COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

2.

SEDUTA DI MARTEDÌ 16 FEBBRAIO 2016

PRESIDENZA DEL VICEPRESIDENTE **MASSIMO ARTINI**

INDICE

PAG.

Sulla pubblicità dei lavori:

Artini Massimo, *Presidente* 3

INDAGINE CONOSCITIVA SULLA SICUREZZA E LA DIFESA NELLO SPAZIO CIBERNETICO

Audizione del professor Stefano Silvestri, *Past president* e membro del comitato direttivo dell'Istituto affari internazionali (IAI), e del dottor Tommaso De Zan, Assistente alla ricerca nell'area Sicurezza e difesa del medesimo Istituto:

Artini Massimo, *Presidente* 3, 7, 10, 12

De Zan Tommaso, *Assistente alla ricerca nell'area Sicurezza e difesa dell'Istituto affari internazionali (IAI)* 7, 12

Lacquaniti Luigi (PD) 10

Silvestri Stefano, Past president *e membro del comitato direttivo dell'Istituto affari internazionali (IAI)* 3, 11

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare (NCD-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCpI); Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Democrazia Solidale-Centro Democratico (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Alleanza Liberalpopolare Autonomie ALA-MAIE-Movimento Associativo Italiani all'Estero: Misto-ALA-MAIE; Misto-Minoranze Linguistiche: Misto-Min.Ling; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI (Unione Sudamericana Emigrati Italiani): Misto-USEI.

PAGINA BIANCA

PRESIDENZA DEL VICEPRESIDENTE MASSIMO ARTINI

La seduta comincia alle 11.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso, la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione del professor Stefano Silvestri, *Past president* e membro del comitato direttivo dell'Istituto affari internazionali (IAI), e del dottor Tommaso De Zan, Assistente alla ricerca nell'area Sicurezza e difesa del medesimo Istituto.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa dello spazio cibernetico, l'audizione del professor Stefano Silvestri, *Past President* dell'Istituto Affari Internazionali (IAI) e membro del comitato direttivo, e del dottor Tommaso De Zan, assistente alla ricerca nell'area Sicurezza e difesa del medesimo istituto.

Saluto e do il benvenuto al professor Silvestri e al dottor De Zan, che ringrazio per la loro disponibilità a essere presenti oggi.

Questo è il secondo appuntamento della nostra indagine, che – lo ricordo – si incentra sugli specifici profili di interesse della Commissione difesa e, quindi, innanzitutto sulla minaccia cibernetica a livello paragonabile all'attacco armato. Peraltro, proprio per far emergere il ruolo che le Forze armate svolgono oggi e quello che dovranno svolgere in futuro in questo campo, l'indagine intende tenere conto anche del ruolo svolto dagli altri soggetti che operano nel complessivo sistema di protezione dello spazio cibernetico nazionale.

A questo fine, la Commissione è interessata ad acquisire anche il contributo di conoscenza che può venire dall'apporto di inquadramento concettuale, di informazione e di esperienza di soggetti che, pur esterni al sistema della difesa in senso stretto, operano comunque in campi di attività riconducibili a questo tema.

Ricordo che, dopo gli interventi del professor Silvestri e del dottor De Zan, darò la parola ai colleghi che intendano porre domande o svolgere osservazioni. Successivamente, i nostri ospiti potranno rispondere alle domande poste.

Do adesso la parola al professor Silvestri.

STEFANO SILVESTRI, Past president *e membro del comitato direttivo dell'Istituto affari internazionali (IAI)*. Farò un'introduzione di tipo generale essenzialmente sui grandi assi della minaccia così come li percepiamo in Istituto: poi il dottor De Zan scenderà un po' più nel dettaglio, anche sulla scorta di varie ricerche che il nostro Istituto ha condotto in ambito *cyber threat*.

Se si considera la minaccia cibernetica, possono esserci vari tipi di opzioni. Ci sono vari tipi di scenari, ma il primo problema che si pone è il fatto che lo spazio cibernetico, pur essendo un bene di interesse comune, non è un bene comune, ma di proprietà di una serie di industrie, di imprese o di Stati, che controllano le

tecnologie e i nodi attraverso cui passano le comunicazioni e lo spazio cibernetico, quindi le reti, e controllano anche gli aspetti fisici, come i cavi, le linee telefoniche e così via.

Questo aspetto è molto importante. Abbiamo indicazioni che le grandi società – come Google, Microsoft ed altre – sono talmente preoccupate da ciò che cercano di rendersi indipendenti con propri cavi e nodi controllati, proprio perché temono non solo la concorrenza, ma anche forme di controllo indiretto sulla loro azione e sulle limitazioni alle loro azioni. È, quindi, chiaro ed evidente che la nostra dipendenza dallo spazio cibernetico ci rende profondamente dipendenti e vulnerabili all'azione di chi controlla e possiede questi nodi.

Questo è largamente inevitabile.

