programmazioni; per l'altro, slegare la *cyber security* da una dimensione puramente tecnica, conferendo alle criticità derivanti dalla stessa il medesimo rilievo di ogni altro rischio aziendale, così da elevarne il profilo e consentirne la trattazione nell'ambito dei Consigli di amministrazione delle aziende ovvero dei Comitati direttivi degli organismi pubblici.

Passando all'ambito del partenariato con le imprese strategiche, nel cui novero si sono aggiunti due nuovi soggetti nel 2015, il profilo più significativo delle attività svolte in seno al TTI ha fatto perno sull'*information-sharing;* processo in virtù del quale l'intelligence alimenta il suo patrimonio informativo e le imprese convenzionate arricchiscono le rispettive *knowledge-base,* così da potenziare, alla luce anche di ormai imprescindibili vincoli di spesa, le proprie capacità di difesa in modo mirato rispetto al *trend* della minaccia.

Gli incontri con le imprese, a seconda del rango dei rispettivi interlocutori, sono stati di taglio strategico ovvero di tipo più tattico-operativo. Nel 2015, nel corso delle sessioni di *policy* rivolte ai vertici aziendali ed ai responsabili delle strutture di sicurezza, sono stati effettuati punti di situazione sullo stato della minaccia cibernetica in Italia, con un particolare *focus* sulle evoluzioni delle azioni digitali effettuate per finalità di spionaggio e di cyberterrorismo, nonché sulle vulnerabilità che caratterizzano gli *Industrial Control Systems.*

Nell'ambito delle sessioni di livello tecnico – allargate, oltre che ai *Security Manager,* anche ai responsabili della sicurezza ICT delle imprese – sono stati svolti approfondimenti su "casi di studio" e sono state condivise informazioni tecniche (cd. *Indicators of Compromise*). Sotto tale profilo, l'obiettivo è stato quello di consentire, in caso di rilevazione della minaccia, la sua rapida identificazione per impedirne l'ulteriore propagazione sia all'interno dei sistemi dei *target* convenzionati, sia nell'ambito di quelli di soggetti, pubblici e privati, che mantengono relazioni con gli stessi.

Molteplici sono stati, inoltre, gli incontri bilaterali, tenutisi nella maggior parte dei casi su richiesta dei singoli operatori, per la trattazione di specifiche tematiche ovvero di puntuali ipotesi di minaccia. Lo scambio tra il Comparto ed i privati si è avvalso della funzionalità di un apposito portale, che ha conosciuto, a partire dalla seconda metà del 2015, una

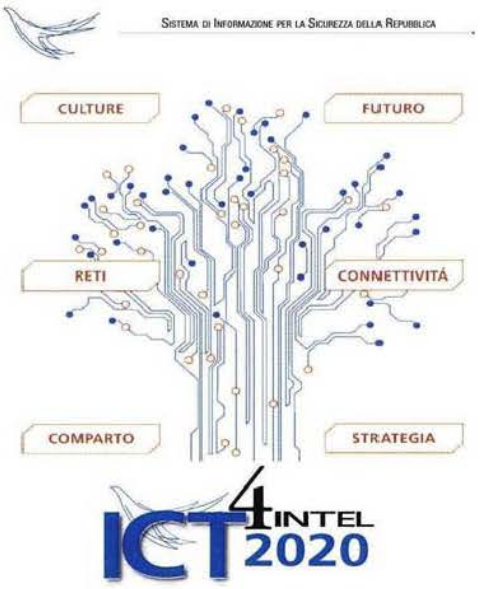
significativa implementazione tecnologica, destinata a rendere ancor più agevole, accrescendone i volumi, il richiamato *info-sharing*. Tra le principali innovazioni dell'applicativo – che sarà alimentato da dati sensibili – si evidenzia quella dell'impiego di strumenti di correlazione mirata e di analisi quantitativa per la valorizzazione del patrimonio informativo.

In ragione, poi, della **trasversalità delle tematiche** trattate, TTC e TTI hanno, in due circostanze, sviluppato iniziative congiunte. La prima, nel mese di marzo, in occasione della visita a Roma del *NATO Assistant Secretary General* per la Divisione *Emerging Security Challenges*, e la seconda, nel dicembre, per l'incontro con il Direttore Generale della *DG Connect* della Commissione Europea.

