunto per approfondire la conoscenza delle questioni accennate. L'indagine si è incentrata sugli specifici profili di interesse della Commissione, fermo restando che – per far emergere più chiaramente il ruolo che le Forze armate svolgono oggi e che dovranno svolgere in futuro in questo campo – essa ha dovuto fare luce anche sul ruolo svolto dagli altri soggetti che operano nel complessivo sistema di protezione dello spazio cibernetico nazionale, acquisendo il contributo di conoscenza, di inquadramento concettuale, di informazione e di esperienza di soggetti istituzionali che, pur esterni al sistema della difesa in senso stretto, operano comunque in campi di attività riconducili al tema di cui si parla.

L'attività di indagine si è articolata principalmente in audizioni di soggetti competenti e qualificati rispetto al tema. In particolare, la Commissione ha audito il Capo di stato maggiore della difesa, generale Claudio Graziano (25 gennaio 2017); il Consigliere militare del Presidente del Consiglio dei ministri, generale di divisione Carmine Masiello (27 luglio 2016); il Capo del VI Reparto Sistemi C4I e Trasformazione dello stato maggiore della difesa, ammiraglio di divisione Ruggero Di Biase (9 marzo 2016); il Comandante del Centro Intelligence Interforze, nonché Capo del Nucleo iniziale di formazione dell'allora costituendo Comando interforze per le operazioni cibernetiche (CIOC), generale di brigata aerea Giandomenico Taricco (9 marzo 2016); il Direttore generale dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM), nella sua qualità di Responsabile del CERT Nazionale, Rita Forsi (7 giugno 2016); il Direttore generale dell'Agenzia per l'Italia digitale, Antonio Samaritani (15 giugno 2016), unitamente al dirigente responsabile del CERT Pubblica Amministrazione (operante presso l'Agenzia), Mario Terranova (15 giugno 2016); nonché alcuni esperti, e segnatamente Roberto Baldoni (Direttore del Centro di ricerca Sapienza in *cyber intelligence e information security*) (9 febbraio 2016), Stefano Silvestri (*Past President* e membro del comitato direttivo dell'Istituto affari internazionali (IAI)) (16 febbraio 2016), Tommaso De Zan (Assistente alla ricerca nell'area sicurezza e difesa dello stesso IAI) (16 febbraio 2016), Alessandro Politi (Direttore della NATO Defense College Foundation) (8 marzo 2016), Andrea Margelletti (Presidente del Centro Studi Internazionali (CeSI)) (28 aprile 2016) e Stefano Mele (esperto in diritto delle tecnologie, privacy e sicurezza delle informazioni, consulente in materia di *cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare*) (28 aprile 2016).

Quanto alle imprese attive nel settore, la Commissione ha rinunciato alle loro audizioni, sebbene previste dal programma dell'indagine, in considerazione della difficoltà di selezionare un numero contenuto di soggetti da ascoltare. La Commissione ha dunque preferito invitare quelle

aziende che avevano manifestato la volontà di rappresentare la propria esperienza a trasmettere una relazione scritta sui temi oggetto dell'indagine. All'invito hanno risposto con propri contributi, che sono stati acquisiti agli atti dell'indagine, Leonardo Spa e Hewlett Packard Enterprise.

La Commissione ha inoltre effettuato attraverso proprie delegazioni tre missioni di studio per visitare le sedi del Comando C4 Difesa e del Centro Intelligence Interforze (CII), a Roma, nonché del Security Operation Center (SOC) di Leonardo Spa, a Chieti.

Essenziale complemento dell'indagine conoscitiva, ancorché formalmente non comprese nel suo programma in quanto svolte congiuntamente con la Commissione Affari costituzionali, sono state le audizioni del Presidente dell'autorità Garante per la protezione dei dati personali, Antonello Soro (7 marzo 2017), e del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS), prefetto Alessandro Pansa (14 giugno 2017).

L'audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) ha segnato un momento di approfondimento di particolare rilievo in quanto si è trattato dell'unica audizione svolta dopo la pubblicazione (avvenuta sulla Gazzetta Ufficiale del 13 aprile 2017) del decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, che ha rivisto gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali dettati dal precedente decreto 24 gennaio 2013, riformando in modo significativo l'architettura istituzionale nazionale di sicurezza e difesa nello spazio cibernetico.

2. LA MINACCIA NELLO SPAZIO CIBERNETICO

Lo spazio cibernetico è la dimensione globale nella quale opera ormai tutta l'economia avanzata. Non c'è settore economico che non si stia spostando sulla rete. Il movente è l'enorme incremento di efficienza e produttività. La tecnologia internet provider (IP), basata su internet, ha fruttato alle aziende al contempo fortissime contrazioni dei costi di produzione e allargamento dei mercati. È facilmente prevedibile che il dominio dell'informatica nelle attività economiche si rafforzerà nel futuro e che le società che non sapranno trasformare le proprie economie al passo con questa rivoluzione saranno destinate a restare isolate, emarginate dal mondo più industrializzato, e a diventare "il terzo mondo del terzo millennio". Se l'Italia non si terrà al passo con la rivoluzione informatica inevitabilmente andrà incontro a un processo di deindustrializzazione e a una fuga di aziende e di cervelli. La costruzione dello spazio cibernetico – cioè dell'infrastruttura che permette a cittadini, imprese, enti pubblici, organizzazioni private, di agire (azionando dispositivi e macchine) e di interagire a distanza mediante la tecnologia informatica – deve essere quindi considerata una delle massime priorità strategiche del sistema Paese.

Costruire lo spazio cibernetico nazionale non è tuttavia sufficiente. È essenziale proteggerlo dall'incursione di terzi malintenzionati, per impedire che diventi una terra di nessuno dove è difficile imporre il rispetto della legge e dei valori costitutivi dello stato di diritto. Oggi lo spazio cibernetico è un mare reso pericoloso dalla pirateria. Il 2004 è stato, sotto quest'aspetto, l'anno di svolta. Prima di allora la pirateria informatica consisteva soprattutto in uno sfoggio di abilità fine a se stesso da parte di esperti che non miravano al profitto; negli anni seguenti si è assistito invece a una crescita esponenziale di azioni malevole per scopi criminali, di lotta politica, di posizionamento geostrategico.

La rivoluzione informatica ha permesso all'economia e alla società in generale, di beneficiare di vantaggi straordinari in termini di aumento della produttività del lavoro umano e di allargamento della rete di comunicazione, ma nel contempo le ha anche esposte a rischi del tutto nuovi e peculiari, a cominciare dal rischio di intrusione e manipolazione da parte di terzi, ossia di soggetti diversi dal legittimo proprietario e principale utilizzatore di un'infrastruttura o di una macchina. Il rischio nasce dal fatto che la tecnologia in questione presenta inevitabilmente delle "vulnerabilità": metaforicamente possono essere immaginate come "porte" che consentono a estranei di penetrare all'interno dei nostri sistemi informatici, valicando le "mura" di difesa che abbiamo eretto per assicurarcene l'uso esclusivo, e di prenderne il comando (se sono o servono

macchine) o di conoscerne e modificarne il contenuto (se sono documenti o memorie di dati). Le vulnerabilità non sono note o riconoscibili in anticipo, anche perché chi concepisce la macchina o l'infrastruttura non si cura principalmente di proteggerla dall'intromissione di terzi. Non può nemmeno escludersi che "porte" di questo tipo vengano applicate intenzionalmente, di nascosto all'acquirente, dal produttore di un *software* o di un componente *hardware* impiegati nella fabbricazione del prodotto finito. Di qui il problema strategico della sicurezza degli approvvigionamenti.

La protezione del proprio spazio cibernetico (la cyber-sicurezza) è essenziale per un Paese e deve procedere di pari passo con la costruzione di quello spazio. Nessuno, infatti, è immune dal rischio. Sfruttando i dispositivi con collegamento in rete – sempre più diffusi anche nelle case (dai televisori di ultima generazione a certi giocattoli per bambini, passando per le telecamere di sorveglianza attivabili da remoto) – è possibile a terzi ostili non solo spiare quel che avviene nello spazio privato domestico o lavorativo, ma anche prendere il controllo di dispositivi e macchinari altrui, dirottandone l'azione, visionare dati riservati (telefonici, di posta elettronica, etc.) oppure distruggere memorie o sequestrarle a scopo di ricatto (rendendole indisponibili al legittimo titolare). Non è indispensabile che un dispositivo sia connesso a internet. È sufficiente che utilizzi una tecnologia IP: così un computer portatile scollegato dalla rete è attaccabile se viene connesso a una memoria esterna (*memory stick*) o a un'interfaccia USB (*Universal Serial Bus*) che sia stata a sua volta "infettata" da software maligno, magari all'insaputa del proprietario, dopo essere stata collegata a una rete. In generale, con l'espansione della cosiddetta "internet delle cose", nello scenario di un futuro prossimo nel quale sempre più oggetti di uso comune saranno interconnessi, il livello di esposizione alla minaccia cresce a dismisura.

La minaccia proveniente dallo spazio cibernetico può riguardare infrastrutture critiche vitali di un Paese (trasporti, energia, sanità, etc.). In generale, la stessa stabilità e sicurezza di un Paese possono essere gravemente pregiudicate da attacchi malevoli nello spazio cibernetico che colpiscano gangli o procedimenti vitali dell'amministrazione o della vita democratica: si pensi a cosa accadrebbe in caso di manipolazione di anagrafi elettorali interamente informatizzate o di programmi *software* di elaborazione dei risultati elettorali comunicati dai seggi al Ministero dell'interno. In generale, si pensi a cosa comporterebbe in termini di ordine pubblico la distruzione o perfino l'alterazione profonda ma impercettibile delle memorie giuridiche custodite nelle banche dati di amministrazioni pubbliche e private (anagrafi, catasti, banche, casellari giudiziari, etc.).

Tra le infrastrutture strategiche va compreso il sistema delle comunicazioni private (via *mail*, telefono, *network* di relazioni sociali) e dell'informazione, che sono vitali per la formazione delle opinioni individuali e dell'opinione pubblica, le quali a loro volta sono il motore dei comportamenti individuali, compresi quelli che stanno al cuore di una società democratica: le scelte elettorali. La diffusione di notizie o documenti riservati se non addirittura classificati carpiti e divulgati da pirati informatici (magari al soldo di potenze straniere ostili) può interferire nella vita pubblica di un Paese, in ipotesi anche alterando il risultato di competizioni elettorali. Effetti simili potrebbe avere in teoria il sistematico inquinamento dei siti di informazione pubblica o di relazioni sociali (tipo Facebook) attraverso l'immissione di fandonie, notizie false e tendenziose (*fake news*). Basti pensare alle sospettate interferenze di Paesi stranieri nello spazio dei media di relazione sociale attraverso la diffusione a pioggia di notizie false concepite ad arte per condizionare i votanti verso determinate scelte di voto oppure alle notizie classificate carpite e poi divulgate da pirati informatici dietro ai quali potrebbero nascondersi centri di *intelligence* di Paesi ostili. Oppure si pensi alle potenzialità del cosiddetto dossieraggio: è oggi tecnicamente possibile perlustrare la rete internet per rinvenirvi in modo sistematico ogni informazione disponibile su una data persona, così da creare un profilo individuale in cui la conoscenza di ogni dettaglio illumina quella degli altri. L'operazione è possibile anche su scala nazionale. È cioè possibile delineare il profilo di ogni cittadino di un intero Paese. Farlo per 56 milioni di italiani – come emerso dall'indagine conoscitiva – non sarebbe un problema. Non servirebbe né grande capacità computazionale, né uno *storage* particolare.

A parte i disservizi, l'aggressione cibernetica è atta a provocare danni materiali paragonabili a quelli di guerra, mediante il sabotaggio a distanza di macchine e dispositivi (centrali elettriche, nucleari, dighe, torri di controllo aeroportuali, sistemi di navigazione aerea, nonché fabbriche altamente automatizzate, che impieghino robot interconnessi, etc.). Attacchi ad assetti critici nazionali possono produrre danni materiali ad esempio attraverso la paralisi o l'alterazione di sistemi che regolano il trasporto civile o le reti energetiche o dei sistemi di comando e controllo militari. Un esempio in tal senso è il *malware* "Energetic Bear", che qualche anno fa colpì più di un migliaio di aziende statunitensi ed europee attive in campo energetico con l'obiettivo di compromettere il corretto funzionamento di centrali elettriche, reti di distribuzione del gas e turbine eoliche. L'attacco fu portato attraverso l'intrusione da remoto nei sistemi di controllo industriale (ICS).

Ciò significa che, dal punto di vista militare, la tecnologia ITC (*Information and Communications Technology*), potendo essere utilizzata per scopi offensivi assimilabili a quelli dell'attacco armato convenzionale, deve essere guardata come una possibile arma. Occorre in altre parole cominciare a considerare le dinamiche del mondo cibernetico dal punto di vista militare. Una volta chiarito che è possibile usare la cibernetica come arma, si pongono per essa le stesse questioni che riguardano ogni altra tipologia di arma (carri armati, navi, aerei): servono regole di ingaggio per il suo utilizzo e cornici normative per stabilire chi, quando e come può decidere di impiegarla.

Anche quando non attacchi infrastrutture critiche, ma, per motivazioni di mero lucro criminale, punti su imprese e famiglie, l'aggressione cibernetica – se massiccia e sistematica – investe l'intero sistema Paese, assurgendo al grado di minaccia alla sicurezza nazionale. Senza protezione, le aziende sono esposte – oltre che a truffe e a ricatti, con conseguente aggravio dei costi d'impresa – a spionaggio industriale, che sfrutta le vulnerabilità dei sistemi informatici per sottrarre, spesso senza che l'attaccato ne abbia consapevolezza, il frutto del lavoro di ricerca aziendale. La singola impresa non può d'altra parte difendersi da sola. L'azienda che opera su internet entra in relazione con altri soggetti: clienti, fornitori, etc. Oltre un certo livello, le relazioni sono mediate dalle macchine, avvengono cioè da macchina a macchina, con la conseguenza che è sufficiente attaccare con successo una piccola società fornitrice per arrivare a colpire la società grande. Non solo singoli attacchi di massicce proporzioni ad aziende nazionali, ma anche plurimi e continui attacchi di piccola scala a cittadini e aziende di un Paese rappresentano un attacco al sistema Paese, in quanto ostacolano il passaggio e la trasformazione tecnologica dell'economia e spingono quanti vogliono innovare e rapportarsi ai mercati mondiali ad abbandonare il Paese o a non mettervi piede. La resilienza del sistema Paese può essere ottenuta solo con uno sforzo diffuso e congiunto. Come per i vaccini, la difesa della comunità passa attraverso l'immunizzazione dei singoli: in questo caso, attraverso la protezione delle famiglie, delle imprese, delle pubbliche amministrazioni e di tutti i soggetti attivi in rete. L'onere di trovare risposte alle sfide del ciberspazio non può ricadere sulle sole istituzioni pubbliche. Non può essere lo Stato a proteggere famiglie e imprese. Spetta però allo Stato rendere la popolazione consapevole del rischio, promuovere e stimolare l'adozione di comportamenti virtuosi di protezione cibernetica e istituire architetture istituzionali preposte. Se un Paese non protegge il suo spazio cibernetico anche privato è destinato a venire emarginato dal mercato del futuro.

È chiaro, quindi, che la protezione dello spazio cibernetico è presupposto indefettibile non solo della prosperità economica, ma più in generale dell'indipendenza non solo economica ma anche politica di un Paese. Che, come tale, deve essere considerata una priorità strategica assoluta del sistema Paese. Per questo non è immaginabile che la protezione dello spazio cibernetico sia affidata a privati o a stranieri. Discorso analogo può farsi per la produzione di *hardware* e *software*. Chi mette in sicurezza i sistemi informatici o li produce ha le chiavi di accesso a quei sistemi o a quei prodotti. La protezione dello spazio cibernetico nazionale è quindi una responsabilità necessariamente pubblica, che nessuno Stato può delegare. Non per nulla praticamente tutti i Paesi avanzati stanno portando avanti una strategia nazionale nel campo di sicurezza e difesa cibernetiche.