Certamente, l'interruzione dei nodi o dei cavi comporterebbe danni anche per i proprietari. Tuttavia, prima di tutto, bisogna vedere quale grado di ridondanza il proprietario ha e, in secondo luogo, potrebbe essere una scelta voluta per ottenere una capitolazione da parte nostra. Qui c'è, quindi, un elemento forte di analisi che andrebbe valutato a livello sia nazionale sia europeo probabilmente, cioè a livello perlomeno di Stati che condividono lo stesso grado di vulnerabilità o un grado analogo. Questo è un primo problema molto complesso.

Il secondo tipo di minaccia, quello della criminalità cibernetica, è il più diffuso. Lo ricordo, perché non è una minaccia di tipo militare, ma che sta diventando sempre più ampia. Mi dicono – sulla base di calcoli fatti non so bene come, ma comunque sulla base di analisi – che il mercato del crimine cibernetico ha superato ormai di molto (è quasi il doppio) il mercato del crimine della droga. Si tratta di un mercato basato, sostanzialmente, su furti e ricatti.

Ora, questo è un aspetto molto delicato. Essendo gran parte delle tecnologie e delle competenze private in questo campo di proprietà delle varie imprese, il fatto che queste siano sottoposte ad attacchi criminali e non necessariamente li riportino – perché questo potrebbe imbarazzarle, diminuire la loro competitività, danneggiarle in borsa o altro – comporta una vulnerabilità di sistema difficile da valutare, in particolare se all'aspetto meramente criminale si aggiungesse anche quello terroristico. È evidente che i terroristi, pur non potendo eguagliare le capacità di uno Stato nell'attacco cibernetico, potrebbero però probabilmente eguagliare o inserirsi in reti criminali.

Il terzo vettore – qui cominciamo ad entrare nel campo più specificamente militare – è quello dell'*intelligence*, che è essenzialmente una raccolta di dati, dunque una minaccia ma solo indiretta rispetto ad altre. Peraltro, può anche diventare il vettore attraverso cui, grazie al furto di dati, si trova la maniera di entrare in un sistema. È l'*intelligence* che prepara la strada all'attacco che verrà condotto. Senza l'*intelligence*, però, non abbiamo l'attacco.

Rispetto a quella del passato, l'*intelligence* attuale è anche un fenomeno relativamente nuovo a livello cibernetico – questo, secondo me, va ricordato – a causa dell'immensa quantità di dati che l'*intelligence* cibernetica può raccogliere e può gestire. Non sempre questo è fatto in maniera efficiente, comporta molte difficoltà, ma sostanzialmente significa che, se si ha un buono strumento di lettura e valutazione dei dati e un chiaro obiettivo, anche semplicemente la raccolta dei dati aperti esistenti sulla rete, considerata l'enorme quantità di dati raccolti, potrebbe essere sufficiente per penetrare segreti di Stato. Va, quindi, anche qui, a livello di valutazione, considerato il problema dell'*intelligence*.

In quarto luogo, entriamo in uno scenario di guerra vera e propria. Si è già fatto più volte ricorso in questi anni all'uso di attacchi *cyber* in contesti operativi militari in funzione di supporto delle operazioni militari. Questo è, a mio avviso, anche l'uso più comune, più semplice, e in un certo senso anche efficace del *cyber*. La saturazione dei sistemi *cyber* georgiani

prima dell'attacco russo contro la Georgia è un esempio in questa direzione, ma come molti altri.

C'è stato poi lo scandalo in Israele. Si è scoperto che i droni e gli aerei spia israeliani che trasmettevano i dati delle informazioni a terra venivano, in realtà, letti dagli americani, che cercavano così di cautelarsi e scoprire se per caso Israele non stesse preparando un attacco all'Iran. Questa, per lo meno, è la versione uscita sulla stampa, ma credo che volessero controllare più in generale le mosse di Israele. Questo vi dà un'idea di come si possa penetrare. Infatti, se riesco a leggere, riesco anche a intervenire per bloccare. Se durante un'operazione militare riesco a bloccare l'*intelligence* avversaria, le capacità di analisi del territorio e le comunicazioni, sono già un passo avanti nel migliorare le *chance* delle mie Forze armate nelle operazioni.

Il quinto scenario è quello della cosiddetta *cyber war*, cioè dell'uso dell'arma cibernetica in funzione strategica, non più in funzione di supporto, ma come arma principale di attacco contro un Paese. È l'ipotesi, discussa anche dalla NATO, prefigurata dal Galles quando ha cominciato a sostenere che gli attacchi cibernetici potrebbero essere analoghi a quelli che fanno scattare il *casus foederis* dell'Alleanza, ai sensi dell'articolo 5 del Trattato istitutivo. Sono, però, varie le valutazioni da fare.

Certamente, è possibile con una conoscenza dettagliata della situazione cibernetica di un Paese paralizzare le sue infrastrutture di trasporto, di comunicazione, energetiche e di molti altri tipi. Paralizzare già soltanto queste significherebbe un grossissimo danno e, sostanzialmente, un grande attacco al Paese. In genere, quando si parla di attacco e di guerra, da un punto di vista giuridico si dice che servono il morto e il danno, non soltanto economico, ma proprio della casa che cade sotto la cannonata o simili, altrimenti è difficile valutare questo come un attacco militare o un caso di guerra aperta. Si può discutere su quest'interpretazione che, peraltro, è quella prevalente.

