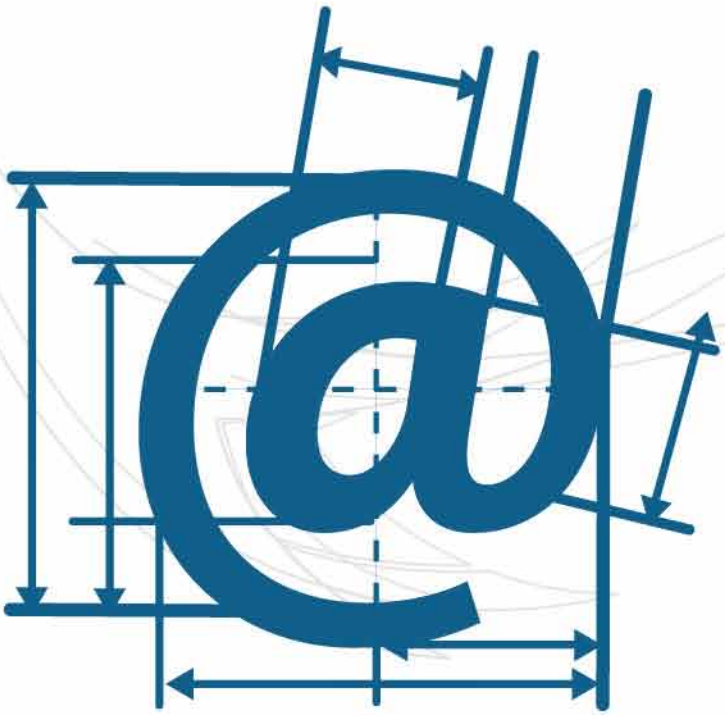
SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

DOCUMENTO DI SICUREZZA NAZIONALE



2018

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

AI SENSI DELL'ART. 38, CO. 1 BIS, LEGGE 124/2007

INDICE

Premessa

In un panorama internazionale in cui il confronto tra attori e schieramenti geopolitici ha assunto toni sempre più aspri, il cyber – con le sue caratteristiche di disponibilità diffusa, accessibilità, elevata "convenienza economica" e ridotti rischi di rilevazione – si è confermato per alcuni Stati uno degli strumenti cui fare ricorso per perseguire obiettivi strategici.

"il cyber si è confermato per alcuni Stati uno degli strumenti per perseguire obiettivi strategici„

Ne è stata un segno la crescente enfasi posta sul tema da parte di Governi ed Organizzazioni internazionali (in primis, NATO e UE), sempre più impegnati a prevedere, nell'ambito dei documenti di difesa e sicurezza, il potenziamento degli assetti cibernetici sotto il profilo tanto difensivo quanto offensivo. Parallelamente, a fronte del perdurare di campagne digitali ostili poste in essere da entità statuali o da gruppi da esse supportati, è proseguito, in seno a vari fori internazionali (OSCE, ONU, etc.), il dibattito sull'opportunità di regolamentare la responsabilità degli Stati nel dominio cibernetico, in base alle norme del diritto internazionale consuetudinario.

In attesa degli esiti di tale articolato e complesso dibattito, mentre taluni Governi hanno ventilato l'adozione di "difese avanzate" – con attacchi di tipo convenzionale in risposta ad attività digitali ostili, anche se "sotto la soglia" – altri sono intervenuti attribuendo pubblicamente campagne digitali ad alcuni Stati (o ai connessi apparati governativi), allo scopo di elevare i "costi" per la conduzione di tali attività attraverso l'esposizione pubblica dei responsabili e l'irrogazione di misure sanzionatorie.

L'obiettivo in tutti questi casi è stato quello di porre in essere forme di deterrenza e dissuasione nel tentativo di intaccare quel senso di impunità e quella spregiudicatezza che hanno costituito sinora la cifra dei più attivi attori ostili.

Sono state oggetto di attribuzione, nel 2018, tanto operazioni con finalità di spionaggio, quanto campagne di influenza/ingerenza volte a fomentare tensioni sociali o ad accrescere l'instabilità politica di alcuni Paesi dell'area euro-atlantica.

Nel periodo di riferimento, del resto, è stato rilevato un innalzamento nella qualità e nella complessità di alcune tipologie di attacco, con l'impiego sinergico di tutti i più avanzati strumenti tecnologici di ricerca informativa.

"un innalzamento nella qualità e nella complessità di alcune tipologie di attacco„

Le evidenze via via raccolte sulla minaccia, portato diretto delle attività informative condotte da AISE ed AISI sotto il coordinamento rafforzato della componente "core" del DIS, sono state messe a disposizione – con gli accorgimenti necessari a salvaguardare lo sviluppo delle cyber operation ed evitare eventuali, ulteriori danni ai target – dell'articolazione del

Dipartimento cui sono affidate funzioni di sviluppo dell'architettura nazionale cyber, onde consentire la disseminazione di misure di prevenzione e difesa di reti e sistemi strategici adeguate all'effettivo livello di rischio.

In quest'ottica, sono state molteplici le iniziative adottate per consolidare la sicurezza dei richiamati assetti: dall'avvio operativo del Nucleo per la Sicurezza Cibernetica (NSC), sede di raccordo tra le amministrazioni titolari di specifiche competenze in materia, alla nomina di una dedicata figura di riferimento, nella persona di un Vice Direttore Generale del DIS, sino al recepimento della Direttiva UE 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cd. Direttiva NIS), avvenuto con D.Lgs. 65/2018.