Lo spazio cibernetico rappresenta una sfida per gli Stati costituiti non solo perché essi stessi (la pubblica amministrazione e i servizi da essa erogati) possono essere fatti oggetto di attacchi per via cibernetica, ma anche perché gli Stati sono organizzazioni di comunità definite da uno spazio fisico, o meglio geografico, cioè il territorio, rispetto al quale lo spazio cibernetico si presenta come una dimensione "alternativa" con caratteristiche peculiari. Lo spazio cibernetico segna la "liquefazione della geopolitica". I confini tra gli Stati – che comunque sono stati sempre permeabili e che erano già stati depotenziati dall'avvento dell'aviazione – sono diventati linee immaginarie. La frontiera non è più barriera. I poteri emergenti e forti non sono statali. Lo spazio cibernetico consente in teoria la costituzione di poli di potere con più basi territoriali in Paesi diversi o con basi rapidamente trasferibili altrove e, quindi, in definitiva senza una base territoriale in senso tradizionale (organizzazioni terroristiche o criminali transnazionali). Un polo di potere siffatto sono le stesse grandi società multinazionali o transnazionali produttrici di sistemi informatici o fornitrici di servizi da cui un numero crescente di esseri umani e organizzazioni sono dipendenti. In quanto generato dalla rete dei dispositivi collegati e dalle strutture che rendono possibile il collegamento, lo spazio cibernetico, pur essendo un bene di interesse comune, non è un bene comune, la cui fruizione non possa essere preclusa. Anzi, è un bene soggetto al controllo di alcuni. Basti pensare che i collegamenti sono resi possibili da più infrastrutture materiali (cavi, infrastrutture telefoniche, satelliti, etc.) di proprietà di imprese private. La dipendenza dallo spazio cibernetico comporta quindi una dipendenza da chi possiede o controlla le infrastrutture che lo rendono possibile. È significativo che alcune grandi imprese stiano cercando di rendersi indipendenti con propri cavi e nodi.

Benché lo spazio cibernetico trascenda le frontiere nazionali e conseguentemente le sottoponga a pressioni distorsive, gli Stati hanno il dovere di tentare di svolgere un ruolo preminente per imporre in quello spazio le stesse regole di convivenza civile che nei secoli si sono affermate nello spazio fisico.

3. LA MINACCIA MILITARE

Come accennato, lo spazio cibernetico, in quanto dimensione dell'interazione umana, è fatalmente destinato a diventare anche il nuovo campo di battaglia e di competizione geopolitica dell'umanità. Prevedibilmente, le prossime guerre non saranno condotte soltanto con i tradizionali armamenti preposti all'offesa e alla difesa via terra, mare e aria, ma saranno probabilmente iniziate e – quantomeno – accompagnate da attacchi perpetrati attraverso lo spazio cibernetico, i quali sono suscettibili di infliggere al nemico danni gravissimi, con effetti sulla società che gli esperti considerano paragonabili a quelli di un conflitto combattuto con armi convenzionali. Gli attacchi cibernetici più sofisticati non solo sono potenzialmente in grado di danneggiare o paralizzare il funzionamento di gangli vitali dell'apparato statale e la fornitura di servizi essenziali ai cittadini, ma possono avere anche effetti potenzialmente distruttivi (soprattutto in prospettiva) se impiegati per indurre il malfunzionamento delle infrastrutture critiche (ad esempio reti di controllo del traffico aereo, dighe, impianti energetici, etc.), generando danni materiali ingenti e la potenziale perdita di vite umane. Non sorprende quindi che la pianificazione delle forze, pressoché ovunque nel mondo, prenda in considerazione la necessità d'assicurare un adeguato livello di ciberdifesa (*cyber-defence*) agli assetti critici nazionali. Attualmente diversi governi si sono dotati delle capacità necessarie per penetrare le reti nazionali degli altri Stati (in uso sia alle autorità pubbliche sia ai privati) a fini di spionaggio o per mappare i sistemi potenzialmente oggetto di un futuro attacco. È anzi concreto perfino il rischio che alcuni Paesi mobilitino la propria industria nazionale al fine di alterare componenti *hardware* da essa prodotte acquisendo così la capacità di superare in maniera pressoché irrilevabile ogni difesa posta in essere dall'utilizzatore dell'assetto finito.

In particolare – come rilevato dal Governo nella Relazione sulla politica dell'informazione per la sicurezza riferita al 2014 – soprattutto da quell'anno emerge come fenomeno evidente il massiccio utilizzo dello spazio cibernetico in contesti di confronto militare: circostanza, questa, che

ha contribuito a connotare la natura "ibrida" di alcuni conflitti. Il ricorso all'azione nel ciberspazio – in modo combinato con strumenti convenzionali e non (pressione economica ed energetica, uso delle informazioni, impiego di forze irregolari, etc.) – ha fatto registrare un livello di complessità, intensità e sofisticazione tale da ricondurre a questo dominio un ruolo determinante specie nell'ambito della conflittualità tra Stati. Particolarmente significativa si è rivelata la duplice modalità di utilizzo dell'ambiente cibernetico sia quale mezzo a supporto di una comunicazione rapida, efficace e praticamente senza limiti, sia come strumento per la conduzione di attacchi a sistemi e reti critiche complementare a quelli convenzionali e idoneo anzi a determinare un effetto di moltiplicazione della forza. Ciò ha contribuito alla creazione, in altri termini, di una "dimensione digitale" della geopolitica, caratterizzata da confini "liquidi", in cui si estrinsecano equilibri di potere non sempre coincidenti con quelli della sfera fisica e della conflittualità cinetica.

A fronte di ciò, rileva sempre la Relazione, è stata confermata la tendenza ad un polimorfismo della minaccia e ad una diluizione del profilo dell'attaccante: elementi, questi, tradottisi, da un lato, nell'operatività di una vasta gamma di attori con finalità ed obiettivi diversi, operanti singolarmente o nell'ambito di organizzazioni più o meno strutturate di natura sia statuale, sia privata che criminale e, dall'altro, nella difficoltà di classificare un insieme così eterogeneo di attori, attese le difficoltà di tracciare confini precisi tra le varie categorie di attaccanti. Un soggetto appartenente ad un gruppo terrorista, ad esempio, può agire come un *hacker* o un *cracker*, mentre un *insider* potrebbe operare su indicazioni di un attore istituzionale, quale un servizio d'intelligence estero.

Sempre più consistente è risultato l'impiego del ciberspazio quale terreno di confronto tra Stati. In tale ambito, alcuni eventi hanno contribuito ad avvalorare le conclusioni delle principali dottrine militari, secondo cui lo spazio cibernetico costituisce la dimensione degli attuali e dei futuri conflitti: gli attacchi ai sistemi informatici dell'Estonia nel 2007, le operazioni *cyber* nel corso della crisi russo-georgiana nel 2008, l'impiego di Stuxnet per rallentare il programma nucleare iraniano nel 2010 e gli episodi registrati nel 2014 nel contesto della crisi ucraina. Di rilievo, nell'ambito di quest'ultima, l'impiego ancor più strutturato del *cyber* sia come fattore di innesco della conflittualità, sia, soprattutto, come elemento complementare e potenziante delle operazioni militari convenzionali. Sotto tale profilo, emblematici sono stati gli attacchi DDoS e i *web defacement*, il danneggiamento fisico e tecnologico di reti di telecomunicazione e le tecniche di *information warfare*, finalizzate alla distorsione delle informazioni in vista dell'acquisizione di un vantaggio competitivo sull'avversario.

Come evidenziato dal Laboratorio Nazionale di Cyber Security del Consorzio Interuniversitario Nazionale per l'Informatica nel libro bianco intitolato "Il Futuro della Cyber Security in Italia" dell'ottobre 2015[1], «lo spazio cibernetico non è escluso dalle logiche geopolitiche e della competizione internazionale. Dal momento che include sia elementi digitali sia fisici – cavi, satelliti, *routers*, computer di amministrazioni pubbliche e privati – esso contiene elementi che hanno una collocazione geografica precisa e dati che hanno rilevanza economica, politica e strategica per la sicurezza nazionale. Le attività nello spazio cibernetico sono dunque influenzate dalla realtà delle vicende internazionali e viceversa».

«Gli ultimi sviluppi legati alla sicurezza nello spazio cibernetico – prosegue il documento citato – hanno infatti riportato i governi al centro dell'azione. Ne sono esempio la nuova strategia di *cybersecurity* degli Stati Uniti (2015) e l'intensificarsi del dialogo con l'UE, che si è dotata di una strategia per la *cybersecurity* per la prima volta nel 2013. A livello internazionale si susseguono inoltre iniziative formali e informali per la descrizione di definizioni e norme condivise, a fronte della presenza di numerosi attori e differenti contesti normativi e tecnologici che implicano importanti limitazioni in termini di *governance* mondiale. I rischi associati allo spazio cibernetico sono di diversa natura, legati alle relazioni internazionali fra Stati e alla presenza di attori non

[1] Laboratorio Nazionale di Cyber Security - Consorzio Interuniversitario Nazionale per l'Informatica, *Il Futuro della Cyber Security in Italia. Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni*, a cura di R. Baldoni – R. De Nicola, ottobre 2015.

statuali. Alcuni Stati dispongono già da tempo di unità offensive e difensive per la *cyber-war*, dirette a infrastrutture economiche e civili, oltre che militari, anche se la realtà suggerisce che si tratta di uno scenario ancora remoto. È però vero che situazioni di confronto, o conflitto, fra Stati rendono oggi meno impossibili, seppur improbabili, atti di *cyber-war*, mentre rendono molto probabile un incremento dello scontro relativo al cyber-spionaggio a danno di apparati governativi, civili e militari, ma anche di imprese private. Attualmente, dunque, le minacce più probabili nello spazio cibernetico di uno stato provengono da attacchi di gruppi sostenuti o tollerati da governi e dallo spionaggio informatico di reparti di intelligence, che cercano di penetrare i sistemi informatici di Paesi esteri a fini politici, economici e militari. Anche l'utilizzo dello spazio cibernetico da parte di organizzazioni terroristiche è una possibile minaccia alla sicurezza nazionale, *in primis* per lo sfruttamento della rete a fini di propaganda, addestramento, autofinanziamento e pianificazione. La capacità di questi gruppi di rappresentare un pericolo reale alle infrastrutture critiche resta più limitata, ma destinata a crescere nel medio-lungo termine, anche a causa dell'aumento della loro competenza tecnica».

«Come e in che misura il diritto internazionale possa regolare la conflittualità fra Stati nel dominio cibernetico – si legge ancora nel citato libro bianco – e il problema dell'attribuzione degli attacchi informatici sono oggi tra i fattori che influenzano maggiormente la cooperazione internazionale fra Stati. A tal proposito, rimane una questione aperta se un attacco cibernetico costituisca o meno un attacco armato e in che misura si possa rispondere. Il "Tallinn Manual on the International Law Applicable to Cyber Warfare" (2013) – espressione di opinioni di un gruppo di esperti indipendenti senza valore vincolante – afferma che il diritto internazionale dei conflitti armati si applica alle operazioni cibernetiche. Durante il vertice NATO del settembre 2014, i Capi di Stato dei Paesi membri hanno avallato l'Enhanced Cyber Defence Policy, approvata il giugno precedente dai ministri della difesa dei paesi dell'Alleanza. Secondo la Policy, la NATO riconosce che il diritto internazionale si applichi al *cyberspace* e che la difesa dello spazio cibernetico sia inclusa nel compito fondamentale di difesa collettiva dell'Alleanza. Afferma, inoltre, che l'eventuale attivazione dell'articolo 5 in seguito ad un attacco cibernetico verrà decisa caso per caso. Una delle maggiori sfide relative alla *cyber-war* e al cyber-terrorismo resterà, nel breve-medio termine, l'assenza di un quadro giuridico certo e condiviso. Nonostante le iniziative internazionali volte alla descrizione di fattispecie e norme condivise, ad esempio sull'attribuzione della responsabilità legale, l'assenza di un quadro giuridico di riferimento certo continuerà a pesare sulla possibilità di *governance*. La collaborazione è rallentata dalla volontà di molti Stati di mantenere la massima libertà d'azione per le proprie attività di intelligence o per i propri attacchi cibernetici».

«Fin dalla sua creazione, – si legge sempre nel libro bianco – internet è stata intesa come un *ungoverned space*, ovvero un luogo non regolamentato dalle autorità politiche nazionali e internazionali. Inoltre, vista la sua conformazione "artificiale" e tecnologica, gran parte delle responsabilità oggettive ricadevano sulle iniziative intraprese da aziende private. Questa "libertà dallo Stato" ha prodotto i suoi effetti fino a quando il cyberspazio ha iniziato a espandersi e ha prodotto dinamiche geopolitiche. Attualmente, l'architettura della *governance* di internet è basata sull'*Internet Corporation for Assigned Names and Numbers* (ICANN) – con sede negli Stati Uniti – composta da un'associazione privata *multi-stakeholder*. Tale impostazione è stata messa in discussione da due principali eventi: le dinamiche geopolitiche che interessano l'odierno sistema internazionale tendenzialmente multipolare e, in secondo ordine, lo scandalo mediatico verificatosi dopo il cosiddetto "Snowden Leaks". Gli USA promettono di rivedere, in chiave più inclusiva, la politica decisionale in seno all'ICANN attraverso le dichiarazioni del Segretario del Dipartimento del Commercio Penny Pritzker, il quale ha dichiarato: "non permetteremo che la rete globale venga cooptata da singole persone, entità o Nazioni e che subentri la loro visione campanilistica. Il modello condiviso non è quindi in discussione, perché garantisce il maggiore potenziale sia per l'innovazione sia per l'inclusione". L'impostazione "americano-centrica" dell'ICANN viene, però, oggi messa in discussione da altri attori rilevanti come Russia e Cina, che puntano al ridimensionamento del ruolo di ICANN e spingono sulla necessità di un maggiore coinvolgimento

inclusivo internazionale e multipolare attraverso l'agenzia delle Nazioni Unite, l'*International Telecommunications Union* (ITU). A tal proposito, durante la Conferenza mondiale sulle telecomunicazioni internazionali, tenutasi a Dubai nel 2012, sono emerse posizioni contrastanti per il futuro del cyberspazio. L'ITU ha cercato di espandere la propria autorità su internet; gli operatori di TLC europei hanno voluto garantire più ricavi cambiando le regole per lo scambio di informazioni tra le reti; Cina, Russia e India hanno avanzato proprie idee relative alla diffusione di controlli governativi su internet; gli Stati Uniti e l'Europa hanno preferito appoggiare il modello *multi-stakeholder* di ICANN. Gli effetti di un passaggio della *governance* da parte di uno Stato-Nazione come gli Stati Uniti a un organismo che risponda direttamente alle Nazioni Unite, da un punto di vista strettamente strategico, provocherebbero uno spostamento del baricentro del potere decisionale a favore soprattutto dei Paesi che in seno al Consiglio di sicurezza delle Nazioni Unite hanno diritto di veto. La conseguenza potrebbe essere, nel medio-lungo periodo, una vera e propria "balcanizzazione" dove a prevalere sarebbero solo gli interessi particolari dei singoli Stati, piuttosto che l'interesse collettivo. È pur vero, come dimostrano gli ultimi avvenimenti internazionali, che l'attuale impostazione di internet, ma in larga misura anche del *cyberspace*, non può essere mantenuta come un luogo anarchico e caotico. A causa dell'intrinseca asimmetria, il dominio cibernetico si presta ad azioni che minano la "sicurezza nazionale" degli Stati, soprattutto se a utilizzare il *cyberspace* sono attori non statali (terroristi e/o la criminalità organizzata). Allo stesso tempo, l'elevata informatizzazione, interconnessione e interdipendenza, oltre a far emergere le *Information and Communications Technologies* (ICT) come il vero "centro di gravità" delle società industrializzate, ha portato anche all'*escalation* del confronto tra gli Stati il quale si concentra sempre di più sull'utilizzo dei sistemi informatici piuttosto che sugli armamenti convenzionali».

4. IL QUADRO NORMATIVO

Nello svolgimento dell'indagine conoscitiva, l'ampia e qualificata platea degli esperti ascoltati dalla Commissione si è lungamente soffermata sul quadro normativo nazionale in tema di difesa cibernetica, evidenziandone i punti di forza e gli elementi di criticità.

L'attenzione degli esperti si è in particolar modo concentrata sull'insieme di quei provvedimenti – di carattere normativo e non – che, a partire dal decreto del Presidente del Consiglio dei ministri (DPCM) del 24 gennaio 2013, hanno contribuito a definire l'architettura istituzionale a protezione dello spazio cibernetico, chiarendo la distribuzione delle funzioni e dei compiti aventi rilievo per la sicurezza cibernetica tra i molteplici soggetti istituzionali competenti nelle diverse fasi della prevenzione e risposta ad eventi dannosi nello spazio cibernetico.

Molte delle considerazioni emerse nel corso delle audizioni, con particolare riferimento alla necessità di una più lineare e agevole catena di comando, hanno trovato risposta nel recente DPCM del 17 febbraio 2017, che, come si vedrà più diffusamente in seguito, reca i nuovi indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

In particolare, è stato sottolineato dal Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS), Alessandro Pansa, come il DPCM del febbraio 2017, anche alla luce dell'esperienza maturata negli anni successivi all'entrata in vigore del DPCM del 2013, semplifichi le procedure ordinarie e straordinarie di gestione delle attività di implementazione dell'architettura nazionale.

