SENATO DELLA REPUBBLICA **CAMERA DEI DEPUTATI**

XVII LEGISLATURA

Doc. XXXIV
n. 7

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

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

(composto dai senatori: *Stucchi,* Presidente; *Giuseppe Esposito*, Vicepresidente; *Casson,* Segretario; *Crimi, Marton* e *Paolo Romani* e dai deputati: *Ferrara, Guerini, Rosato, Speranza, Tofalo* e *Villecco Calipari*)

RELAZIONE SULLE PROCEDURE E LA NORMATIVA PER LA PRODUZIONE ED UTILIZZAZIONE DI SISTEMI INFORMATICI PER L'INTERCETTAZIONE DI DATI E COMUNICAZIONI

(Relatori: senatore Giuseppe ESPOSITO e deputato Angelo TOFALO)

approvata nella seduta del 13 febbraio 2018

Trasmessa alle Presidenze delle Camere il 13 febbraio 2018

TIPOGRAFIA DEL SENATO

Senato della Repubblica Camera dei Deputati

Comitato Parlamentare per la sicurezza della Repubblica
Il Presidente

Roma, 13 febbraio 2018
Prot. n. 3106/CSR

Caro Presidente,

il Comitato che presiedo ha approvato all'unanimità la Relazione sulle procedure e la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni.

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

In adempimento del voto espresso dal Comitato mi onoro, pertanto, di trasmettere la relazione a Lei e al Presidente della Camera dei deputati.

L'occasione mi è gradita per rinnovarLe i sensi della mia più alta considerazione.

Con vivo cordialità!

Giacomo Stucchi

Sen. Pietro GRASSO
Presidente del
Senato della Repubblica

Senato della Repubblica Camera dei Deputati

Comitato Parlamentare per la sicurezza della Repubblica
Il Presidente

Roma, 13 febbraio 2018
Prot. n. 3106/CSR

Gent.ma Presidente,

il Comitato che presiedo ha approvato all'unanimità la Relazione sulle procedure e la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni.

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

In adempimento del voto espresso dal Comitato mi onoro, pertanto, di trasmettere la relazione a Lei e al Presidente del Senato della Repubblica.

L'occasione mi è gradita per rinnovarLe i sensi della mia più alta considerazione.

Con viva cordialità!

Giacomo Stucchi

On. Laura BOLDRINI
Presidente della
Camera dei Deputati

INDICE

1. GENESI, CONTENUTI E FINALITÀ DELL'INDAGINE . . . . . *Pag.* 8

2. SINTESI DELLE AUDIZIONI SVOLTE DAL COMITATO . . . . . » 10

2.1. Audizioni del mondo istituzionale e accademico . . . . . » 10

2.2. Audizioni delle società e degli operatori . . . . . » 21

3. CONCLUSIONI E PROPOSTE . . . . . » 33

1. Genesi, contenuti e finalità dell'indagine

L'indagine è stata deliberata il 30 giugno 2016, con la finalità di ricostruire il quadro generale delle procedure e dei sistemi di controllo attivati nei confronti dei sistemi informatici invasivi e delle società che li producono, allo scopo di individuare gli strumenti normativi più idonei alla tutela della sicurezza informatica del Paese.

Sono stati designati quali relatori, il vice presidente, senatore Giuseppe Esposito e il deputato Angelo Tofalo.

Il Comitato ha convenuto sull'opportunità che fossero auditi soggetti istituzionali, soggetti provenienti dal mondo accademico e operatori privati. Il ciclo delle audizioni ha preso avvio con i funzionari provenienti dal Dipartimento delle informazioni per la sicurezza (DIS) e dalle Agenzie. Per il DIS il dottor Savio, presidente della Commissione ICT, e il dottor Valensise, responsabile dell'Ufficio centrale per la segretezza (UCSe); per l'Agenzia informazioni e sicurezza esterna (AISE), il vice direttore Caravelli; per l'Agenzia informazioni e sicurezza interna (AISI), il dottor Aimola, capo reparto contro la minaccia cibernetica. Altri soggetti istituzionali auditi sono stati: l'ammiraglio Simoncini, capo del Reparto informazioni e sicurezza dello Stato maggiore della difesa (RIS); il dottor Di Legami, direttore della Polizia postale e delle comunicazioni; il generale Vecchione, comandante delle Unità speciali della Guardia di finanza.

Queste audizioni si sono rivelate utili ai fini della costruzione della cornice giuridica della questione a partire dal decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, nota come «decreto Monti», fino ad arrivare al recente decreto sulla tutela dello spazio cibernetico che era in fase di elaborazione nel periodo in cui si sono svolte le audizioni. Ogni audito ha illustrato la minaccia cibernetica e il lavoro svolto dalla propria struttura di appartenenza e ha fatto considerazioni sul caso Hacking Team e sull'utilizzo del *software* Galileo.

Il Comitato ha svolto poi due audizioni di soggetti provenienti dal mondo accademico, il professor Baldoni e il professor Teti. Queste audizioni hanno fornito uno sguardo più ampio sulla minaccia cibernetica e sugli strumenti per contrastarla e sono state l'occasione per acquisire elementi utili al fine di comprendere la direzione da prendere, nei limiti delle attribuzioni di questo Comitato, per migliorare normativa e strumenti in materia.

Si sono altresì svolte le audizioni degli operatori di telecomunicazioni che hanno visto intervenire i rappresentanti di Telecom, Vodafone e Wind Tre.

Successivamente, si è tenuta l'audizione del sostituto procuratore di Milano, dottor Alessandro Gobbis, responsabile del procedimento che vede coinvolta Hacking Team.

Si è svolta quindi la serie di audizioni delle società produttrici di strumenti di captazione con Area, IPS, SIO, Cyber Intuition, proseguita nelle settimane successive con Hacking Team, Sind, Reaqta, RCS Lab, CSH&MPS, Cy4Gate, ITD Solutions e Yarix.

Infine, è stato audito il dottor Diego Piacentini, commissario per l'attuazione dell'Agenda digitale.

Le principali tematiche trattate ed emerse nel corso di questo articolato ed approfondito percorso di audizioni – di cui nel capitolo successivo si fornirà una sintesi – possono così riassumersi:

– l'evoluzione del quadro normativo in materia di sicurezza cibernetica: dal decreto del Presidente del Consiglio dei ministri 24 gennaio 2013 al decreto del Presidente del Consiglio dei ministri 17 febbraio 2017;

– il ricorso ed il funzionamento dei captatori utilizzati per intercettazioni e la necessità di un intervento legislativo;

– gli aspetti concernenti le possibili misure di prevenzione e di verifica necessarie per elevare il grado di affidabilità delle aziende produttrici di *software*, a fronte di tentativi di intrusione sull'esempio di quelli subiti dalla Hacking Team. Fra le ipotesi operative, è stata fra l'altro prospettata la creazione di un albo qualificato, con relativa certificazione, delle aziende operanti nel settore che dovrebbero pertanto possedere determinati requisiti di sicurezza. In tale ambito si è ipotizzata la costituzione di un organo al quale affidare il compito di controllare le aziende;

– la complessità di una situazione in cui la nostra *intelligence* e gli altri soggetti istituzionalmente impegnati nella difesa dai rischi cibernetici sono chiamati ad un rilevante impegno di innovazione e crescita per fronteggiare adeguatamente la rapida e pressoché ininterrotta evoluzione degli strumenti tecnologici;

– l'esigenza di accrescere il volume degli investimenti e delle risorse personali, tecnologiche e finanziarie anche nell'ottica di tutelare il principio della sovranità nazionale nel campo della sicurezza cibernetica;

– alcune possibili contromisure alla crescenti minacce di tipo cibernetico: creazione di un eco-sistema *cyber* nazionale; formazione di una rete che preveda la collaborazione ed interazione tra settore pubblico, mondo privato ed accademico in modo da rafforzare la cultura della sicurezza informatica.

2. Sintesi delle audizioni svolte dal Comitato

2.1. Audizioni del mondo istituzionale e accademico

Audizione del presidente della Commissione permanente Information Communication Technology *del Dipartimento delle informazioni per la sicurezza, dottor Enrico Savio, seduta n. 223 del 26 luglio 2017*

Con l'audizione del dottor Savio, presidente della Commissione permanente *Information Communication Technology* del Dipartimento delle informazioni per la sicurezza ha preso avvio l'«indagine conoscitiva sulle procedure e la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni».

Il dottor Savio, nell'immaginare il perimetro delle attività dell'indagine conoscitiva, ha individuato due dimensioni da prendere in considerazione: la prima è quella delle aziende come possibili fornitrici di beni o di servizi (con riferimento all'area della IT e della ICT più ampiamente intesa); la seconda è quella delle aziende come *target* possibili da difendere rispetto a contesti che possono incidere sull'interesse nazionale, e quindi tramutarsi in una esigenza di sicurezza nazionale.

L'evoluzione rapidissima della dimensione cibernetica ha indirizzato la riflessione, in particolare a partire dal 2010-2011, in un'ottica di sviluppo di una via italiana alla *cyber security*, fino all'elaborazione del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, che ha modellato inizialmente il quadro strategico nazionale e l'infrastruttura cibernetica nazionale.

L'esistenza di molti ambiti di competenza, anche di carattere specifico, non sempre comunicanti tra di loro, e, per altro verso, la trasversalità, l'asimmetricità e la concentrazione nel tempo della minaccia cibernetica, hanno determinato la necessità di costruire una visione più unitaria e il più possibile coordinata del contesto in cui operare.

Con riferimento più specifico al tema dell'indagine conoscitiva, il dottor Savio ha evidenziato la necessità di approfondire gli aspetti di carattere giuridico, considerato che la velocità delle *performance* delle tecnologie e l'adeguamento normativo non vanno di pari passo.