Stato della minaccia cibernetica

Ambiti e attori

Il panorama della minaccia ha continuato a caratterizzarsi per l'elevata rimunerativitá dello strumento cyber per gli attori ostili, in ragione dell'ampia disponibilità di tool offensivi e dei bassi livelli di rischio operativo. Dal monitoraggio delle Tecniche, Tattiche e Procedure (TTP) utilizzate è emerso un accresciuto livello di complessità e sofisticatezza delle azioni, l'uso combinato di strumenti offensivi sviluppati ad hoc con quelli presenti nei sistemi target impiegati in modo ostile, nonché il "riuso" di oggetti malevoli (malware) allo scopo di ricondurne la matrice ad altri attori (cd. operazioni false flag).

In tale contesto, lo sforzo più significativo posto in essere dal Comparto ha riguardato il contrasto di campagne di spionaggio digitale, gran parte delle quali verosimilmente riconducibili a gruppi ostili strutturati, contigui ad apparati governativi o che da questi ultimi hanno ricevuto linee di indirizzo strategico e supporto finanziario.

"lo sforzo più significativo ha riguardato il contrasto di campagne di spionaggio digitale„

Quanto alle finalità perseguite, gli attacchi hanno mirato, da un lato, a sottrarre informazioni relative ai principali dossier di sicurezza internazionale, e, dall'altro, a danneggiare i sistemi informatici di operatori, anche nazionali, attivi nello Oil&Gas, nonché quelli di esponenti del mondo accademico italiano, nell'ambito di una campagna globale mirante a profilare settori d'eccellenza di università e centri di ricerca.

Sul fronte delle infrastrutture di attacco, i gruppi responsabili di azioni di cyber-espionage hanno proseguito nell'impiego di servizi IT commerciali (domini web, servizi di hosting, etc.), forniti da provider localizzati in diverse regioni geografiche, anche per rendere difficoltoso il processo di individuazione/attribuzione, mentre, sul versante dei vettori, è rimasto elevato il ricorso alle tecniche di spear-phishing, che hanno ancora una volta garantito alti tassi di successo alle azioni intrusive, attesa pure la persistente, scarsa consapevolezza delle vittime. Tra queste ultime si sono annoverate, non di rado, figure apicali di Istituzioni e di primarie realtà del settore privato, nei confronti delle quali l'attaccante ha svolto attività di profilazione (analisi del-

le abitudini digitali) funzionali rispetto ad azioni di social engineering e, in alcuni casi, al reclutamento di natura convenzionale. Si sono confermati, inoltre, target privilegiati i soggetti coinvolti nella supply chain ICT – tra cui Managed Service Provider (MSP), società di consulenza, produttori/rivenditori di tecnologie e altri operatori che forniscono supporto tecnologico a terzi – destinatari di un volume di attacchi accresciuto rispetto al passato. Qui, l'attaccante ha colpito le infrastrutture tecnologiche degli obiettivi finali tramite la violazione preventiva di quelle dei fornitori, abusando sovente anche delle relazioni di fiducia connesse al rapporto contrattuale.

"target privilegiati i soggetti coinvolti nella supply chain ICT„

Attenzione è stata rivolta anche alla cd. minaccia ibrida, considerata quale impiego combinato di strumenti convenzionali e non, le cui traduzioni operative sono risultate (e saranno sempre più) amplificate grazie alla digitalizzazione che ha interessato ogni aspetto della vita sociale, arrivando ad esplicitarsi anche in operazioni di influenza/ingerenza poste in essere per condizionare il corretto svolgimento di fondamentali dinamiche dei processi democratici. Anche qui, senza il rischio di esposizioni per l'attaccante, attesa la sua capacità di mantenersi al di sotto di una soglia rilevabile di responsabilità, e con l'impiego di un quantitativo di risorse notevolmente inferiore rispetto a quelle necessarie per condurre azioni convenzionali.

"la cd. minaccia ibrida si è esplicitata anche in operazioni di influenza/ ingerenza „

LA DISINFORMAZIONE ON LINE: LA RISPOSTA DELLA UE

Le campagne di disinformazione, attuate prevalentemente tramite l'uso dei social network, rappresentano uno degli strumenti attraverso cui attori ostili tentano di orientare l'opinione pubblica, interferendo finanche con processi fondamentali per la vita democratica, come le elezioni.

In vista dell'appuntamento elettorale europeo del maggio 2019, la Commissione europea e l'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza, su mandato del Consiglio UE, hanno varato, nel dicembre 2018, il "Piano d'Azione contro la disinformazione". L'iniziativa si concentra sul miglioramento delle capacità di individuare, analizzare e rendere note le fake news, sul rafforzamento della risposta comune e coordinata tra gli Stati, sulla mobilitazione del settore privato nel contrasto alla disinformazione e sulla sensibilizzazione dell'opinione pubblica per accrescere la resilienza della società.

Il Comparto, al pari di quanto fatto dalle comunità intelligence dei principali partner internazionali, ha istituito agli inizi del 2018 un esercizio ad hoc teso a cogliere – all'interno del perimetro definito dal quadro normativo vigente – eventuali indizi di influenza, interferenza o condizionamento del processo elettorale del 4 marzo.

Tale esercizio è stato riattivato nel mese di novembre in vista dell'appuntamento per il rinnovo del Parlamento europeo.

Quanto all'hacktivism, nel cui ambito hanno continuato ad operare sigle minori sotto l'egida del più noto collettivo digitale "Anonymous Italia", le sortite più significa-

tive hanno riguardato l'avvio, ovvero il proseguimento, di una serie di operazioni, tra cui "#OpBlackWeek", con la pubblicazione on line di dati esfiltrati da sistemi di istituzioni operanti nei settori dell'Istruzione, del Lavoro, della Sanità, dei Sindacati, delle Forze dell'ordine, dei Comuni e delle Regioni.