La riunione con il rappresentante della NATO, oltre a costituire utile occasione per l'illustrazione della *Enhanced Policy on Cyber Defence* dell'Alleanza, ha consentito agli attori privati di acquisire elementi sulla *NATO Industry Cyber Partnership*, quale modello di partenariato che mira, tra l'altro, ad agevolare l'innovazione e la conoscenza nell'ottica della creazione di soluzioni di *cyber* difesa interoperabili, cui hanno fatto richiesta di adesione, nel 2015, alcuni soggetti convenzionati.

L'incontro con il responsabile della *DG Connect*, invece, è stato incentrato sulla trattazione di due tematiche: la *Network and Information Security* (NIS), direttiva dell'Unione ratificata in dicembre dal Comitato dei Rappresentanti Permanenti della UE; la "*contractual Public-Private Partnership*" che include, tra i suoi princìpi fondanti, la creazione di un ecosistema ove rendere strutturale la cooperazione tra Accademia ed imprese.

Ulteriore iniziativa volta a consolidare il partenariato con gli attori convenzionati e, più in generale, con gli operatori dei settori industriali e di servizi con carattere strategico per la sicurezza nazionale, è stata l'**ICT 4INTEL 2020**, dedicata, nell'edizione 2015, al *cyber* secondo il paradigma rischi/opportunità. L'evento – che ha avuto luogo in novembre, presso la Scuola di formazione del Comparto – si è articolato in una prima sessione "chiusa" alla Comunità intelligence su temi di interesse strutturale (*agenda in tavola 1*) ed in una successiva giornata di lavori, dedicata alla *Partnership* Pubblico-Privato.



Obiettivo della seconda sessione, cui hanno partecipato anche rappresentanti di Università e Centri di ricerca, è stato quello di individuare rinnovate modalità di sinergia per meglio gestire le sfide e le opportunità connesse con il dominio cibernetico. L'ICT 4INTEL 2020 ha costituito, altresì, l'occasione per presentare ufficialmente il nuovo Polo Tecnologico quale "incubatore" di idee e soluzioni, nel cui ambito opera un "*Laboratorio Malware*" – primo esperimento di livello nazionale tra **INTELLIGENCE** (per l'individuazione delle esigenze operative), **ACCADEMIA** (per la capacità di ricerca avanzata) ed **INDUSTRIA** (per la sperimentazione e la produzione di nuovi modelli tecnologici di difesa) – mirante a sviluppare una capacità in materia di *malware reverse engineering*, allo scopo di individuare metodologie di rilevazione, analisi e rimozione di codici malevoli.

tav. 1

TEMATICHE *WORKSHOP* ICT4INTEL

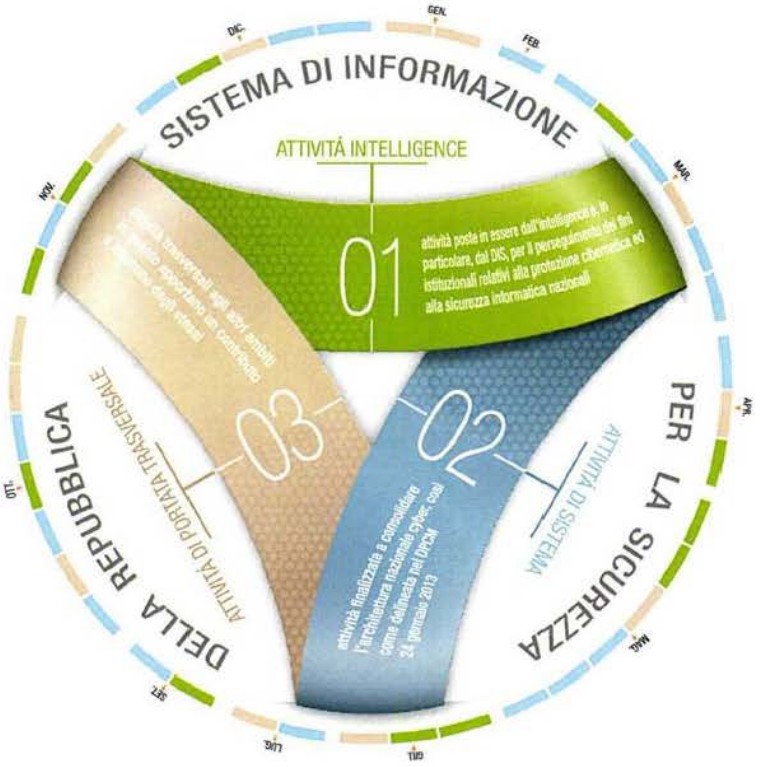
Tematiche dei *workshop* riservati al personale dell'intelligence:

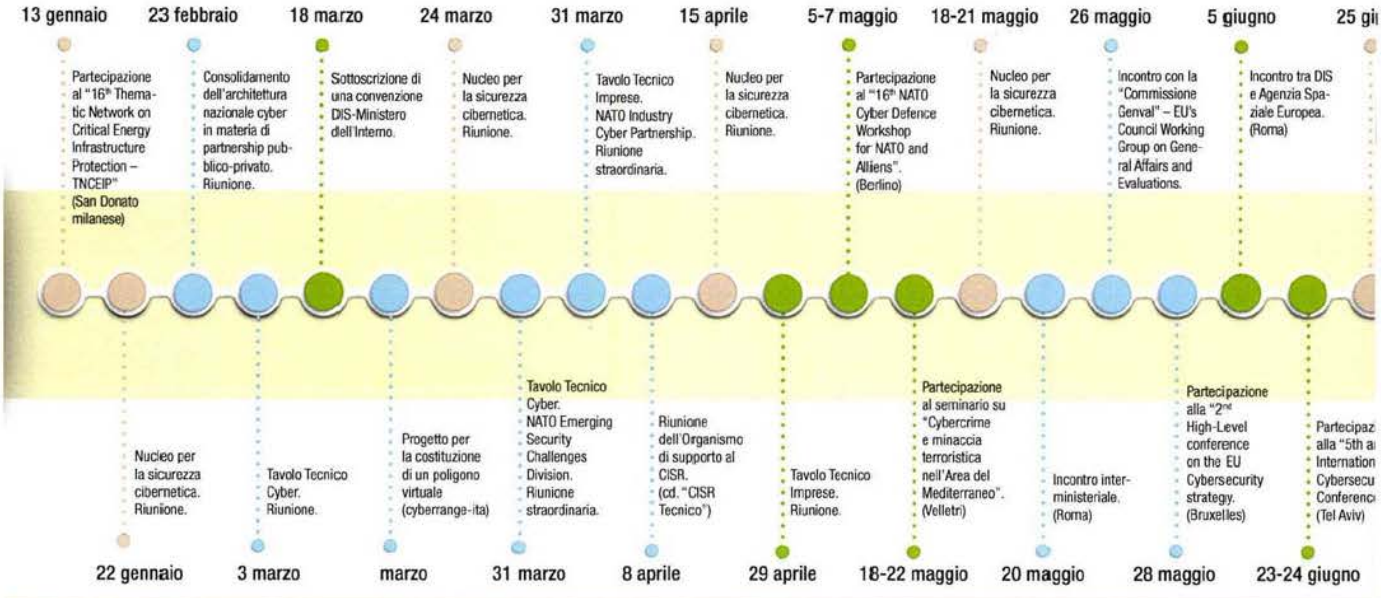
- la minaccia cibernetica: profili operativi e giuridico-legali;
- le caratteristiche dell'analisi e dell'analista *cyber*;
- il ruolo dell'OSINT nella prevenzione dei *cyber attacks*;
- la tecnologia quale "fattore abilitante" per la protezione cibernetica;
- il Centro di Eccellenza per la Ricerca *Cyber* Avanzata (CERCA) quale Polo Tecnologico di eccellenza nazionale;
- strumenti innovativi a supporto della protezione e confidenzialità delle informazioni.

QUADRO STRATEGICO NAZIONALE

INDIRIZZI STRATEGICI

- Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
- Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
- Incentivazione della cooperazione tra istituzioni ed imprese nazionali
- Promozione e diffusione della cultura della sicurezza cibernetica
- Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*
- Rafforzamento della cooperazione internazionale