Al riguardo, la necessità di un bilanciamento, da un lato, delle capacità di difesa e, quindi, dei doveri dello Stato (sicurezza e legalità, *in primis*) e, dall'altro, dei diritti dei cittadini (quindi, *privacy* ma anche libertà di movimento sulla rete), inducono a riflettere su alcuni elementi che preludono al tema tecnologico, uno dei quali è dato dall'evoluzione della tutela.

Nel quadro attuale, le capacità intrusive che gli organismi hanno per le finalità istituzionali sono bilanciate in un rapporto tra proposizione dell'esecutivo e valutazione di un organo giudiziario indipendente.

Il dottor Savio, in merito, ha segnalato al Comitato, quale tema a monte rispetto a quello dell'applicazione tattica degli strumenti di legge, quello della legittima difesa cibernetica, considerando che, in tale ambito,

si rischia di anticipare il momento della prevenzione, perché il tempo, in una minaccia cibernetica, è cruciale per la capacità di risposta, per evitare o contenere il danno (eventuale servizio sospeso, furto di beni privatissimi come le identità piuttosto che del *know how* industriale, fino a danni rilevanti per la sicurezza nazionale).

L'eccesso di «anticipo nella difesa» rischia però di trasformarsi in attacco preventivo, circostanza che pone seri interrogativi dal punto di vista della legittimità, addirittura, costituzionale del tema, poiché è la tipizzazione delle condotte che consente agli apparati di informazione e sicurezza del comparto *intelligence* nazionale di orientarsi nel quadro di riferimento della minaccia cibernetica.

Il dottor Savio ha fatto presente che il dibattito su tale tematica è molto aperto anche in ambito internazionale. Si pone poi l'interrogativo del limite fino a cui spingere l'attività preventivo-proattiva e del rischio legato ad un'accentuazione della componente tecnologica non opportunamente guidata sul piano normativo. In tal senso, si è evidenziata la necessità di uscire da una logica emergenziale, cioè legata agli eventi, per introdurre, invece, l'elemento securitario nella dimensione cibernetica in una modalità sostanzialmente permanente.

Il dottor Savio si è poi soffermato sul caso della Hacking Team e sulla riflessione che ne è scaturita, relativa alla creazione di un albo nazionale delle aziende, una sorta di certificazione del possesso di determinate caratteristiche, non solo in termini di *performance* tecnologica per l'offerta al mercato, ma anche di resilienza rispetto al mercato stesso, data l'entità delle obbligazioni commerciali che queste aziende contraggono con i loro clienti.

La dimensione cibernetica, inoltre, è pienamente connessa alla minaccia terroristica, poiché utilizzata sia come mezzo di reclutamento, che come mezzo di propaganda del messaggio radicale di supporto logistico connettivo.

L'ultimo aspetto di minaccia, evidenziato nell'audizione, riguarda la fenomenologia *cyber* definita di tipo «ribellista», Anonymous tra tutti, che va considerato con attenzione, perché al di là dei danni che può produrre o delle azioni contrarie all'ordinamento che possono essere poste in essere, esso ha un effetto trascinatore, poiché è un *brand* particolarmente accattivante, quale area di possibile reclutamento di risorse *hacker*.

Per quanto riguarda il ruolo della Commissione ICT, l'audito ha ricordato al Comitato l'esistenza di un quadro strategico nazionale di sicurezza cibernetica. Tale ruolo ha portato la Commissione ad avvalersi di professionalità tecnologiche, guardando anche al reclutamento dei nativi digitali perché, sia per le attività TECHINT, ovvero la raccolta di informazione in modalità tecnologica (tipo gli strumenti di intrusione), sia per le attività HUMINT, quali la raccolta da fonti o canali di informazione, il linguaggio è destinato a mutare.

Il dottor Savio ha sottolineato inoltre che l'investimento sui nativi digitali è un elemento fondamentale, poiché essi avranno, sul piano delle operazioni, una dialettica completamente diversa, oltre alla capacità di

comprendere le evoluzioni tecnologiche rispetto alla *value proposition* delle aziende alle quali si fa riferimento.

Il dottor Savio ha illustrato altresì il lavoro svolto dalla Commissione interorganismi ICT, istituita nel 2014, che, oltre a concertare con i direttori delle Agenzie e coordinare le attività in ambito cibernetico, si occupa anche dell'approvvigionamento e della gestione delle dotazioni tecnologiche. L'unitarietà della gestione, necessaria a causa della trasversalità e transnazionalità della minaccia *cyber*, ha comportato una razionalizzazione del lavoro e delle spese. La Commissione cura inoltre i rapporti con i SOC *(Special Operation Center)* di società e aziende di interesse nazionale in modo da creare una rete e monitorare gli attacchi.

Audizione del dirigente dell'Ufficio centrale per la segretezza del DIS, dottor Bruno Valensise, seduta n. 229 del 14 settembre 2016

Il dottor Valensise ha inizialmente descritto il funzionamento e le competenze dell'Ufficio centrale per la segretezza, che sono: l'area affari giuridici internazionali, cui attiene, fra le altre cose, la tutela amministrativa del segreto di Stato; l'area che partecipa allo studio e alla produzione di norme in materia di tutela di informazioni classificate, cui è assegnata anche la competenza sulla stesura di accordi generali di sicurezza, in particolare con i Paesi esteri con i quali è necessario scambiare informazioni classificate; le attività propedeutiche al rilascio delle abilitazioni di sicurezza personali e industriali.

Quest'ultimo argomento è stato trattato ampiamente, anche alla luce delle norme contenute nei decreti del Presidente del Consiglio dei ministri del 6 novembre 2015, recanti rispettivamente la disciplina della firma digitale dei documenti classificati e le disposizioni per la tutela amministrativa del segreto di Stato, delle informazioni classificate e a diffusione esclusiva, sui quali questo Comitato ha espresso parere favorevole l'8 e il 22 luglio 2015.

Il dottor Valensise ha evidenziato che uno degli obiettivi della revisione di queste procedure era quello di semplificare il rapporto con le imprese, aiutandole a cercare di perseguire le prospettive del *business*, sia a livello nazionale che internazionale, in una cornice di sicurezza adeguata.

Le misure di semplificazione sono state attuate, tra l'altro, anche con una riscrittura della modulistica, che riporta informazioni necessarie e utili in tema di richiesta di abilitazioni di sicurezza personali e industriali.

Il dottor Valensise ha risposto alle domande dei commissari e ha spiegato le procedure per la concessione del NOS, del NOSI e del NOSIS.

Si è soffermato in particolare sui controlli effettuati verso coloro che detengono le abilitazioni di sicurezza, citando l'attività di istruzione alla sicurezza che prevede che i funzionari della sicurezza semestralmente convochino i soggetti abilitati, al fine di istruirli sul perimetro di sicurezza nel quale operano.

Il dottor Valensise ha poi svolto alcune considerazioni sul caso Hacking Team e ha risposto alle numerose domande dei commissari sul tema.

Infine ha risposto a quesiti sulla gestione della documentazione classificata nel caso di richieste da parte della magistratura, sulla collaborazione con il Ministero degli affari esteri e della cooperazione internazionale e con l'Unità per le autorizzazioni dei materiali d'armamento, e sulle peculiarità delle gare di appalto classificate.

Audizione del capo Reparto contro la minaccia cibernetica dell'AISI, dottor Massimo Aimola, seduta n. 232 del 22 settembre 2016

Il dottor Massimo Aimola ha aperto la sua relazione fornendo alcuni chiarimenti tecnici sul funzionamento del *software Remote Control System* (RCS), particolarmente adatto ai sistemi di vigilanza, poiché caratterizzato dalla capacità di organizzare il pacchetto di *file* da esfiltrare, eludendo i meccanismi difensivi dei *target*, che operano in difesa con i *firewall*, l'antivirus e le sonde.

Ha quindi descritto le procedure di risposta agli attacchi con il fine di esfiltrazione di dati e si è soffermato in particolare sulle modalità per contrastare le tecniche di anonimizzazione degli attaccanti per rintracciarne il vero IP *(Internet Protocol address)*.

Ha altresì illustrato alcune pratiche di difesa preventiva messe in atto dal Reparto contro la minaccia cibernetica dell'AISI, in cooperazione con il reparto omologo dell'AISE, come l'utilizzo di *honeypot*, o, nel caso del terrorismo jihadista, le tecniche di infiltrazione e di individuazione e «pedinamento» dei soggetti attivi nella propaganda e nel reclutamento *on line* e di infiltrazione.

Il dottor Aimola ha approfondito, anche in risposta ad alcuni quesiti dei commissari, la vicenda degli attacchi sferrati a importanti amministrazioni centrali di vari Paesi europei dal gruppo di *hacker* APT28 e ha illustrato a grandi linee la scena *hacker* e dell'attivismo *on line* nazionali.

L'audito ha approfondito le modalità procedurali e la connessa problematica della violazione degli *account* di posta elettronica, evidenziando che tali attacchi mirano più alla profilazione dei soggetti in termini di dati da utilizzare, piuttosto che alla sottrazione di materiali.

Il dottor Aimola ha quindi sottolineato l'importanza di investire risorse nell'ambito *social*, studiando il comportamento di *influencer*, realtà oggi molto estesa e significativa.

I commissari hanno poi rivolto all'audito una serie di quesiti di tipo tecnico sulle modalità di intercettazione, relativi all'utilizzo delle garanzie funzionali in ambito *cyber* nonché di tipo giuridico sul rapporto tra sicurezza e libertà fondamentali.

Sotto il primo profilo, in particolare, è stato fatto riferimento alle questioni relative agli sviluppi sul piano della crittografia in termini di acquisizione di risorse adeguate, sotto il secondo profilo è stato trattato il problema della conservazione o costituzione di banche dati sulle intercet-

tazioni telematiche, tematica questa sulla quale si ritiene di dover intervenire sul piano normativo.