Indubbiamente, può essere che cose di questo genere creino anche vittime e danni. Posso benissimo immaginare, se paralizzo le comunicazioni e la rete ferroviaria e aerea civile, che dei treni si scontrino e degli aerei precipitino e, quindi, che ci siano danni e morti.

Quali sono le difficoltà che si trovano in caso di guerra cibernetica ? Ce ne sono sia per l'attaccante sia per il difensore. Per l'attaccante, a meno veramente di avere in mano tutto del Paese che si attacca, è in realtà molto difficile appurare esattamente il livello di danno sostanziale inferto. Abbiamo danneggiato il Paese o lo abbiamo paralizzato ? Questo dipende da fattori come la ridondanza dei sistemi, la capacità di aggirare l'eventuale paralisi di un sistema attraverso l'utilizzo di altri. Questo era uno dei fattori che veniva adeguatamente preparato all'interno dei sistemi telefonici dalla NATO per rispondere a casi di attacchi massicci nel Patto di Varsavia. Parlo del tentativo di far circolare le comunicazioni attraverso diversi snodi. Conosciamo nel sistema elettrico il tentativo di evitare i *black out* attraverso passaggi diversi della rete elettrica.

È difficile, quindi, capire questo, il livello di ridondanza, e soprattutto la durata dell'effetto attacco, cioè quanto sarà rapido il Paese con i suoi sistemi di emergenza nel bloccare gli effetti dell'attacco e nel ripristinare il funzionamento del sistema. Potrebbe essere anche interesse del Paese ripristinare il funzionamento del sistema, ma non rendere la cosa del tutto visibile mentre si prepara la risposta o la difesa. Questo è un problema per l'attaccante.

Per il difensore, il problema primo e principale è la capacità di attribuire l'attacco a un nemico preciso. Finora è molto difficile. L'attacco condotto a suo tempo contro l'Estonia è stato da questo Paese attribuito alla Russia, ma in realtà non si sa se a un gruppo di *hacker* russi o a un ente ufficiale russo. Il secondo è arrivato dal Brasile. Se, dunque, l'Estonia avesse voluto intervenire per bloccare l'attacco, sarebbe dovuta intervenire contro il Brasile a quel punto, non contro la Russia. La

questione è rimasta aperta persino per l'attacco condotto recentemente contro la Sony in America, che si dice sia stato condotto dalla Corea del Nord. Non si sa se si tratti della Corea del Nord, della Cina o di qualcun altro. Non c'è una firma.

Ora, alcune società dicono di essere in grado, con le apposite tecnologie, di isolare le cellule di emissione. Potrebbe essere che questo sia uno sviluppo ulteriore, che però finora non ho mai visto attuato. Se ci fosse, consentirebbe anche un'efficace dissuasione degli attacchi cibernetici, sia che si tratti di una dissuasione *in kind*, sia che si tratti di una diversa: potrei passare a un'*escalation* e rispondere a un attacco cibernetico strategico con l'uso di armi cinetiche, tradizionali.

Siamo comunque a livello di una grossa difficoltà ed è a mio avviso questa la ragione per cui finora si parla di arma cibernetica soprattutto per il suo uso in contesti operativi militari come funzione di supporto, mentre per l'uso come arma strategica c'è la possibilità, ma viene ancora tenuta un po' arretrata.

L'ultimo punto che vorrei sottolineare di questi scenari di minaccia è uno che faremmo molto male a sottovalutare, perché è quello su cui c'è più esperienza, che viene più usato, ed è lo spazio cibernetico usato come spazio di propaganda: la propaganda militare, in caso di guerra, per la preparazione della guerra e per mantenere il consenso delle popolazioni o per affossarlo è un fatto vecchissimo, fa parte proprio dell'arte della guerra.

Con la diffusione dello spazio cibernetico e dei mezzi a disposizione di tutti i cittadini per entrare nello spazio cibernetico, questo subisce un rigonfiamento enorme, un'esplosione, e rende molto necessaria un'intensificazione di tutto quello che possiamo considerare guerra psicologica, guerra dell'informazione, guerra della propaganda. Su questo – sia a scopo difensivo, sia a scopo offensivo – credo che si giochi gran parte degli equilibri che vedremo nei prossimi anni.

È evidente che tutto questo non è facile. Abbiamo visto anche semplicemente come un uso intelligente e ben mirato della propaganda aiuti i terroristi dell'ISIS e permetta di reclutare in maniera intensa. Ancora di più questo può valere in caso di guerra tra Paesi. Vediamo come funzionano la propaganda e la distorsione delle informazioni in Russia, in Siria e così via. Qui c'è un problema grosso di utilizzazione dello spazio *cyber*, a mio avviso da noi ancora sottovalutato.