Si è confermato di segno limitato l'attivismo di individui/gruppi riconducibili al cyberterrorismo, che hanno fatto registrare anche nel 2018 l'utilizzo di piattaforme social e di applicazioni di messaggistica per lo più per finalità di propaganda e proselitismo.

"di segno limitato l'attivismo di individui/gruppi riconducibili al cyber-terrorismo„

A distanza di cinque anni dalla sua istituzione, il Tavolo Tecnico Imprese (TTI) – una delle più riuscite esperienze nazionali di partenariato pubblico-privato nel settore – ha attestato come la collaborazione tra Istituzioni ed operatori strategici sia nodale per un Paese che aspira a mettere in sicurezza il suo perimetro cibernetico. Sullo sfondo di un accresciuto interscambio di dati tecnici, il TTI ha continuato ad essere la sede di iniziative finalizzate alla condivisione di analisi sui profili di rischio connessi all'impiego di determinate soluzioni tecnologiche, favorendo, al tempo stesso, lo scambio informativo su malware/campagne ostili in danno di specifici settori economico-industriali.

"la collaborazione tra Istituzioni ed operatori strategici nodale per la sicurezza cibernetica nazionale„

Andamento della minaccia

A compendio dello scenario descritto, sono state elaborate, come di consueto, statistiche relative alle azioni digitali condotte contro gli assetti informatici rilevanti per la sicurezza nazionale. Ciò sulla base degli elementi informativi acquisiti autonomamente da AISE ed AISI ovvero scambiati nel quadro dei rapporti di cooperazione con i principali Servizi collegati esteri e nell'ambito degli Organismi internazionali dedicati alla materia. In termini di metodo, deve essere sottolineato che esigenze di riservatezza sull'entità numerica delle minacce rilevate ne impongono la trasposizione solo in valori percentuali e che il significativo incremento di attacchi registrato nel 2018 va ascritto principalmente alle maggiori capacità di rilevamento e ad una loro più accurata classificazione e sistematizzazione, che ha permesso di ricavare una più granulare mappatura dello scenario della minaccia cyber in Italia.

Con tali premesse, dai dati del periodo in esame emerge un numero complessivo di azioni ostili più che quintuplicato rispetto al 2017, prevalentemente in danno dei sistemi informatici di pubbliche amministrazioni centrali e locali (72%).

Un'analisi più approfondita degli eventi che hanno interessato i soggetti pubblici attesta un incremento pari a oltre sei volte (+561%) rispetto all'anno precedente. È stato rilevato, in particolare, un sensibile aumento di attacchi contro reti ministeriali (24% delle azioni ostili, in aumen-

"azioni ostili prevalentemente in danno di pubbliche amministrazioni centrali e locali„

to di 306 punti percentuali) e contro infrastrutture IT riconducibili ad enti locali (39% del totale del periodo in esame, con una crescita in termini assoluti pari a circa 15 volte).

Le citate attività sono da ascrivere in larga parte ad azioni di stampo hacktivista, tra cui la richiamata campagna "#OpBlackWeek", volta a screditare le Istituzioni nazionali, ad opera delle principali crew attive nel panorama italiano: Anonymous Italia, LulzSec ITA ed AntiSec ITA.

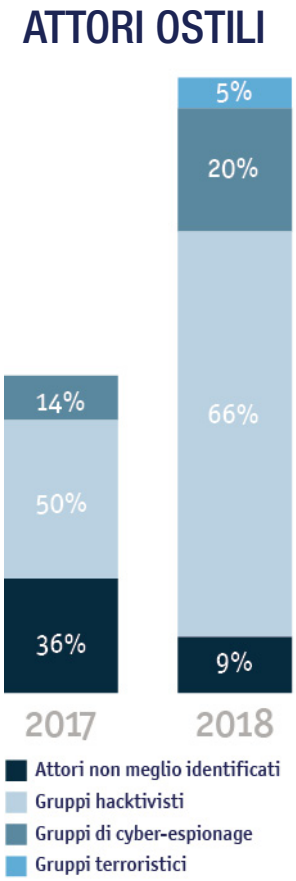
A tali formazioni vanno attribuiti anche gli attacchi contro risorse web e social media delle principali forze politiche nazionali (assimilate, ai fini della presente rilevazione, ai "soggetti pubblici" ed inserite nella categoria "Altro", di cui rappresentano circa un quarto del totale), impiegati per veicolare messaggi di dissenso e protesta, specie in prossimità della tornata elettorale del 4 marzo.

Ai medesimi collettivi è da ricondurre pure un cospicuo numero di attacchi – più che triplicati rispetto al 2017 – in danno di soggetti privati, afferenti per lo più i settori delle telecomunicazioni (6%) e dei trasporti (6%, triplicati rispetto al 2017), con particolare focus verso operatori del settore energetico (11%) e relativi fornitori (questi ultimi computati nell'ambito della categoria "Altro"), in linea con il rilancio internazionale delle campagne "#OpNuke" ed "#OpGreenRights": la prima, nata come forma di protesta per lo sviluppo dell'energia nucleare, la seconda, attuata in favore dell'impiego di fonti di energia sostenibili.