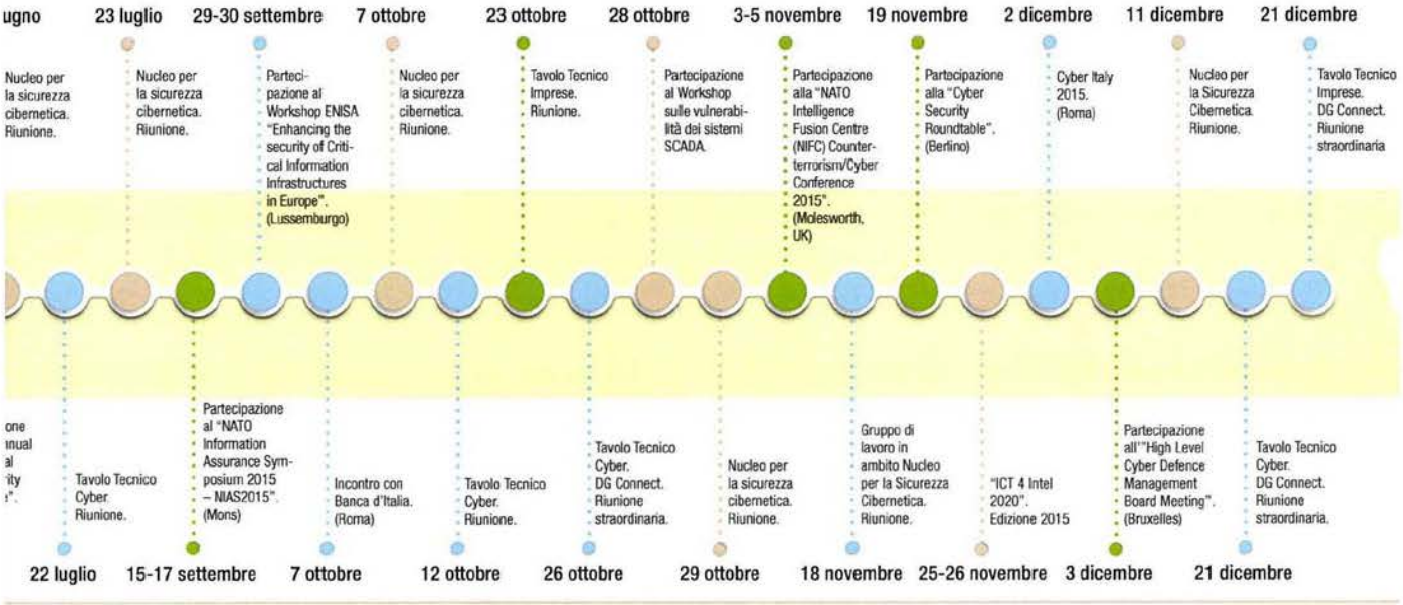
IL RUOLO DELL'INTELLIGENCE

NELLA PROTEZIONE CIBERNETICA E NELLA SICUREZZA INFORMATICA NAZIONALE

PIANO NAZIONALE

INDIRIZZI OPERATIVI

- Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
- Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
- Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento
- Cooperazione internazionale ed esercitazioni
- Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali
- Interventi legislativi e *compliance* con obblighi internazionali
- *Compliance* a *standard* e protocolli di sicurezza
- Supporto allo sviluppo industriale e tecnologico
- Comunicazione strategica
- Risorse
- Implementazione di un sistema di *Information Risk Management* nazionale



PAGINA BIANCA

Stato della minaccia cibernetica in Italia

Nel corso del 2015 lo spazio cibernetico si è consolidato quale "terreno di conflittualità diffusa" confermando, ancora una volta, il divario difficilmente colmabile tra il rapido, costante ampliamento della superficie di attacco e la non altrettanto veloce capacità di garantirne una difesa efficace. In tale contesto, i repentini cambiamenti del mercato tecnologico, il costante incremento del livello di digitalizzazione delle informazioni e le indifferibili, quanto crescenti, necessità di nuove funzioni operative nell'ambito dell'informazione e dei relativi canali di comunicazione, cui sovente non ha corrisposto un adeguato potenziamento infrastrutturale degli *asset*, hanno continuato a determinare uno scenario estremamente dinamico, spesso aggravato da una persistente mancanza di conoscenza e sensibilità della minaccia. Rispetto a quest'ultima, pertanto, l'intelligence ha operato adottando un approccio olistico, basato sull'integrazione di risorse, processi e tecnologie ai fini di una più efficace attività di prevenzione, monitoraggio e risposta. In tale contesto, le strategie del Comparto hanno fatto perno:

- sull'*info-sharing* con tutti gli *stakeholder* nazionali, al fine di accrescere il patrimonio informativo attraverso la costante acquisizione di

elementi sulla minaccia, sul profilo dei suoi attori, sui *modus operandi* adottati, sui *target* d'interesse, sia attuali che potenziali, e sulla tipologia/portata dell'impatto;

- sul supporto nei confronti di soggetti di interesse strategico, volto ad orientarne le attività di *remediation*, favorendo altresì l'adozione di misure corrispondenti allo "stato dell'arte" della sicurezza cibernetica;
- su una più stretta cooperazione internazionale, nell'ambito di consessi sia multilaterali che bilaterali. In ragione di ciò, è stato possibile valutare le minacce in una cornice più ampia, comparando i diversi paradigmi comportamentali degli attori ostili ed analizzando le evidenze su vasta scala, al fine di circoscrivere le finalità delle campagne digitali d'interesse, così da meglio identificarne gli attori.

