caso del corteo torinese del 15 dicembre, segnato da atti vandalici ai danni di uffici postali e istituti bancari.

Intenso è stato inoltre l'attivismo antimilitarista, tanto sulla piazza, quanto sul piano propagandistico, con appelli all' "azione diretta" contro le sinergie tra enti/istituti di ricerca universitaria e "industria delle armi" e, anche in questo caso, con indicazioni operative su aziende attive nel settore della difesa. Pure la storica lotta contro l'asserita "occupazione militare della Sardegna" ha attirato l'interesse delle componenti anarchiche, attraverso un'inedita chiave di lettura intesa a equiparare la situazione sarda alla resistenza del popolo curdo ad Afrin, in Rojava (Kurdistan siriano). Tematica, quest'ultima, che ha rappresentato, un ulteriore ambito di condivisione tra insurrezionalisti italiani e stranieri, con la promozione della campagna internazionale "Fight4Afrin".

L'attività informativa ha del resto confermato l'intensità dei collegamenti internazionali dell'anarco-insurrezionalismo, evidenziando assidui contatti, sia fisici che virtuali, tra militanti, nonché una loro sostenuta mobilità tra diversi Paesi, in occasione di iniziative propagandistiche e di mobilitazione. Il tema dominante resta la "solidarietà rivoluzionaria ai compagni prigionieri", come testimoniato dal lancio, a fine novembre, per il secondo anno consecutivo, della campagna "Per un Dicembre Nero" mediante la pubblicazione, su un sito d'area internazionale, di un documento, in greco e spagnolo (poi tradotto

"l'attività informativa ha confermato l'intensità dei collegamenti internazionali dell'anarco-insurrezionalismo„

LA VALENZA "RIVOLUZIONARIA" DEL ROJAVA

I circuiti anarchici hanno dedicato particolare attenzione alla resistenza curda a DAESH e all'esperimento di "autorganizzazione politico-sociale" attuato nella regione siriana del Rojava, ispirato al modello di "confederalismo democratico" teorizzato dal leader del Partito dei lavoratori del Kurdistan (PKK) Abdullah Ocalan, dal 1999 detenuto in Turchia.

Spinti da una propaganda d'area tesa ad esaltare la componente ideale della lotta curda, ritratta come "un'estrema battaglia per l'umanità e la libertà", sin dagli inizi dell'offensiva jihadista nel Kurdistan siriano militanti di varie nazionalità hanno raggiunto il teatro bellico impegnandosi direttamente al fianco delle milizie curde in apposite brigate internazionali.

É in tale quadro che s'inserisce, nel settembre 2018, la diffusione sul web di un "Comunicato finale", in inglese, che, nel dichiarare lo scioglimento della milizia internazionale filo-curda delle "International Revolutionary People's Guerrilla Forces", celebra l'esperienza anarco-insurrezionalista in difesa della "rivoluzione sociale" in Rojava. Gli autori tendono ad identificare l'impegno anarchico in teatro come contingente e prodromico rispetto alla "rivoluzione su scala internazionale". Si muovono in questo senso le incitazioni a non abbandonare la lotta, a proseguire nelle prassi offensive in tutto il mondo e a continuare ad organizzare percorsi insurrezionali, pure nei rispettivi Paesi di provenienza.

Spunti di attivazione sono stati colti anche negli ambienti dell'estremismo marxista, tradizionalmente sensibili alla causa curda, che, in collaborazione con omologhi circuiti esteri, sono stati impegnati a sostenere le formazioni combattenti attraverso specifiche campagne finalizzate alla spedizione di materiale medico.

in italiano e rilanciato su siti anarchici nazionali), volto a promuovere l'"azione diretta" esprimendo "solidarietà offensiva" agli anarchici detenuti in vari Paesi, tra cui l'Italia. Appello, questo, cui hanno fatto seguito i comunicati apparsi sul web in dicembre con i quali sono stati rivendicati tre attacchi incendiari compiuti nello stesso mese: ad Atene, contro una stazione di polizia; a Parigi, ai danni di sei autovetture della municipalità; a Santiago del Cile, contro un camion. Negli ultimi due casi, il messaggio non ha mancato di celebrare i "compagni in prigione" in Italia, con specifico riferimento ai militanti arrestati, nel settembre 2016, nell'ambito dell'operazione "Scripta Manent".

I CIRCUITI MARXISTI-LENINISTI

I ristretti circuiti dell'estremismo marxista-leninista hanno continuato ad evidenziarsi per l'impegno propagandistico-divulgativo della stagione brigatista, inteso ad accreditarne l'attualità e a promuovere l'indottrinamento di "nuove leve". Questo, come di consueto, facendo perno soprattutto su una lettura in chiave rivoluzionaria dei più recenti sviluppi della congiuntura interna e internazionale.

In tale quadro, sono rimasti centrali la lotta alla "repressione", l'"antifascismo", l'"antimperialismo" e l'esteso panorama delle istanze sociali, a partire dall'emergenza abitativa e dalle vertenze occupazionali.

Il tema forte è sempre quello della solidarietà ai "prigionieri politici", anche stranieri, che ha animato iniziative contro il "carcere duro", quali i presidi del 4 maggio e del 28 settembre presso il Tribunale dell'Aquila in occasione di scadenze processuali a carico di Nadia Desdemona Lioce, ristretta nel capoluogo abruzzese e leader delle "Nuove Brigate Rosse" responsabili degli omicidi di Massimo D'Antona e Marco Biagi.

Nella prospettiva della "lotta di classe" hanno continuato a trovare spazio i richiami, a fini di proselitismo, ad un "nuovo proletariato urbano" composto da lavoratori immigrati, precari, disoccupati e "senza casa", mentre si inscrivono nel filone internazionalista ed "antimperialista" le manifestazioni in appoggio alla resistenza palestinese ed in chiave "anti-israeliana", come la protesta in occasione del Giro d'Italia, che per l'edizione 2018 ha preso il via da Gerusalemme Ovest.

"richiami ai fini di proselitismo ad un 'nuovo proletariato urbano'„

IL MOVIMENTO ANTAGONISTA

L'eterogenea galassia dell'antagonismo si è distinta soprattutto per il tentativo di superare una persistente tendenza alla "parcellizzazione delle lotte", così da dare maggiore compattezza al fronte della contestazione.

Ancorché declinato su specifiche realtà del territorio nazionale, il dinamismo antagonista sul versante delle proteste ambientaliste ha ricercato convergenze e sinergie, con l'obiettivo di strumentalizzare in chiave oltranzista l'attività dei cd. "Fronti del No", che si oppongono alla realizzazione di infrastrutture di vario genere (grandi opere, installazioni energetiche e militari, ripetitori, discariche, inceneritori, etc.).

Gli attivisti hanno provato a serrare i ranghi concentrando la protesta antisistema sull'"antifascismo" e sull'"antirazzismo", come testimoniato dalla manifestazione nazionale di Macerata del 10 febbraio, organizzata all'indomani del raid omicida a sfondo razzista compiuto nella città marchigiana da un simpatizzante di estrema destra ed indicata, nella propaganda d'area, come punto di partenza per favorire il rilancio di un percorso di mobilitazione il più possibile comune e condiviso.

„tentativo di strumentalizzare in chiave oltranzista l'attività dei cd. 'Fronti del No'„

LA MOBILITAZIONE "ANTIFA"

Nell'ambito della mai sopita ostilità tra estremismi di opposta matrice, l'"antifa" definisce la posizione più avanzata e intransigente dell'antagonismo di sinistra nel contrasto alla destra, consistente in un impegno militante che privilegia la "dimensione combattiva" rispetto al confronto politico-culturale.

Nel 2018, la propaganda e le pratiche della mobilitazione "antifa" hanno evidenziato una rinnovata radicalizzazione in reazione ad una percepita crescita di visibilità e protagonismo dell'estrema destra su questioni riguardanti la sicurezza, l'immigrazione e il disagio sociale. In questo quadro sembrano inserirsi taluni episodi di aggressione contro attivisti della destra radicale, danneggiamenti a sedi aggregative nonché la divulgazione sul web di documenti e "dossier" dai toni istigatori.

L'accentuata propensione allo scontro rischia di aggravare la conflittualità tra i due fronti, con una possibile intensificazione di provocazioni, aggressioni e reazioni in grado di generare criticità sul piano dell'ordine pubblico.