L'ultimo punto da ricordare non è una minaccia, come ho già detto, ma la maggiore massa critica delle competenze, oltre che delle tecnologie e degli *hardware*, per un sistema cibernetico all'interno di grandi aziende multinazionali. In genere, hanno un Paese di riferimento, che pone dei grossi problemi di politica se vogliamo difendere questo bene di interesse pubblico in qualche maniera controllato.

Sono molto utili iniziative come quelle prese dall'Unione europea del codice di condotta e simili, ma sono ancora a un livello molto parziale. È chiaro che servirà un approccio anche diplomatico multilaterale per cercare di affrontare questi temi assieme agli Stati Uniti, in particolare, ma anche insieme agli altri Paesi e agli altri grandi attori cibernetici. Credo che comunque l'amministrazione pubblica, lo Stato, dovrebbe compiere un grosso sforzo nel campo della ricerca, dell'investimento, delle competenze, per avere personale effettivamente capace di gestire e di essere aggiornato su questi punti. Questo si fa mantenendo anche canali di ricerca specifici in quei settori, perché i ricercatori sono poi quelli che sanno come funziona il sistema.

Si può cercare di evitare alcune di queste cose chiudendosi all'interno di un sistema proprietario, cioè un sistema non collegato con il resto della rete. Tuttavia, stiamo attenti, perché prima di tutto la mancanza di collegamenti è spesso più apparente che reale. A un certo punto, se si vuole fare agire il sistema proprietario, si deve in qualche maniera metterlo in collegamento. Inoltre, un sistema proprietario è tanto invulnerabile quanto lo sono i singoli utilizzatori e i singoli terminali del sistema stesso.

Quello dell'*intelligence* americana è un sistema proprietario, ma ha oltre 800.000 fruitori, con i necessari livelli di sicurezza, per cui è un sistema proprietario che sembra un colabrodo. Lo abbiamo visto con il caso Snowden o con Wikileaks, e questi sono solo i casi noti, perché sono diventati pubblici.

Sicuramente, una spia che abbia penetrato il sistema non va in pubblico e, molto contenta, « mangia » le sue informazioni. Anche il sistema proprietario, secondo me, non è quindi sufficiente, e comunque deve essere aggiornato e tenuto a livello delle effettive evoluzioni tecnologiche.

PRESIDENTE. Ringrazio il professor Silvestri.

Passo ora la parola al dottor De Zan.

TOMMASO DE ZAN, *Assistente alla ricerca nell'area Sicurezza e difesa dell'Istituto affari internazionali (IAI)*. Prima di cominciare il mio intervento, vorrei ringraziare la Commissione difesa per la possibilità di condividere alcune riflessioni in materia di protezione cibernetica.

Il mio intervento si concentrerà su tre argomenti principali: in primo luogo, su alcuni elementi di analisi dell'economia e della sicurezza cibernetica; in secondo luogo, sugli investimenti pubblici in materia di sicurezza cibernetica, e cercherò di farlo in maniera comparata, ovvero valutando quello che fanno anche alcuni Stati d'interesse per l'Italia; in terzo luogo, cercherò di rapportare all'Italia e di analizzare quanto detto finora dal professor Silvestri e quanto aggiunto con il mio intervento.

Partiamo da alcune considerazioni sull'economia della sicurezza cibernetica. Secondo un recentissimo rapporto del *World Economic Forum*, tra i rischi macroeconomici che gli operatori del settore ritengono siano quelli principali, vi sono la disoccupazione e lo *shock* del prezzo dell'energia. Se si prosegue nella scala, troveremo i fallimenti della *governance* nazionali, le crisi fiscali, le bolle finanziarie, ma anche gli attacchi cibernetici. In un certo senso, questo rapporto consacra, quindi, il rischio cibernetico per chi fa *business* a livello sia nazionale, sia internazionale.

Se si guardano i dati, alcuni Stati e alcune linee di *business* sono più preoccupati per questi attacchi cibernetici. È sicuramente una caratteristica delle economie avanzate. I CEO delle aziende statunitensi e canadesi sembrano essere quelli che temono di più le possibili conseguenze di un attacco informatico ai propri sistemi e alle proprie reti. In Europa, invece, gli Stati più preoccupati sono Estonia, Germania, Olanda e Svizzera. Tra questi non sembra esserci l'Italia. A livello globale, altri operatori particolarmente impauriti da questa situazione sembrano essere soprattutto nell'Asia e nel Pacifico. Non mi stupirei che fossero dei *businessmen* cinesi.

Quali sono i rischi principali ? Soprattutto spionaggio economico, anche portato avanti da attori statali, probabilmente il maggiore oggetto del contenzioso per quello che riguarda le relazioni digitali tra Stati Uniti e Cina; il crimine *on line* con lo scopo di profitto.

Se vogliamo cercare di fornire alcuni dati, alcune stime sui costi del crimine cibernetico mondiale, un recente rapporto dell'UNICRI *(United Nations Interregional Crime and Justice Research Institute)*, un'agenzia ONU con sede a Torino, ha stimato tra i 375 e i 575 miliardi di euro i danni al *business* mondiale. Questo è un dato in aumento rispetto al 2014, quando il CSIS *(Center for* Strategic *and International Studies)*, un centro di ricerca americano di studi strategici, e McAfee avevano stimato intorno ai 445 miliardi i danni.