Audizione del vice direttore dell'AISE, dottor Giovanni Caravelli, seduta n. 238 del 12 ottobre 2016

Il dottor Caravelli ha introdotto le tematiche da trattare nell'audizione: il *cyberspace* e il ruolo dell'*intelligence*, il quadro normativo e l'organizzazione dell'Agenzia, le capacità operative sviluppate in ambito *cyber* e l'utilizzo dello strumento SIGINT a supporto della *cyber defence*, l'attività di *lawful interception* nell'ambito della *cyber defence* – (le intercettazioni preventive) –, le operazioni cibernetiche, la produzione informativa realizzata in cooperazione con l'AISI, con altri attori istituzionali italiani e con i Servizi collegati esteri e, infine, l'attività informativa inerente a minacce *cyber* e la visione dell'AISE sullo sviluppo e sull'evoluzione in questo settore.

Ha quindi menzionato le strutture che si occupano della sicurezza cibernetica, – CYBINT, e INFOSEC nel reparto «Ricerca e protezione tecnologica» e SIGINT e GEOINT nel reparto «Ricerca elettronica» –, come riorganizzate con il decreto del Presidente del Consiglio dei ministri 10 agosto 2016, n. 2.

Il potenziamento derivante dal cambio strutturale si è indirizzato su tre aree di lavoro: le attività info-operative di ausilio al contrasto delle minacce tradizionali; la difesa e la prevenzione della crescente minaccia *cyber*; l'aggiornamento tecnologico e delle risorse umane.

Le capacità che l'Agenzia impiega sono riconducibili al settore HUMINT, sia convenzionale che virtuale (possibilità di creare delle identità – avatar, che operano come vere e proprie persone fisiche), al settore WEBINT, allo sviluppo di strumenti operativi tecnologici che permettano la *lawful interception*, principalmente attraverso l'esame del traffico nazionale, alla SIGINT a supporto della difesa cibernetica (individuazione di possibili attacchi e scambio di informazioni con i Servizi collegati) e alle operazioni speciali nel ciberspazio.

Queste ultime operazioni sono state illustrate dall'audito nello specifico: *digital investigation*, *computer network exploitation* (CNE) ovvero controllo remoto delle risorse informatiche e *computer network attack* (CNA), ne è stato descritto il funzionamento, anche con esempi di attacchi reali, avvenuti o sventati, a compagini industriali nazionali o estere e ad infrastrutture strategiche; infine, è stato spiegato come avviene il monitoraggio della minaccia in profondità e come si attuano le tecniche di anonimizzazione.

Con riferimento al *cyber crime* il dottor Caravelli ne ha evidenziato la velocità della crescita, che rende necessario, in stretto coordinamento con l'AISI, un continuo monitoraggio ed una complessa attività di ricerca sul *web*, con un'analisi di dettaglio dei tipi di minacce in relazione alle quali devono essere determinate le varie attività informative.

Al termine, le domande dei commissari hanno toccato tutti gli argomenti della relazione, riguardanti gli strumenti per l'indentificazione del «nemico» e la creazione di *database* dedicati, la rete degli organismi pubblici, parapubblici o privati che attuano procedure di *cyber defence* in Italia, la tipologia di *software* utilizzati per i captatori informatici, l'impiego di risorse finanziarie per la *cyber security.*

Audizione del direttore del Centro di Ricerca in cyber intelligence and information security *presso l'Università di Roma «La Sapienza», professor Roberto Baldoni, seduta n. 241 del 25 ottobre 2016*

L'audizione del professor Baldoni è cominciata con una breve storia dell'evoluzione del *cyber* spazio e della minaccia alla sicurezza cibernetica.

Il professore ha descritto il fenomeno rappresentato dalla rivoluzione degli *smartphone* che, creando le condizioni per un'interconessione continua, non solo ha coinvolto le relazioni umane, ma anche tutti i settori dell'economia, oggi fortemente compenetrata con il *cyber space*, solo pensando all'*Internet of things*, a *Industry 4.0,* all'agricoltura di precisione, alle *autonomous car*, alle *smart city* o ai droni.

Passando quindi ai conseguenti profili di sicurezza, l'audito ha illustrato i vari tipi di *malware* (ad esempio i sistemi di *botnet*, che si aggiornano regolarmente, rendendo sempre più difficile la creazione degli antivirus con i quali, ad oggi, si riesce a gestire il 30 per cento dei *malware* circolanti).

In particolare, l'audito si è soffermato sui *software* di monitoraggio, *malware* con caratteristiche specifiche di persistenza all'interno del sistema, e peculiarità relative all'esfiltrazione dei dati sensibili e alle modalità di attacco per la distruzione di dati sensibili o la compromissione delle *facilities* del *target*, in caso di *cyber-physical system*.

Il professor Baldoni ha proseguito con il tema della risposta alla minaccia cibernetica, identificando quattro punti essenziali: evitare l'isolamento nelle risposte alle possibili evoluzioni di famiglie di *malware* e nell'analisi di futuri *threat* e delle future minacce, promuovendo la cooperazione di accademia, settore pubblico e settore privato; evitare la dispersione di risorse, concentrando quindi competenze e informazioni, consolidando i *data center*, determinando una riduzione della superficie d'attacco e, di fatto, conseguendo anche un risparmio; investire non tanto nella tecnologia, che subisce un'obsolescenza continua, quanto piuttosto nelle risorse umane, formandole e specializzandole, poiché la *human capability* è la condizione necessaria per una gestione corretta della tecnologia; infine, creare un ecosistema *cyber* nazionale, con un centro di pianificazione e controllo di una strategia a livello nazionale, che colloqui con il settore privato, e un'appropriata struttura di certificazione delle tecnologie a livello governativo.

Audizione del professor Antonio Teti dell'Università degli Studi «Gabriele d'Annunzio» di Chieti-Pescara, seduta n. 258 del 31 gennaio 2017

Il professor Teti, affrontando il tema della sicurezza delle informazioni, ha messo in risalto anzitutto la relazione tra azienda commerciale e strutture governative che si avvalgono dei loro applicativi, che pone vari problemi: il confronto con altri clienti aventi eventuali interessi in contrapposizione con quelli del proprio Stato di appartenenza o che utilizzino le tecnologie dell'azienda per finalità contrastanti con gli interessi nazionali, l'«affidabilità» delle risorse umane dell'azienda e l'assenza di controllo dei rapporti dell'azienda con altre entità pubbliche, private, nazionali e internazionali, l'assenza di controllo sui rapporti di tipo commerciale dell'azienda con altre strutture ad essa collegate.

Il professor Teti ha citato il caso di Israele dove è stato creato l'*Israel National Cyber Bureau* e di Beersheba dove si sta costruendo una *cyber city* che fungerà da *hub*, cioè da contenitore per le aziende, per le strutture governative, per le scuole e per il mondo universitario, contenitore che svilupperà anche delle *start up,* in cui la collaborazione e l'interazione tra Stato e aziende saranno reali ed effettive.

Con riferimento ai quesiti dei commissari sull'esistenza di metodologie per garantire la sicurezza dei dati, l'audito ha affermato che la sicurezza informatica non esiste e che, per altro verso, il *cyber* spazio non necessita di strumenti di grande livello tecnologico per prelevare delle informazioni, citando la prassi dei terroristi che colloquiano tra di loro utilizzando una *mailbox* di posta elettronica e scambiando messaggi all'interno delle bozze.

Il professor Teti si è soffermato su altri due aspetti: l'esistenza di *open source intelligence* nel *cyber* spazio e l'imprescindibiltà di un ingente impiego di risorse finanziarie nella *cyber security* a livello governativo, così come pure la necessità di offrire una formazione specifica su queste tematiche a livello universitario.

Audizione del direttore del Servizio della Polizia postale e delle comunicazioni, dottor Roberto Di Legami, seduta n. 246 del 10 novembre 2016

Il dottor Di Legami ha dapprima brevemente spiegato l'uso che le Forze di polizia fanno dei captatori e di come viene garantito il rispetto delle norme sulle intercettazioni (esecuzione da parte delle forze di polizia di un ordine del magistrato), formulando anche delle ipotesi di allargamento dell'utilizzo dei captatori a cui deve però corrispondere un adeguamento delle norme e delle garanzie.

Un nodo centrale esaminato è stato quello relativo alle ditte fornitrici del servizio, per le quali bisognerebbe elaborare *standard* di sicurezza unici e di controllo, per esempio relativamente alla conclusione dell'intercettazione.

Allo stato, il dottor Di Legami ha sottolineato che la scelta delle ditte che forniscono il prodotto per l'intercettazione avviene principalmente su base fiduciaria, mentre occorre porre uno *standard* di sicurezza (ISO 27001, ISO 9002 e così via) e l'esibizione di certificazioni per il personale impiegato.

Nell'ottica di una disciplina normativa più puntuale sul tema, l'audito ha suggerito la creazione di misure condivise con il «settore giustizia» di implementazione delle prescrizioni del Garante per la protezione dei dati personali e standardizzate su tutto il territorio nazionale; ciò diventerebbe oggetto di capitolato all'interno di un contratto tipico, che sarebbe poi sottoscritto dalle singole procure e dalle singole ditte.

L'approccio alla disciplina delle misure di sicurezza, a parere del dottor Di Legami, deve, tuttavia, essere caratterizzato da un certo grado di elasticità, considerato che la tecnologia si evolve con una velocità tale per cui l'eccessiva rigidità rischierebbe di svuotare la valenza della norma in un breve arco di tempo.

Il dottor Di Legami ha poi fatto alcune considerazioni sul caso Hacking Team e in generale sulle ditte che offrono servizi simili.

Infine, i commissari hanno posto quesiti sul numero delle operazioni svolte dalla Polizia postale e sulla congruità del numero del personale impiegato anche in relazione alle richieste della magistratura.

Audizione del capo del II Reparto informazioni e sicurezza dello Stato maggiore della difesa (RIS), ammiraglio Fabrizio Simoncini, seduta n. 242 del 26 ottobre 2016

L'ammiraglio Simoncini ha introdotto la relazione con la definizione di spazio cibernetico, che trasversale ai domini sui quali tradizionalmente si estende l'operato dell'Amministrazione della difesa (dominio terrestre, dominio marittimo, dominio aereo e dominio spaziale). Nell'ambito del dominio cibernetico ha quindi individuato tre livelli sostanziali: il livello fisico infrastrutturale, rappresentato dalle macchine (le architetture delle reti, i *computer*, i *router*...); il livello logico informativo rappresentato dal volume dei dati gestiti dalle macchine *(database, file*, ma anche *software* gestiti dalle macchine); il livello sociale cognitivo, ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei *social network*, gli indirizzi IP delle macchine).

L'audito si è soffermato quindi sulle caratteristiche fondamentali del *cyber space*, anzitutto quanto alla mancanza di geospecificità, perché, pur in presenza di uno spazio virtuale creato con macchine che possono essere geolocalizzate, lo spazio stesso è in realtà sconfinato; inoltre, quanto alla limitata capacità di attribuzione delle azioni all'interno del *cyber space*, perché, anche qualora riconducibili ad un attore fisico, quest'ultimo può facilmente conseguire l'anonimato; occorre poi aver ben presente la com-

pressione della dimensione temporale nel mondo cibernetico, dove i tempi di risposta sono brevissimi, quasi prossimi allo zero.

L'ammiraglio Simoncini ha evidenziato che questa complessità dell'ambiente cibernetico richiede pertanto l'adozione di strategie di difesa e di misure di sicurezza che comportano il ricorso a particolari professionalità nello specifico settore, non sempre disponibili nell'ambito delle amministrazioni o delle istituzioni dello Stato.

In merito alle disposizioni che disciplinano l'acquisizione di beni e servizi, l'ammiraglio ha ritenuto che, con riferimento alle aziende che operano nell'ambito in esame, occorre individuare criteri che non si fermino al possesso del NOS, alle capacità finanziarie delle aziende, al possesso del certificato antimafia, ma pensare invece a criteri *ad hoc*, per creare un albo di aziende certificate.

L'audito ha descritto quindi le soluzioni organizzative che l'Amministrazione della difesa ha adottato, illustrando il funzionamento del suo reparto nell'ambito cibernetico, in rifermento sia alla gestione dei *software* che dell'*hardware*, che si è giovata delle capacità tecniche sviluppate *in house*.

Infine, l'ammiraglio ha fornito chiarimenti in merito al Comando interforze operazioni cibernetiche (CIOC), in via di costituzione presso il Ministero della difesa, che si configurerebbe come un comando operativo nello spazio cibernetico a cui il RIS fornirebbe supporto di tipo tecnico-militare.

I commissari hanno rivolto quesiti per capire come, in presenza del CIOC, si configurerebbe la catena di comando e la responsabilità politico-istituzionale relativa al RIS che si dovrebbe riferire quindi sia al Ministro della difesa che al Presidente del Consiglio.

Audizione del comandante del Comando Unità speciali della Guardia di finanza, generale Gennaro Vecchione, seduta n. 269 del 1º marzo 2017

Il generale Vecchione ha aperto la relazione enunciando gli argomenti da trattare: gli elementi informativi circa l'impegno istituzionale delle Unità speciali a presidio del settore operativo in esame, i principali fenomeni fraudolenti emersi in esito all'osservazione, il dispositivo di contrasto messo in campo dalla Guardia di finanza e il profilo particolare che attiene alla protezione dei dati personali per le intercettazioni telefoniche e telematiche, e, infine, il sistema di remotizzazione e di controllo in merito.

Quanto al primo aspetto, il generale, premettendo che il Corpo è deputato alla tutela delle entrate, al controllo della spesa pubblica, al contrasto alla criminalità organizzata, al riciclaggio e a tutto ciò che riguarda la tutela dell'economia e della finanza, ha evidenziato che il *dark web* rappresenta un territorio di assoluto interesse, perché rileva sia sotto il profilo fiscale, sia ai fini delle connessioni con eventuali fenomeni di riciclaggio e, più in generale, di utilizzazione per attività illecite, oltre che per lo sviluppo delle criptovalute (*bitcoin* o *onecoin*), che sono in rapida ascesa.

Sono state poi descritte le metodologie utilizzate dal Corpo per adeguare la tecnologia investigativa all'evoluzione dei comportamenti, gli

ambiti di collaborazione del Nucleo speciale *privacy* della Guardia di finanza con il Garante per la protezione dei dati personali, anche con riferimento alla direttiva sulla sicurezza delle attività di intercettazione telefonica e telematica che sia l'autorità giudiziaria che le forze di polizia devono adottare.

Il generale si è poi soffermato sui seguenti aspetti: gli strumenti di indagine (intercettazioni di telecomunicazioni, intercettazioni telefoniche e ambientali e inoculazione di virus) che consentono di individuare e di monitorare gli apparecchi dei soggetti indagati dall'autorità giudiziaria; l'organizzazione del Corpo e dei Reparti speciali che operano sul territorio, dei quali ne evidenzia il costante contatto con realtà operative come Interpol, Europol, l'Organizzazione mondiale delle dogane, la Commissione dell'Unione europea, l'Ufficio europeo antifrode.

I settori d'interesse del Corpo vanno dal crimine organizzato, al riciclaggio, al finanziamento al terrorismo, all'uso indebito di mezzi di pagamento, alla contraffazione *on line*, alla pirateria e sicurezza dei prodotti, alla tutela del consumatore, al contrabbando delle sigarette (in merito al quale è stato stipulato un protocollo di intesa con la Federazione italiana tabaccai), alla vendita di farmaci contraffatti, ai giochi e delle scommesse illegali, settore quest'ultimo per il quale il generale ha segnalato la presenza di tre importanti operazioni in corso.

Il generale Vecchione ha passato poi la parola al colonnello Parascandolo, comandante del Nucleo speciale frodi tecnologiche, che ha illustrato al Comitato le tecnologie per monitorare il *dark web*, mondo capace di generare ingenti profitti e di creare delle significative perdite per le economie e il sistema Paese.

Il colonnello fatto particolare riferimento all'esistenza a livello mondiale di cinque rilevanti *marketplace* consolidati, dove si trovano *tutorial* su come costruire qualcosa di illecito, tipo le armi, come effettuare il *carding* (le truffe sulle carte di credito, la copia dei dati personali e dei dati bancari), ma anche dove è possibile acquistare *malware* e *trojan*.

Gli auditi, quindi, hanno replicato ai quesiti posti dal presidente del Comitato e dai commissari su varie questioni: sulla valutazione dell'efficacia degli strumenti normativi per la promozione e l'utilizzazione dei sistemi informatici e per l'intercettazione dei dati e l'utilizzo dei captatori nelle comunicazioni, anche in relazione alla tutela della sfera della vita privata nei soggetti estranei all'indagine in corso; sulla collaborazione operativa delle Unità speciali della Guardia di finanza con i Servizi e con il sistema di informazione e sicurezza, sul fenomeno in crescita della moneta virtuale.

Audizione del sostituto procuratore della Repubblica presso il Tribunale di Milano, dottor Alessandro Gobbis, seduta n. 280 del 29 marzo 2017

Partendo dalla vicenda Hacking Team, il dottor Gobbis ha delineato le caratteristiche dell'intrusore informatico, che consente l'intercettazione

telematica delle comunicazioni criptate, realizzando da remoto tutto ciò che può fare un utilizzatore del dispositivo informatico.

Tali caratteristiche determinano una modalità di penetrazione nella *privacy* dell'interessato molto invasiva, che sotto il profilo giuridico va dall'intercettazione di comunicazioni e conversazioni, all'attivazione della videocamera, dall'intercettazione ambientale con l'attivazione del microfono, all'acquisizione da remoto di tutti i contenuti *(file*, fotografie e scritti) presenti nel dispositivo.

Facendo ancora riferimento al caso Hacking Team, l'audito si è soffermato sulle conseguenze giuridiche del trafugamento del codice sorgente e, più in generale, sulla recente giurisprudenza delle Sezioni unite della Corte di cassazione, che ha fissato i criteri per le intercettazioni telefoniche con riferimento a varie tipologie di reati.

Quindi sulla base di quesiti formulati dai commissari, il dottor Gobbis ha toccato vari aspetti della tematica in esame: le collaborazioni con le Agenzie straniere, la possibilità di individuare tecnicamente i soggetti in grado di scaricare e ricostruire un codice, gli eventuali danni in termini di sicurezza nazionale, generati da vicende come Hacking Team, il quadro normativo attuale – ma soprattutto *de iure condendo* – relativo all'utilizzazione dei captatori informatici.

Audizione del dottor Diego Piacentini, commissario per l'attuazione dell'Agenzia digitale, seduta n. 306 del 12 luglio 2017

Il dottor Piacentini ha iniziato la sua relazione illustrando il Piano triennale per l'informatica nella pubblica amministrazione 2017-2019, documento di indirizzo strategico del Governo, per la realizzazione del sistema operativo del Paese, attraverso l'individuazione di una serie di componenti fondamentali, tra cui la *security*, sui quali costruire servizi per i cittadini, le amministrazioni pubbliche e le imprese. Il Piano contiene moltissime indicazioni che riguardano le infrastrutture fisiche e la connettività, la razionalizzazione dei *data center*, le piattaforme abilitanti, l'uso dell'identità digitale (SPID), l'Anagrafe Nazionale della Popolazione Residente (ANPR), la fatturazione elettronica, l'uso del sistema pagoPA.

L'audito, quindi, ha ceduto la parola al dottor Varisco, responsabile della *cyber security,* per la descrizione delle linee guida in materia di sicurezza indicate nel Piano e delle azioni da intraprendere per garantire la sicurezza delle infrastrutture informatiche e il supporto nella prevenzione e nel trattamento degli incidenti di sicurezza informatica.

Il dottor Varisco si è soffermato sul ruolo del CERT-PA *(Computer Emergency Response Team* della pubblica amministrazione), l'organo di controllo, relativamente al tema *security*, all'interno di AgID che ha tra i suoi obiettivi quello di fornire il primo punto di contatto da e verso le amministrazioni durante gli incidenti di sicurezza, anche se, in un'ottica di un eventuale potenziamento dell'organo, ci si pone l'obiettivo di fornire servizi reattivi, per la prevenzione del rischio come il *vulnerability asses-*

sment penetration testing, oppure tutte le *best practice*, come gli *alerting*, i *monitoring* o i *logging*, diffuse nel mondo privato, da introdurre nella dimensione pubblica.

Particolare importanza in tema di prevenzione riveste la piattaforma di *infosharing*, affinché soggetti pubblici e privati possano comunicare con un unico linguaggio e ad essere allineati sulle possibili criticità, sia a livello nazionale che internazionale.

Altri aspetti evidenziati sono stati l'esistenza di un *National vulnerability database* in cui sono raccolti e rielaborati tutti gli incidenti informatici, il documento «Misure minime per la sicurezza ICT delle pubbliche amministrazioni», per incentivare le amministrazioni ad effettuare tutti i *test* essenziali per la sicurezza, il sito «forum.italia.it» aperto ai dipendenti della pubblica amministrazione, la piattaforma GitHub su cui è attivo un *ticketing system.*

2.2. Audizioni delle società e degli operatori

*Audizione dell'*Executive vice president security *di Telecom Italia, dottor Stefano Grassi, seduta n. 268 del 28 febbraio 2017*

Il dottor Grassi anzitutto ha illustrato in linea generale la procedura di esfiltrazione dati mediante captatori informatici, distinguendo l'intercettazione mediante rete fissa da quella mediante rete mobile. Quindi, ha descritto la procedura mediante la quale si estrinseca la collaborazione tra TIM e polizia giudiziaria in tema di intercettazioni.

Ha poi fatto riferimento al quadro normativo e alla proposta di legge recante «Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali», che individua tra l'altro la tipologia dei reati per i quali è ammesso l'utilizzo dei captatori, cioè criminalità organizzata di stampo mafioso o con finalità di terrorismo. In merito, ha evidenziato che le operazioni di inoculazione dei captatori sul *target* dovranno essere svolte esclusivamente dalla polizia giudiziaria.

L'audito è passato quindi a descrivere come vengono trattate in TIM le informazioni classificate o coperte dal segreto di Stato, evidenziando, tra l'altro, la collaborazione dell'azienda con il comparto *intelligence* e la partecipazione di TIM al tavolo delle aziende e delle imprese che gestiscono le infrastrutture critiche del Paese, che si riunisce periodicamente presso il DIS, e che svolge attività di condivisione di informazione (*infosharing*) in materia di sicurezza informatica.

Il dottor Grassi è soffermato altresì sulle esigenze di protezione del patrimonio informativo dell'azienda, che vanno dalla continuità del servizio, alla riservatezza delle comunicazioni, ai dati di traffico, alle identità digitali, ai *data base* e alle carte di credito dei clienti, e sugli attuali elementi di rischio per TIM: l'utilizzo dei *social,* una crescente attività di *social activism*, l'aumento dei servizi *cloud*, la grande diffusione di *device* come *smartphone* e *tablet.*

L'audito ha precisato inoltre che, a fronte della protezione dei dati, delle reti, dei sistemi e dei servizi dei *device*, dei *modem*, delle ADSL, le principali minacce che impattano su questi ambiti sono i virus, i *malware*, le truffe, gli *hacker*, il furto di dati e gli attacchi massivi come i *Destributed Denial of Service* (DDoS).

Il dottor Grassi, ha descritto infine la strategia che è utilizzata in Telecom per la gestione del rischio, che si sostanzia in tre linee di difesa: la prima linea è rappresentata dai controlli di primo livello dei *process owner*; la seconda è costituita da *compliance* e *risk management*; la terza consiste, infine, nell'attività di *assurance* di *internal audit.*

L'audito ha fornito quindi risposte a vari quesiti dei commissari: su eventuali esercitazioni da parte di Telecom integrate con altri *asset* strategici del Paese a livello di *cyber attack*, sulla sicurezza fisica attiva per quanto riguarda le strutture sulle quali passano i dati, sulla gestione del conflitto tra l'apparato di sicurezza del nostro Paese, che tratta di questioni riservatissime, e la tutela della libertà individuale e della *privacy* delle persone.

Audizione del Safety, Security & Facility Director *di Vodafone Italia Spa, dottor Stefano Bargellini, seduta n. 276 del 15 marzo 2017*

Il Presidente ha introdotto la seduta ricordando che l'obiettivo dell'indagine è quello di arrivare a definire un quadro di garanzie, che permetta agli operatori di lavorare e ai cittadini di non veder invasa la propria *privacy,* e a delineare una disciplina compatibile, da una parte, con le esigenze giudiziarie e, dall'altra, con quelle della *privacy* dei soggetti coinvolti.

Il dottor Bargellini ha aperto l'intervento affermando che il tema specifico della sicurezza è stato suddiviso, in Vodafone, in due grandi aree: una relativa alla sicurezza fisica dell'azienda e al rapporto con gli organi di polizia e con la magistratura; un'altra area, relativa alla prevenzione delle frodi nell'utilizzo delle SIM Vodafone, alla sicurezza informatica e allo studio dell'evoluzione degli attacchi informatici, sia nel mondo della rete, sia nel mondo della *ICT.*

Sotto il primo profilo, l'audito ha evidenziato un rapporto di collaborazione costante, sia con l'autorità giudiziaria, sia, per gli aspetti della prevenzione, con la Polizia di Stato, con l'Arma dei carabinieri, con la Guardia di finanza e con i settori dell'*intelligence.*

Per gli aspetti tecnici, il dottor Bargellini ha passato la parola all'ingegner Corradi, *head of ICT Security, Privacy & Fraud Management*, che ha illustrato un primo filone di attività tecniche tendenti a garantire la connettività voce e dati per tutti i cittadini italiani, ma anche ad evitare la possibilità di intercettare o captare conversazioni o scambi di dati e connettività *internet* dei clienti Vodafone in modo illecito attraverso la criptazione delle conversazioni e dei *database.*

L'ingegnere si è soffermato sugli aspetti di sicurezza preventiva, che si attuano sia garantendo le misure di sicurezza sui nuovi prodotti, sia attraverso il monitoraggio a campione degli accessi alle banche dati e del motivo di tali accessi. Vodafone si avvale anche degli *ethical hacker*, professionisti della sicurezza che realizzano i cosiddetti *penetration test,* per scoprire eventuali vulnerabilità, prima che le stesse possano essere sfruttate in modo illecito.

Tra gli altri sistemi di protezione esterna l'ingegner Corradi ha segnalato: i *firewall*, una sorta di protezione da *internet* verso i portali Vodafone e verso i dati dei clienti, l'*Intrusion Detection System* (IDS), una sorta di telecamera digitale che blocca i pacchetti ritenuti malevoli *(malware)*, gli strumenti anti-*phishing* per intercettare e bloccare le *e-mail* fasulle che contengono all'interno un *malware.*

I commissari hanno quindi formulato vari quesiti: sull'esistenza di una convenzione di Vodafone con l'*intelligence* (alle cui richieste Vodafone ha dato sempre attuazione attraverso la procura generale presso la Corte di appello di Roma); sui controlli effettuati dall'azienda sulle apparecchiature (che non siano effettivamente tecnologie *dual use)* e sulle componenti utilizzate per le stesse; sulla riservatezza e la sicurezza dei controlli effettuati per il tramite Vodafone dall'autorità giudiziaria, dalla polizia giudiziaria e dall'*intelligence*; sulla possibilità tecnologica di verificare e tenere pulite da *malware* tutte le reti, anche esterne.

Audizione del responsabile Company Security Governance *di Wind Tre Spa, dottor Fabrizio Marcelli, seduta n. 277 del 16 marzo 2017*

Il dottor Marcelli ha iniziato la sua relazione premettendo che l'azienda ha sempre riservato una particolare attenzione agli ambiti della *security* e garantito la completa collaborazione con l'autorità giudiziaria e con gli enti istituzionali preposti alla sicurezza nazionale. Tale collaborazione si estrinseca principalmente attraverso sistemi dedicati, banche dati dedicate, accessi controllati in modo rigido, con *multi factor authentication* (strumenti di autenticazione multi fattore) anche di natura biometrica, con la tracciatura di tutte le operazioni, a livello capillare, effettuate sia dagli addetti, sia da coloro che svolgono attività amministrative sui sistemi e con *audit* periodici sulle operazioni, per verificare il funzionamento dei processi.

L'audito ha continuato con la trattazione del tema dei captatori informatici, riguardo al quale ha presentato che gli operatori di telecomunicazioni intervengono sostanzialmente a corollario, per consentire a chi è autorizzato, di espletare le operazioni di inoculazione del *software*. Queste operazioni consistono soprattutto nell'ampliamento della banda e nell'invio di messaggi per richiedere determinate attività di manutenzione.

Per quanto concerne l'esigenza di una disciplina particolare in merito, l'audito ha ritenuto, da un lato, imprescindibile l'esistenza di un sistema di garanzie che delimitino l'area di azione delle informazioni e degli opera-

tori addetti e, dall'altro, ha reputato fondamentale che i soggetti che mettono a disposizione i *software* per i captatori informatici siano certificati e che i *software* stessi siano in possesso della ISO-27001, la certificazione sulla sicurezza delle informazioni (allo scopo di essere sicuri che i *software*, acquisiti per determinate operazioni, eseguano solo quelle). Tale certificazione si ottiene attraverso un processo lungo, che richiede dei *pre-assessment*, per verificare le condizioni effettive per il certificato e per svolgere eventuali attività di *remediation* rispetto agli *assessment*, qualora si riscontrino aspetti non perfettamente allineati agli *standard* obbligatori previsti dalla normativa.

I commissari hanno formulato quindi quesiti relativi al disegno di legge approvato dalla Commissione giustizia del Senato in materia di intercettazioni e, in particolare, sui captatori informatici, sulle operazioni svolte dall'azienda con tali strumenti, sulle infrastrutture critiche territoriali e sull'esistenza di una eventuale pianificazione nazionale, sull'esistenza di un'unità dedicata per eseguire l'attività tecnica connessa alle intercettazioni con i captatori, sui controlli effettuati per garantire il mantenimento della riservatezza delle informazioni in possesso degli operatori.

Audizione del dottor Alessandro Cortesi, del dottor Andrea Franco Formenti e del dottor Alessandro Mistò, in rappresentanza della Area Spa, seduta n. 286 del 3 maggio 2017

Il dottor Formenti, fondatore e socio di Area Spa, ha iniziato l'audizione con una descrizione dell'azienda, il cui mercato di riferimento è costituito al 100 cento per cento da autorità pubbliche e i cui ambiti storici di operatività sono quelli della giustizia, degli affari interni, della difesa, della sicurezza nazionale, nonché di altre autorità eventualmente coinvolte nell'attività di polizia giudiziaria. I prodotti di Area rientrano nella categoria della cosiddetta *Lawful Interception* (LI), ovvero tutto ciò che riguarda l'intercettazione delle comunicazioni a fini di giustizia o ad uso dell'autorità. A questa categoria di prodotti si affiancano la *data retention*, cioè la raccolta di dati che descrivono la comunicazione tra i soggetti, e l'utilizzo della tecnologia di Area nell'ambito *cyber*, soprattutto per attività di *cyber intelligence*, ai fini di *cyber protection* o *critical infrastructure.*

L'audito ha accennato quindi alle fonti normative cui Area fa riferimento: il codice penale, il codice di procedura penale e le relative norme di attuazione, la giurisprudenza della Corte di cassazione, le delibere del Garante in materia di protezione dei dati personali in rapporto all'entità delle intercettazioni disposte dall'autorità giudiziaria, le linee guida del Ministero della giustizia a favore delle procure della Repubblica per l'acquisizione dei sistemi a supporto delle attività di intercettazione delle telecomunicazioni, prevalentemente attraverso la redazione di bozze o *template*, modelli di contratto quadro e capitolato tecnico, il codice delle co-

municazioni, specificamente nella parte riferita agli operatori di comunicazione nell'ambito della prestazione obbligatoria a fini di giustizia.

Il dottor Formenti è passato poi a descrivere l'offerta di Area, suddivisa in tre pilastri fondamentali: l'intercettazione delle comunicazioni in forma passiva, cioè la duplicazione del flusso originario; i prodotti di prossimità fisica riferiti alle intercettazioni ambientali (microspia, GPS installato nell'auto, microcamera nascosta); le manipolazioni della sessione di comunicazione, con il meccanismo dell'«uomo nel mezzo» che consente di rompere il sistema di cifratura.

Nell'illustrare le problematiche connesse alle varie tecnologie per l'acquisizione delle informazioni, l'audito si è soffermato sui rischi connessi al mercato della vulnerabilità, alla raccolta di informazioni mediante *social engineering* (manipolazioni che causano una richiesta di intervento ad un servizio clienti «fittizio»), all'identità digitale quanto alla certezza della presenza fisica che vi è dietro.

In questo quadro, il dottor Fomenti ha evidenziato le proposte di Area:

– un sistema di gestione delle identità digitali sotto copertura, utilizzando l'antico strumento dell'infiltrato, ma digitale, il quale raccoglie tutte le informazioni nelle comunità chiuse a cui gli infiltrati digitali partecipano, li firma con i meccanismi di sicurezza digitale tipici di un eventuale utilizzo anche processuale, e li mette in sicurezza dal punto di vista tecnico;

– un sistema di definizione del tabulato telematico, che risolve e disambigua l'indirizzamento IP attraverso sonde correlate messe all'interno dell'operatore prima dell'affaccio su *internet* e che, all'esterno dello stesso, consente di avere un tabulato telematico perfettamente univoco.

Audizione del dottor Mauro Collalto e del dottor Fabio Romani, in rappresentanza della IPS Spa, seduta n. 286 del 3 maggio 2017

La relazione del dottor Collalto, amministratore delegato della IPS Spa, nonché del Gruppo Resi, socio unico di IPS, ha preso avvio con una descrizione degli ambiti di attività delle due aziende: Resi che realizza sistemi di registrazione per *call center*, oltre a sistemi di analisi di dati ad uso *marketing* per grandi aziende o per la pubblica amministrazione, e IPS che, invece, svolge essenzialmente attività di intercettazione su reti *internet*, attraverso sonde che analizzano e catturano il traffico di interesse per l'autorità giudiziaria: specificamente, per la parte OSINT *(Open Source INTelligence)* si tratta di sistemi che analizzano le fonti aperte (banche dati pubbliche, ma anche *web, social network)* per il reperimento di informazioni, e che oggi assumono maggior valore rispetto alle intercettazioni tradizionali, soprattutto per le attività di indagine preventiva e propedeutica, con particolare riferimento alla criminalità organizzata, e all'antiter-

rorismo, rispetto al quale l'utilizzo di queste reti di comunicazione è molto diffuso.

Entrando più nel vivo sul tema dei captatori informatici, l'audito ha evidenziato che IPS non realizza questi virus per due motivi: perché si tratta di una tecnologia ad alta obsolescenza che richiede continua manutenzione, e perché, operando IPS sul mercato internazionale, si rischia di subire attacchi dallo stesso prodotto che si immette su tale mercato, pertanto l'azienda si è concentrata su strumenti alternativi ai captatori informatici, considerato che molte informazioni si possono reperire dalla rete, dalle pagine Facebook, sul *deep web* e sul *dark web*.

Il dottor Collalto si è soffermato quindi sulle problematiche presentate dal sistema dei captatori informatici, anche nell'ottica di migliorare il quadro normativo in termini garantistici, dato che tale sistema di intercettazione è comunque molto utilizzato: per la gestione di questi sistemi, infatti, secondo l'audito occorrono aziende strutturate, con sufficienti risorse economiche e di personale, a fronte del fatto che oggi proliferano aziende *freelance* e ditte individuali che si pongono sul mercato con oggetti tutt'altro che professionali.

Il dottor Collalto ha sottolineato che il grande utilizzo dei captatori informatici avviene su *computer*, ma soprattutto su *smartphone*, dotati di *software* che consentono comunicazioni sicure, «inintercettabili».

In merito, ha proposto come unica soluzione, quella di obbligare chiunque operi in qualsiasi forma nel settore delle comunicazioni elettroniche – che sia Apple che vende il dispositivo, Telecom Italia che offre la connessione radio, WhatsApp o Facebook – a rispettare la regola dell'intercettabilità delle comunicazioni, in presenza delle giuste autorizzazioni e motivazioni.

Ulteriori suggerimenti emersi consistono nell'impedire l'utilizzo di un certo tipo di comunicazione, senza mettere a disposizione una porta verso l'autorità giudiziaria per l'ascolto in chiaro, e nel richiedere agli operatori di mettere in commercio solo dispositivi che abbiano una funzione *embed*, cioè che non renda necessario inoculare il captatore, perché lo stesso è già integrato nel telefono e, su richiesta, può essere attivato.

Audizione della dottoressa Stefania Ranzato, dell'ingegner Nicola Mazzini e del dottor Fulvio Guatta, in rappresentanza della Cyber Intuition Srl, seduta n. 287 del 3 maggio 2017

La relazione della dottoressa Ranzato si è aperta con l'illustrazione del prodotto distribuito dall'azienda a livello nazionale e internazionale, in grado di bloccare le minacce di tutte le famiglie *ransomware*, che ad oggi attaccano sia enti governativi sia aziende e *corporate*, in particolare impetendo l'infezione ed evitatando la criptazione completa dei dati (in genere, per riavere i dati trafugati è necessario pagare un riscatto in *bitcoin*, sovvenzionando di fatto le associazioni criminose che stanno alla base dei *cyber* attacchi). Ha quindi evidenziato l'esistenza di attacchi co-

noscitivi della rete per individuarne la vulnerabilità, rispetto alla quale si può preparare in un secondo momento un attacco mirato: si tratta di un'attività di *cyber* spionaggio dedicata, oggi non più limitata al banale furto del dato. L'aspetto significativo si sostanzia nel fatto che ogni anno nel mondo si verificano 7,87 miliardi di *cyber* attacchi e che l'Italia dopo gli Stati Uniti è il secondo Paese più colpito al mondo.

Ha inoltre segnalato che gli attacchi sono prevalentemente mirati verso gli enti governativi e si stanno estendendo anche in ambito finanziario (quindi bancario), sanitario, legale, scolastico e industriale.

