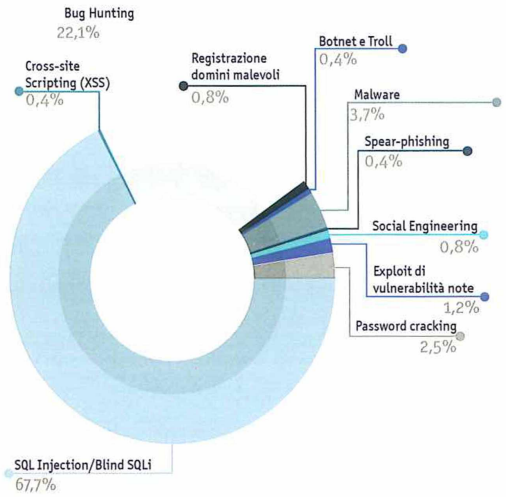
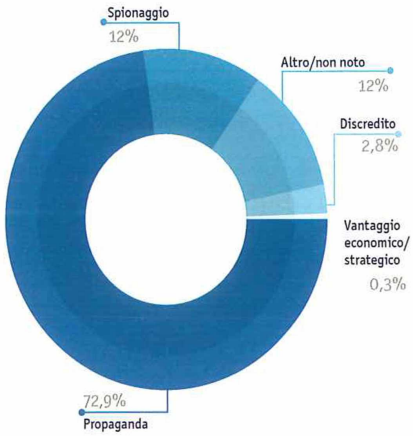
TIPOLOGIA ATTACCHI



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"

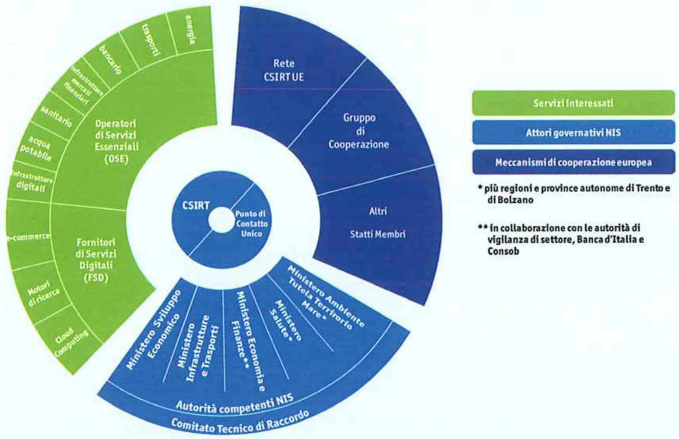
Il 13 novembre 2018 il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) del Dipartimento della P.S. ha segnalato all'Unità di Allertamento del Nucleo per la Sicurezza Cibernetica (NSC) un attacco informatico ad un fornitore di servizi di Posta elettronica 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.