Un altro dato assolutamente interessante da considerare è che all'interno di aziende e compagnie si impiegano circa 255 giorni a rendersi conto che i propri sistemi sono stati penetrati. Tra gli esempi forse più calzanti, possiamo ricordare Target, che per via di un attacco cibernetico ha perso i dettagli delle carte di credito di 40 milioni dei suoi clienti. Questo ha generato, chiaramente, una caduta delle sue quotazioni e il CEO di Target ha

dovuto dare le dimissioni. Più di recente, una compagnia di telecomunicazioni britannica, Toc Toc, ha perso 53 milioni di dollari in seguito alla perdita di dati dei 156.000 clienti.

In che cosa si sono concentrate queste perdite ? Sicuramente nel fatturato del commercio *on line*, in maggiori chiamate ai *call center* e nei costi legati alla riparazione dei sistemi danneggiati. Un aspetto sicuramente preoccupante è che molti di questi *businessman* credono che il pericolo stia aumentando e non sono convinti di riuscire a sostenere l'innovazione tecnologica in un settore come il *cyber crime*.

Riporto ancora alcuni dati prima di soffermarmi sugli elementi di analisi. Secondo uno studio del *Ponemon Institute*, che ha valutato circa 252 industrie e aziende in sette Stati (Stati Uniti, Russia, Germania, Giappone, Regno Unito, Brasile e Australia), la media dei danni annuali di aziende di grandi e medie dimensioni, ovvero con più di mille dipendenti, è all'incirca sui 7,7 milioni di dollari, con un picco di 15 milioni di dollari per le aziende statunitensi.

Non tutti i settori di *business* sono ugualmente colpiti. I *cyber* criminali sembrano concentrarsi prevalentemente sui settori finanziario ed energetico. Il costo più alto sembra derivare principalmente dall'interruzione dell'attività, quindi, dalla cosiddetta *business disruptive* e, secondariamente, dalla perdita di dati.

Questo serve a fornirvi alcuni valori sulla dimensione dell'economia sulla sicurezza cibernetica. Questi dati ci forniscono un quadro non esaustivo. C'è anche un po' di difficoltà ad accettarli, nel senso che bisognerebbe valutare le metodologie con cui si è arrivati a questi dati. Al di là di ciò, questi dati ci forniscono l'ordine di grandezza di un problema che per essere compreso ha bisogno che siano definiti alcuni criteri di analisi.

Il primo è che oggigiorno lo spazio cibernetico tende ancora a favorire l'attaccante piuttosto che il difensore. Ciò è legato inevitabilmente al problema dell'attribuzione. Ancora oggi, le agenzie di *law enforcement* fanno fatica ad attribuire un determinato attacco a chi l'ha sostenuto. Secondo alcune stime, riusciamo ad arrestare soltanto il 2 per cento di chi ha portato avanti un attacco. Se si pensa a quello che è disponibile oggi *on line*, i costi per chi vuole cominciare a intraprendere il *business* del *cyber crime* sono piuttosto bassi. Basta andare su *You Tube* per trovare dei video in cui si presentano dei primi rudimentali strumenti di *hacking*, con i quali sicuramente non si possono fare penetrazioni informatiche particolarmente sofisticate, ma che possono senza dubbio portare un danno economico.

Vengo al secondo elemento di analisi. A mano a mano che passano gli anni si è sempre più connessi sia a livello individuale che di grandi imprese. Più connessione significa essere connessi all'interno di un *network*, e tutti i *network* possono essere « hackerati » se vengono utilizzati gli strumenti adeguati.

Un terzo elemento di criticità è l'*Internet* mobile e la possibilità di portare all'interno del proprio posto di lavoro il proprio *device*, ad esempio il proprio cellulare, quindi di connettere il proprio dispositivo alle reti all'interno della propria industria o della propria istituzione.

In ultimo, nonostante da due anni gli attacchi cibernetici siano su tutti i giornali, a livello di *business* stanno nascendo o si stanno sviluppando delle unità di sicurezza informatica. Questo vuol dire che non si stanno consolidando, e la differenza è abbastanza sostanziale.

Che cosa si potrebbe fare, quindi, a livello di *business* ? È assolutamente fondamentale costituire una *partnership* tra il pubblico e il privato, in cui si riesca a far incontrare gli interessi di entrambi i settori. A livello aziendale, si deve assolutamente tenere in considerazione che le capacità di un singolo non possono interporsi con le capacità di tutto il *cyber crime*. Questo connubio tra privato e pubblico è assolutamente necessario.

In questo contesto, all'interno di una possibile *partnership* tra pubblico e privato, è assolutamente fondamentale definire dei ruoli e delle responsabilità ben definite, nonché dei meccanismi per la

gestione del rischio. A livello di *business*, si dovrebbe anche cominciare ad accettare il fatto che la sicurezza cibernetica deve entrare a far parte del rischio aziendale: non soltanto il rischio fisico, ma anche il rischio cibernetico. Pertanto, si deve costituire un profilo di gestione di questo rischio. È inevitabile acquisire la giusta *expertise* tecnica.