Nel corso del 2015 la **matrice statuale** ha continuato a caratterizzare le più significative attività di cyberspionaggio in danno di obiettivi nazionali di rilevanza strategica. Il *trend* registrato è stato quello di un incremento qualitativo e quantitativo delle azioni contro alcune Istituzioni e l'industria ad alto contenuto tecnologico ed innovativo, con l'obiettivo di esfiltrare informazioni sensibili e *know-how* pregiato, nonché di accedere ai rispettivi sistemi in vista di successive azioni di *disruption.*

Le principali caratteristiche di tale matrice sono state individuate ancora una volta nella scelta degli obiettivi – di norma *target* pubblici e privati operanti nei settori diplomatico, della difesa, dell'aerospazio, delle telecomunicazioni ed energetico – e nelle modalità di attacco impiegate, connotate, in alcuni casi, da una relativa semplicità attuativa, sebbene di estrema pervasività e persistenza, ed in altri, da sofisticate tecniche elusive e crittografiche e da una puntuale selezione dei *target,* nei cui confronti si è agito con intrusioni molto mirate. Il ***modus operandi*** ha continuato a tradursi in una minaccia persistente e avanzata – *Advanced Persistent Threat - APT* – con l'impiego di *software* malevolo (cd. *malware)* nelle reti informatiche dei soggetti selezionati, al fine di infettarne i relativi *computer.*

Inoltre, i "gruppi" operanti nell'ambito delle campagne APT hanno mostrato sempre più di:

- impiegare *malware* modulare, con componenti deputate allo svolgimento di specifiche funzioni e dispiegate o meno a seconda del *target*;
- reingegnerizzare i *malware*, innescando, tra l'altro, una proliferazione di tecnologie digitali facilmente reperibili nella Rete;
- fare ricorso – nella scrittura dei codici malevoli – a stringhe di caratteri in lingue diverse ovvero riconducibili ad altri attori ostili, al fine di rendere maggiormente difficoltosa ed incerta l'attribuzione di un attacco;
- sottrarre credenziali amministrative di *host* della *intranet* dell'obiettivo per preservare il controllo del sistema anche a fronte di attività di *remediation*;
- utilizzare *proxy* (individui o gruppi) nella conduzione degli attacchi, così da garantire agli attori ostili in *background* l'anonimato e la possibilità di negare ogni coinvolgimento (cd. *"plausible denial"*).

Tra gli elementi di novità, quello più significativo è stato l'affacciarsi, nel panorama dello spionaggio digitale, di gruppi *cyber*-criminali che sono riusciti ad impiegare *software* malevolo, appannaggio esclusivo in passato di attori statuali. Tali gruppi – dediti prevalentemente al furto di dati bancari e di carte di credito – hanno cominciato, grazie a più affinate capacità, a sottrarre informazioni pregiate, a collocare le stesse sul "mercato" ed ad offrire un vero e proprio servizio (il cd. *cyberespionage-as-a-service*) ad entità statuali ovvero a *competitor* commerciali. Da evidenziare, in tale contesto, come queste realtà abbiamo mostrato di possedere un *modus operandi* diverso, decisamente meno sofisticato rispetto a quello di attori statuali, caratterizzato prevalentemente dal riutilizzo di *software* malevolo compilato da altri, così da non dover sostenere i costi di sviluppo, e dalla mancanza di verticalizzazione dell'attività di *targeting*, avendo quale principale obiettivo quello di colpire quante più vittime possibili.

In linea di continuità con quanto osservato nel 2014, si è assistito al consolidamento di attività legate all'effettuazione di *due diligence* occulte

attraverso la sottrazione di dati di natura finanziaria – o relativi a piani di investimento e di politica industriale – nell'ottica di acquisizioni di pacchetti azionari di società italiane da parte di ***competitor* stranieri** ed alla veicolazione di minacce da parte di **soggetti** ed **aziende** operanti nel settore informatico e della sicurezza cibernetica.

Attenzione, infine, è stata dedicata all'evento che ha interessato i sistemi della *Hacking Team* – produttrice dello *spyware "Remote Control System Galileo"* – che ha determinato la compromissione dei sistemi informatici aziendali e sul quale sono ancora in corso accertamenti di natura tecnica e giudiziaria.