L'ingegner Mazzini ha poi descritto il prodotto aziendale RaPToR *(Ransomware Prevention Toolkit & Rescue)*, che fornisce una protezione da attacchi di tipo *ransomware* e si affianca ai comuni antivirus, in quanto agisce in un'area che si colloca prima del riconoscimento della minaccia da parte degli antivirus. La funzionalità di RaPToR si può rappresentare in quattro punti: riconoscere i *ransomware*, evitarne la propagazione, garantire il recupero dei dati nel caso di attacchi mirati, completamente differenti da quelli conosciuti o effettuati attraverso altre tecniche, e proteggere le macchine dell'intera rete.

Il dottor Guatta, responsabile legale e *privacy* della Cyber Intuition, ha precisato infine che il prodotto è stato oggetto di studi e di adeguamento alle normative, anche europee, sul trattamento dei dati sensibili.

Audizione del dottor Elio Cattaneo, del dottor Nevio Devidé e della dottoressa Cristina Galoppi, in rappresentanza della SIO Spa, seduta n. 287 del 3 maggio 2017

La relazione si è aperta con l'intervento del dottor Devidé, *managing director* della SIO Spa, che ha fornito una descrizione del contesto operativo della società: la SIO mette a disposizione l'*hardware*, i *software*, il personale di manutenzione richiesti dalle procure della Repubblica o dagli enti per raccogliere le evidenze di indagine (le procure/enti sono le amministratrici del sistema e le responsabili del trattamento dei dati); inoltre, finanzia e gestisce tutti i collegamenti verso l'operatore di telefonia, per permettere le intercettazioni di voci e di dati, limitatamente a quello che l'operatore stesso è autorizzato o obbligato a dare; inoltré, fornisce la tecnologia per acquisire le informazioni non provenienti dall'operatore di telefonia, cioè dal mondo ambientale o tattico; infine, finanzia, realizza e gestisce, per conto della Procura, anche le modalità di trasporto verso i fruitori, che sono le forze di polizia giudiziaria.

Per la distribuzione e la raccolta delle informazioni ottenute mediante l'installazione di un *malware* o pervenute dal *web*, la SIO ha realizzato un nodo tecnologico presso una *server farm* di Telecom Italia, unico soggetto preposto a dialogare con il mondo esterno. Da quel punto, laddove necessario, vengono distribuite, in maniera sicura verso le procure e dalle procure verso gli operatori di polizia giudiziaria, le tipologie di informazioni: i dati audio, i dati provenienti dall'operatore di telefonia, le piattaforme

per raccogliere le informazioni dal mondo *social web*, le piattaforme legate alle targhe e ai varchi, le geolocalizzazioni, l'audio ambientale, il mondo dei *trojan*, dei captatori informatici, gli *smartphone*, i dati video, le piattaforme particolari, le localizzazioni anche senza operatore, nonché la condivisione di documenti all'interno dello stesso procedimento penale.

In conclusione, il dottor Devidé ha evidenziato, anche nella prospettiva di una più completa disciplina normativa, che la valutazione del grado di affidabilità e sicurezza delle filiere utilizzate per le attività d'indagine, deve essere condotta sia garantendo la qualità tecnica di tutti i nodi tecnologici resi disponibili (HW e SW), sia correlando le politiche di accesso ai sistemi, di fruibilità delle informazioni, le modalità di mappatura delle attività, con strumenti di gestione e controllo delle operazioni svolte, nonché con un tracciamento, il più possibile automatizzato e notificato, di tutte le eventuali anomalie compiute dal singolo operatore (nei confronti del quale, sia che si tratti di un dipendente della pubblica amministrazione, sia di un rappresentante di un'azienda, rimane imprescindibile l'aspetto fiduciario su cui basare le attività di crescita di un sistema sempre più perfezionato).

Audizione del dottor David Vincenzetti e del dottor Dario Faggioni, in rappresentanza della Hacking Team srl, seduta n. 288 del 9 maggio 2017

Il dottor Vincenzetti, dopo aver illustrato i passaggi salienti della nota vicenda relativa all'attacco informatico che nel luglio del 2015 ha colpito la Hacking Team srl, e fornito i chiarimenti sollecitati dai commissari, è entrato nel vivo delle tematiche relative all'indagine, rispondendo ai quesiti del Presidente in merito al nuovo prodotto che la società è in procinto di presentare e alle difficoltà collegate all'inoculazione di un *malware*, direttamente o da remoto attraverso il *phishing* o tramite messaggi di operatori telefonici, contenenti l'invito a collegarsi, nonché alla possibilità di intervenire a monte dell'installazione del virus per impostare determinati *standard* che indichino il *target* esatto, e prevengano le ingerenze nella vita privata dei soggetti estranei all'indagine in corso.

Sotto quest'ultimo profilo, il soggetto audito ha affermato che l'intervento per escludere dall'intercettazione i soggetti estranei all'indagine è possibile solo *a posteriori*. Con riguardo invece alla difficoltà di inoculare i virus da remoto, l'audito ha chiarito che la difficoltà a provocare infezioni remote risiede nel fatto che il mercato è cambiato radicalmente per cui gli *exploit* (i virus che permettono di eseguire il codice malevolo sul sistema informatico) sono diventati molto più rari e molto più costosi (Google aumenterebbe i costi per mantenere esclusiva la partecipazione a quello che il dottor Vincenzetti definisce «Cyber club»).

L'audito ha precisato che il prodotto «*Project Zero*», impiegando i migliori *hacker* del mondo e *server farm* sconfinate, consente la presenza abbondante di *exploit*, che saranno ad ottimo prezzo in quanto acquisiti da Hacking Team prima degli stessi *broker* e di Google.

Audizione del dottor Enrico Fincati e del dottor Nicola Franzoso, in rappresentanza della SIND srl, seduta n. 289 del 10 maggio 2017

Il dottor Fincati ha esordito descrivendo l'attività della SIND, che opera nei mercati della sicurezza aeroportuale e della sicurezza militare.

In particolare, per quanto riguarda l'*intelligence*, SIND offre prodotti di intercettazione, di criptazione dati, di telecomunicazioni criptate, di invio di segnali e trasmissione dati criptati.

Il dottor Franzoso, nell'illustrare gli aspetti tecnici dei sistemi di intercettazione, ha precisato che detti sistemi, dall'intercettazione vocale, a quella video, a quella ambientale, transitano oggi tutti all'interno della rete.

Quindi, gli auditi hanno replicato a vari quesiti dei commissari: sull'eventuale invasività nell'utilizzo dei captatori e sulle tecniche di «pulizia» delle riprese video, delle fotografie e dei flussi audio per arginare gli effetti dell'uso dello strumento, in termini di tutela della riservatezza; sull'eventuale analisi dell'*hardware* dei singoli *device* da fornire al cliente; sulle caratteristiche dei *software* di riconoscimento facciale.

Audizione del dottor Alberto Pelliccione, in rappresentanza della ReaQta srl, seduta n. 290 del 10 maggio 2017

Il dottor Pelliccione ha aperto la relazione enunciando la trattazione di due argomenti principali: l'uso dei captatori da parte della polizia e l'uso dei captatori a livello di *intelligence.*

Sotto il primo profilo, le criticità sono legate alla gestione dell'integrità dei dati e alle modalità operative per portare a termine le indagini; sotto il secondo profilo, occorre approfondire la provenienza degli strumenti di intercettazione, oltre a capire come agire operativamente a seconda delle operazioni di *intelligence* poste in essere.

Nello specifico, l'audito ha posto all'attenzione del Comitato le possibili soluzioni, per garantire l'integrità dei dati acquisiti dai dispositivi degli indagati (considerando che il captatore è un agente attivo che può creare e modificare contenuti), per non compromettere la sicurezza degli indagati, e per gestire in sicurezza i captatori all'interno delle forze di polizia.

Per quanto concerne l'integrità dei dati e la metodologia di acquisizione attiva mediante captatori informatici l'audito ha evidenziato l'opportunità di una normativa puntuale, che garantisca la catena delle operazioni eseguite durante la fase di indagine da eventuali abusi.

Con riguardo alla problematica della sicurezza l'audito ha sottolineato che il captatore riduce drasticamente il livello di sicurezza di qualunque dispositivo sul quale viene installato, pertanto, se il profilo indagato è pubblico o politico e l'indagine si protrae nel tempo, questi diventerà oggetto di potenziali altri attacchi *(cyber crime*, altre *intelligence* o chiunque altro).

Quanto all'uso dei captatori a livello di *intelligence* il dottor Pelliccione ha affrontato varie questioni: la provenienza dei captatori ad uso *intelligence*, la necessità di differenziare le *cyber* strategie offensive, ma anche difensive, la necessità di garantire la segretezza e la non tracciabilità delle operazioni svolte a livello di *intelligence.*

Audizione del dottor Fabio Cameirana e dell'ingegner Duilio Bianchi, in rappresentanza della RCS LAB Spa, seduta n. 290 del 10 maggio 2017

Il dottor Cameirana ha presentato la società, che opera nel mercato delle intercettazioni esclusivamente in Italia per l'autorità giudiziaria, a stretto contatto con le forze di polizia, per fornire prodotti di ausilio tecnico per le indagini: il sistema MITO, un registratore installato nelle procure della Repubblica e poi remotizzato presso tutte le sale di ascolto della polizia giudiziaria, i sistemi VS, che gestiscono la registrazione e la decodifica di tutto il traffico telematico delle intercettazioni IP, i sistemi di *business intelligence*, fondati sull'analisi dei tabulati e dei traffici pregressi e di cella, che vengono acquisiti dall'autorità giudiziaria, le divisioni tattiche, che si occupano principalmente delle installazioni di sistemi ambientali, GPS, apparati di videosorveglianza, nonché gli strumenti per le intercettazioni telematiche attive.

L'ingegner Bianchi, quindi, si è soffermato sulla distinzione tra intercettazioni telematiche passive e attive, dove questa seconda tipologia prevede diverse modalità: agendo materialmente sul terminale, o agendo da remoto mediante l'«ingegneria sociale», che aggancia il *target*, studiando i suoi interessi, impersonando un operatore telefonico.