Questo deve avvenire da un punto di vista sia umano, cioè si deve acquisire l'*expertise* di tecnici informatici, sia da quello degli strumenti tecnologici nella prevenzione di attacchi. In questo caso, sembra esserci una correlazione positiva nella prevenzione degli attacchi informatici tra chi utilizza strumenti di *cyber intelligence* e chi non lo fa. Ora vorrei passare ad alcune valutazione sugli investimenti statali, partendo dagli Stati Uniti. Nel 2014, per quello che era il bilancio federale, gli Stati Uniti investivano 9 miliardi di dollari. All'inizio di febbraio, per il *budget* fiscale del 2017, Obama ha proposto invece 19 miliardi di dollari, un incremento del 110 per cento rispetto al 2014. Quest'incremento del *budget* per la *cyber security* è aumentato costantemente dal 2014 in poi: del 37 per cento nel 2015, del 55 per cento nel 2016 e del 110 per cento nel 2017, se il *budget* verrà approvato.

È importante anche definire in che cosa si investe, non soltanto la quantità di denaro che si investe. La scelta degli Stati Uniti è quella di investire molto nel Dipartimento della difesa, a cui vengono allocati circa 5,5 miliardi di dollari. Nonostante questo, secondo alcuni studi ufficiali all'interno dell'amministrazione americana, i fondi allocati non sono abbastanza, perché si crede di far fatica a stare dietro all'innovazione tecnologica. Oltre a questo, bisogna comunque fare delle riflessioni su che cosa viene investito, come ho detto. Nel 2016, l'America ha investito in sistemi di rilevamento delle intrusioni.

Spostandoci verso l'Europa, la Francia, che si è dotata di una nuova strategia nazionale cibernetica nell'ottobre 2015, ha stanziato a partire dal 2014 circa un miliardo di euro l'anno. Ha investito principalmente in strumenti per comunicazioni sicure, tecnologia per la criptazione e sistemi per la sorveglianza dei *copy network*. Oltretutto, ha deciso che circa il 40 per cento di questo *budget* sarebbe andato alle aziende francesi strategiche.

Passando alla Gran Bretagna, Osborne ha confermato (a novembre 2015) circa 2,5 miliardi di euro per la sicurezza cibernetica. Secondo le stime britanniche, è un incremento del 76 per cento rispetto all'ultima revisione della spesa. Anche qua, in cosa si è investito? Circa 20 milioni di euro sono stati stanziati per un nuovo centro di eccellenza e circa 165 milioni per la formazione di nuove *start up* nel settore.

Ora, se si vuole paragonare la spesa per la sicurezza cibernetica in termini di spesa per la tecnologia informatica, gli Stati Uniti spendono il 16 per cento; Singapore ha deciso che spenderà circa il 10 per cento, come la Corea del Sud, mentre Israele l'8 per cento. In questo contesto, c'è anche l'Italia, che non è isolata dal resto del mondo e non è un'isola felice. Gli attacchi informatici ci sono anche nel nostro Paese.

Secondo Microsoft, l'Italia ha riportato un tasso di esposizione ai *malware* pari al 19 per cento della media mondiale, contro una media di Stati Uniti, Inghilterra e Francia compresa tra il 12 e il 13 per cento. Di questi attacchi informatici che l'Italia subisce, la maggior parte è ascrivibile ai fenomeni di crimine cibernetico (circa il 93 per cento), mentre il restante 7 per cento proviene da quegli attori che mirano prevalentemente alla ricerca di dati sensibili a livello di *intelligence*.

Quali sono, invece, i costi per l'Italia? Se si legge il decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, che getta un po' le fondamenta del nostro quadro strategico e del piano nazionale, da tale decreto non dovevano derivare oneri aggiuntivi al bilancio dello Stato. Di recente, sembra siano stati allocati circa 150 milioni di euro nella legge di stabilità, anche se non è ancora chiarissimo come lo saranno, a parte circa 15 milioni per la Polizia postale.

A mio giudizio, sembra chiaro che l'Italia abbia bisogno di investire in questo settore, ma ancora più importante è investire e avere delle logiche di valutazione di come avvengono questi investimenti. Non credo che l'Italia possa più permettersi di investire senza valutare se quest'investimento porta a vantaggi veri in termini di protezione dello spazio cibernetico.

PRESIDENTE. Grazie, dottor De Zan per questo ulteriore apporto. Do ora la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

LUIGI LACQUANITI. Ringrazio i componenti dell'Istituto.

La domanda che rivolgo, in particolare al professor Silvestri, piuttosto generale, è in ordine alla definizione di spazio cibernetico che ci ha fornito. Ha specificato che non si tratta di bene comune, ma di bene di interesse pubblico. Giudico molto interessante questa definizione.

Proprio in ragione dell'evoluzione della materia che stiamo trattando, dell'importanza che ha assunto oggi e che sempre più andrà ad assumere in futuro, a suo giudizio si può pensare che nell'evoluzione della giurisprudenza si possa avere un'estensione del concetto di bene comune anche allo spazio cibernetico ?