Se il recente intervento normativo è stato valutato positivamente in quanto da tempo auspicato a livello scientifico e dottrinale, d'altro canto il "monitoraggio" costante dell'assetto che regola la sicurezza cibernetica è stato considerato un elemento imprescindibile del buon funzionamento del complessivo sistema di sicurezza del Paese alla luce della straordinaria capacità di evoluzione della minaccia cibernetica e della conseguente necessità di disporre di aggiornati meccanismi di prevenzione e risposta.

4.1 Definizioni

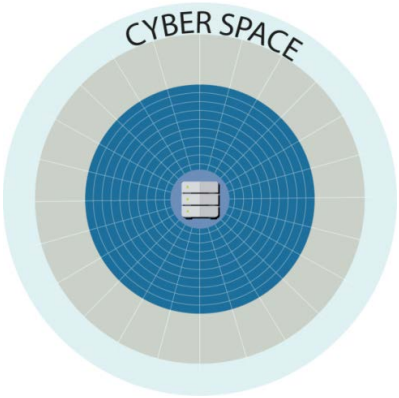
Sia il DPCM del 2013, sia il DPCM del 2017, sia, infine, i Documenti strategici che definiscono il quadro e il piano nazionale della sicurezza cibernetica recano una serie di definizioni concernenti i termini maggiormente utilizzati nel campo dell'*Information Communications Technology* (ICT) e della sicurezza cibernetica, facendo al riguardo riferimento alle espressioni impiegate in ambito internazionale ed europeo (ONU, NATO e UE).

Spazio cibernetico

Per quanto concerne, ad esempio, la definizione di "spazio cibernetico", a fronte di una pluralità di interpretazioni dottrinali il DPCM del 2017 chiarisce che per tale dominio si intende l'insieme delle infrastrutture informatiche interconnesse, comprensivo di *hardwar*e, *software*, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete.

Come si vedrà più diffusamente in seguito, la NATO, nel corso del vertice di Varsavia del luglio 2016, ha ufficialmente riconosciuto il cyberspazio come il quinto dominio operativo militare, dopo terra, aria, cielo e spazio, ovvero un nuovo "terreno" di operazioni nel cui ambito l'Alleanza dovrà essere in grado di difendersi nel modo più efficace, prestando particolare attenzione agli aspetti di difesa delle infrastrutture critiche.

Sicurezza cibernetica



A sua volta la sicurezza cibernetica viene definita dal medesimo Documento come la condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi.

Con riferimento al tema della sicurezza cibernetica, nel richiamato vertice di Varsavia del luglio 2016 la NATO ha sottolineato come ciascun membro dell'Alleanza dovrà essere in grado di individuare tempestivamente la minaccia cibernetica, rispondere prontamente all'offensiva, anche in contesti ibridi, e condividere le informazioni con gli altri Stati della NATO.

Minaccia cibernetica

Per minaccia cibernetica deve intendersi il complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanziano – in particolare – nelle azioni di singoli individui od organizzazioni, statali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a controllare indebitamente, danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi.

Gli attacchi cibernetici – che possono originare da qualsiasi punto della rete globale – sono in grado di determinare rilevanti conseguenze anche sulle infrastrutture informatizzate critiche di interesse nazionale: sono quindi caratterizzati da forte asimmetria.

Infrastrutture informatizzate critiche di interesse nazionale

In particolare, il decreto del Ministero dell'interno 9 gennaio 2008 individua come infrastrutture informatizzate critiche di interesse nazionale i sistemi e i servizi informatici di supporto alle

funzioni istituzionali: dei ministeri, delle agenzie e degli enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute; della Banca d'Italia e delle autorità indipendenti; delle società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500 mila abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque; di ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti, autorità provinciali di pubblica sicurezza.

Tipologia di attacchi

Dal punto di vista della pericolosità gli attacchi vengono generalmente classificati secondo diversi livelli di gravità.

Un elenco esemplificativo era già contenuto nella Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico approvata dal Comitato parlamentare per la sicurezza della Repubblica (Copasir) in data 7 luglio 2010. Il Documento menziona un'ampia gamma di tipologie che spaziano dalle minacce poste in essere da organizzazioni criminali nazionali o transnazionali – le quali sfruttano lo spazio cibernetico per reati quali la truffa, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali (*cyber crime)* – alla vera e propria guerra cibernetica, di sovente descritta come il quinto settore dell'attività militare accanto ai tradizionali domini di terra, mare, cielo e spazio (*cyber war)*.

A loro volta gli attori che possono avvalersi dello strumento informatico per azioni ostili vanno dal singolo *hacker* individuale, che agisce a scopo di lucro, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici, come nel caso degli attacchi informatici verso l'Estonia nel 2007, passando per la criminalità organizzata e i gruppi terroristici (cyber-terrorismo). Questi ultimi, ad esempio, usano il cyber-spazio per tutto lo spettro delle loro attività, dal reclutamento al finanziamento, alla propaganda e, in misura sempre maggiore, anche l'attacco informatico vero e proprio teso a procurare un danno all'avversario[2].

Infine, in crescente aumento sono le condotte illegali volte a sfruttare le potenzialità della rete per sottrarre segreti industriali a fini di concorrenza sleale (nel mercato dei brevetti civili) o di superiorità strategica (nel caso di sottrazione di disegni e apparecchiature militari o *dual-use*: cosiddetto *cyber espionage)*.

Nel corso dell'indagine conoscitiva l'attenzione della Commissione si è focalizzata prevalentemente sul tema della guerra cibernetica, fenomeno che ha assunto un rilievo sempre maggiore a seguito dell'intensificarsi di eventi cibernetici riconducibili a questa categoria e allo sviluppo da parte di molti Paesi particolarmente avanzati da un punto di vista tecnologico di specifiche capacità operative nel dominio cibernetico.

In particolare, attraverso le audizioni dei più alti rappresentanti della catena di comando militare e lo svolgimento di qualificate missioni, sono stati acquisiti importanti elementi conoscitivi in relazione alle più recenti misure di difesa cibernetica in via di implementazione a livello nazionale, con particolare riferimento alle iniziative che attengono alla realizzazione di uno specifico comando

[2] Comitato parlamentare per la sicurezza della Repubblica, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico,* Doc. XXXIV, n. 4, pag. 13. La Relazione è consultabile al seguente link: https://www.senato.it/service/PDF/PDFServer/BGT/525461.pdf.

interforze per le operazioni cibernetiche e allo sviluppo della capacità di condurre operazioni militari cibernetiche nel dominio digitale.
Da un punto di vista giuridico sono state passate in rassegna una serie di problematiche connesse all'applicabilità all'attacco cibernetico delle vigenti categorie del diritto internazionale, con particolare riferimento al concetto stesso di "aggressione". In tale ambito si è analizzata la più recente posizione della NATO in materia di *cyber defence*, con specifico riferimento alle conclusioni del vertice di Varsavia del luglio 2016, nel corso del quale "Gli attacchi informatici" sono stati considerati come "una sfida chiara alla sicurezza dell'Alleanza e (…) un pericolo per la società moderna, al pari di un attacco convenzionale".
Nel comunicato ufficiale rilasciato alla chiusura del vertice si sottolinea in particolare come la NATO continuerà ad implementare la propria politica di *cyber defence* "con l'intento di rafforzare le capacità dell'Alleanza, beneficiando di tecnologie all'avanguardia" e rafforzando la cooperazione con l'Unione europea che, tra l'altro, ha di recente approvato la nuova direttiva per la sicurezza delle reti e dell'informazione (Direttiva Network and Information Security, meglio nota con l'acronimo NIS).

4.2 Evoluzione della normativa nazionale: i primi interventi a tutela della sicurezza cibernetica

Il panorama giuridico italiano in materia di difesa e sicurezza dello spazio cibernetico è rappresentato da una serie di provvedimenti normativi che, a partire dai primi anni novanta, sono stati adottati al fine di mettere in sicurezza questo nuovo dominio operativo.

A fronte di una prima normativa di carattere penale, finalizzata a disciplinare nuove forme di reato connesse all'utilizzo illegale della rete, sono successivamente intervenuti specifici provvedimenti volti a rafforzare la riservatezza delle informazioni digitali e l'integrità delle infrastrutture critiche nazionali informatizzate.

In particolare, nella direttiva del Presidente del Consiglio dei ministri del 16 gennaio 2002 sulla *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni* le informazioni gestite dai sistemi informativi pubblici sono rappresentate come "una risorsa di valore strategico per il governo del Paese" che deve essere efficacemente protetta e tutelata "al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse". La direttiva raccomanda, pertanto, a tutte le pubbliche amministrazioni l'avvio immediato di alcune iniziative finalizzate al conseguimento di un primo importante risultato di allineamento ad una "base minima di sicurezza" delle informazioni gestite dalle pubbliche amministrazioni.

Nel 2003 vengono a loro volta adottati il codice in materia di protezione dei dati personali ed il codice delle comunicazioni elettroniche, quest'ultimo volto a garantire i diritti inderogabili di libertà delle persone nell'uso dei mezzi di comunicazione elettronica, nonché il diritto di iniziativa economica ed il suo esercizio in regime di concorrenza nel settore delle comunicazioni elettroniche. Ai sensi dell'articolo 3 di questo codice, qualunque limitazione al fondamentale diritto di libertà "può essere imposto soltanto se appropriato, proporzionato e necessario nel contesto di una società democratica e la sua attuazione deve essere oggetto di adeguate garanzie procedurali conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ai principi generali del diritto dell'Unione europea, inclusi un'efficace tutela giurisdizionale e un giusto processo".

Successivamente, nel 2006, è entrato in vigore il codice dell'amministrazione digitale (decreto legislativo n. 82 del 2005), successivamente novellato dal decreto legislativo n. 179 del 2016 anche al fine di istituire e disciplinare l'Agenzia per l'Italia digitale (AgID), nuovo organismo con il compito di promuovere l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione e nel rapporto tra questa, i cittadini e le imprese.

In sintesi, si può rilevare che anche prima dell'entrata in vigore del DPCM del 24 gennaio 2013, che per primo ha delineato – da un punto di vista normativo complessivo – l'assetto istituzionale preposto alla protezione cibernetica, sono stati varati in Italia diversi provvedimenti

volti a garantire un più elevato livello di sicurezza informatica e delle telecomunicazioni e, quindi, delle informazioni e dei servizi resi attraverso i sistemi di interconnessione della rete.

Allo stesso tempo è emersa la necessità di accrescere le capacità di messa in sicurezza dello spazio cibernetico anche attraverso la definizione di un quadro strategico nazionale in grado di specificare i compiti e le attività delle diverse componenti istituzionali chiamate ad operare in questo ambito della sicurezza nazionale sempre più connotato dall'intensificarsi della minaccia cibernetica e dalla complessità di questa nuova fonte di attacco.

4.3. Il DPCM del 24 gennaio del 2013

Nel gennaio del 2013 il Governo Monti, anche sulla base di analoghe iniziative intraprese a livello europeo ed internazionale, ha adottato il DPCM del 24 gennaio del 2013, che, fino all'entrata in vigore del successivo DPCM del 17 febbraio 2017, ha definito l'architettura istituzionale "deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali".

Nel dicembre del medesimo anno, in attuazione di un'espressa disposizione contenuta nel DPCM del 2013, sono stati approvati il *Quadro Strategico nazionale per la sicurezza dello spazio cibernetico* e il *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*.

Nell'insieme questi documenti individuano, per la prima volta in maniera organica, i compiti affidati a ciascuna componente istituzionale, con competenze nel settore della sicurezza e della difesa cibernetica, ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.

Nel corso delle audizioni svolte nell'ambito dell'indagine conoscitiva, l'ampia platea degli esperti ha illustrato nel dettaglio la catena di comando delineata nel DPCM del 2013, offrendo altresì una serie di elementi di riflessione in merito a possibili miglioramenti in un'ottica di maggiore efficienza dei meccanismi di risposta.

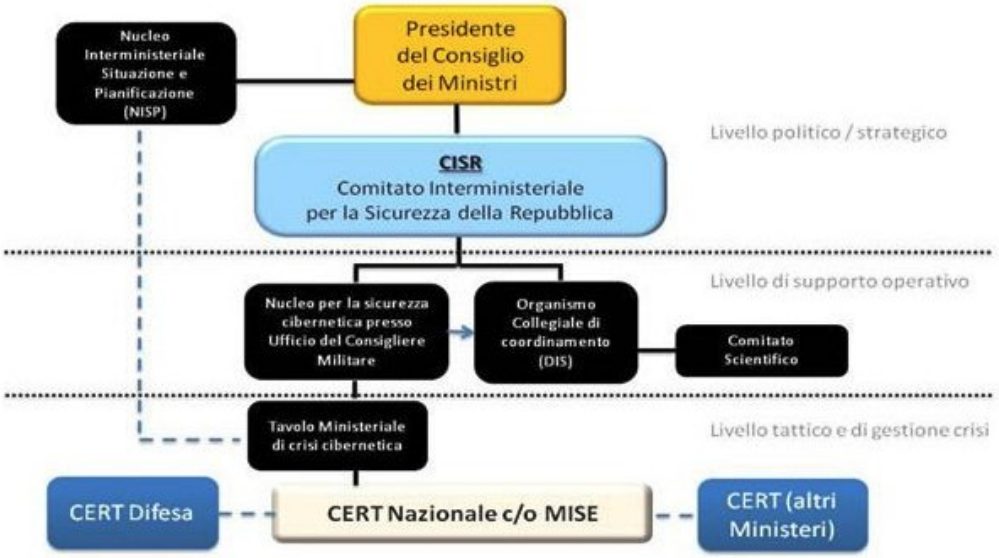
Nello specifico, il sistema delineato dal DPCM del 24 gennaio 2013 pone al vertice del potere decisionale il Presidente del Consiglio dei ministri e i Ministri facenti parte del Comitato interministeriale per la sicurezza della Repubblica (CISR), a cui sono demandati i compiti di indirizzo politico-strategico. Ad essi, infatti, spetta la definizione della strategia nazionale di *cyber-security*, nonché l'emanazione delle conseguenti direttive d'indirizzo. A supporto del Comitato viene individuato un apposito organismo collegiale di coordinamento (articolo 5), presieduto dal Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS).

A supporto del Presidente del Consiglio dei ministri, per gli aspetti relativi alla prevenzione e all'approntamento rispetto a situazioni di crisi, il DPCM istituisce il Nucleo per la sicurezza cibernetica (NSC), costituito in via permanente presso l'Ufficio del Consigliere militare e da questi presieduto. Il Nucleo è altresì composto da un rappresentante rispettivamente del DIS, dell'AISE (Agenzia informazioni e sicurezza esterna), dell'AISI (Agenzia informazioni e sicurezza interna), del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale. Per gli aspetti relativi alla trattazione di informazioni classificate, il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

Il DPCM prevede, inoltre, l'istituzione – presso la Scuola di formazione del Sistema di Intelligence – di un comitato scientifico composto da esperti della materia, provenienti dalle università, dagli enti di ricerca, dalle pubbliche amministrazioni e dal settore privato. Al comitato scientifico è affidato il compito di predisporre ipotesi di intervento rivolte a migliorare gli *standard* ed i livelli di sicurezza dei sistemi e delle reti, nel quadro delle azioni finalizzate ad incrementare le condizioni di sicurezza dello spazio cibernetico d'interesse del Paese. Spetta, inoltre, al comitato assicurare ogni necessario contributo per lo svolgimento delle attività spettanti rispettivamente

all'organismo collegiale di coordinamento ed al Nucleo per la sicurezza cibernetica, nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi.

Nel sistema delineato dal DPCM del 24 gennaio 2013 un ruolo di rilevo viene assegnato agli operatori privati che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici. Ai sensi dell'articolo 11 del DPCM, tali soggetti sono tenuti a comunicare ogni significativa violazione della propria sicurezza o dell'integrità dei propri sistemi informatici al Nucleo per la sicurezza cibernetica e, se richiesto, agli organismi di informazione per la sicurezza e devono, altresì, adottare le misure di sicurezza e le migliori pratiche (*best practices*) eventualmente predisposte dall'organismo collegiale di coordinamento posto a supporto del CISR. Sono inoltre tenuti a riferire gli eventi rilevanti agli organismi di informazione per la sicurezza e a consentire ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza, nei casi previsti dalla legge n. 124 del 2007. Da ultimo, collaborano alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.



Fonte:
https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html

4.4 Il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la protezione cibernetica e la sicurezza informatica 2013

Con decreti del Presidente del Consiglio dei ministri del 27 gennaio 2014 sono stati adottati il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" ed il "Piano nazionale per la protezione cibernetica e la sicurezza informatica", in attuazione dell'articolo 3, comma 1, del decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013.

Nello specifico, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico, elaborato dal Tavolo Tecnico Cyber (TTC) – che opera presso il DIS e al quale partecipano i rappresentanti *cyber* del CISR (Affari esteri, Interno, Difesa, Giustizia, Economia e finanze, Sviluppo economico), dell'Agenzia per l'Italia Digitale e del Nucleo per la sicurezza cibernetica – delinea le linee strategiche nazionali nel medio-lungo periodo.

In particolare, il Quadro fornisce una panoramica delle principali minacce – dalla criminalità informatica allo sfruttamento delle tecnologie ICT per fini terroristici, dall'"hacktivismo" allo spionaggio cibernetico, dal sabotaggio per via informatica ai conflitti nella 5ª dimensione – e delle vulnerabilità sfruttate per la conduzione di attacchi nello spazio cibernetico.

Il documento, oltre a definire i ruoli e i compiti dei soggetti pubblici, individua strumenti e procedure per potenziare le capacità cibernetiche del Paese; gli indirizzi strategici che includono il miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali; il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese; l'incentivazione della cooperazione tra istituzioni e imprese nazionali; la promozione e diffusione della cultura della sicurezza cibernetica; il rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*; infine, il rafforzamento della cooperazione nazionale in materia di sicurezza cibernetica.

Per quanto riguarda, invece, gli obiettivi di medio periodo relativi al biennio 2014-2015, il Piano nazionale per la protezione cibernetica e la sicurezza informatica 2013 ha individuato una serie di indirizzi operativi tra i quali si evidenziano il potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare, il potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati, la promozione e diffusione della cultura della sicurezza informatica. Ulteriori ambiti settori d'interesse riguardano la formazione e l'addestramento, la cooperazione internazionale, il miglioramento dell'operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali, nonché l'implementazione di un sistema di *Information Risk Management* nazionale.

Come si vedrà in seguito, molti di questi settori di intervento sono menzionati anche nel più recente Piano nazionale per la protezione cibernetica adottato nel marzo del 2017.

4.5 Criticità emerse dall'indagine conoscitiva in relazione al quadro strategico del 2013

Le audizioni svolte antecedentemente all'entrata in vigore del nuovo DPCM del febbraio del 2017 hanno messo in evidenza una serie di criticità del sistema strategico delineato nel 2013 e la conseguente necessità di un più aggiornato quadro di riferimento in materia di protezione cibernetica.

D'altro canto la necessità di aggiornare periodicamente le linee strategiche del Paese nel campo della protezione cibernetica è stata messa in relazione all'estrema velocità di sviluppo della minaccia cibernetica e alla conseguente necessità che il Paese disponga di un sistema di risposta agli attacchi cibernetici altrettanto evoluto e al passo con le sfide in termini di sicurezza e difesa del Paese provenienti dallo spazio cibernetico.

In particolare, è stata sottolineata la necessità di una più chiara linea politica di responsabilità in materia di sicurezza cibernetica e di un più efficiente meccanismo di risoluzione delle crisi cibernetiche in seno al Nucleo per la sicurezza cibernetica (NSC), anche attraverso una sua riorganizzazione interna. È stata poi evidenziata la sovrapposizione di ruoli e di competenze degli attori pubblici nel rapporto con il settore privato, la necessità di disporre di maggiore operatività in termini quantitativi e qualitativi nelle attività quotidiane di prevenzione, gestione e contrasto della minaccia cibernetica a livello di *Computer Emergency Response Centers* (Certs), nonché l'esigenza di destinare al settore maggiori risorse.

Da più parti, inoltre, sono state evidenziate alcune importanti novità, anche di carattere legislativo, intervenute successivamente al 2013 che imponevano necessariamente una rivisitazione dei ruoli e delle competenze dei principali attori istituzionali.

In primo luogo, per quanto concerne le novità legislative, il decreto-legge n. 174 del 2015 ha profondamente inciso sulle competenze del CISR prevedendo che tale organismo possa essere convocato dal Presidente del Consiglio dei ministri, con funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale.

In secondo luogo, poi, come ricordato anche dal Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS), Alessandro Pansa, nel corso della sua audizione presso le Commissioni Affari costituzionali e Difesa, il recepimento della direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

(cosiddetta "direttiva NIS", ossia *Network and Information Security*), che deve avvenire nel prossimo anno, richiedeva "un nuovo sistema e un aumento fortissimo dei livelli di sicurezza delle reti e di sistemi informativi dei Paesi dell'Unione, a cui noi entro quella data ci dovremo adeguare".

Infine, la necessità di una revisione dell'architettura strategica in materia di sicurezza cibernetica è stata motivata anche alla luce della pubblicazione, nel 2015, a cura del Ministero della difesa, del Libro bianco per la sicurezza internazionale e la difesa, nel cui ambito la minaccia cibernetica riveste un ruolo importante nell'analisi delle diverse minacce che attengono alla stabilità interna e ed internazionale. A tal proposito, il documento prefigura lo sviluppo di specifiche capacità in materia di difesa cibernetica "al fine di preservare la sicurezza del Sistema Paese e di rafforzare la tenuta delle strutture politiche, economiche e sociali".

4.6 Il DPCM del 17 febbraio 2017

Nel febbraio 2017, nella fase conclusiva dell'indagine conoscitiva, il Governo Gentiloni ha emanato la nuova direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

Nel nuovo assetto strategico al Presidente del Consiglio dei ministri viene affidata l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza. In tale funzione, egli provvede anche al coordinamento delle politiche dell'informazione per la sicurezza, impartisce le direttive e, sentito il CISR, emana le disposizioni necessarie per l'organizzazione e il funzionamento del sistema di sicurezza cibernetica.

Il DPCM, nelle more del recepimento della direttiva NIS, rafforza, in particolare, il ruolo del CISR, che emanerà direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese e si avvarrà in questa attività del supporto del coordinamento interministeriale delle amministrazioni CISR tecnico e del DIS.

Nello specifico, con il nuovo DPCM è il direttore generale del DIS a dover adottare le iniziative idonee a definire le necessarie linee di azione per innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati e avanzati supporti tecnologici. Per la realizzazione di tali iniziative, "è previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore".

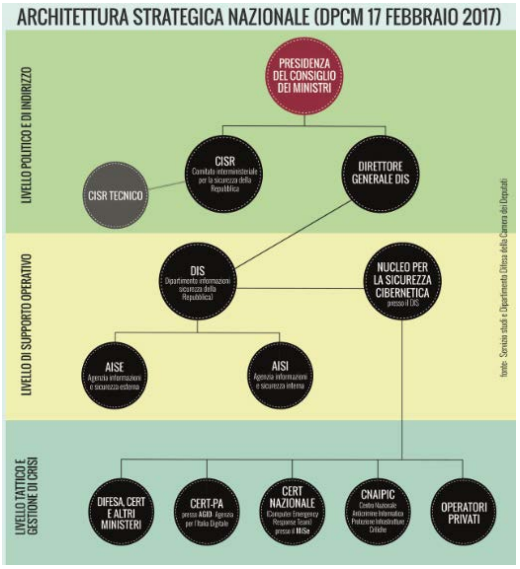
Sempre il Direttore del DIS è chiamato a predisporre gli opportuni moduli organizzativi, di coordinamento e di raccordo, prevedendo il ricorso anche a professionalità delle pubbliche amministrazioni, degli enti di ricerca pubblici e privati, delle università e di operatori economici privati.

Tra le novità c'è che il Nucleo per la sicurezza cibernetica (NSC), composto da rappresentanti dei ministeri principali, delle agenzie di intelligence, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale, viene ricondotto all'interno del DIS ed assicurerà la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale, in raccordo con tutte le strutture dei ministeri competenti in materia. Infatti, nel campo della prevenzione e della preparazione a eventuali situazioni di crisi cibernetica, spetta al Nucleo per la sicurezza cibernetica:

1. promuovere la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e curare l'elaborazione delle necessarie procedure di coordinamento interministeriale;
2. mantenere attiva, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica;
3. valutare e promuovere procedure di condivisione delle informazioni, anche con gli operatori privati interessati, al fine di diffondere gli allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

4. acquisire le comunicazioni circa i casi di violazione o di tentativo di violazione della sicurezza o di perdita dell'integrità dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), nonché dalle strutture del Ministero della difesa e dai CERT;
5. promuovere e coordinare, in raccordo con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale, per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica;
6. costituire il punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE e le altre organizzazioni internazionali e gli altri Stati – ferme restando le specifiche competenze del Ministero dello sviluppo economico, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa e delle altre amministrazioni interessate dalla normativa vigente – assicurando comunque in materia ogni necessario raccordo.

Nello specifico campo dell'attivazione delle azioni di risposta e ripristino rispetto a situazioni di crisi cibernetica, il Nucleo per la sicurezza cibernetica:



1. riceve, anche dall'estero, le segnalazioni di eventi cibernetici e dirama gli allarmi alle amministrazioni e agli operatori privati;
2. valuta se l'evento assuma dimensioni, intensità o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richieda l'assunzione di decisioni coordinate in sede interministeriale;
3. informa tempestivamente il Presidente del Consiglio dei ministri, per il tramite del Direttore generale del DIS, sulla situazione in atto.

Il Nucleo riferisce direttamente al direttore generale del DIS per la successiva informazione al Presidente del Consiglio dei ministri e al Comitato interministeriale per la sicurezza della Repubblica (CISR).

In sintesi, nel nuovo programma strategico, il Sistema delle informazioni per la sicurezza acquisisce un ruolo strategico sia nella fase di indirizzo tecnico sia in quella operativa.

A sua volta il CISR viene rafforzato anche alla luce di quanto già stabilito nella legge 11 dicembre 2015, n. 198. In particolare, al CISR viene assegnata la facoltà di emanare direttive al fine di innalzare il livello della sicurezza informatica del Paese, avvalendosi a tal fine del supporto del CISR Tecnico e del Dipartimento per le informazioni e la sicurezza (DIS). Viene meno sia il comitato scientifico, sia il cosiddetto NISP (Nucleo Interministeriale Situazione e Pianificazione), entrambe strutture tecniche precedentemente poste a supporto del CISR.

Lo spostamento del Nucleo per la sicurezza cibernetica dalla competenza dell'Ufficio del Consigliere militare di Palazzo Chigi a quella del Dipartimento delle informazioni per la sicurezza (DIS) sembra rispondere all'esigenza di una maggiore agilità della catena di comando e di un maggiore coordinamento con tutte le strutture istituzionali previste nel nuovo quadro strategico.

Infine è stato attribuito al Ministero dello sviluppo economico il compito di istituire un centro di valutazione e certificazione nazionale per la verifica dell'affidabilità della componentistica delle apparecchiature ICT che vengono utilizzate da parte della pubblica amministrazione nelle strutture critiche e nelle strutture strategiche ed è stato inoltre previsto l'accesso alle banche dati dei

soggetti privati e ai cosiddetti SOC *(Security Operation Center*) dal parte del DIS, in modo tale da poter avere una visione unitaria del sistema.

4.7 Il nuovo piano nazionale per la protezione cibernetica e la sicurezza informatica

In linea con quanto previsto dal DPCM del 17 febbraio 2017, nel marzo del 2017 il Governo ha adottato il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica. Il Piano rappresenta il documento operativo di breve periodo nel quale vengono individuate le priorità, gli obiettivi specifici e le linee d'azione per dare concreta attuazione a quanto descritto nel Quadro strategico.

Come evidenziato nel corso dell'audizione del Direttore generale del DIS, Alessandro Pansa, il nuovo piano non rappresenta "un mero aggiornamento del passato, ma è una nuova idea, una nuova formulazione del piano nazionale. (…) Questo piano ha redatto una *road map* attraverso la quale bisognerà portare avanti un processo che coinvolgerà tutti gli attori per il potenziamento e la reindirizzazione di tutti gli obiettivi e le iniziative che sono state portate avanti".

In particolare, sono indicati i seguenti undici indirizzi operativi:

1. potenziamento delle capacità di *intelligence*, di polizia e di difesa civile e militare;
2. potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;
3. promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento;
4. cooperazione internazionale ed esercitazioni;
5. operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*;
6. interventi legislativi e c*ompliance* con obblighi internazionali;
7. c*ompliance* a standard e protocolli di sicurezza;
8. supporto allo sviluppo industriale e tecnologico;
9. comunicazione strategica;
10. risorse;
11. implementazione di un sistema di *cyber risk management* nazionale.

4.8 Le relazioni presentate al Parlamento sul tema della sicurezza cibernetica

Da diversi anni il tema della sicurezza cibernetica costituisce oggetto di analisi nell'ambito delle relazioni sulla politica dell'informazione per la sicurezza inviate dal Governo (Presidenza del Consiglio dei ministri) al Parlamento ai sensi dell'articolo 38 della legge n. 124 del 2007.

Tale norma prevede che, entro il mese di febbraio di ogni anno, il Governo trasmetta al Parlamento una relazione scritta riferita all'anno precedente sulla politica dell'informazione per la sicurezza e sui risultati ottenuti. Alla relazione è allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica.

Già nella Relazione sulla politica dell'informazione per la sicurezza relativa all'anno 2009 la *cyber-security* veniva definita "un fondamentale campo di sfida per l'*intelligence* (…) un fattore di rischio di prima grandezza, direttamente proporzionale al grado di sviluppo raggiunto dalle tecnologie dell'informazione".

Questa prima analisi è stata seguita – nelle relazioni presentate al Parlamento negli anni successivi – da ulteriori riflessioni, che, a fronte di una costante intensificazione, hanno denunciato la minaccia cibernetica come: una "sfida crescente per le politiche di sicurezza degli Stati"; un "obiettivo informativo prioritario dell'attività d'*intelligence* nazionale"; "la sfida più impegnativa per il sistema Paese". In particolare, nella Relazione riferita all'anno 2012, la tesi secondo cui la minaccia cibernetica è "la sfida più impegnativa per il sistema Paese" viene motivata in considerazione "dei suoi peculiari tratti caratterizzanti che attengono tanto al dominio digitale nel quale viene condotta, quanto alla sua natura diffusa e transnazionale, quanto ancora agli effetti

potenziali in grado di produrre ricadute peggiori di quelle ipotizzabili a seguito di attacchi convenzionali e di incidere sull'esercizio di libertà essenziali per il sistema democratico".

A sua volta, nella Relazione relativa all'anno 2013, si dà conto del fatto che il monitoraggio informativo svolto in tale anno "ha consentito di rilevare come la concentrazione degli eventi cibernetici di maggior rilievo si sia tradotta in un significativo incremento di attività intrusive finalizzate all'acquisizione di informazioni sensibili e alla sottrazione di *know-how* pregiato. Ciò in danno del patrimonio informativo di enti governativi, militari, ambasciate, centri di ricerca, nonché di società operanti nei settori aerospaziale, della difesa e dell'energia, anche di fonte alternativa" .

Ancora, nella Relazione riferita all'anno 2014 si analizza l'evoluzione delle modalità operative e l'ampio spettro di finalità e attori, cui corrisponde un ventaglio altrettanto diversificato nelle tipologie di rischio per la sicurezza del sistema Paese: dagli attacchi alla sicurezza delle infrastrutture critiche nazionali allo spionaggio digitale, dall'hacktivismo contro obiettivi istituzionali al cyber-jihad.

Per quanto riguarda gli ultimi due anni, la Relazione riferita al 2016 ha evidenziato un costante *trend* di crescita dei fenomeni di minaccia collegati con il ciberspazio in termini di sofisticazione, pervasività e persistenza, a fronte di un livello non sempre adeguato di consapevolezza in merito ai rischi e di potenziamento dei presidi di sicurezza.

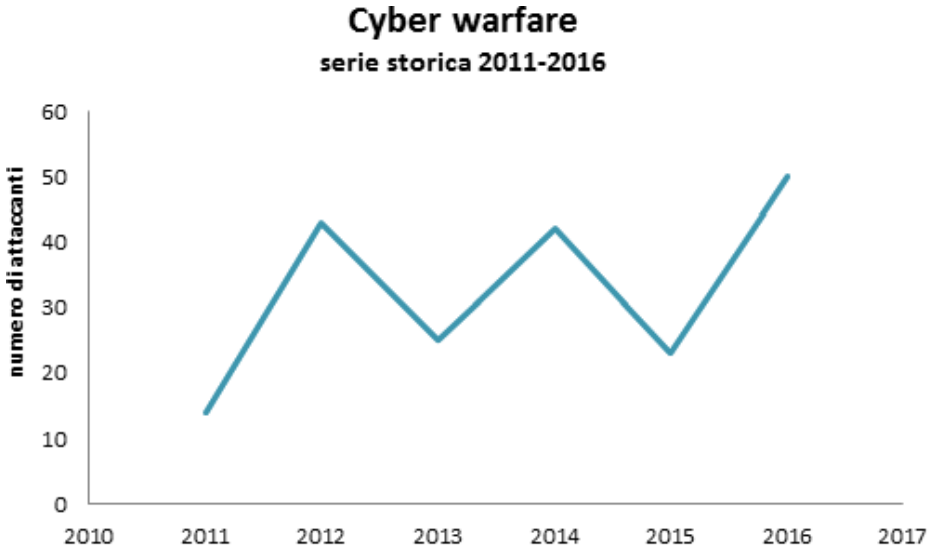
Se nel 2015 i principali settori oggetto di attacchi *cyber* risultavano quelli delle telecomunicazioni, dell'aerospazio, dell'energia e della difesa, nel 2016 figurano ai primi posti il settore bancario – con il 17 per cento delle minacce a soggetti privati (+14 per cento rispetto al 2015) – nonché le Agenzie di stampa e le testate giornalistiche che, insieme alle associazioni industriali, si attestano sull'11 per cento.