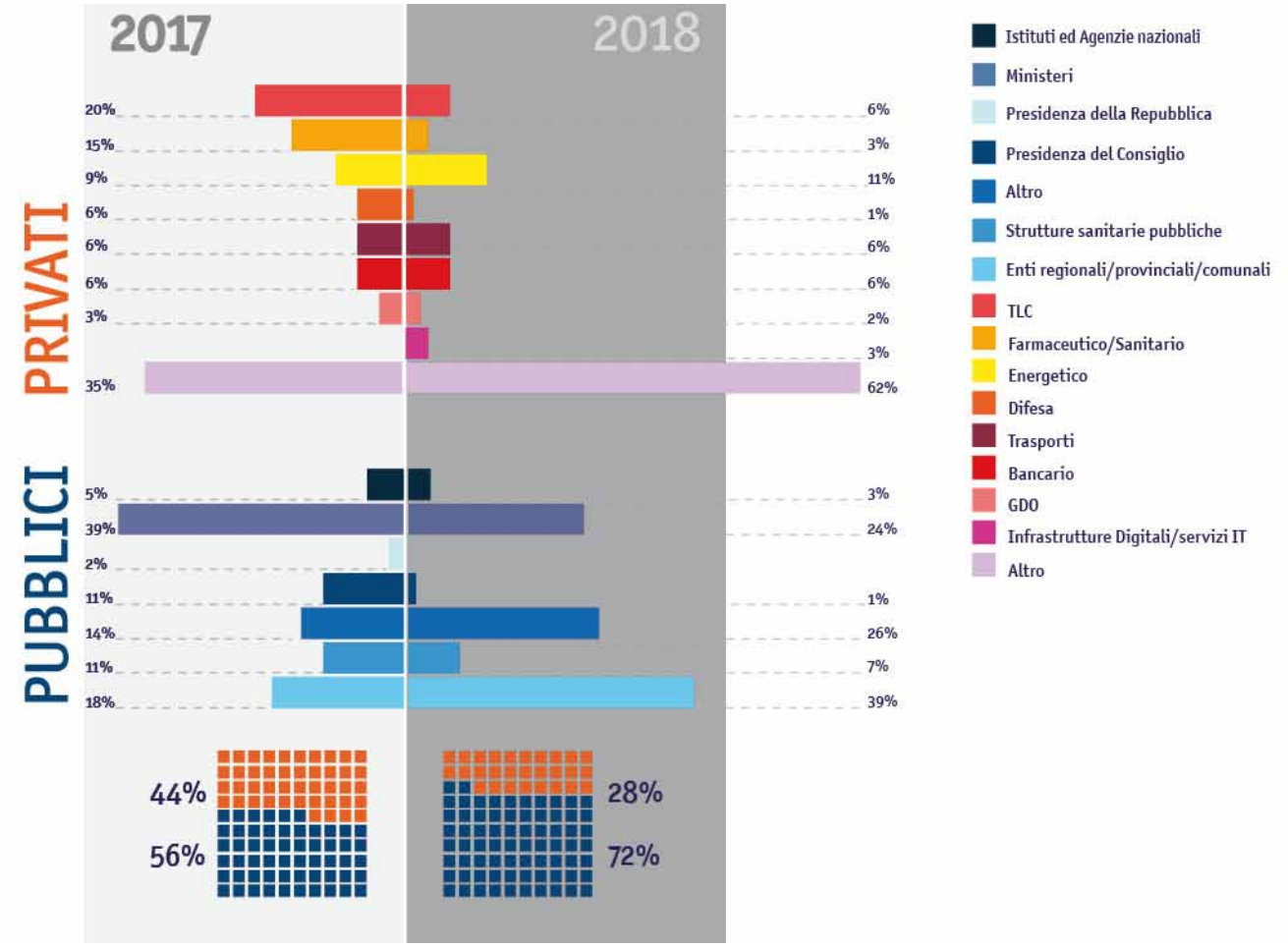
Per ciò che concerne gli attori ostili, il trend del 2018, in linea di continuità con quello degli ultimi anni e in coerenza con quanto appena descritto, ha identificato l'hacktivismo come la minaccia più consistente (66%), almeno in termini numerici. Tale dato va ascritto alla fase di particolare fermento che ha interessato i già citati Anonymous Italia, LulzSec ITA ed AntiSec ITA, caratterizzata da rinnovata capacità di pianificazione delle campagne ostili e dalla ricerca di una maggiore indipendenza da risorse tecnologiche di terze parti.

"l'hacktivismo è la minaccia più consistente, almeno in termini numerici„

Si sono mantenuti pressoché invariati gli attacchi di matrice statuale (20%), nonché i residuali tentativi di intrusione informatica riferibili a gruppi terroristici (5%), finalizzati, questi ultimi, principalmente al defacement di siti web afflitti da vulnerabilità facilmente



RIPARTIZIONE DEGLI ATTACCHI PER TIPOLOGIA DI TARGET



sfruttabili, sintomo del possesso di un know how limitato da parte di quelle formazioni.

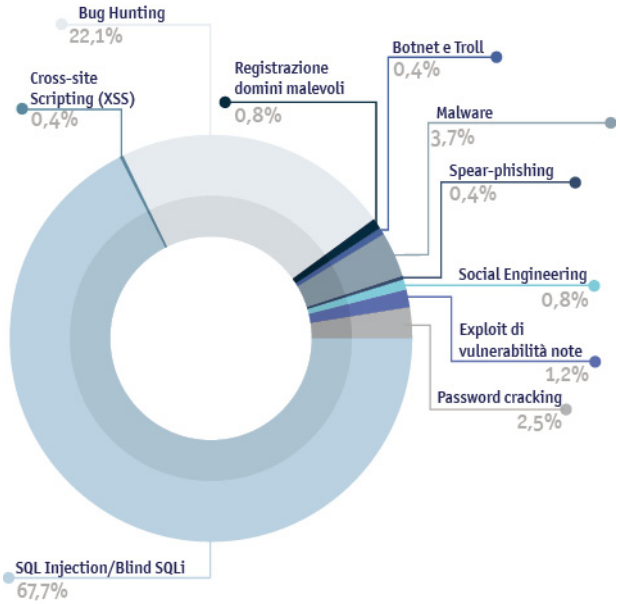
L' accennata adozione, di una più dettagliata tassonomia di classificazione delle tipologie di attacco ha consentito di rilevare nuove "sfumature" nel modus operandi degli attori ostili che, nel fare sempre più ricorso a tecniche di Bug Hunting (consistenti nella scansione di network e sistemi propedeutica allo sfruttamento di vulnerabilità note), hanno affiancato alle SQL Injection (circa il 68% del totale) l'impiego di malware (circa il 4%) e strumenti di password cracking (2,5%).

In termini di esiti, è stata confermata una netta prevalenza delle esfiltrazioni di informazioni sensibili da assetti informatici compromessi, ovvero – specie nel caso di azioni hacktiviste – la violazione di risorse IT dei target, con l'obiettivo di pubblicare manifesti e comunicati inerenti le singole campagne (cd. defacement).

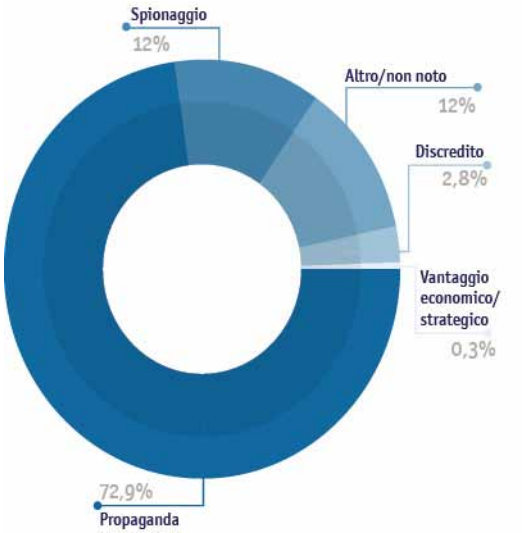
"netta prevalenza delle esfiltrazioni di informazioni sensibili"

Le finalità degli attacchi, perpetrati principalmente per scopi di propaganda (pari all'incirca al 73%), sono apparse coerenti con il richiamato, rinnovato vigore – tanto sul piano ideologico, quanto su quello operativo – del movimento hacktivista, che ha continuato a caratterizzarsi per la tendenza a

TIPOLOGIA ATTACCHI



FINALITÀ ATTACCHI



selezionare i target esclusivamente in funzione della tipologia di vulnerabilità riscontrate, sfruttabili con capacità tecniche ridotte e con un basso dispendio di risorse. Benché marginali in termini numerici (12%), le finalità di spionaggio hanno fatto registrare un considerevole aumento, specie in danno di assetti istituzionali ed industriali.

"tendenza a selezionare i target in funzione delle vulnerabilità"

POTENZIAMENTO DELLE CAPACITÀ CIBERNETICHE NAZIONALI

Tra le più significative iniziative di sviluppo dell'architettura nazionale cyber va annoverato l'avvio operativo del Nucleo per la Sicurezza Cibernetica (NSC) sotto la presidenza di un dedicato Vice Direttore Generale del DIS.

Riunitosi per la prima volta nel nuovo assetto il 21 febbraio, il NSC è stato convocato, come da previsione normativa, con cadenza mensile, agendo in chiave di prevenzione, preparazione, risposta e ripristino rispetto ad eventuali situazioni di crisi cyber, con l'obiettivo di rafforzare le capacità di difesa cibernetica del Paese.

Nell'esercizio delle sue funzioni, il NSC ha:

- verificato lo stato di attuazione delle misure di coordinamento interministeriale per finalità di preparazione e gestione delle crisi cibernetiche;
- raccolto ed analizzato dati su violazioni di sicurezza e compromissioni di reti e sistemi delle Amministrazioni titolari di funzioni critiche;
- promosso e coordinato la partecipazione nazionale ad esercitazioni cyber tra cui meritano particolare menzione la "Cyber

Europe 2018" – volta a incrementare la capacità di reazione e di intervento degli Stati UE – e la "European Union Hybrid Exercise-Multi Layer 2018 Parallel and Coordinated Exercise" (EU HEX-ML 18 PACE), rivolta a Istituzioni e Stati UE, nonché a Paesi NATO, al fine di verificarne le capacità di gestione di attacchi ibridi, comprendenti la componente cyber, contro infrastrutture critiche di vari settori.

"Il NSC ha gestito, in via straordinaria, eventi significativi,"

Il Nucleo ha poi gestito, in via straordinaria, eventi significativi che, pur non configurando situazioni di crisi cibernetica nazionale, hanno comportato lo sviluppo di attività di coordinamento delle azioni di risposta e di ripristino.

Rinnovato impulso è stato poi impresso all'implementazione degli indirizzi strategici previsti dal "Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico" e di quelli operativi inclusi nel discendente "Piano Nazionale", attraverso:

- l'avvio di un gruppo di lavoro, allargato ai Ministeri CISR, per la realizzazione di un "perimetro di sicurezza nazionale cibernetica", volto ad elevare i livelli di sicurezza degli assetti vitali del Paese;
- la costituzione di un ulteriore gruppo di lavoro, volto ad individuare linee guida per un procurement "sicuro" di prodotti e servizi ICT per la PA, coordinato dall'Agenzia per l'Italia Digitale (AgID), al quale hanno aderito, oltre ai componenti NSC, anche Consip;
- una stretta collaborazione con il MiSE per la creazione – in conformità alle normative italiane ed europee – del Centro di Valutazione e Certificazione Nazionale (CVCN) per la verifica delle condizioni di sicurezza delle soluzioni ICT destinate al funzionamento di reti, servizi delle infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale;
- lo sviluppo di sinergie – anche mediante la stipula di un protocollo tra DIS, AgID e Confindustria – volte ad assicurare l'interazione tra i Centri ad alta specializzazione, istituiti dal MiSE nell'ambito del Piano nazionale Impresa 4.0, e i Digital Innovation Hub (DIH) promossi da Confindustria in attuazione dell'iniziativa europea "Digitising

"L'INCIDENTE PEC"

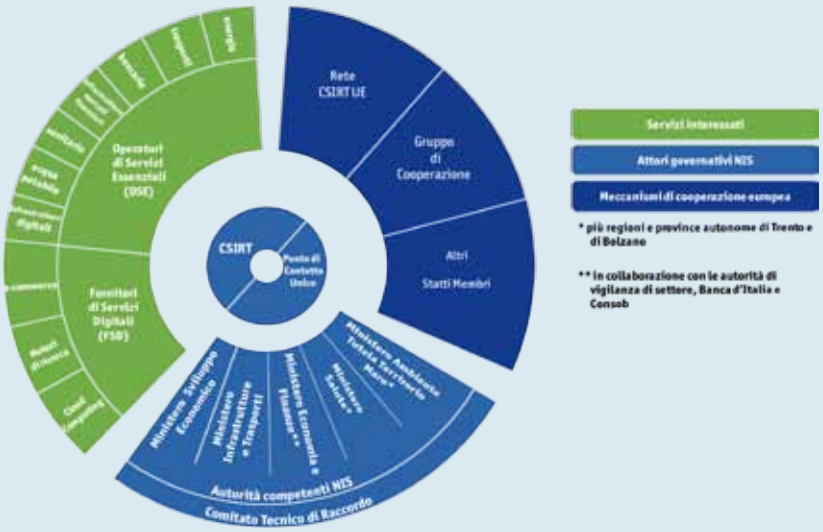
Il 13 novembre 2018 il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) del Dipartimento della P.S. ha segnalato all'Unità di Allertamento del Nucleo per la Sicurezza Cibernetica (NSC) un attacco informatico ad un fornitore di servizi di Posta elettronica certificata (Pec). L'attacco ha colpito circa 3.500 domini per un totale di 524.000 utenze, tra soggetti pubblici e privati, determinando anche una temporanea interruzione dei servizi informatici degli uffici giudiziari dei distretti di Corte di Appello. Il NSC – informandone costantemente il Presidente del Consiglio dei ministri – ha quindi provveduto, in stretto raccordo con i Ministeri di Giustizia e Difesa, con il CNAIPIC e con il CSIRT italiano, ad attivare un piano di protezione cibernetica che ha consentito di mitigare i danni e di procedere al ripristino delle funzionalità.

European Industry", per facilitare le imprese nella valutazione del proprio livello di maturità digitale e tecnologica;

- l'avvio di un'iniziativa, d'intesa con il Garante per la protezione dei dati personali, finalizzata ad agevolare l'armonica implementazione delle normative vigenti in materia di sicurezza informatica da parte degli attori privati interessati, tenendo conto del Regolamento (UE) 2016/679 "General Data Protection Regulation" (GDPR), del Decreto di recepimento della Direttiva NIS e delle Misure Minime di Sicurezza ICT emanate da AgID.

Il DIS, come accennato, ha contribuito attivamente alla redazione del Decreto Legislativo di recepimento della Direttiva NIS (D.Lgs. n. 65 del 18 maggio 2018), partecipando alle attività del gruppo di lavoro istitu-

LA DIRETTIVA NIS IN ITALIA



Il decreto legislativo che ha recepito nell'ordinamento nazionale la Direttiva (UE) 2016/1148 (cd. Direttiva NIS) si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD) che:

- sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l'obbligo di notificare, senza ingiustificato ritardo, al Computer Security Incident Response Team (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento, gli incidenti con impatto rilevante sulla continuità e/o sulla fornitura del servizio.

Tra le strutture previste dalla Direttiva NIS, un ruolo di rilievo spetta:

- al citato CSIRT, incaricato, oltre che di ricevere le notifiche degli eventi cyber rilevanti, di definire le procedure per la prevenzione e la gestione degli incidenti informatici;
- alle Autorità competenti NIS, responsabili dell'attuazione del decreto, chiamate a vigilare sulla sua applicazione e ad esercitare le relative potestà ispettive e sanzionatorie.

ito presso il Dipartimento Politiche Europee della Presidenza del Consiglio dei ministri.

Tale normativa ha assegnato al DIS il ruolo di Punto di Contatto unico NIS (PoC NIS) con il compito di assicurare, a livello nazionale, il coordinamento in materia di sicurezza delle reti e dei sistemi informativi e, a livello europeo, il raccordo necessario a garantire la cooperazione transfrontaliera delle Autorità NIS italiane con una serie di attori: Stati membri, NIS Cooperation Group (NIS CG) della Commissione e rete dei Computer Security Incident Response Team (CSIRT).

Nella sua qualità di PoC NIS, il DIS ha organizzato una serie di incontri con le Autorità competenti NIS e il CSIRT italiano al fine di coordinare l'attuazione del D.Lgs. 65/2018, favorendo il processo di identificazione degli OSE per ciascuno dei settori previsti dalla Direttiva UE, conclusosi con l'individuazione di 465 soggetti.

"il processo di identificazione degli OSE si è concluso con l'individuazione di 465 soggetti„

A seguire la fotografia dell'ecosistema nazionale cyber a fine 2018, quale risultante dall'adozione del citato D.Lgs. 65/2018, nonché del Decreto "Telco" del MiSE del 12 dicembre 2018, che dispone, per gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione

IL "CYBERSECURITY PACKAGE"

Il cd. Cybersecurity Package, di cui alla Comunicazione congiunta della Commissione Europea e dell'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza al Parlamento Europeo in tema di "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE" del 13 settembre 2017, si sostanzia in una serie di linee d'azione, suddivise in tre obiettivi generali e segnatamente:

1. potenziamento della resilienza della UE agli attacchi cibernetici: riforma dell'ENISA e introduzione di un framework di certificazione europeo, rapido e pieno recepimento della Direttiva NIS, sviluppo di un protocollo quadro (cd. Blueprint) in risposta alle crisi di sicurezza cibernetica della UE su larga scala, creazione di un Centro europeo di ricerca e competenze sulla sicurezza cibernetica con l'obiettivo di rafforzare l'ecosistema dell'Unione attraverso il coinvolgimento di ricerca e settore privato per lo sviluppo di nuove tecnologie (specie nei settori della crittografia, quantum computing e intelligenza artificiale), superando l'attuale frammentazione e ridondanza degli investimenti;
2. creazione di un'efficace deterrenza cibernetica nei confronti di attori statuali e non: sostegno al partenariato pubblico-privato, implementazione di un quadro relativo ad una risposta diplomatica congiunta dell'Unione Europea alle attività cyber malevole – cd. "Cyber Diplomacy Toolbox" – che individua, nell'ambito della politica estera e di sicurezza comune della UE, le possibili misure, incluse quelle sanzionatorie, che l'Unione e i singoli Stati membri possono adottare per prevenire ovvero rispondere ad un attacco informatico;
3. rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica: collaborazione UE-NATO e cooperazione in materia di capacity building in ambito cyber con Stati terzi.

elettronica accessibili al pubblico, l'adozione di misure di sicurezza e l'obbligo di notifica degli incidenti significativi.

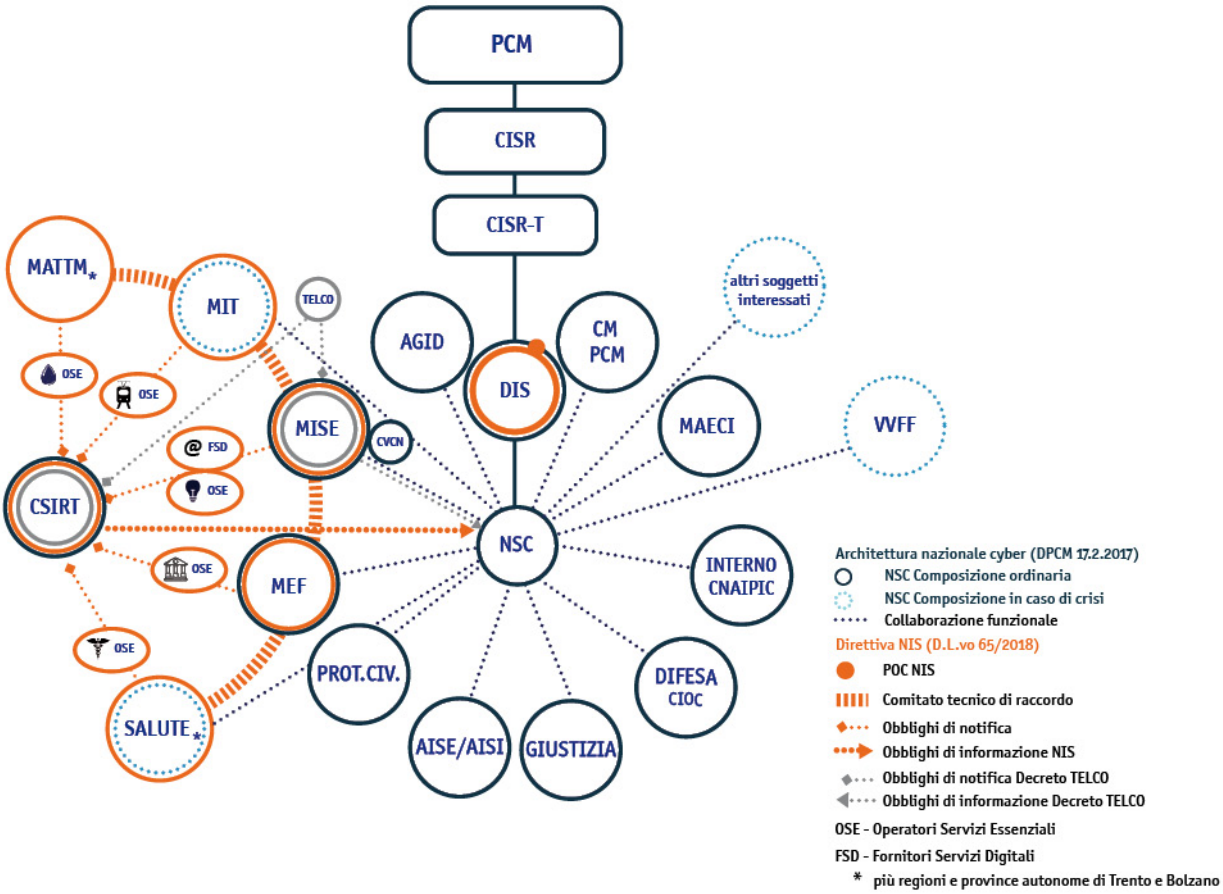
Nel corso dell'anno sono state inoltre definite – unitamente al MAECI e con il contributo delle Amministrazioni interessate – posizioni nazionali unitarie nell'ambito dei principali consessi internazionali (UE, NATO e OSCE), in relazione a documenti di policy con potenziale impatto sulla sicurezza nazionale cyber.