Inoltre, ha dato una definizione di attacco di guerra come di attacco bellico. Mi rendo conto che la domanda è complessa, perché si tratta di giurisprudenza ed in ambito internazionale è tutto molto più complesso. In ogni caso, si può pensare, anche in ragione dell'evoluzione del concetto di spazio cibernetico e di attacco cibernetico, che il diritto internazionale possa ricomprendere nell'ambito degli attacchi di guerra anche attacchi che utilizzino lo spazio cibernetico, ma che non comportino quelle conseguenze che ha elencato, come il decesso del cittadino o del componente della Forza armata e la distruzione di un bene immobile, di un bene patrimoniale, di un bene di uno Stato estero ?

PRESIDENTE. Vorrei porre una domanda anch'io a entrambi i nostri ospiti.

Mi ha colpito molto, così come all'onorevole Lacquaniti, la trattazione di bene comune e di bene di interesse pubblico. Nella sua valutazione – per motivi storici o, forse, per incapacità di tutte le Nazioni, non esclusivamente la nostra – non si è vista la rete informatica come qualcosa che sia solamente nel futuro, ma diventi estremamente necessaria per lo sviluppo di una civiltà. La maggior parte dei sistemi, specialmente in Italia, sono di proprietà privata. Nella sua audizione, il professor Baldoni segnalava, come penso sia abbastanza noto, che noi siamo uno dei pochi Paesi al mondo, tra i grandi, che non ha una proprietà pubblica della rete infrastrutturale.

La mia domanda tocca sia la parte di *business*, sia quella concettuale: che tipo di concessione sia normativa sia di *business* e, quindi, di facilitazione al *business*, si deve realizzare come Paese o introdurre nel Paese per ripristinare questo livello, a mio modo di vedere, di sovranità ?

Inoltre, vorrei un minimo di valutazione sulle ridondanze. Lei ha condotto un ragionamento molto acuto sul fatto che, in caso di attacco, non vadano mostrate le proprie ridondanze. Il problema è che questo Paese, e penso proprio all'Italia, dal 1999, cioè da quando Telecom ha cambiato volto, ha dismesso a livello nazionale tutto quel sistema di ridondanze di cui si era dotato con le tasse che gli italiani avevano pagato. Telecom aveva normalmente, anche in situazioni non cittadine, tre ridondanze con sistemi diversi. Ebbene, quanto tempo occorrerà per ritornare ad avere quell'autonomia fondamentale ? Lei ha detto una cosa molto precisa: che si dipende assolutamente dalla gestione di un altro attore.

Mi riallaccio, infine, alla parte dei ricercatori. Credo che la Commissione abbia fatto benissimo a deliberare questa indagine conoscitiva che costituisce un primo punto di partenza, anche a livello nazionale, per definire concetti e operatività anche da un punto di vista più elevato di

decisione politica. Che impatto avremo ? Che tempi ci vorranno, lavorandoci in maniera robusta fin da ora ?

Infine, la disparità di investimenti con gli Stati che ci sono vicini, Inghilterra, Francia – non parlo degli Stati Uniti o di Israele – è spaventosa. Anche da parte nostra deve essere importante questa consapevolezza. Se si pensa agli importi degli Stati Uniti rispetto all'effettivo bilancio sulla difesa – gli Stati Uniti hanno un bilancio di circa 500 miliardi di euro l'anno e oltre – 19 miliardi non sono così impattanti, gravosi per uno Stato in prospettiva rispetto a quello che può essere uno strumento così importante.

Do la parola ai nostri ospiti per la replica.

STEFANO SILVESTRI, Past president *e membro del comitato direttivo dell'Istituto affari internazionali (IAI)*. Non vorrei togliere lavoro e, soprattutto, non vorrei dare opinioni che mi provochino l'ira del mio collega, professor Ronzitti, che si occupa di diritto internazionale e di questi aspetti in tempi di diritto nell'Istituto. Prendete, quindi, le mie osservazioni come quelle di un laico in questa situazione. Tra l'altro, su questi problemi della *cyber security* stiamo preparando una nota proprio per il Servizio Studi della Camera, che consegneremo un po' prima della fine del mese, e che tratterà alcuni di questi problemi.

Quanto alla domanda se è possibile un'evoluzione dello spazio cibernetico a bene comune, occorre considerare che un bene comune o è comune o non è, nel senso che l'aria, l'alto mare, questo genere di cose sono beni comuni. È tuttavia possibile stabilire delle regole a cui attenersi. Per lo spazio esterno, per esempio, abbiamo stabilito alcune regole in termini di non messa in orbita di armamenti nucleari e di alcuni altri tipi di interventi nello spazio esterno, augurandoci che siano rispettate, ma comunque sono regole che valgono a tentare di mantenere questo spazio a disposizione. Oggi stiamo arrivando al punto in cui è talmente alto il numero dei detriti nello spazio esterno e di quelli che potrebbero crescere se continuano le sperimentazioni delle armi antisatellite, che ormai comincia a essere urgente una legge comune per la pulizia dello spazio esterno.