I soggetti pubblici costituiscono la maggioranza delle vittime degli attacchi *cyber* con il 71 per cento degli attacchi, mentre si attestano attorno al 27 per cento gli attacchi contro i soggetti privati. In entrambi i casi si registra un aumento pari, rispettivamente, al 2 per cento ed al 4 per cento. Un decremento del 6 per cento è stato viceversa osservato nell'ambito dei *target* non meglio identificati o diffusi (che costituiscono, complessivamente, il 2 per cento), solitamente oggetto di campagne hacktiviste.

4.9 Dati statistici acquisiti nel corso delle audizioni e dai più recenti documenti di analisi

La documentazione acquisita nel corso dell'indagine conoscitiva contiene una serie di dati significativi in relazione all'evoluzione delle diverse tipologie di attacco con particolare riferimento agli attacchi riconducibili al campo della *cyber-war*. Tali dati trovano conferma, oltre che nelle relazioni degli auditi, anche nel recente "Rapporto CLUSIT 2017" sulla sicurezza ICT.

Dai dati emerge che in termini assoluti il numero di attacchi più elevato degli ultimi 6 anni è riconducibile alle categorie del c*yber-crime* e della c*yber-war*.



Fonte: elaborazione da dati Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Nello specifico, nel 2016 si è registrato un aumento del 9,8 per cento degli attacchi compiuti per finalità *cyber-crime* e del 117 per cento degli attacchi di *cyber-war*, mentre rimangono sostanzialmente stabili, in lieve calo (dell'8 per cento), gli attacchi rientranti nel campo della *cyber-espionage*.

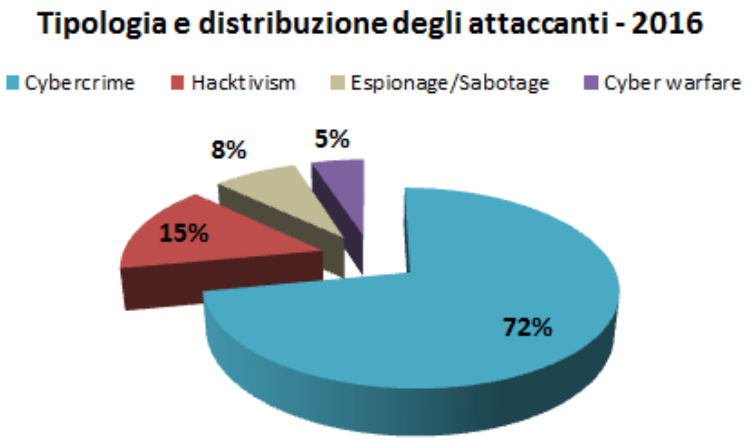
A questo proposito, nel rapporto CLUSIT 2017 si precisa che, "rispetto al passato, oggi risulta più difficile distinguere nettamente tra queste due ultime categorie: sommando gli attacchi di entrambe, nel 2016 si assiste ad un aumento del 16 per cento rispetto all'anno precedente (138 contro 119)".

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015
Cyber crime	170	633	609	526	684	751	9,80%
Hacktivism	114	368	451	236	209	161	-22,97%
Espionage / Sabotage	23	29	67	69	96	88	-8,33%
Cyber warfare	14	43	25	42	23	50	117,39%
TOTALE	**321**	**1.073**	**1.152**	**873**	**1.012**	**1.050**	**3,75%**

Fonte: elaborazione da dati Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Nel 2014 il *cyber-crime* si era confermato la prima causa di attacchi gravi a livello globale, attestandosi al 60 per cento dei casi analizzati (era il 36 per cento nel 2011). Nel 2015 tale percentuale era il 68 per cento, che sale al 72 per cento nel 2016, mostrando un *trend* inequivocabile.

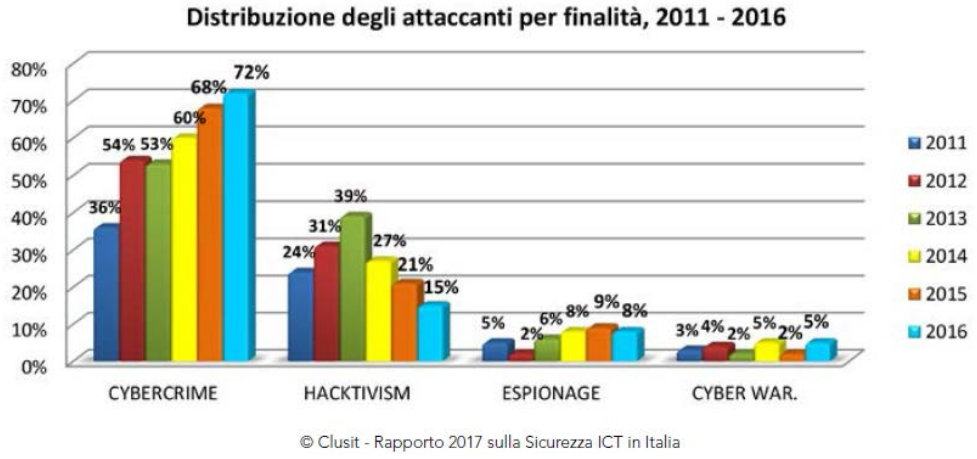
Il richiamato rapporto fa presente che nel quarto trimestre 2016 l'Italia si è collocata al quarto posto nel mondo per numero di utenti *online* complessivamente colpiti da attacchi di *cyber-crime* (29 per cento).



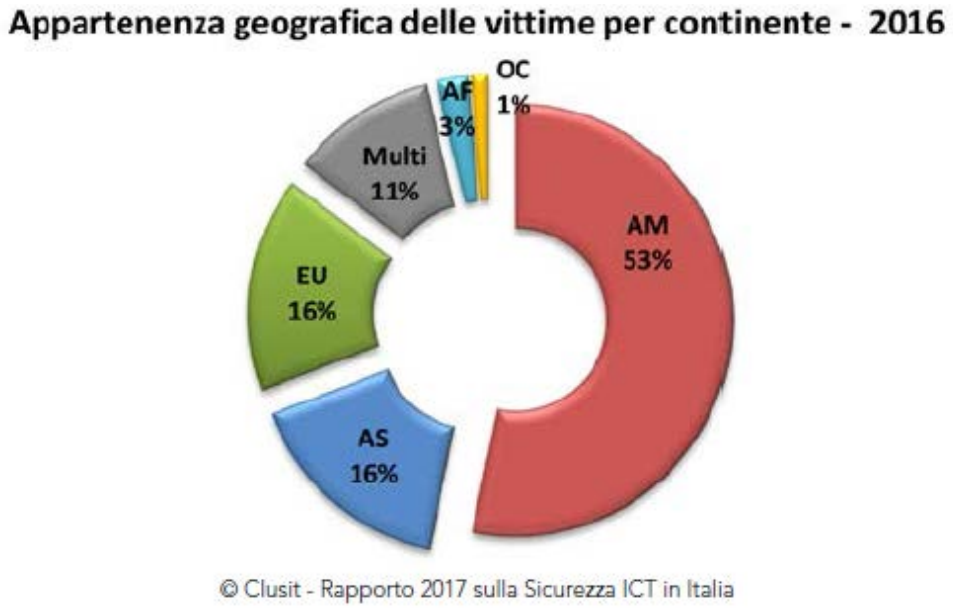
Fonte: elaborazione da dati Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Più nel dettaglio, gli attacchi di *cyber-crime* passano dal 68 per cento al 72 per cento del totale, mentre l'hacktivismo diminuisce di 23 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un sesto dei casi analizzati.

Per quanto riguarda le attività di *espionage*, rispetto alla percentuale degli attacchi gravi registrati nel 2015, la quota di attacchi nel 2016 è in lieve calo (dal 9 per cento all'8 per cento del totale), mentre l'*information warfare,* come precedentemente rilevato, risulta essere in forte crescita.



Sempre in base ai dati riportati nel rapporto CLUSIT 2017, diminuiscono leggermente nel secondo semestre del 2016, rispetto al primo semestre, le vittime di area americana (dal 55 per cento al 53 per cento), mentre crescono gli attacchi verso realtà basate in Europa (dal 13 per cento al 16 per cento) ed in Asia (dal 15 per cento al 16 per cento).



4.10 Iniziative a livello europeo in materia di sicurezza cibernetica

Tra le più recenti iniziative assunte a livello europeo per incidere sugli ordinamenti degli Stati membri si ricorda la direttiva 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cosiddetta "direttiva NIS"), che rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza informatica.

Attraverso l'adozione da parte dei singoli Stati membri di una serie di misure strategiche e organizzative comuni in materia di sicurezza cibernetica, la direttiva mira a raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni in ambito europeo, nella convinzione che il rafforzamento del dominio digitale rappresenti un importante volano di crescita del sistema economico dell'Unione, incidendo, positivamente sulla propensione ad investire degli operatori economici, con particolare riferimento al commercio internazionale.

La direttiva in esame prevede l'adozione di una serie di iniziative da parte degli Stati membri volte a migliorare le capacità di sicurezza cibernetica dei singoli Paesi, aumentare il livello di collaborazione in ambito europeo nella prevenzione delle minacce cibernetiche e nelle eventuali misure di risposta ad attacchi *cyber*, sviluppare una cultura della sicurezza con particolare riferimento a quei settori vitali per l'economia e la società e che si basano sulle tecnologie dell'informazione e della comunicazione.

Più nel dettaglio la direttiva NIS prevede:

- sul piano strategico: l'adozione di una strategia nazionale NIS, che contempli la fissazione di obiettivi e priorità, delinei l'architettura di governo (comprensiva di ruoli e responsabilità attribuite ai diversi soggetti), preveda programmi di sensibilizzazione (*awareness*), piani di ricerca e sviluppo, nonché renda operativo un piano di valutazione dei rischi;
- sul versante architetturale e operativo: l'istituzione di una (o più) Autorità nazionale NIS e di un punto unico di contatto nazionale per la ricezione delle notifiche di incidenti e la cooperazione per la loro risoluzione; la costituzione di uno o più *Computer Security Incident Response Teams* (CSIRTs), cui è – tra l'altro – attribuita la responsabilità della gestione degli incidenti e dei rischi, con specifico riferimento a quelli che dovessero interessare gli operatori di servizi essenziali, dovendo fornire loro supporto per la risoluzione degli incidenti di impatto significativo; specifici obblighi di sicurezza informatica per gli operatori di servizi essenziali (nei settori dell'energia, del trasporto,

bancario e finanziario, sanitario, idrico e delle infrastrutture digitali), nonché per i fornitori di servizi digitali (come i motori di ricerca *online*, i negozi *online*, i servizi di *cloud computing*).

5. LA MINACCIA CIBERNETICA NEL DIRITTO INTERNAZIONALE

Il diritto internazionale stabilisce in quali casi si può parlare di attacco di guerra contro uno Stato. L'identificazione giuridica di un atto come atto di guerra rileva naturalmente al fine dell'inquadramento giuridico delle possibili reazioni. Tuttavia, le norme del diritto internazionale sono state pensate per gli attacchi militari "tradizionali": quelli che si consumano nello spazio fisico (per terra, mare, aria), mediante armamenti convenzionali o cosiddetti non convenzionali (nucleari, *etc*.). Oggi però è possibile sferrare un attacco anche con carattere distruttivo (con morti, feriti e danni materiali ingenti) agendo soltanto nello spazio cibernetico, mediante un utilizzo ostile della tecnologia informatica. La potenza distruttiva della tecnologia informatica è tale che si può ormai parlare di arma cibernetica e di *cyber* guerra (*cyber-war, cyber-warfare*). Dal punto di vista strategico, è possibile che l'arma cibernetica sarà in futuro usata in combinazione con l'arma tradizionale, per esempio come "facilitatore di attacchi cinetici attraverso i domini tradizionali di aria, terra, mare e spazio". Diversi Governi (USA, Cina, Australia, Regno unito, Danimarca) prevedono nei propri documenti strategici il rafforzamento non più soltanto della difesa cibernetica (*active cyber-defence*), ma apertamente dello sviluppo di capacità offensive nel ciberspazio (*offensive cyber-operations*). Diventa quindi urgente – come è emerso in particolare dall'audizione dell'avvocato Stefano Mele, da cui sono tratte le considerazioni svolte in questo capitolo – capire quanto facilmente le norme vigenti di diritto internazionale in materia di guerra possano essere estese alla fattispecie della *cyber* guerra. La questione più delicata è se, quando e in che forma sia legittima – secondo il diritto internazionale – la reazione di uno Stato a un attacco cibernetico.

Secondo quanto emerso, la clausola Martens, comparsa nella IV Convenzione dell'Aia e poi ripresa nelle quattro convenzioni di Ginevra del 1949, già ci dà la possibilità di estendere gli istituti che conosciamo e di cercare di comprendere e verificare se possiamo adattarli alle nuove situazioni. Nel 2013 il gruppo di esperti delle Nazioni unite che si occupò delle questioni sollevate nel campo della sicurezza internazionale dalla tecnologia informatica e delle comunicazioni (ICT) ha affermato che il diritto internazionale vigente si applica anche nel dominio cibernetico. Nella Relazione del 2015 il gruppo chiarì che gli Stati esercitano la loro giurisdizione sulle infrastrutture informatiche situate sul loro territorio, che nell'utilizzo degli strumenti informatici gli Stati devono rispettare, oltre agli altri princìpi di diritto internazionale, quello dell'inviolabilità della sovranità territoriale altrui, della parità tra le diverse sovranità territoriali, dell'assestamento dei conflitti mediante mezzi pacifici e, soprattutto, la non ingerenza nelle questioni interne di altri Stati, [cioè] i princìpi fondamentali del diritto internazionale consuetudinario. Soprattutto, gli Stati non possono commettere atti internazionalmente illeciti mediante strumenti informatici, neanche attraverso deleghe a terze parti, quindi nemmeno dando in carico a soggetti terzi, a gruppi criminali o a soggetti che fanno questo di lavoro l'operazione militare contro uno Stato". "La responsabilità sarà sempre dello Stato che ha dato mandato a questi gruppi civili o paracivili di fare questo genere di attività.

Se si guarda alla Carta delle Nazioni unite, rileva innanzitutto il divieto di aggressione sancito dall'articolo 2, paragrafo 4: «Tutti gli Stati membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni unite». Un attacco cibernetico può essere reputato lesivo del divieto stabilito da questa disposizione se ricorrono tre condizioni: che la condotta sia imputabile a uno Stato (la norma non si riferisce ad azioni di individui o gruppi); che l'azione costituisca minaccia o utilizzo della forza contro uno dei beni tutelati dalla norma (integrità territoriale, indipendenza politica, etc.); che l'azione sia rivolta verso un altro Stato (ossia avvenga nell'ambito delle relazioni internazionali). La

verifica della sussistenza della prima condizione comporta una difficoltà innanzitutto di ordine tecnico (ricondurre un'azione alla responsabilità di un soggetto), ma poi anche di ordine giuridico (nel caso il soggetto non sia uno Stato, stabilire se vi sia responsabilità di uno Stato rispetto all'azione di quel soggetto, anche solo per omissione di controllo). Quanto alla terza condizione, essa impone di considerare soltanto le azioni perpetrate a danno di altri Stati (cioè riconducibili all'ambito delle "relazioni internazionali"). La difficoltà maggiore è posta dalla seconda condizione. Stabilire se un atto costituisce o meno utilizzo della forza in violazione dell'articolo 2 è essenziale per decidere se lo Stato colpito può legittimamente reagire con la forza per difendersi. L'articolo 51 della Carta delle Nazioni unite[3] consente, infatti, l'uso della forza per legittima difesa e la Corte internazionale di giustizia ha da tempo stabilito che l'articolo si applica a qualsiasi uso della forza, indipendentemente dal mezzo. Di conseguenza, esiste già una norma di diritto internazionale che permette una legittima difesa anche contro l'attacco informatico. Siccome però manca una definizione universalmente accettata di attacco armato, un'azione cibernetica potrebbe oggi essere classificata in modo certo alla stregua di un attacco armato solo qualora la sua intensità e i suoi effetti siano paragonabili a quelli di un attacco armato e ci sia un livello superiore di danno visibile. L'attacco cibernetico è in grado di produrre danni del genere: se si spegne una centrale che eroga l'energia elettrica, come avvenuto Ucraina, l'effetto si riversa sulla popolazione, sui soggetti che rimangono senza energia e che possono anche morire di freddo. Il problema però è che un attacco informatico potrebbe non avere come obiettivo primario il danneggiamento materiale e ciononostante essere atto a compromettere seriamente le capacità di svolgere le funzioni dello Stato bersaglio o possa minare la stabilità politica, economica e sociale dello Stato, anche senza che ci siano evidenti danni fisici. Dobbiamo necessariamente cominciare a ragionare anche in assenza di evidenti danni fisici. Se si aggiunge che per invocare la legittima difesa occorrono altre tre condizioni (il pericolo imminente, con mancanza di possibilità di soluzioni pacifiche; la proporzionalità; l'immediatezza), ciascuna delle quali pone problemi interpretativi, si comprende quanto sia difficile pensare di applicare l'articolo 51 a un attacco informatico.