"alla particolare attenzione il cd. Cybersecurity Act"

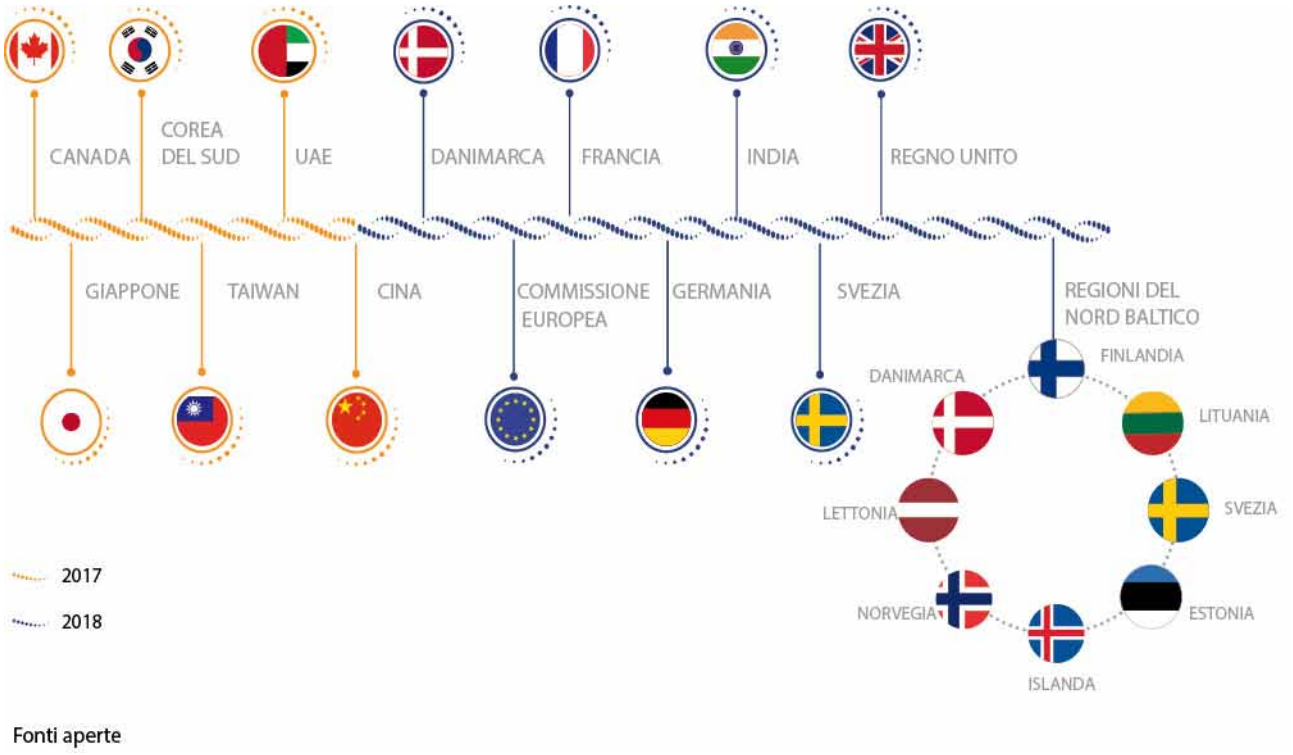
Alla particolare attenzione, considerata l'entità dei riflessi che seguiranno alla sua adozione, la "Proposta di Regolamento relativo all'European Network and Information Security Agency (ENISA) e alla certificazione della cybersicurezza per tecnologie ICT" (cd. Cybersecurity Act) che mira, da un lato, a rafforzare il mandato della citata Agenzia europea e, dall'altro, a introdurre un framework europeo di certificazione per soluzioni ICT destinate al mercato unico, così da ridurne le vulnerabilità attraverso sistemi standardizzati di verifica di sicurezza.

Quanto ai rapporti con l'accademia e il mondo della ricerca, particolare focus è stato posto sull'accrescimento della protezione e della resilienza ad attacchi cyber, nonché sulla promozione dello sviluppo secondo logiche di security-by-design di comunicazioni

ECOSISTEMA CYBER ITALIANO



STRATEGIE INTELLIGENZA ARTIFICIALE



Fonti aperte

wireless, servizi cloud e sistemi di controllo industriale; tecnologie, queste, nodali per il processo di trasformazione digitale nelle Pubbliche Amministrazioni e nel settore industriale. In particolare, il DIS ha sostenuto la creazione, all'interno del Consorzio Interuniversitario Nazionale per l'Informatica (CINI), di un Laboratorio Nazionale di Intelligenza Artificiale e Sistemi Intelligenti (IA&SI), attesa la rilevanza dell'intelligenza artificiale quale fattore per lo sviluppo economico e sociale del Paese.

"creazione di un Laboratorio Nazionale di Intelligenza Artificiale e Sistemi Intelligenti"

Infine, ad ulteriore sviluppo di "Be Aware Be Digital", la campagna nazionale per la formazione e la promozione di un utilizzo consapevole delle tecnologie ICT, è stato realizzato il primo videogioco ambientato nel cyberspazio, scaricabile su smartphone e tablet, rivolto agli studenti delle scuole secondarie di primo e secondo grado. Cybercity Chronicles, questo il nome, oltre ad ingaggiare gli utenti con nemici ed enigmi, contiene anche un Cyberbook per agevolare la familiarizzazione con le parole del dominio cibernetico, sfruttando le informazioni e gli insegnamenti appresi nel corso del gioco.

"videogioco ambientato nel cyberspazio"