Sapete quanta resistenza c'è per la messa in orbita dei cosiddetti satelliti spazzini, perché si teme che divengano armi anti-satellite rispetto a satelliti che invece funzionano, non solo rispetto ai detriti. Bisognerà arrivare a una gestione probabilmente non nazionale, ma per esempio delle Nazioni Unite, di questi sistemi tale che consenta la migliore utilizzazione dello spazio esterno.

Secondo me, con lo spazio cibernetico bisogna cercare di avanzare in questa direzione, cioè un sistema di regole e di leggi. Per questo avevo sottolineato l'importanza del codice di condotta, che è volontario, ha una serie di limiti, ma pone problemi. Da quello si può poi evolvere verso una situazione negoziale che arrivi a fare questo.

In ogni caso, credo che sarebbe importante – il codice di condotta è un aiuto in questo senso, ma non è il solo – che si approvino strumenti legali, come trattati e accordi, che riconoscano l'importanza dell'interesse comune su questo bene e riconoscano esplicitamente un impegno in direzione del rispetto, perlomeno in condizioni non di guerra, degli interessi comuni di tutti. Questo non è ancora un bene comune, ma è un passo avanti importante, che a mio avviso è interessante. Su questo stiamo riflettendo. Non appena avremo qualcosa di scritto, di valutato, ve lo manderemo.

Il livello delle ridondanze è una delle poche forme di difesa che c'è. Evidentemente, le ridondanze costano. Fino a che c'era la mano pubblica che pagava le ridondanze c'erano. Nel momento in cui la mano pubblica non paga, le ridondanze vengono utilizzate e non ci sono più.

Qui il problema è capire quanto vogliamo investire nella nostra sicurezza. Credo che ci siano poche alternative, in questo caso, alla mano pubblica e al fatto che bisogna pagare per mantenere in funzione delle ridondanze. Si può cercare di

pagare il meno possibile, di vedere come queste possano favorire anche il *business* e, quindi, di non pagarle per intero, ma in qualche misura secondo me bisognerà arrivare a questo.

Certo, la privatizzazione del sistema, da questo punto di vista, aumenta la possibilità di vulnerabilità, ma aumenta anche il numero degli attori e, in quanto tale, potrebbe determinare l'esistenza di nuovi tipi di ridondanze, che potrebbero facilitare anche la sicurezza. Comunque, questa è un'analisi che andrà sicuramente fatta. Qualunque sia l'autorità di riferimento per la sicurezza nazionale, credo che questa debba essere probabilmente la prima preoccupazione. Non possiamo risolvere i nostri problemi di vulnerabilità all'improvviso, ma possiamo perlomeno cercare di attenuarne gli effetti.

TOMMASO DE ZAN, *Assistente alla ricerca nell'area Sicurezza e difesa dell'Istituto affari internazionali (IAI)*. Per quello che riguarda il rapporto tra gli operatori critici, strategici, nazionali e lo Stato, sicuramente si deve pensare a delle forme di *partnership* tra pubblico e privato. In questo senso, si potrebbero svolgere delle analisi su che cosa è stato fatto negli altri Paesi, come negli Stati Uniti.

È evidente che c'è un problema di questo genere, soprattutto perché in Italia la maggior parte degli assetti critici è in mano ai privati, ma non è un problema solo italiano. Lo hanno anche altri Paesi in Europa. Adottare una visione su quello che dovrebbe essere il rapporto tra il pubblico e il privato diventa un elemento fondamentale. Modelli ce ne sono parecchi. Andrebbero solamente analizzati e poi implementati, secondo me, a livello nazionale.

Per quello che riguarda il tema delle ridondanze, lo studio che stiamo realizzando per il Parlamento si concentrerà soprattutto sull'argomento delle sovrapposizioni tra i moltissimi enti e istituzioni a livello pubblico che hanno determinati ruoli. Un secondo aspetto su cui si concentrerà lo studio è il tema della *governance*.

Tutto questo deve essere considerato insieme agli investimenti. Non credo che si possano considerare le cose in maniera separata. Come ha detto il professor Silvestri, credo che sia tutta una questione di divisione: quanto vogliamo essere protetti, tenuto conto che non potremo mai esserlo al cento per cento, quanto perlomeno vogliamo attenuare questo rischio.

In un possibile movimento di riconsiderazione della politica cibernetica, va anche tenuto conto del fatto che implementazione non vuol dire necessariamente raggiungimento degli obiettivi. Questo vuol dire che va bene istituire una matrice di valutazione dell'implementazione di piani nazionali, ma forse un'altra domanda che dovremmo porci è se stiamo veramente ottenendo gli obiettivi di sicurezza che ci eravamo preposti.

PRESIDENTE. Ringrazio il professor Silvestri e il dottor De Zan per il loro contributo alla nostra indagine conoscitiva e dichiaro conclusa l'audizione.

La seduta termina alle 12.05.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. RENZO DICKMANN

Licenziato per la stampa il 29 aprile 2016.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO