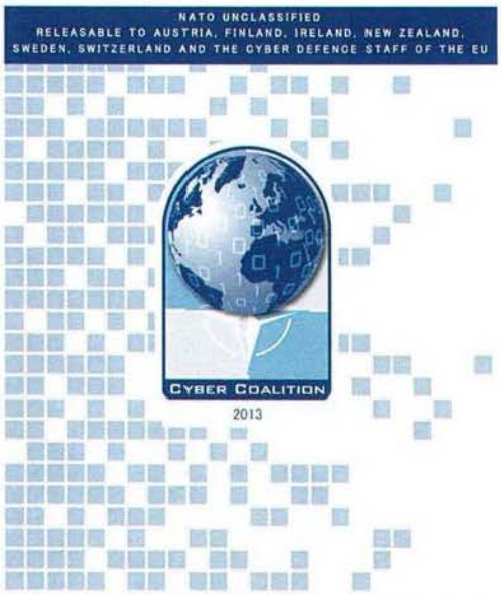
Alla fine del 2013, lo stesso Dicastero ha avviato una prima sperimentazione dei processi e delle procedure per la costituzione del CERT-N che, chiamato ad operare sia a livello preventivo che reattivo, rappresenta il punto di contatto nazionale con le omologhe strutture di altri Paesi e con il CERT europeo, gestito dall'*European Network and Information Security Agency* (ENISA).

Allo scopo, poi, di testare l'efficacia delle procedure e del flusso di informazioni tra i soggetti pubblici e privati, anche alla luce dell'architettura nazionale *cyber* delineata dal richiamato DPCM 24 gennaio 2013, ed individuare le principali criticità ai fini di un'efficace gestione degli incidenti informatici di maggiore rilevanza, il TTC non ha mancato di fornire supporto all'organizzazione ed allo svolgimento dell'***esercitazione nazionale di cyber-security "CybIt 2013".*** Quest'ultima – tenutasi il 5 dicembre ed organizzata dal Ministero dello Sviluppo Economico su mandato del Nucleo per la Sicurezza Cibernetica – ha visto la partecipazione di rappresentanti del Comparto intelligence, del Nucleo per la Sicurezza Cibernetica, del medesimo MiSE (CERT-N), del Ministero dell'Interno (CNAIPIC), del Ministero della Difesa (CERT-Difesa), dell'AgID, delle Unità Locali di Sicurezza (ULS) del Ministero dell'Economia e delle Finanze e del Ministero degli Affari Esteri, nonché della Società Generale d'Informatica (Sogei) SpA. Tenuto conto che lo scenario simulato prevedeva un attacco *cyber* ad un nodo di distribuzione dell'energia elettrica di rilievo strategico, all'esercitazione hanno aderito anche rappresentanti di dui dei principali operatori privati di settore: Enel e Terna.

Sempre in materia di esercitazioni e nell'ottica di arricchire ulteriormente le esperienze dei soggetti nazionali chiamati a gestire possibili eventi *cyber*, i componenti del TTC hanno partecipato come osservatori alla "***Cyber Coalition 2013***", esercitazione internazionale di matrice NATO che, avviata il 25 novembre sotto l'egida, per l'Italia, del Ministero della Difesa, ha simulato la protezione di una rete informatica da "attacchi malevoli" al fine di migliorare il coordinamento e la cooperazione, e di perfezionare le procedure di scambio in-

formativo tra l'Alleanza militare ed i suoi membri.



Protezione delle infrastrutture critiche e *partnership* pubblico-privata

Il TTC – nella consapevolezza che la tutela dello spazio cibernetico costituisce un obiettivo strategico da perseguire con il concorso di tutti gli attori che operano nell'ambito dello stesso – ha sin dall'inizio adottato un approccio multidimensionale mirante a garantire, accanto all'interazione delle componenti istituzionali sopra richiamate (sia civili che militari), anche il **coinvolgimento del settore privato**. Tale coinvolgimento, che trova fondamento nella naturale convergenza tra interessi di sicurezza nazionale e quelli di imprese ed operatori privati, mira alla definizione di azioni congiunte, utili ad accrescere la sicurezza cibernetica del Paese.

In tale ottica, è stato istituito il cd. "***Tavolo Imprese***" che, nel corso della sua prima riunione, tenutasi nel mese di novembre, ha visto la partecipazione dei 10 soggetti con i quali il Dipartimento Informazioni per la Sicurezza (DIS) ha sottoscritto, in ragione della loro centralità nella *governance* nazionale cibernetica, apposite convenzioni ex articolo 11 del DPCM del 24 gennaio 2013: i gestori di servizi di pubblica utilità e gli attori privati di rilevanza strategica per il sistema-Paese. Nell'ambito del richiamato incontro, prevalentemente dedicato all'illustrazione delle attività di implementazione dell'architettura nazionale *cyber* sviluppate con il supporto del TTC, si è convenuto sulla necessità di pervenire alla graduale strutturazione di uno scambio informativo che, nel rispetto delle normative vigenti, consenta la realizzazione di un'efficace comunicazione su questioni di interesse in materia di *cyber security*.

A garanzia della correttezza del citato scambio informativo ed in una logica di leale collaborazione istituzionale, il Dipartimento Informazioni per la Sicurezza, come evidenziato nella Premessa di questa Relazione, ha sottoscritto, nel mese di novembre, un **protocollo d'intenti con il Garante per la protezione dei dati personali**, mirante, tra l'altro, a comunicare al Garante il piano ricogniti-

vo degli archivi informatici cui ha accesso il Comparto ai sensi dell'art. 13, comma 2 della Legge 124/07, a sistematizzare le modalità di esecuzione degli accertamenti svolti dal Garante su tali accessi e a consentire all'intelligence di avvalersi, fuori dei casi di parere già previsti dalla normativa vigente, dell'attività consultiva della Autorità su tematiche attinenti al trattamento dei dati personali.

Le richiamate iniziative assunte all'interno del nostro Paese, pur utili e necessarie, non sono tuttavia sufficienti a fornire adeguate risposte ad una minaccia che travalica i confini nazionali. Con tale premessa sullo sfondo, il TTC, facendo perno sul Ministero degli Affari Esteri, ha seguito una serie di **iniziative internazionali di settore**, allo scopo di definire una comune posizione nazionale, utile a fornire contributi alla definizione dei quadri regolatori e delle strategie multilaterali di approccio bilanciato allo spazio cibernetico, tanto sul piano delle tutele quanto sul piano delle opportunità. Particolare attenzione è stata dedicata:

- ai ***rapporti di cooperazione bilaterale Italia-Israele***. Alla partecipazione di una delegazione nazionale (composta da rappresentanti delle istituzioni, del mondo accademico e delle imprese) alla Conferenza di sicurezza cibernetica tenutasi a Tel Aviv il 9-12 giugno ha fatto seguito un successivo incontro in Italia (2-3 settembre) in vista del rafforzamento delle condizioni per possibili convergenze tra *start-up* israeliane e PMI nazionali. Tali incontri, prodromici al vertice bilaterale italo-israeliano svoltosi a Roma il successivo 2 dicembre, hanno portato, nell'ambito di quest'ultima occasione, alla sottoscrizione di una *Joint Declaration* mirante a tracciare le linee lungo le quali informare future forme di cooperazione di settore tra i due Paesi. Il 27-28 gennaio del 2014, nell'ambito della conferenza-fiera *Cybertech* di Tel Aviv, si sono tenuti ulteriori incontri istituzionali e imprenditoriali;
- alla ***"Terza conferenza sullo spazio cibernetico"*** di Seoul del 17-18 ottobre. A tale evento, i cui esiti sono compendiati nel documento *"Outcome Document of Seoul Conference on Cyberspace"*, hanno preso parte, oltre ad attori istituzionali, anche una significativa componente dell'industria nazionale;
- alla proposta di ***Dichiarazione in materia di privacy e cyber security*** presentata dal Brasile in ambito UNESCO (in occasione della 37ª Conferenza Generale tenutasi a Parigi il 5-20 novembre) ed alla proposta di Risoluzione *"Il diritto alla privacy nell'era digitale"* presentata dalla Germania all'Assemblea Generale dell'ONU nel novembre 2013. Rispetto a tali documenti, finalizzati nella sua formulazione originaria a promuovere forme di controllo centralizzato della rete da parte dei Governi, l'Italia ha fornito, unitamente ad altri Stati UE, contributi che hanno agevolato l'adozione di testi fi-

nali nei quali le contrapposte esigenze di sicurezza e *privacy* sono risultate più bilanciate;