Quanto alla proporzionalità, si pone la questione se la difesa per essere legittima debba avvenire nelle stesse forme dell'attacco. La proporzionalità della difesa consiste – come noto – nel non eccedere la misura occorrente per reprimere o respingere l'attacco. Ci si può quindi domandare se il principio della proporzionalità significhi che ad un attacco a livello informatico si debba rispondere con una difesa a livello informatico. Al riguardo va detto che il diritto internazionale, ancorché in riferimento ad attività diverse dall'attacco informatico, ha già chiarito che non è necessario. A un attacco informatico si può cioè rispondere lecitamente, da un punto di vista del diritto internazionale, con un attacco cinetico. Non c'è obbligo di rispondere con lo stesso tipo di misura, fermo restando che qui si ragiona di attacchi informatici che per portata giustificano l'attivazione dell'articolo 51 o dell'articolo 2, paragrafo 4, della Carta delle Nazioni unite, ovvero di attacchi che provochino rilevanti problemi a livello nazionale e sul territorio o addirittura danni fisici. Si aggiunga che una reazione è legittima da parte di uno Stato se avviene nell'immediatezza dell'attacco: dunque nel minor tempo possibile, o comunque in un lasso di tempo ragionevole. Non si può invocare la legittima difesa per un intervento che risponde oggi a un attacco passato. Ciò può essere un problema, in quanto, come noto, l'attacco cibernetico è di difficile attribuzione, laddove la reazione presuppone l'identificazione dell'attaccante.

[3] "Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale".

6. IL RUOLO DELLA DIFESA

Dalle audizioni del Capo di Stato maggiore della Difesa, generale Claudio Graziano, del Capo del VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa, ammiraglio Ruggero Di Biase, e del Comandante del Centro Intelligence Interforze (CII), nonché Capo del Nucleo iniziale di formazione dell'allora costituendo Comando interforze per le operazioni cibernetiche (CIOC), generale Giandomenico Taricco, è emerso che la difesa si avvale di due tipi di dominio di rete: l'uno chiuso, per le informazioni classificate; e l'altro aperto, cioè in collegamento con la rete di pubblico accesso e con internet, per le informazioni non classificate. Le diverse Forze armate condividono la componente materiale dell'infrastruttura di rete (il *layer* fisico, ossia il supporto trasmissivo, la rete fisica). Le dorsali – formate dalla rete numerica nazionale e dai ponti radio – sono della difesa. La rete in fibra ottica è una delle più estese nell'ambito dalla pubblica amministrazione: 13.000 chilometri che coprono l'intero territorio nazionale, comprese le isole. Per l'operatività vengono utilizzati sistemi nazionali di Leonardo s.p.a. e di raggruppamenti temporanei di imprese nazionali.

L'area di vertice interforze, che include lo Stato maggiore della Difesa e il Segretariato generale, e le singole Forze armate condividono tra loro questo strato di *networking*. Ogni Forza armata è poi organizzata col proprio dominio e ha la sua intranet. Le intranet di Forza armata e l'intranet dell'area di vertice interforze sono federate in una relazione di *trust* reciproca. Pertanto, i servizi vengono condivisi in maniera pienamente interoperabile, come se si trattasse di un'unica rete. Inoltre ogni Forza armata, ed anche l'Arma dei carabinieri, ha costituito un proprio CERT per la tutela dei rispettivi sistemi informatici, mentre la difesa nel suo insieme ha costituito un CERT difesa, che ha il compito di prevenire la minaccia cibernetica, rilevare le attività di natura malevola e reagire contro gli incidenti informatici che interessano il sistema della difesa nel suo insieme. A parte questo, è merito della Difesa essere stata la prima, tra le pubbliche amministrazioni statali, a chiedere l'iscrizione al registro (cosiddetto RIPE, con sede in Olanda) che fornisce i pacchetti di indirizzamento IPv6 (più avanzati degli ordinari), che oggi, con l'avvento dell'internet delle cose, stanno diventando indispensabili.

6.1 Il CERT Difesa

Il CERT Difesa si articola in due organismi: il CERT *Coordination Center*, costituito in seno al II Reparto (Informazioni e Sicurezza) dello Stato maggiore della Difesa; e il CERT *Technical Center*, costituito in seno al Comando C4 Difesa, a sua volta inserito nel VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa. I due CERT svolgono attività di indirizzo, coordinamento e informazione rispetto ai CERT delle singole Forze armate. Nelle situazioni di crisi riguardanti i sistemi della difesa, il CERT Difesa coordina le attività da porre in essere. In sintesi, il CERT *Coordination Center* svolge attività di informazione e di allertamento anche a scopo di prevenzione e collabora e condivide informazioni con i corrispondenti CERT nazionali e internazionali (quello della NATO, il *Nato Computer Incident Response Capability* o NCIRC); il CERT *Technical Center* è invece preposto a prevenire, rilevare e contenere sul piano tecnico-operativo gli incidenti informatici, oltre che a coordinare e supportare l'azione dei CERT di Forza armata in caso di emergenza cibernetica. Il CERT *Technical Center* è quindi l'organo preposto alla gestione tecnico-operativa di tutti gli assetti e sistemi di *Information and Communication Technology* del comparto Difesa.

6.2 Il CERT Technical Center

Il Comando C4 – nel quale è costituito il CERT *Technical Center* – svolge le proprie funzioni in tre ambiti di attività. Il primo è l'area del *networking*, che comprende la gestione dell'intera infrastruttura di rete. In quest'ambito opera il *Network Operation Center* (NOC). Il secondo è l'area dei servizi informativi (di natura sia gestionale, sia operativa) erogati agli utenti

attraverso l'infrastruttura di rete, che comprende la gestione dei *data center* che ospitano quei servizi. In quest'ambito opera l'*Infrastructure Operation Center* (IOC). Il terzo è l'area della sicurezza, preposta a garantire l'applicazione degli indirizzi di settore in materia e a dare attuazione alle misure di *information assurance* e *cyber defence*. In quest'ambito operano il *Security Operation Center* (SOC), preposto a garantire servizi di sicurezza finalizzati alla protezione dell'infrastruttura ICT del comparto e a rilevare ogni forma di anomalia di natura di sicurezza su tale infrastruttura, e il CERT *Technical Center*, che garantisce i servizi di sicurezza finalizzati alla prevenzione, alla reazione e al contenimento di incidenti informatici.

6.3 Il quadro capacitivo attuale e i progetti di rafforzamento

Lo sviluppo di capacità di *cyber defence* nel comparto Difesa si incentra al momento sul programma *Cyber Defence Capability*. Per capacità di *cyber defence* deve intendersi la capacità di proteggere adeguatamente la propria infrastruttura di rete, in questo caso quella della difesa. Questa capacità comprende le capacità di prevenzione, rilevazione di attacchi, reazione e ripristino dell'efficienza. Si tratta di proteggere l'infrastruttura, di prevenire gli incidenti informatici, di rilevarli quando l'attività malevola ha avuto effetto ed è quindi riuscita a penetrare nell'infrastruttura, di disporre di strumenti di analisi per comprendere la complessità dell'evento e la tipologia dei *malware*, di reagire e contrastare la minaccia, di ripristinare prontamente l'infrastruttura rimuovendo i danni, in modo che possa continuare a erogare i servizi istituzionali.

Ciò premesso, lo scopo del programma di sviluppo della *Cyber Defence Capability* è accrescere le capacità del CERT *Technical Center* e di proteggere le infrastrutture ICT (*Information Comunication Technology*), a cominciare da quelle della rete aperta (dominio non classificato). In sostanza, si tratta di proteggerle da attività di natura malevola: cioè quelle mirate a sottrarre informazioni e dati, a compromettere la loro integrità o a denegare agli utenti i servizi in rete. Il programma tende all'acquisizione di strumenti per prevenire, proteggere, rilevare, analizzare, reagire e ripristinare. Il modello di riferimento nella definizione del programma è stato il *framework* capacitivo della NATO, sul quale si basa il *Computer Incident Response Capability* della NATO (NCIRC), che, detto incidentalmente, è stato realizzato da un'azienda italiana, Leonardo.

Quanto allo sviluppo temporale del programma, questo è diviso in due fasi: mirate alla realizzazione rispettivamente di una capacità operativa iniziale (IOC) e di una finale (FOC), fermo restando che quest'ultima è "finale" solo rispetto al programma in questione. Una volta completato il programma, saranno state realizzate molte delle capacità che la NATO già possiede.

La prima fase si è conclusa nei tempi previsti e ha permesso di acquisire i requisiti minimi basilari per la *cyber defence*. È stata creata tra l'altro una sala di controllo (*control room*) presso il Comando C4 Difesa, attiva tutti i giorni, 24 ore al giorno, capace di integrare tutti i dati provenienti dalle sonde che operano sull'infrastruttura di rete (sonde di *intrusion detection* e di *intrusion prevention*, strumenti di analisi del traffico e dei pacchetti *Internet Protocol* che transitano sulla rete). Questi dati vengono poi correlati tra loro per formare la cosiddetta *Cyber Operational Picture*, sulla base della quale il personale preposto prende le decisioni attivando, se del caso, misure di contrasto alla minaccia.

La seconda fase, che punta a consolidare le capacità già acquisite e a proseguire il processo di crescita capacitivo, avrebbe dovuto partire con l'esercizio finanziario 2014, ma è stata ritardata per il quadro finanziario non favorevole. Per non fermare il programma, i vertici militari hanno comunque garantito un finanziamento, ancorché parziale, che ha consentito di continuare l'impresa con una fase cosiddetta di evoluzione, mirata soprattutto a consolidare le capacità acquisite. L'obiettivo – al momento dell'audizione – è conseguire la *Final Operational Capability* entro il 2018.

Sebbene, come detto, il programma capacitivo miri soprattutto al rafforzamento della protezione della rete aperta della Difesa, è pianificato anche un irrobustimento della protezione della rete chiusa (dominio classificato). Questo perché la minaccia *cyber* non viaggia solo sulla rete internet, ma può attaccare anche reti chiuse, generandosi per così dire dall'interno. I *malware* sono infatti in grado di superare anche le protezioni cosiddette *air-gap* (vuoto d'aria), cioè quelle delle reti chiuse, isolate. A parte il caso di dolo, se un utente (violando le usuali regole di sicurezza) collega un dispositivo esterno (come una "pennetta") a una macchina di dominio classificato, può immettere *virus* nel dominio; per la stessa via, i *malware*, all'insaputa dell'utente, caricano informazioni classificate su questo supporto esterno; e quando poi il supporto è di nuovo collegato al dominio aperto, le inoltrano ai creatori del *malware*, che riescono quindi a "esfiltrarle" anche da domini chiusi.

Oltre ad acquisire tecnologia (macchinari e *software*) è essenziale formare il personale capace di operare nel settore. Lo strumento da solo, per quanto sofisticato, ha bisogno dell'uomo. Bisogna quindi investire anche sulla risorsa umana. La Difesa si è posta anche questo obiettivo e sta cercando di accrescere sul piano sia quantitativo sia qualitativo gli organici delle articolazioni preposte all'attività di *cyber defence*. Lo sta facendo attraverso un processo interno di selezione e formazione del personale militare e civile, da qualificare sulla base dei nuovi profili di impiego e *iter* formativi. Sono stati definiti i nuovi profili funzionali di impiego e gli *iter* formativi. La Difesa dispone di due istituti di formazione: la Scuola delle telecomunicazioni interforze di Chiavari; e il CIFI/GE presso il Centro intelligence interforze. Questi due organismi formano il personale specialistico delle Forze armate. In parallelo c'è l'assunzione diretta di personale civile e militare con appropriate qualificazioni. Si tratta di reclutare personale in possesso di esperienza pregressa in questo settore e, quindi, in possesso di una formazione di un determinato livello. Per talune figure specialistiche – per esempio *forensic analyst*, *vulnerability evaluator*, *risk manager*, *penetration tester* – la Difesa sta cercando di conseguire certificazioni specialistiche (sia *in house*, sia attraverso corsi specialistici offerti da organizzazioni di riferimento del settore).

6.4 L'Autonomous System Internet Provider Independent

Altro progetto importante della Difesa per conseguire la crescita capacitiva nel settore della *cyber*-sicurezza è l'*Autonomous System Internet Provider Independent*. Ad oggi, le intranet di Forza armata e l'intranet dell'area di vertice interforze sono, come detto, federate in una relazione di *trust* reciproca. Tuttavia ciascuna accede a internet, cioè alla rete pubblica, in modo autonomo e si approvvigiona del collegamento a internet attraverso operatori commerciali. Col progetto citato la Difesa punta a realizzare un'infrastruttura di accesso diretto unico per l'intero comparto difesa, a banda larga e ridondato, alla grande nuvola internet (cosiddetta *Big Internet*). In sostanza, l'obiettivo è che il Comando C4 Difesa si connetta direttamente con i nodi di accesso nazionale alla *Big Internet* (il Namex di Roma e il Mix di Milano), scavalcando gli operatori privati e diventando esso stesso *internet service provider* per l'intero comparto della difesa. In altre parole, l'obiettivo è allacciare la rete in fibra ottica delle Forze armate direttamente al Mix di Milano e al Namex di Roma, per realizzare un accesso diretto della rete della difesa alla rete pubblica di internet, in modo che la difesa diventi sistema autonomo (*Autonomous System*), svincolato dai *provider* commerciali e – per così dire – *provider* di se stessa. I vantaggi attesi derivano innanzitutto dall'unificazione dell'attività di comando e controllo nella protezione cibernetica delle infrastrutture della difesa, ma poi anche dalla riduzione dei costi e dall'aumento della qualità del servizio.

6.5 Il piano di business continuity e disaster recovery

Un'altra attività intrapresa dalla difesa è finalizzata a garantire *business continuity e disaster recovery*, ossia a rendere l'infrastruttura ICT della difesa capace di erogare i servizi istituzionali pure in caso di eventi disastrosi, anche di natura malevola, ovvero in caso di

incidenti informatici dovuti ad attacchi cibernetici. Per questo, occorre la riorganizzazione di tutti i *data center* in un unico polo di *private cloud*. La Difesa sta introducendo questa tecnologia nei propri centri di elaborazione dati, con lo scopo di assicurare la resilienza del sistema necessaria per evitare soluzioni di continuità nella disponibilità dei servizi. La Difesa ha quindi redatto un Piano che è stato validato dall'Agenzia per l'Italia digitale. La prima fase mira alla razionalizzazione e al consolidamento dei *data center* dell'area di vertice interforze. La seconda fase ha invece per obiettivo la convergenza dei *data center* delle Forze armate in un unico *private cloud* della difesa, predisposto per garantire ai servizi anche funzioni di *business continuity e disaster recovery*.

6.6 La rete interministeriale di gestione delle crisi cibernetiche

Il Nucleo di sicurezza cibernetica ha inoltre affidato alla Difesa il compito di presentare un progetto di realizzazione di una rete interministeriale di gestione delle crisi cibernetiche che possa garantire lo scambio di informazioni anche in uno scenario di crisi cibernetica, là dove vengano meno le reti e le infrastrutture della pubblica amministrazione ministeriale. Deve trattarsi di un sistema di comunicazione ben protetto, robusto, ridondato e sicuro, in grado di garantire lo scambio di informazioni (anche classificate come segrete) in situazioni di crisi da attacco cibernetico, così da rendere possibile il coordinamento delle reazioni necessarie, che sarebbe impossibile senza comunicazione. Lo studio di fattibilità è stato richiesto alla Difesa in virtù del fatto che essa dispone già di una complessa rete propria di comunicazione, la DIFENET, oltre che del fatto che ha grande esperienza di gestione di reti classificate. La soluzione ipotizzata è quella di ospitare presso i *data center* della Difesa i nodi che dovranno erogare i servizi, e cioè di utilizzare la connettività DIFENET, che in parte già serve alcuni dicasteri e organismi pubblici, e per il resto completare la connessione materiale realizzando i necessari circuiti per raggiungere tutti i Ministeri. Una volta completata, la rete interministeriale potrebbe assumere il ruolo di rete di gestione delle crisi nazionali.