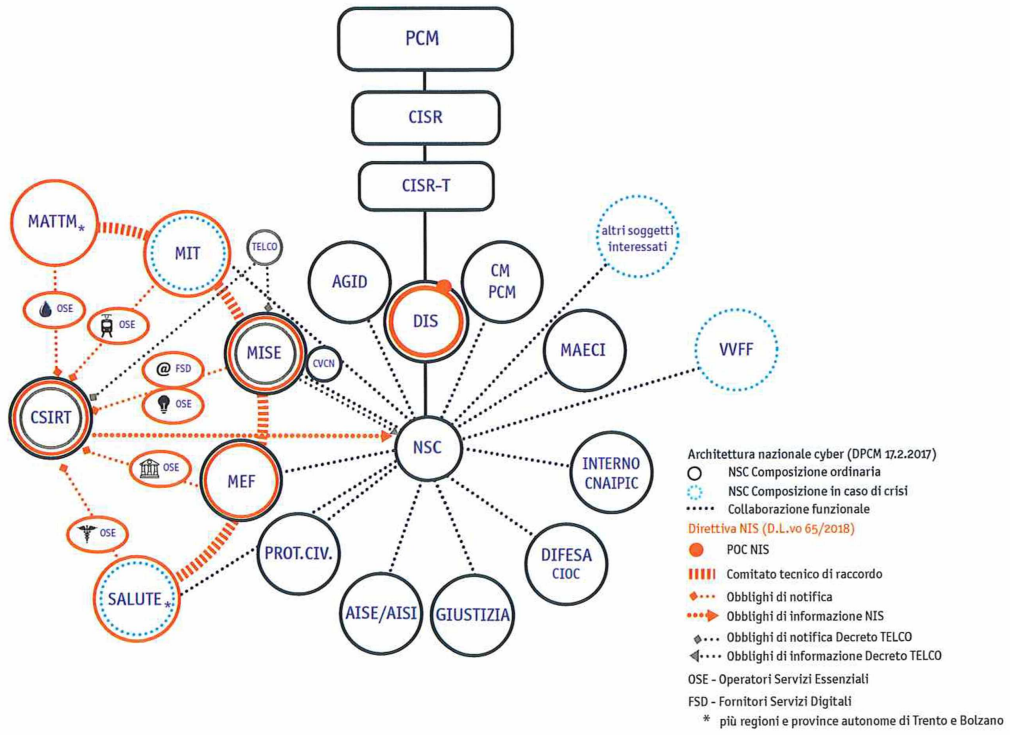
Nel corso dell'anno sono state inoltre definite – unitamente al MAECI e con il contributo delle Amministrazioni interessate – posizioni nazionali unitarie nell'ambito dei principali consessi internazionali (UE, NATO e OSCE), in relazione a documenti di policy con potenziale impatto sulla sicurezza nazionale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

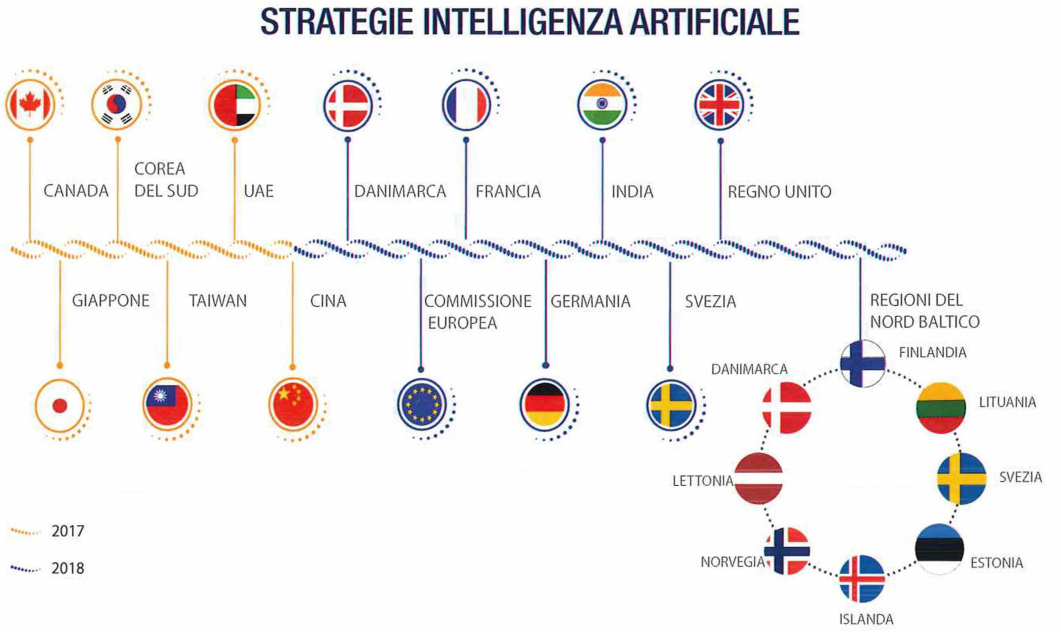
"alla particolare attenzione il cd. Cybersecurity Act,"

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





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"