- alla ***presidenza italiana dell'Unione Europea (secondo semestre 2014)***. Il programma relativo al filone *cyber-security* è stato condiviso dal Ministero degli Affari Esteri con le competenti Amministrazioni del Tavolo Tecnico *Cyber* e con le stesse definito in tutti i suoi aspetti.

Attività del Comparto intelligence

Con riguardo alle **attività svolte dal Comparto intelligence**, il DIS, nel quadro delle attribuzioni di coordinamento della ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionale (articolo 4, lit. d.bis) della Legge 124/2007), ha assunto una serie di iniziative tese ad assicurare con continuità il più efficace concorso delle capacità dell'intelligence – espresse in formato integrato da DIS, AISE ed AISI – in termini di analisi tecnica, di *information assurance* (nel caso di eventuali compromissioni di sistemi o reti classificate), di attività info-operative e di analisi.

In particolare, nell'ambito del perseguimento degli obiettivi informativi in materia *cyber*, così come indicati nel documento di pianificazione per il 2013 approvato dal CISR, sono state poste in essere attività miranti a tutelare, sotto l'azione di coordinamento del DIS, *asset*, sia pubblici che privati, di particolare rilevanza strategica per il Paese.

Le attività info-operative condotte dal Comparto – per il cui dettaglio si rinvia all'apposito Capitolo della presente Relazione – hanno dato vita ad azioni improntate all'analisi, all'individuazione, alla classificazione ed al contenimento della minaccia. Di fronte a quest'ultima – concretizzatasi nei casi più significativi in attacchi informatici di tipo *Advanced Persistent Threat* (*vds. box 19*) miranti ad esfiltrare informazioni sensibili a soggetti di rilevanza industriale, scientifica e tecnologica, nonché ad attori di rilievo politico-strategico – il Comparto ha provveduto, a seconda dell'entità e della tipologia di reti/sistemi interessati, a fornire contributi atti a contestualizzare la minaccia e a supportare, ove necessario, le successive attività di *remediation* e di assistenza sistemistica, anche sotto il profilo dell'*information assurance*.

Al fine di rafforzare le capacità di prevenzione dell'intelligence, le attività info-operative hanno mirato, sul piano generale, ad acquisire elementi conoscitivi sulle più rilevanti vulnerabilità di sicurezza delle infrastrutture ICT (*Information and Communication Technology*) di enti ed aziende di interesse strategico per il Paese. La collaborazione instaurata dal Comparto con le articolazioni di sicurezza ICT di tali attori si è tradotta, specie di fronte ad eventi in corso, nell'individuazione delle più adeguate misure ai fini della mitigazione della minaccia e del contenimento dei suoi effetti.

box 19

GLI *ADVANCED PERSISTENT THREAT* (APT)

Gli APT consistono in un attacco mirato, volto ad installare una serie di *malware* all'interno delle reti del *target* al fine di riuscire a mantenere attivi dei canali che servono ad esfiltrare informazioni sensibili, ancorché non classificate.