6.7 La cyber active defence

I progetti fin qui descritti tendono al rafforzamento della protezione del sistema informatico della Difesa (e dell'intera amministrazione statale centrale) contro gli incidenti e gli attacchi cibernetici. Nel contempo, però, la Difesa – come necessario per tenere il passo con l'evoluzione degli scenari internazionali – sta lavorando a sviluppare una propria capacità di difesa cibernetica "attiva" (*active cyber defence*), vale a dire una capacità non solo strettamente difensiva (*cyber defence*), ma in qualche misura proattivamente difensiva (*active cyber defence*), la quale è a sua volta il presupposto per l'acquisizione di capacità di sfruttamento delle vulnerabilità altrui (tecnicamente *exploitation*) e poi, eventualmente, di attacco nello spazio cibernetico. L'obiettivo è in sostanza quello di diventare soggetti attivi, ovvero capaci di eseguire *penetration test* al di fuori del proprio ambito e cosiddetta analisi forense, cioè analisi degli effetti malevoli. A tal fine la Difesa sta costituendo un'apposita struttura, denominata Comando interforze per le operazioni cibernetiche (CIOC). Su quest'ultimo tema si è soffermato in modo particolare nella sua audizione il Comandante del Centro Intelligence Interforze (CII), generale di brigata aerea Giandomenico Taricco.

Mentre la difesa cibernetica in senso stretto (*cyber defence* o *cyber security*) comprende misure di separazione fisica o di protezione (reti autonome, *firewall*, antivirus) e protocolli di sicurezza (procedure, modi di fare), la difesa proattiva (*active cyber defence*) – primo grado verso le capacità di *exploitation* (sondare restando invisibili) e di attacco (produrre danni) nello spazio cibernetico – implica un'interazione attiva con l'esterno per proteggere la propria rete. *Computer network defence* (CND), *computer network exploitation* (CNE), *computer network attack* (CNA) formano nel complesso il dominio delle *computer network operation* (CNO). Per metafora: si entra in casa degli altri, perché, per proteggersi, non basta difendere il proprio

fortino. In sostanza, l'*exploitation* è l'operazione che serve ad acquisire informazioni sugli avversari, restando invisibili, per capire cosa fanno e quindi come possono reagire e cosa possono subire (è quindi un'attività di *intelligence*); l'*attack* è invece l'operazione che provoca effetti e produce danni. L'acquisizione d'informazioni (l'*intelligence*) è fondamentale nello spazio cibernetico come in quello fisico. Bisogna avere dati per capire l'evoluzione della minaccia, giorno per giorno. Senza informazioni non è possibile costruire un "ordine di battaglia" nella dimensione *cyber*. L'"ordine di battaglia" (ossia la "rappresentazione" di ciò che un'unità militare deve aspettarsi in territorio nemico) è indispensabile nella dimensione del confronto *cyber* come in ogni confronto di natura militare. Prima di eventualmente attaccare, occorre sapere che tipo di organizzazione ha il nemico e dove e come è possibile attaccarlo. Il *computer network exploitation* è quindi in qualche modo l'equivalente concettuale della *signal intelligence* (SIGINT) o della *comunication intelligence* (COMINT), ossia della raccolta di informazioni mediante intercettazione e analisi di segnali emessi per la messa in comunicazione di persone o di macchine.

Nell'odierno scenario geopolitico, nel quale le tecnologie informatiche dimostrano sempre più di poter essere impiegate per nuocere, come vere e proprie armi, e sempre più spesso le realtà statuali stesse utilizzano la rete come campo di battaglia al di fuori del sistema di regole riconosciute nelle relazioni internazionali dai Paesi democratici, è essenziale che l'Italia – come molti altri Paesi stanno facendo – sviluppi capacità attive di operazione (CNO). Diversamente il rischio è che infrastrutture o istituzioni strategiche soccombano (siano paralizzate o gettate nel disordine) ad attacchi che possono venire non solo dalla criminalità (si pensi al *ransomware Wonna Cry* che a maggio 2017 ha attaccato anche pubbliche amministrazioni di un gran numero di Stati), ma anche da alcuni Stati. Si tratta in potenza di attacchi idonei a minare, anche gravemente, la stessa capacità di difesa militare del Paese. Infatti l'aver messo in rete non solo i servizi connessi alla difesa, ma anche i sistemi d'arma (aerei, navi, carri armati, centri di comando) rappresenta, sì, un grandissimo vantaggio, perché comporta un'efficacia operativa superiore, ma è anche un motivo di debolezza perché la rete è attaccabile dal nemico ed è canale di attacchi del nemico.

È importante notare che, mentre in tema di *cyber defence* l'esperienza della NATO può servire da modello e da punto di riferimento, ciò non è possibile in tema di *computer network operation*, perché questo è un argomento delicato, che non è affrontato in contesto multilaterale o multinazionale e non è discusso a livello NATO. Non solo non se ne parla nella NATO, ma non se ne parla affatto a livello internazionale, perché la tecnologia applicata, essendo una tecnologia strategica, dà un grande vantaggio competitivo a chi la possiede, con la conseguenza che le conoscenze vengono protette da chi le detiene e gli investimenti nascosti, perché rivelarli comporterebbe un danno economico e strategico.

La costruzione di una struttura per le CNO – cui la Difesa sta attendendo, in stretto coordinamento con gli organi del comparto dell'informazione per la sicurezza della Repubblica, attraverso il Centro intelligence interforze (CII) – ha richiesto, tra l'altro, la formazione di personale preparato. Considerato che non esistono, fuori del mondo della difesa, scuole di formazione per questo tipo di personale, è necessario – e in parte è stato fatto – costituire percorsi formativi appositi, ritagliati sulla specifica esigenza: occorrono ingegneri, ma anche operai, perché non tutti devono essere superesperti. Servono probabilmente conoscenze di settore che, messe assieme, costruiscono sinergicamente capacità. Il percorso formativo già costruito è risultato soddisfacente, al punto che il personale addestrato dalla Difesa è risultato, in confronto con quello di altri dicasteri, molto competitivo. Tra l'altro, per formare e addestrare il personale è stato allestito a Ponte Galeria (Roma) un *cyber* laboratorio (che una delegazione della Commissione ha visitato). È stata condotta un'attività esercitativa specialistica. Le esercitazioni sono condotte anche in ambiente internazionale, ma le più significative si svolgono spesso solo nell'ambiente nazionale.

Grazie al lavoro fin qui condotto la Difesa è in grado oggi di cominciare a sviluppare un ordine di battaglia *cyber*. Ha inoltre sviluppato sistemi di pianificazione della condotta di operazioni *cyber*. Ha realizzato sistemi perimetrali per *Computer Network Defence* (CND), con verifica e filtro in tempo reale di eventuali minacce, a complemento della protezione a mezzo di antivirus e di *firewall*.

6.8 Il Comando interforze per le operazioni cibernetiche (CIOC)

Come anticipato, la difesa sta costituendo una struttura dedicata alle CNO: il Comando interforze per le operazioni cibernetiche (CIOC). Su di esso si è diffuso in particolare il Capo di Stato maggiore della Difesa, nella sua audizione. Il progetto CIOC prevede la realizzazione – entro il 2017 – del Nucleo iniziale del Comando interforze per le operazioni cibernetiche, che ha già preso forma, – ed entro il 2018 – l'attivazione della capacità di condurre operazioni cibernetiche. Ovviamente, la capacità acquisita non sarà definitiva, ma dovrà evolvere con la minaccia, che è certamente una minaccia permanente e in costante evoluzione.

Data la peculiare natura della minaccia cibernetica e considerato l'attuale architettura di difesa, che fa capo al DIS, il CIOC opererà in stretto collegamento con il sistema delle informazioni per la sicurezza. In particolare, come chiarito dall'audizione del Direttore generale del DIS (svolta fuori del programma dell'indagine conoscitiva), è stato instaurato un meccanismo di soluzione e coordinamento dei rapporti tra il comparto intelligence e il Ministero della difesa, in modo da definire un quadro preciso delle attività nel settore della *cyber security* che fanno capo alla difesa e di quelle che fanno capo al comparto. Un protocollo stabilito tra comparto intelligence e difesa consente ai due sistemi di muoversi congiuntamente in modo coordinato e senza sovrapposizioni. È chiaro comunque che si incontrano difficoltà enormi nel definire quando una minaccia cyber deve attivare il sistema di difesa del Paese, piuttosto che il sistema di sicurezza. Fare chiarezza sul punto è però indispensabile perché, se la risposta a una minaccia dev'essere militare, il procedimento decisionale è di un tipo (e coinvolge il Parlamento), se invece la risposta è non militare, il quadro normativo di riferimento è un altro.

Già il Quadro strategico nazionale per la sicurezza dello spazio cibernetico (di cui al decreto del Presidente del Consiglio dei ministri 27 gennaio 2014) attribuisce al Ministero della difesa il compito di dotarsi della capacità di pianificare, condurre e sostenere operazioni nello spazio cibernetico, e questo per prevenire, localizzare, difendere, contrastare e neutralizzare le minacce e le azioni avversarie a danno dei sistemi e dei servizi della difesa, sia sul territorio nazionale, sia sui teatri operativi fuori dai confini nazionali, nel quadro delle missioni militari. In questa cornice, il Piano nazionale per la protezione cibernetica prevede a sua volta la realizzazione del Comando interforze per le operazioni cibernetiche, che ha rappresentato una priorità del Governo nella corrente legislatura, come si evince anche dal programmatico Libro bianco per la sicurezza internazionale e la difesa dell'aprile 2015. Questo, nell'ambito della riorganizzazione del vertice interforze, prevede la costituzione di un Comando operativo di vertice interforze articolato negli esistenti Comandi operativi, nel Comando interforze per le operazioni speciali e nel costituendo Comando interforze per operazioni cibernetiche.

Il Comando sarà impegnato su un duplice fronte: da un lato, contribuirà alla sicurezza nazionale, potenziandone le capacità di difesa da attacchi cibernetici, dall'altro svilupperà capacità di pianificazione e conduzione di CNO a supporto delle operazioni militari sia in Italia, che al di fuori dei confini nazionali.

Il progetto CIOC poggia su quattro elementi cardine. Il primo è quello organizzativo, si tratta di sviluppare le componenti di uno specifico comando, inteso come organizzazione formata da persone, logisticamente supportate e dottrinalmente preparate. Il secondo è quello delle infrastrutture necessarie: si tratta di realizzare sistemi e modalità d'azione protetti. Il terzo è il

personale: occorrerà formare personale idoneo, attraverso selezione e formazione. Il quarto è quello degli ambienti virtuali: si tratta di realizzare "poligoni" per lo sviluppo e la crescita delle capacità *cyber* delle Forze armate.

Il nucleo iniziale del CIOC è rappresentato dalle strutture già realizzate (il CERT Difesa e il SOC). Su queste fondamenta la difesa sta edificando la capacità di svolgere le *computer network operations*. Le capacità necessarie per sviluppare operazioni nel network dei computer (CNO) consentiranno – una volta integrate nei domini tradizionali: terrestre, marittimo e aerospaziale – di effettuare le operazioni cibernetiche nella loro dimensione più importante.

La capacità di operazioni *cyber* del CIOC sarà a sua volta implementata attraverso cellule operative cibernetiche: in altre parole il CIOC emanerà, per ciascun comando operativo, cellule per la condotta delle operazioni cibernetiche. Le cellule saranno collegate con il CIOC e con i vari sensori periferici della maglia, compresi i singoli mezzi in movimento e in futuro i singoli combattenti, che saranno dotati dei sistemi cibernetici anche per consentirne la geolocalizzazione tramite satellite e per garantire la conoscenza capillare dell'area delle operazioni. Le Cellule operative cibernetiche (COC) emanate dal CIOC saranno schierate nei comandi delle Forze proiettate all'estero nei teatri operativi di missioni internazionali. Le COC – in sistema con il CIOC operante nella madrepatria – dovranno garantire, da un lato, la protezione degli assetti militari impiegati nei teatri di missione, che sono sempre più decentralizzati, e dall'altro la condotta delle possibili operazioni cibernetiche nell'area delle operazioni militari. Si pensi al sistema informatizzato cosiddetto del «soldato futuro». Si tratta di dispositivi *hi-tech* che trasferiscono al comando informazioni da aerei, navi e personale, consentendo al comando di conoscere la situazione sul terreno in presa diretta, attraverso un sistema di monitoraggio. Un attacco alla rete di questi dispositivi sarebbe fatale, e dovrebbe quindi essere contrastata con una risposta immediata. È evidente che, se il sistema di monitoraggio viene interrotto o alterato mentre un'operazione è in corso, i rischi per i militari sono elevatissimi.

Quanto alle responsabilità, fuori dal territorio nazionale, nelle missioni, questa non potrà che essere del comandante dell'operazione, che risponderà della sicurezza totalmente, per le ragioni testé dette. Dovranno quindi esistere regole d'ingaggio relative alla dimensione *cyber*. Se nel corso di operazioni tradizionali avviene un attacco cibernetico che metta a rischio la sicurezza del personale, il comandante dovrà rispondere, sulla base di regole di ingaggio, se necessario attaccare su quel fronte per garantire la sicurezza e la funzionalità del sistema. Sul territorio nazionale, invece, la responsabilità non sarà soltanto della difesa, ma in alcuni casi competerà agli organi di informazione per la sicurezza, mentre in altri settori sarà della difesa, fermo il coordinamento con il sistema delle informazioni per la sicurezza. Sarà fondamentale il coordinamento fra i settori della difesa e dell'intelligence, che dovranno lavorare insieme in cellule integrate.

Il costituendo CIOC colmerà una lacuna dell'assetto organizzativo italiano, dato che in altri Paesi già esiste un organismo simile, mentre in altri è in corso di realizzazione. Negli USA l'*United States Cyber Command*, alle dipendenze dello *United States Strategic Command*, opera per comandi regionali o comandi funzionali (per esempio, il comando supremo in Europa è un comando regionale; l'USSTRATCOM è un comando funzionale). In Gran Bretagna il comando *cyber* afferisce a un organismo congiunto con gli organi di sicurezza britannici. I comandi *cyber* francesi, spagnoli e olandesi sono sostanzialmente simili. Non solo tutti i principali Paesi, ma anche molte organizzazioni internazionali, compresa la NATO, si stanno dotando di strutture militari di comando e controllo per operazioni nello spazio cibernetico. È quindi evidente che un ritardo dell'Italia nello sviluppo di capacità in questo settore comporterebbe l'impossibilità di operare in un contesto interalleato. D'altra parte gli stessi obiettivi definiti sia in ambito europeo sia in ambito NATO comprendono la realizzazione di solide capacità di *cyber defence* e di protezione delle infrastrutture. Questo proponimento è stato rafforzato anche nel vertice NATO di Varsavia, con la sottoscrizione del *Cyber defence pledge*, con cui da una parte vengono definite le misure minime di sicurezza cibernetica cui tutti i Paesi membri devono attenersi e

dall'altra parte si introduce il principio per cui chi non si conforma agli standard, non può partecipare alle attività (*no-compliance no-participation*).

Come detto, lo sviluppo delle capacità di CNO richiede la disponibilità di ambienti virtuali per l'esercitazione: sorte di poligoni virtuali per l'addestramento e il mantenimento delle capacità del personale. Una struttura del genere è in via di allestimento presso la Scuola telecomunicazioni delle Forze armate di Chiavari. Auspicabilmente in futuro essa sarà federata con le analoghe strutture di Paesi amici e alleati, tra cui il centro di eccellenza NATO di Tallin. L'istituto opererà in sinergia con il mondo accademico e quello industriale. Il mondo accademico è infatti un riferimento essenziale, dato che soprattutto in questo settore, che è in continua e rapidissima trasformazione, studio e sperimentazione sono indispensabili. È previsto altresì l'allestimento di un Cyber Lab, che sarà realizzato nella sede del Comando interforze delle operazioni cibernetiche e permetterà di acquisire gli strumenti necessari per studiare i *malware* e trovare i rimedi contro la minaccia, oltre a fornire supporto ai responsabili della progettazione, sviluppo e gestione delle reti, man mano che la minaccia viene identificata e neutralizzata.

In conclusione, il CIOC è necessariamente un organismo interforze, dato che la minaccia cyber non ha un ambito spaziale definito (non riguarda in modo esclusivo né terra, né mare, né cielo). Lo spazio cibernetico consiste in un dominio creato dall'uomo, trasversale agli altri quattro domini tradizionali (terrestre, marittimo, aereo e spaziale), caratterizzato da mancanza di geospecificità, in quanto supera i confini geografici, soprattutto per la difficoltà di identificare l'agente (attribuzione).