Il fenomeno dell'***hacktivism*** ha continuato a trovare nella comunità *Anonymous* il principale punto di riferimento sia come contesto organizzativo, sia come *brand* delle proprie azioni, ed a far registrare un ulteriore scostamento del movimento dalle originarie istanze rivendicative verso campagne di più marcata impronta antagonista e antigovernativa. Vanno ricondotte a tale ultimo ambito le offensive digitali, in danno di *target* istituzionali, che hanno tratto spunto da situazioni di tensione e di scontro sociale, tradottesi essenzialmente in attacchi *Distributed Denial of Service* (DDoS) contro siti *web* istituzionali e di esponenti della politica nazionale, in attività finalizzate alla ricerca di vulnerabilità delle infrastrutture *target* ed in azioni di disturbo digitale attraverso tecniche di *SQL Injection. Anonymous,* inoltre, in linea di continuità con il suo tradizionale approccio, non ha mancato di attivarsi a livello internazionale, in concomitanza con eventi e situazioni di particolare visibilità/interesse, dando vita, ad esempio, all'operazione *"ClimateMarch"*, in corrispondenza con il *summit* di Parigi sul clima, ovvero caricando sui *social media,* all'indomani degli attacchi parigini del 13 novembre, analogamente a quanto fatto dopo gli attentati del precedente gennaio, nella stessa Capitale francese, un video con il quale, oltre a dichiarare guerra a DAESH, ha dato avvio alla *"Operation Paris"* ed al conseguente oscuramento di risorse informatiche ritenute vicine a quella formazione jihadista.

Quanto ai **gruppi terroristici**, essi hanno continuato ad impiegare massicciamente i *social media* al fine di sfruttarne al meglio opportunità

e potenzialità. DAESH, in particolare, ha fatto costante uso della rete quale "moltiplicatore di forza" e "cassa di risonanza" per la diffusione e amplificazione dei suoi messaggi propagandistici. Frequente è stato il ricorso a:

- tecniche di manipolazione e "dirottamento" dei filoni di discussione sui *social network,* per veicolare la propaganda attraverso *hashtag* con elevata visibilità, sovente non correlati a tematiche relative all'Islam;
- specifiche applicazioni che, consentendo di ripubblicare sugli *account* dei loro utenti i *post* di DAESH, ne ha provocato di fatto un aumento esponenziale, con conseguente maggiore risonanza pubblica.

Sulla base del costante monitoraggio effettuato dall'intelligence, le capacità dei gruppi terroristici di porre in essere attacchi *cyber* non hanno raggiunto il livello analogo – per numero di vittime e rilevanza dei danni materiali – a quello di un'azione terroristica convenzionale. L'attivismo cibernetico sinora rilevato, in tale ambito, si è tradotto in attacchi il cui *modus operandi* ha fatto ricorso a tecniche di *web-defacement* e DDoS.

Sul fronte della **criminalità informatica**, è stata rilevata la crescente diffusione di *software* malevoli, riconducibili soprattutto alle tipologie *ransomware* e *banking trojan,* finalizzati entrambi all'illecito conseguimento di benefici di natura economica.

CryptoWall, CryptoLocker e *RansomWeb* sono tra i *ransomware* che hanno conosciuto, nel corso del 2015, una elevata propagazione, mentre con riguardo ai cd. *banking trojan,* le varianti maggiormente riscontrate sono state quelle afferibili a *Vawtrak* e *Dyre, software,* questi, programmati per acquisire le credenziali di accesso degli *account* dei siti di banca *on-line* al fine di effettuare illeciti trasferimenti di fondi verso conti bancari controllati da gruppi di cybercriminali. In aggiunta, la minaccia di tipo avanzato e persistente denominata *"Carbanak",* che consente il controllo da remoto di talune applicazioni per l'attivazione di sportelli bancomat, ha interessato i sistemi informatici anche di alcuni istituti bancari nazionali.

PAGINA BIANCA

Serie statistiche

La minaccia sopra delineata è stata anche rappresentata, al fine di consentirne una lettura rapida ed agevole, nelle serie statistiche di seguito riportate, frutto di una attività di sistematizzazione ed analisi dei dati relativi ad eventi cibernetici rilevati, nel corso del 2015, principalmente da AISE ed AISI, ma anche da parte degli altri attori che compongono l'architettura nazionale, sia pubblici che privati.