Gli APT constano generalmente di sei fasi:

1. ***Ricognizione:*** consiste nella raccolta di informazioni sul *target* e sui soggetti che gravitano intorno allo stesso (ad es. partner e *vendor*), specie mediante tecniche di ingegneria sociale.
2. ***Intrusione nella rete:*** le citate tecniche consentono l'invio di email – generalmente a personale che riveste posizioni sensibili e delicate all'interno del *target*, in particolare i *senior manager* – contenenti link che rinviano a siti che scaricano *software* malevoli sulla macchina dell'utente ovvero email cui è allegato un file infetto. Ciò consente all'attaccante di accedere alla rete dell'obiettivo.
3. ***Consolidamento della presenza nella rete:*** il *malware* inoculato consente di installare moduli aggiuntivi che permettono di mappare la rete e di rilevare le relative vulnerabilità. L'attaccante, acquisite le credenziali di amministratore del sistema, si "mette in ascolto" di tutti i dati che passano sulla rete.
4. ***Sfruttamento delle vulnerabilità:*** tale fase consiste nello sfruttamento delle vulnerabilità dei servizi presenti sulla rete dell'organizzazione. Ciò consente di prolungare l'attacco e di penetrare sempre più nella rete del *target*, raccogliendo i dati di interesse.
5. ***Esfiltrazione dei dati:*** i dati raccolti vengono quindi generalmente cifrati, compressi ed inviati al di fuori della rete *target* verso un server normalmente intermedio rispetto a quello di comando e controllo impiegato dall'attaccante per gestire da remoto tutte le fasi dell'APT.
6. ***Mantenimento della persistenza:*** gli attaccanti cercano di mantenere la loro presesenza nelle reti del soggetto target anche se l'attacco viene da questi rilevato.

Alla valutazione di primo impatto ha, in alcuni casi, fatto seguito da parte dei soggetti attaccati la modulazione, sulla base delle immediate disponibilità e delle risorse/beni da proteggere, di interventi tesi a "segregare" in prima battuta le reti colpite, rinviando ad un secondo momento l'attuazione di interventi più strutturati, da attuare attraverso vere e proprie "compartimentazioni" dei sistemi, al fine di ricondurre il rischio ad un adeguato livello di accettabilità.

Le azioni poste in essere dal Comparto, oltre a fornire un contributo in termini di

riduzione delle vulnerabilità e, quindi, dei livelli di esposizione al rischio di sicurezza *cyber* da parte dei soggetti *target*, si sono tradotte anche in una specifica opera di supporto formativo. Sotto quest'ultimo profilo, le attività svolte hanno puntato ad accrescere la consapevolezza da parte degli "addetti ai lavori" delle caratteristiche peculiari rivestite dalla minaccia *cyber* e sulla necessità della costante effettuazione del monitoraggio delle reti, anche attraverso l'*auditing and securing* dei dispositivi di sicurezza perimetrali.

Particolare attenzione è stata posta anche alla rilevazione ed allo studio delle cosiddette *armi digitali*, ovvero dell'evoluzione delle procedure e degli strumenti attraverso i quali si concretizza la minaccia cibernetica. In tale contesto, prioritario interesse continua a rivestire l'incremento della cooperazione internazionale, soprattutto ai fini della condivisione di informazioni, di prassi, di strumenti e di capacità operazionali atti a consentire l'individuazione delle principali direttrici di sviluppo della minaccia e dei *target* di primario interesse degli attori ostili più strutturati.

In prospettiva, la riduzione del rischio di compromissione dello spazio cibernetico non potrà prescindere dall'adozione di un approccio sistemico, che includa l'adozione di appositi accorgimenti tecnici, tra i quali emergono:

- l'implementazione di opportune politiche di controllo degli accessi a dati e sistemi sensibili;
- l'uso di consolidate tecniche di crittografia a protezione di dati e sistemi, tenuto conto che firme e certificati digitali, sebbene non forniscano una garanzia assoluta, costituiscono ottimi strumenti di sicurezza;
- la garanzia della disponibilità di dati e di sistemi in uso presso *asset* critici, allo scopo di evitare soluzioni di continuità nell'erogazione di un servizio qualora sia necessario sostituire, a seguito di attacco, i *software* impiegati.

È in tale direzione che sono orientati i passi a supporto dell'ulteriore implementazione dell'architettura istituzionale delineata dal DPCM 24 gennaio 2013. Essi non potranno che estrinsecarsi nel raccordo delle iniziative organizzative e di *policy*, così come definite nel Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico e nel Piano Nazionale per la protezione cibernetica e la sicurezza informatica nazionale.