6.9 Il procurement

La tecnologia cambia molto velocemente mentre i procedimenti pubblici per l'acquisto di materiali sono troppo lenti, con la conseguenza che, da quando l'amministrazione definisce l'esigenza a quando il contratto va in esecuzione, è passato troppo tempo e si acquistano cose obsolete. Avere un processo di acquisto veloce è fondamentale. Occorre inoltre saper cosa comprare. Nella pubblica amministrazione la regola è comprare al massimo ribasso. Ma comprare al massimo ribasso significa spesso comprare tecnologia straniera. E nulla assicura che questa tecnologia non contenga installati all'origine mezzi per esfiltrare le informazioni dell'utente. Le verifiche di sicurezza sono fondamentali. Si dovrebbe puntare almeno a controllare ciò che si acquista e utilizza nelle amministrazioni pubbliche, e soprattutto in quelle che trattano informazioni strategiche. Altri Paesi (il Regno unito) hanno imposto che ogni pezzo di *hardware* e *software* che entra nel loro territorio sia trasparente per l'autorità governativa, nel senso che chi vende deve dare completamente conto del progetto.

7. I PRINCIPALI PAESI EUROPEI

7.1 Francia

Il 29 aprile 2013 è stato pubblicato il nuovo Libro bianco sulla difesa e la sicurezza nazionale della Francia, che definisce la politica di difesa del paese in una prospettiva di medio (5 anni) e lungo periodo (15 anni). Il documento fa seguito ad altri tre Libri bianchi, pubblicati in materia rispettivamente nel 1972, nel 1994 e nel 2008.

Il Libro bianco 2013 segna un passo avanti sulla presa in considerazione della minaccia informatica e dello sviluppo delle capacità di *cyberdefence*. Prevede una postura strategica che mira a determinare l'origine degli attacchi, a organizzare la resilienza della Nazione, ad approntare la risposta anche tramite la lotta informatica offensiva.

Si prevede che la Francia si renda autonoma nella produzione dei sistemi di sicurezza, rafforzi le risorse umane dedicate alla *cyberdefence* e accresca l'affidabilità dei sistemi informativi dello Stato e dei grandi operatori.

Sul piano militare, sarà sviluppata ed attrezzata una catena di comando unificata, mentre sarà creata una riserva operativa ed una riserva civile per la *cyberdefence*, al fine di accrescere la resilienza del Paese.

A partire dal luglio 2009 è operativa in Francia l'Agenzia Nazionale per la Sicurezza dei Sistemi Informativi (l'*Agence Nationale de la Sécurité des Systèmes d'Information* - ANSSI), evoluzione della *Direction centrale de la sécurité des systèmes d'information*.

Alle dipendenze del Primo Ministro, l'Agenzia è pienamente integrata all'interno del vertice decisionale politico-strategico e costituisce, per esplicita menzione di legge, l'autorità nazionale in materia di sicurezza dei sistemi informativi.

L'ANSSI è stata pensata come una struttura attraverso la quale la «funzione cybersecurity» viene centralizzata e collegata stabilmente all'organo responsabile della pianificazione strategica integrata in materia di sicurezza nazionale, il *Secrétaire Général de la Défense et de la Sécurité Nationale*[4].

L'Agenzia, in particolare, è un organismo centrale di coordinamento tra le differenti amministrazioni governative con competenze in materia di sicurezza cibernetica e si occupa di garantire la coerenza e l'efficacia delle misure adottate per salvaguardare la sicurezza delle infrastrutture strategiche informatizzate del Paese. Coordina la risposta ad attacchi o incidenti cyber ed è responsabile della cooperazione internazionale.

A livello più operativo, ha spiegato il professor Baldoni, spetta al Centro per la Sicurezza dei Sistemi Informativi, istituito presso l'Agenzia Nazionale, il compito di identificare gli attacchi contro le infrastrutture critiche nazionali e di mitigarne gli effetti.

Il Centro svolge altresì la funzione di CERT nazionale in quanto provvede all'analisi delle minacce e degli incidenti di natura cibernetica che possono interessare le infrastrutture critiche nazionali o altri enti governativi.

Sempre a livello operativo, svolgono un ruolo rilevante il Centro Pianificazioni e Operazioni e il Centro Analisi per le Operazioni di Difesa Cibernetica istituiti presso il Ministero della Difesa francese. Il Centro Analisi, in particolare, si occupa di individuare, esaminare e rispondere ad attacchi cibernetici in collaborazione con Centro per la Sicurezza dei Sistemi Informativi. "Qualora un attacco *cyber* sia in grado di determinare una situazione di crisi tale da pregiudicare la sopravvivenza della nazione ovvero le sue capacità militari, il suo potenziale economico e la sua sicurezza, le agenzie e i servizi dello Stato, nei limiti del mandato assegnato loro dal primo ministro, sono autorizzati a condurre tutte le operazioni di natura tecnica necessarie a stabilire l'origine dell'attacco, attribuirne la responsabilità e a mitigarne gli effetti. Tale possibilità è prevista dal Codice della Difesa Militare come modificato dalla legge n. 2013-116822[5].

Infine, occorre notare che in Francia è stata istituita la Riserva di Cyber Defence, alimentata da cittadini volontari con esperienza nel settore. La riserva svolge un ruolo importante nel sensibilizzare la popolazione francese sulla importanza della sicurezza informatica ai fini della tutela, dell'integrità e della sovranità della nazione.

La Riserva, posta sotto l'autorità dello stato maggiore della difesa, non svolge, né partecipa a operazioni di *cyber-defence*, anche se è prevista la futura istituzione di una componente operativa della stessa.

---

[4] Comitato parlamentare per la sicurezza della repubblica, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, Doc. XXXIV, n. 4, 2010, p. 12.

[5] La citazione è tratta da R. Baldoni e R. De Nicola, *Il futuro della Cyber Security in Italia,* a cura del Consorzio interuniversitario Nazionale per l'informatica, 2015, p. 73.

7.2 Germania

Nel 2016, a dieci anni dalla formulazione del suo precedente documento strategico, la Germania ha presentato il Libro Bianco 2016 per la sicurezza ed il futuro della Bundeswehr[6].

Il Documento definisce la politica di difesa tedesca per i prossimi dieci anni e il ruolo che la Germania è pronta ad assumere nel contesto strategico internazionale.

Tra le nuove priorità del governo tedesco vi è certamente la sicurezza cibernetica, da raggiungere sempre attraverso una più intensa collaborazione internazionale.

La sicurezza cibernetica è da tempo diventata un obiettivo tedesco in ambito di difesa, viste le sue implicazioni per le operazioni militari. Il Governo, ha pertanto optato per la creazione del nuovo "Dipartimento per la sicurezza informatica e cibernetica" – (*Commando Cyber und Informationsraum, KdoCIR*) – da creare in cooperazione con il ministero degli Interni) che dovrà essere reso pienamente operativo entro il 2023, in collaborazione con il Ministero degli interni. Già nel 2017 dovrà essere in grado di assicurare l'inizio delle attività grazie anche al parziale inserimento, al suo interno, di parte dei 4.400 civili specializzati.

Nel Documento Berlino auspica, inoltre, una maggiore collaborazione europea nel settore cibernetico e quelli ad alto utilizzo di tecnologie *hi-tech*.

In particolare, una forte collaborazione a livello Nato ed europeo volta alla definizione di regole comuni in ambito *cyber* e la messa in sicurezza delle infrastrutture critiche viene considerata essenziale per il conseguimento di elevato livello di sicurezza nel dominio *cyber*.

7.3 Regno Unito

Il governo del Regno Unito ha quasi raddoppiato gli investimenti nel campo della sicurezza cibernetica, passando da 860 milioni di sterline, per il solo 2016, a 1,9 miliardi di sterline nei prossimi cinque anni. Il Governo ha, altresì, aperto un Centro di *cyber security innovation* a Cheltenham ed ha annunciato di voler investire oltre 40 milioni di sterline nella costituzione di un nuovo *Cyber Security Operations Centre* (Csoc), con il compito di difendere le infrastrutture delle reti facenti capo al ministero della Difesa del Regno Unito. Il centro dovrebbe nascere presso l'*Information Systems and Services* (Iss), che a oggi gestisce tutte le comunicazioni militari, situato nella base di Corsham in Wiltshire.

A sua volta nel Regno Unito è *l'Office of Cyber Security & Information Assurance* (Ocsia) a portare avanti il *National Cyber Security*, ovvero il programma governativo in materia di sicurezza cibernetica.

L'Ocsia è di ausilio nel settore della *cyber security* al ministro della Difesa, al Government Communications Headquarters (Gchq), al Communications-Electronics Security Department, al Centre for the Protection of National Infrastructure, al Foreign & Commonwealth Office e al Department for Culture, Media & Sport.

8. CONCLUSIONI

Gli elementi acquisiti nel corso dell'indagine conoscitiva permettono di formulare talune considerazioni conclusive in merito al tema della difesa cibernetica, con particolare riferimento alla complessità delle questioni che riguardano l'approntamento di un adeguato sistema di risposta alle minacce provenienti dal *cyber space* e allo sviluppo di capacità cibernetiche utilizzabili per scopi militari.

In via preliminare si osserva che l'indagine conoscitiva è stata limitata ai soli profili di competenza della IV Commissione difesa, e pertanto non sono state affrontate dalla Commissione tutta una serie di questioni che sebbene di estrema attualità e rilevanza nel campo della minaccia cibernetica attengono in via prioritaria alle competenze di altre Commissioni.

---

[6] Cfr. *Il libro bianco della Difesa tedesco: quali opportunità di cooperazione,* a cura dell'Osservatorio di politica internazionale.

Occorre infatti considerare che attualmente la minaccia cibernetica si presenta come una minaccia trasversale, capace di aggredire interessi e ambiti diversi, pubblici e privati, civili e militari.

A fronte della vastità degli interessi potenzialmente aggredibili da un attacco cibernetico, vi è tutta una serie di misure di contrasto la cui attuazione ricade sotto la responsabilità di soggetti diversi, ciascuno dei quali, nell'ambito di una più generale strategia nazionale di sicurezza e difesa cibernetica, è tenuto a proteggere i propri *asset* ed assicurare una risposta pronta ed efficace alle minacce.

Ciò premesso in via generale, per quanto concerne il tema della difesa cibernetica, l'ampia e qualificata platea dei soggetti auditi ha espresso un orientamento unanime in merito alla necessità di potenziare le capacità nazionali di *cyber defence* in considerazione dello sviluppo crescente di strumenti cibernetici in ambito militare e al loro utilizzo in situazioni di conflittualità tra Stati.

In linea con l'analisi svolta nel Libro bianco per la sicurezza internazionale e la difesa del 2015 e, da ultimo, nel Piano nazionale per la protezione cibernetica del maggio 2017, nel corso dell'indagine è stato evidenziato dagli auditi come gli effetti di attacchi cibernetici portati alle reti e ai servizi informatici di un Paese possono essere particolarmente distruttivi e determinare effetti sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali.

Da qui la necessità di garantire un adeguato sistema di difesa cibernetica che preveda l'acquisizione di una specifica capacità di condurre *Computer network operations* nella triplice articolazione di operazioni di difesa attiva (*Computer network defence*), di raccolta informativa (*Computer network exploitation*) e di attacco (*Computer network attack*).

A questo riguardo, come sottolineato in altra sezione del documento conclusivo, nel corso dell'audizione del Capo di Stato maggiore della Difesa, generale Graziano, sono state illustrate le caratteristiche fondamentali del progetto relativo alla costituzione di un apposito Comando Interforze Operazioni Cibernetiche (CIOC) e allo sviluppo di specifiche capacità *cyber* integrate in ambito interalleato, potenzialmente in grado di operare nell'ambito di operazioni congiunte.

L'illustrazione del progetto relativo alla realizzazione del CIOC e all'implementazione delle capacità di *cyber defence* nazionali ha trovato un generale consenso della Commissione; pur tuttavia nel corso dell'indagine sono state sollevate una serie di questioni di carattere prevalentemente giuridico e normativo che appare opportuno definire preliminarmente alla completa realizzazione del progetto CIOC e all'avvio delle richiamate *Computer network operations*, con particolare riferimento al loro utilizzo in contesti multilaterali.

La prima questione attiene alla copertura politico-legale delle *Computer network operations*, con particolare riferimento al *Computer network attack* e alla definizione delle relative regole d'ingaggio.

La portata potenzialmente distruttiva di taluni strumenti d'arma cibernetici impone necessariamente la definizione di precise regole concernenti i limiti di utilizzabilità di tali apparati e, più in generale della stessa operazione nel cui ambito si trovano ad operare.

In secondo luogo occorre, poi, definire una chiara catena di comando in merito all'avvio di questa tipologia di operazioni, con particolare riferimento a quelle svolte in contesti multilaterali.

Al riguardo, gli elementi raccolti nel corso dell'indagine conoscitiva inducono a ravvisare una lacuna nell'ordinamento giuridico in quanto non esiste allo stato una normativa di carattere generale che, analogamente a quanto recentemente disposto dalla legge n. 145 del 2016 per la partecipazione delle Forze armate italiane a una missione internazionale, definisca i singoli passaggi attraverso i quali è possibile per l'Italia prendere parte ad un'operazione militare che utilizzi sistemi cibernetici.

Al riguardo, le caratteristiche proprie del dominio cibernetico e soprattutto la velocità di azione di un attacco cibernetico sembrano richiedere la definizione di un'apposita normativa di riferimento che tenga conto della rapidità con la quale in ambito militare devono essere assunte le misure di risposta ad un attacco cibernetico.

Al contempo tale disciplina dovrà tener conto del necessario coinvolgimento parlamentare nel procedimento decisionale riguardante l'avvio di un'operazione di difesa cibernetica, analogamente a quanto previsto per l'avvio di un'operazione militare di tipo convenzionale.

Per quanto concerne, poi, gli strumenti operativi a disposizione della Difesa per lo svolgimento di operazioni cibernetiche, un punto di debolezza sottolineato dagli esperti sembra essere rappresentato dai limitati poteri di *intelligence* che allo stato il quadro normativo nazionale assegna alla Difesa.

Al riguardo, è stato sottolineato come risulti necessario "percepire anche per il settore cibernetico l'importanza dell'*intelligence* e creare un patrimonio informativo che ci consenta di utilizzarlo ai fini che decidiamo di perseguire".

Tale riflessione appare certamente meritevole di approfondimento anche in vista di eventuali iniziative legislative volte a chiarire i singoli ambiti di competenza dei diversi settori istituzionali nel campo dell'*intelligence* cibernetica e le necessarie forme di coordinamento in un settore particolarmente strategico nella prevenzione della minaccia cibernetica.

Infine, gli ultimi due elementi di riflessione attengono all'approvvigionamento di dotazioni cibernetiche sicure in ambito Difesa e alle risorse finanziarie da destinare alla difesa cibernetica, con particolare riferimento al campo della ricerca.

Per quanto concerne la prima di queste due tematiche, l'autorevole contributo di esperti del settore ha posto in risalto la necessità di disporre di tecnologie ICT sicure con particolare riferimento ai sistemi di comunicazione e alle banche dati che hanno valore per la sicurezza nazionale. È stato infatti osservato come la vulnerabilità del *cyber space* sia in gran parte dovuta al fatto che la stragrande maggioranza delle reti e dei sistemi che formano il dominio digitale sono stati progettati e realizzati pensando a criteri di usabilità e tutt'al più di resilienza, senza tenere in debito conto fin dall'inizio aspetti di sicurezza.

In tempi più recenti sta invece progressivamente acquisendo una posizione di primaria importanza all'interno di ogni organizzazione che gestisce dati o comunicazioni sensibili la necessità di disporre di sistemi informativi realizzati in maniera sicura. Alcuni paesi hanno imposto, per la realizzazione delle infrastrutture critiche nazionali, l'acquisto di solo *hardware* certificato, altri l'impiego di prodotti realizzati da ditte nazionali, più facilmente controllabili e monitorabili, con particolare riferimento alla fornitura di materiale militare.

A livello nazionale, nel corso dell'indagine conoscitiva è emersa la necessità non solo di individuare parametri di sicurezza che devono essere garantiti da eventuali fornitori stranieri che intendono partecipare a gare nazionali, ma anche di sviluppare una specifica capacità ICT (*Information Communication Technology*) in ambito nazionale.

In tale ottica finanziare la ricerca nel settore della sicurezza cibernetica all'interno di un più generale progetto strategico di sicurezza nazionale appare un obiettivo prioritario anche al fine di garantire la realizzazione di applicazioni avanzate, a beneficio di un maggior grado di indipendenza nella prevenzione e gestione dei rischi relativi ai nostri dati, alle nostre transazioni, alle nostre infrastrutture critiche e, più in generale alla sicurezza dei cittadini e alla difesa del Paese.

PAGINA BIANCA

170170024410