Completa il quadro della minaccia il *ranking* frutto della comparazione delle serie statistiche del 2015 con quelle del 2014, al fine di tracciarne le tendenze, secondo la seguente legenda:

▲	▼	▶
Trend in crescita	*Trend* in diminuzione	*Trend* stabile

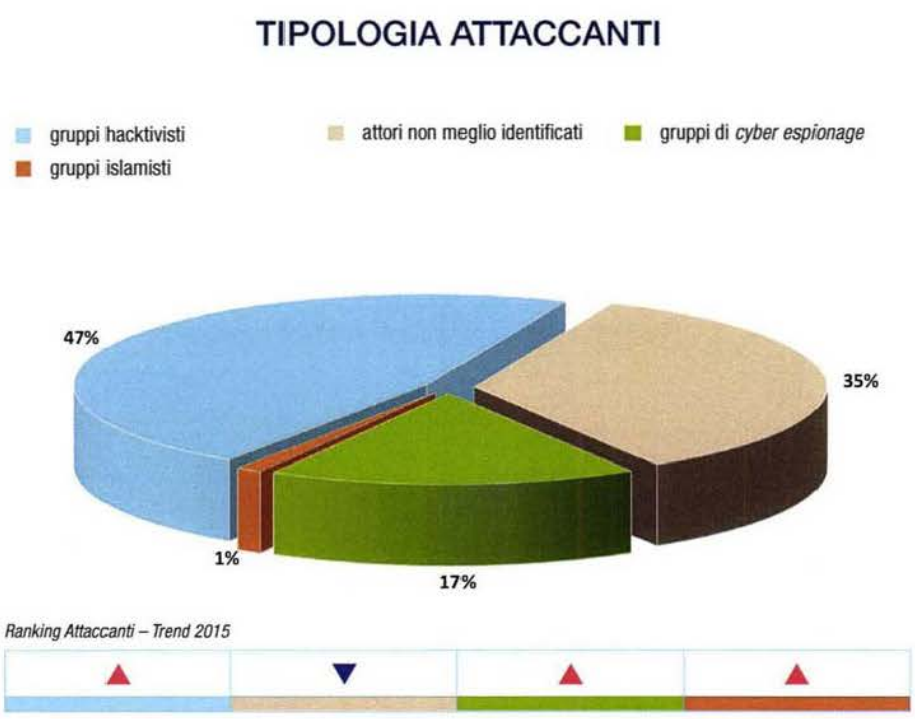


Grafico 1 – Tipologia attaccanti

Per quel che concerne la tipologia di **attori ostili**, così come mostrato nel ***Grafico 1***, questi sono raggruppabili in cinque categorie, di cui la principale – solo per percentuale di azioni svolte (47%) e non per grado di pericolosità – rimanda ai gruppi hacktivisti. Significativa è, anche, la quota di **attori non meglio identificati** (35%), che trova la sua ragion d'essere soprattutto nelle criticità poste dalla questione dell'*attribution*. Seguono, poi, **gruppi professionisti dello spionaggio digitale** (17%), nel quale, come più sopra indicato, sono coinvolti anche gruppi criminali, specializzatisi negli ultimi tempi nell'esfiltrazione di informazioni pregiate. Emergono, infine, i **gruppi *hacker* islamisti** (1%), con il ricorso a tecniche tipiche dell'*hacktivism*.