L'audito ha evidenziato quindi i limiti di questa modalità che prevede l'appoggio ad un terminale esterno che non può essere controllato e del quale non si hanno informazioni di dettaglio riguardo al sistema operativo.

Si è passati quindi a tracciare il tema della sicurezza del sistema, che la società ha gestito investendo sul *software* spia affinché non vada a degradare le condizioni di sicurezza del terminale: i dati sul terminale sono cifrati e i *server* utilizzati sono di transito per evitare che il dato dal terminale vada direttamente sul *server* in procura, perché questo potrebbe rappresentare un rischio, mentre in tal modo si riesce a nascondere la destinazione finale.

Audizione del dottor Salvatore Macchiarella, dell'ingegner Agostino Specchiarello e dell'ingegner Gabriele Quattrocchi, in rappresentanza della CSH srl, seduta n. 290 del 10 maggio 2017

L'ingegner Specchiarello, *senior security engineer* della CSH srl, ha presentato brevemente l'azienda che, nata per occuparsi di intercettazione audio e video, ha successivamente allargato l'ambito all'intercettazione informatica.

Nel corso della presentazione l'audito ha posto al Comitato come primo problema, ai fini di un intervento normativo, quello della restrizione sull'utilizzo dei captatori informatici, che rende difficoltosa l'acquisizione di determinati tipi di dati, come, ad esempio, quelli audio con riferimento ai *computer* portatili e ai dispositivi mobili, perché l'intercettazione tramite questi sistemi può risultare molto invasiva.

L'ingegner Specchiarello, nel descrivere le caratteristiche tecniche del prodotto che CSH srl fornisce alle procure e alla polizia giudiziaria, loro unici clienti, ha segnalato che il problema principale per gli operatori è rappresentato oggi dalle vulnerabilità, dai vettori di infezione, considerato che il settore della sicurezza informatica si evolve giorno dopo giorno, rendendo sempre più complesso effettuare gli attacchi e inoculare il virus, e che i costi per la ricerca e lo sviluppo delle vulnerabilità sono estremamente elevati.

I commissari hanno chiesto quindi agli auditi una valutazione sui *software* sia di tipo offensivo che difensivo attualmente presenti all'interno del sistema Paese.

Audizione del dottor Eugenio Santagata, del dottor Andrea Melegari e dell'ingegner Mario Orsini, in rappresentanza della CY4Gate srl, seduta n. 301 del 28 giugno 2017

Il dottor Santagata ha inizialmente descritto l'azienda CY4Gate, che nasce dalla fusione di due aziende *leader* mondiali: una nel campo della difesa elettronica e l'altra nel campo dell'intelligenza semantica: la difesa elettronica, utilizzata dalle Forze armate, consiste in un'attività di *intelligence* per fornire informazioni, utili per la difesa, attraverso un'analisi dettagliata dello spettro elettromagnetico e anche in un'attività di attacco per impedire le comunicazioni o rompere i *datalink*; l'intelligenza semantica consiste in una serie di algoritmi che estraggono significato da testi, quindi da dati non strutturati, attraverso un'analisi profonda del testo stesso.

CY4Gate progetta e commercializza soluzioni sia difensive che offensive che servono nelle operazioni antiterrorismo, nelle operazioni anticrimine o nelle operazioni di *attribution*, cioè di ricerca del mandante di certi tipi di attacco (ad esempio: WannaCry o Petya). Si tratta di soluzioni per l'analisi dei dati, di captatori informatici – che possono estrarre dati da dispositivi mobili e fissi, sia in ambiente Android che in ambiente IOS –, di laboratori per l'analisi dei *malware*, per il *reverse engineering* dei *malware* e per l'*intelligence* sugli attacchi.

Il dottor Santagata ha segnalato che oggi la *road map cyber* digitale di un Paese non può prescindere da due pilastri fondamentali: l'*attribution*, ovvero la comprensione di chi ha sferrato l'attacco, e i motivi; la «deterrenza» cioè la capacità a livello sistemico di condurre attacchi *cyber* su larga scala, ambito nel quale occorre una spinta culturale e un quadro

normativo compiuto, pur senza trascurare i rischi e la delicatezza della sfera in cui ci si muove.

Audizione del dottor Carlo Brigada, del dottor Massimo Bruni e del dottor Sergio Antonio Ajani, in rappresentanza della società ITD Solution Spa, seduta n. 315 del 2 agosto 2017

Il dottor Brigada ha dapprima fornito una breve descrizione della società, che ad oggi, lavora con tutti i *top spender* dell'*information technology* in Italia: Telecom Italia, Wind, Vodafone, Leonardo, il gruppo Poste Italiane.

Quindi, il dottor Bruni ha precisato che la ITD non produce tecnologia, ma offre servizi professionali, intervenendo sui prodotti con dei *team* di esperti in grado di sviluppare applicazioni e infrastrutture IT. Con riguardo alla tematica delle intercettazioni, la società possiede una forte competenza in ambito *data communication*, cioè di comunicazioni digitali, fornendo agli operatori di telecomunicazioni presenti sul territorio nazionale piattaforme di monitoraggio e analisi del traffico per fini commerciali, per la verifica della corretta operatività della rete, della qualità della conversazione eccetera.

Il Comitato ha posto quindi vari quesiti sulle garanzie di maggior sicurezza che il prodotto offrirebbe, dopo l'intervento di ITD, considerato che inizialmente i prodotti sono *general purpose*, per cui possono essere utilizzati in chiaro, ma nel momento in cui vanno a monitorare dei dati sensibili, devono essere securizzati, nel rispetto della normativa sulla *privacy*, in quanto effettivi strumenti di intercettazione.

Il dottor Bruni, approfondendo la tematica della *cyber security*, si è soffermato sulle attuali tecnologie per la protezione dei *data center* e sulle nuove sfide della criminalità informatica rappresentate dal *cloud*, che lascia aperto il problema della protezione degli accessi alle informazioni.

Audizione del dottor Mirko Gatto e del dottor Alessandro Beulcke, in rappresentanza della società Yarix, seduta n. 315 del 2 agosto 2017

Il dottor Gatto ha iniziato l'audizione con una breve descrizione delle attività della società Yarix, articolata fondamentalmente su cinque servizi: il primo, la *security assessment* o *ethical hacking,* erogato ad aziende private e pubbliche amministrazioni con i quali si effettuano *penetration test* nei sistemi dei clienti autorizzati per individuare vulnerabilità attraverso un *team* di analisti che opera sul *deep web* o sulla rete oscura, *darknet,* alla ricerca di attori di minaccia, più o meno noti. Il secondo settore di attività è la *digital forensics* ovvero la scienza che fissa i parametri entro cui operare per condurre un'investigazione informatica; la terza attività riguarda la *compliance*: ISO 27001, che è la normativa di riferimento per la *cyber security*, PCI-DSS, che riguarda la sicurezza sui pagamenti e quindi

il mondo *retail* e il settore finanziario e GDPR, cioè le nuove regole in materia di *privacy* cui ci si dovrà adeguare entro maggio 2018.

La quarta attività si ricollega alla costituzione nel 2014 di un *Security Operation Center,* un centro di monitoraggio presidiato per ventiquattro ore al giorno, che ha base in Italia: tale attività ha consentito alla società di entrare a far parte del FIRST (*Forum for Incident Response and Security Team*), il centro di monitoraggio privato più importante al mondo, che permette oggi un confronto su un tavolo internazionale con aziende della portata di eBay, NASA, Apple, NSA; infine, l'ultima attività che svolge la Yarix è quella di *cyber intelligence* con un *team* di analisti che si inserisce nella *darknet*, nelle *chat* presenti nei gruppi di *cyber* organizzazioni criminali per intercettare attori di minaccia emergenti o non conosciuti.

I commissari hanno formulato quesiti all'audito sull'utilizzo del *dark web* e del *deep web* in Italia, sulle caratteristiche dell'azienda e del *software* dalla stessa prodotto.

3. Conclusioni e proposte

Alla luce delle risultanze emerse dall'insieme delle audizioni svolte e dalla documentazione acquisita nel corso dell'indagine, il Comitato reputa opportuno avanzare le seguenti proposte:

1) si manifesta l'esigenza di un rafforzamento dell'Ufficio centrale per la segretezza (UCSe), all'interno del DIS, al quale affidare la vigilanza operativa sulle aziende interessate e lo svolgimento di verifiche costanti e periodiche sulla sussistenza dei necessari *standard* di sicurezza ed affidabilità; si pone l'accento altresì, in via generale, sulla necessaria e precisa individuazione delle diverse responsabilità che fanno capo alla fornitura dei *software*, all'attivazione dei virus e degli strumenti di captazione ed alla corretta utilizzazione dei dati e delle informazioni in tal modo acquisite;

2) nell'ambito del DIS – il cui ruolo nella difesa della sicurezza cibernetica risulta rafforzato per effetto del decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, recante «*Architettura istituzionale per la tutela della sicurezza cibernetica del Paese*» – si rende utile prevedere un'apposita struttura competente nella creazione di progetti sorgenti da impiegare nei sistemi di captazione da remoto in modo da avere a disposizione nell'immediato futuro prodotti certificati di origine italiana, muniti dei requisiti di qualità, sicurezza ed affidabilità;

3) occorre coordinare, da parte del DIS, la rete dei vari CERT *(Computer Emergency Response Team)* in modo che rispondano ad una regia unitaria e coerente nella definizione dei criteri minimi di certificazione della qualità delle varie aziende;

4) si auspica, infine, la valorizzazione di apposite linee guida tra le aziende coinvolte e gli uffici giudiziari competenti, sull'esempio di alcune

procure italiane, per il corretto impiego delle strumentazioni volte ad attività di intercettazione e captazione.

€ 4,00