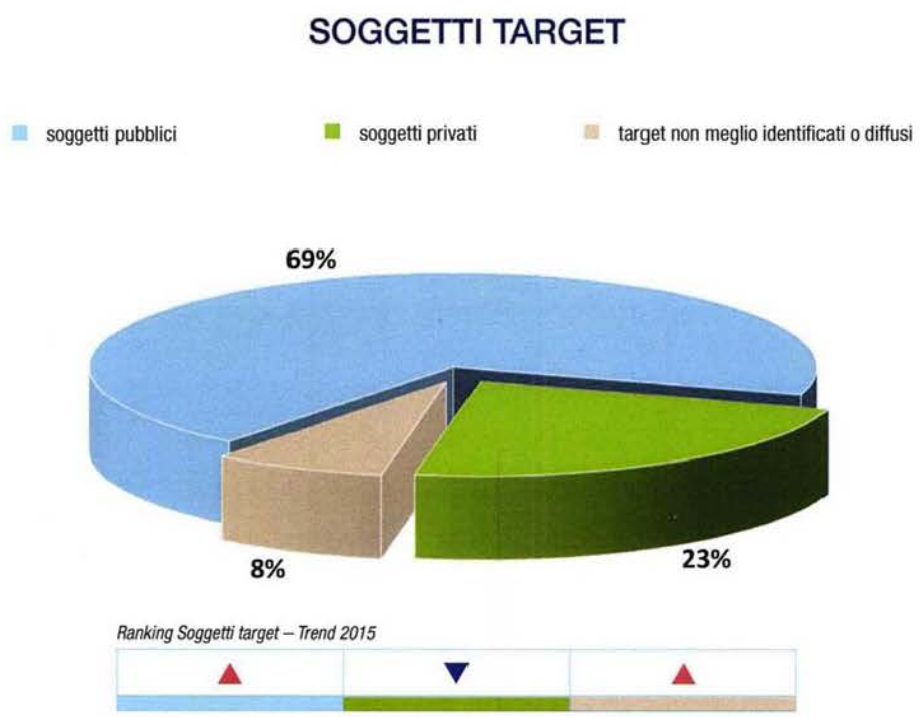


Grafico 2 – Tipologia dei soggetti target

Cambiando prospettiva, i dati sui **soggetti *target*** (***Grafico 2***) mostrano il divario tra gli attacchi perpetrati nei confronti di **soggetti pubblici**, che costituiscono la maggioranza con il 69%, e quelli in direzione di **soggetti privati**, attestati attorno al 23%. La rimanente aliquota, quella pari all'8%, è costituita generalmente da *"soft target"*, obiettivi non di rilievo strategico che presentano vulnerabilità comuni e, pertanto, semplici da sfruttare, verso i quali è di norma l'*hacktivism* a condurre attacchi.

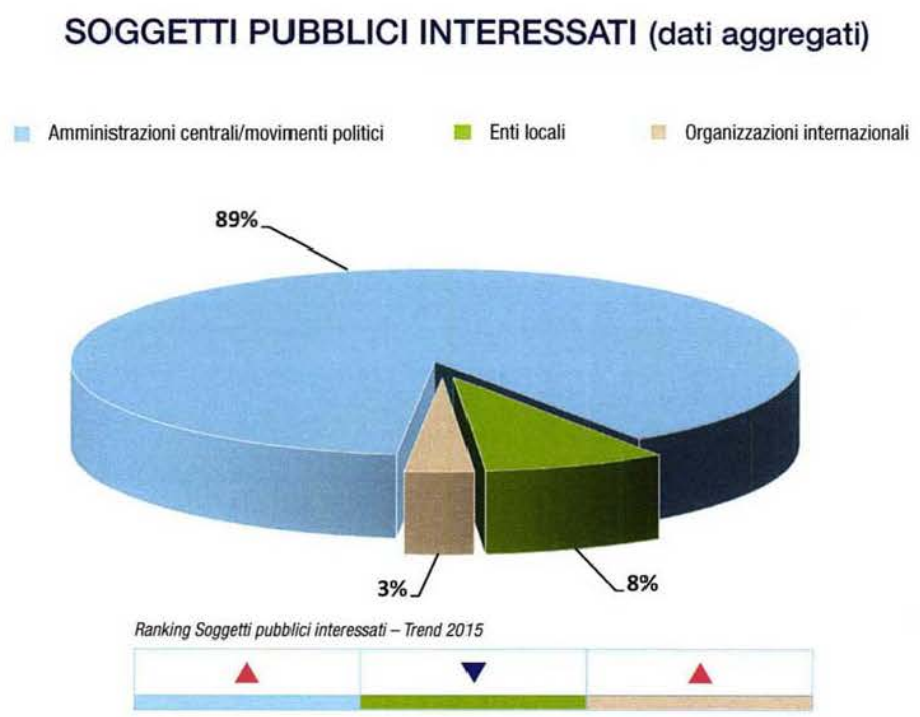


Grafico 3 – Tipologia dei soggetti pubblici interessati dagli attacchi (dati aggregati)

L'affinamento dei dati per categoria (pubblico-privato) fa emergere un maggior grado di dettaglio per quel che riguarda i **soggetti pubblici** (***Grafico 3***). La maggioranza degli Enti interessati da attacchi *cyber* sono risultate le **Pubbliche Amministrazioni Centrali** (89%), mentre quelli contro **Enti locali** hanno assunto una rilevanza pari all'8%. Le prime costituiscono *target* preferenziali per attività sia di spionaggio digitale, in quanto detentrici di informazioni pregiate sotto il profilo geo-politico e politico-strategico, sia di matrice *hacktivist*, poiché rappresentano obiettivi "simbolici", selezionati in ragione del particolare messaggio o rivendicazione da veicolare, nonché per la loro capacità di conferire agli attacchi elevata visibilità.

Da evidenziare il valore del tutto residuale (3%) delle attività ostili in danno di **Organizzazioni internazionali**, anch'esse oggetto, principalmente, di azioni dimostrative riconducibili al filone *hackivist*.