In tale quadro, ha assunto specifico rilievo strategico, nelle progettualità antagoniste, il coinvolgimento nelle mobilitazioni della popolazione straniera, ritenuta, in particolare dai segmenti più oltranzisti, un bacino di reclutamento "capace di produrre conflitto". Una linea, questa, evidenziatasi anche a livello locale, ove i vari "movimenti per l'abitare" hanno mostrato interesse verso la "propensione ribellistica" delle fasce più disagiate e precarie, pure attraverso appelli ad una ripresa delle occupazioni abusive, intese quale "pratica militante di riappropriazione del reddito".

L'impegno antagonista sulla tematica migratoria ha continuato a qualificarsi come un ambito sensibile per l'ordine pubblico in ragione del concorrente attivismo di componenti della destra radicale, con il rischio di un'intensificazione di episodi di conflittualità fra opposti estremismi.

„rischio di un'intensificazione di episodi di conflittualità fra opposti estremismi„

Il dinamismo della destra radicale

Costante attenzione informativa è stata riservata al panorama dell'ultradestra che, caratterizzatosi per una pronunciata vitalità, ha riproposto, specie con riguardo alle formazioni più strutturate, alcune consolidate linee di tendenza: competizioni "egemoniche" e fluidità di rapporti, interesse ad accreditarsi sulla scena politica mantenendo uno stretto ancoraggio alla "base", propensione ad intensificare le relazioni con omologhe formazioni estere.

Le strategie d'inserimento nel tessuto sociale hanno fatto leva su iniziative pro-

pagandistiche e di protesta, soprattutto in talune periferie urbane, centrate sull'opposizione alle politiche migratorie, nell'ambito di una più ampia mobilitazione su tematiche sociali di forte presa (sicurezza, lavoro, casa, pressione fiscale). Tale attivismo, di impronta marcatamente razzista e xenofoba, si è accompagnato ad una narrazione dagli accenti di forte intolleranza nei confronti degli stranieri che, al di là del richiamato omicidio di Macerata, potrebbe aver concorso ad ispirare taluni episodi di stampo squadrista, oltre che gesti di natura emulativa, e potrebbe conoscere un inasprimento con l'approssimarsi dell'appuntamento elettorale europeo.

Le varie campagne propagandistiche hanno tradito l'intento di coniugare l'esigenza di proiettare un'immagine "moderata" con la determinazione a preservare, per ragioni di proselitismo, i rapporti con quel variegato sottobosco comprendente anche segmenti politicizzati delle tifoserie calcistiche, nonché sigle di matrice neonazista, antisemita e skinhead. In quest'ultimo ambito, si è registrato un rimarchevole fermento organizzativo e programmatico da parte di componenti hammerskin attestate nel Nord Italia, interessate ad espandere il proprio raggio d'azione a livello nazionale attraverso un ambizioso "progetto federativo" rivolto a gruppi minori. Strumenti privilegiati di proselitismo sono la promozione di concerti d'area e di manifestazioni di carattere sia politico-culturale sia commemorativo-nostalgico, nonché di iniziative a sfondo sociale. La determinazione di tali ambienti ad acquisire peso ne ha influenzato i rapporti con altre compagini nazionali, in alcuni casi portando alla ricerca di sinergie, in altri accentuando la concorrenzialità.

"iniziative propagandistiche e di protesta centrate sull'opposizione alle politiche migratorie„

In Alto Adige i tradizionali contatti tra gruppi skinhead germanofoni e circuiti neonazisti tedeschi si sono ulteriormente rafforzati, facendo registrare la presenza di militanti altoatesini ad iniziative di protesta d'impronta xenofoba svoltesi in Germania.

Si è confermata, più in generale, la spiccata proiezione internazionale delle principali formazioni d'area, con assidui e stretti rapporti con i maggiori gruppi stranieri dell'ultradestra, funzionali all'affermazione di un "fronte identitario paneuropeo", a difesa delle radici etnico-culturali dell'Europa, di orientamento filorusso e pro-Assad e in contrapposizione alla UE, agli USA e alla NATO.

Un contesto, questo, che ha confermato l'interesse dell'area nei confronti della crisi ucraina, anche in termini di sostegno attivo ai due schieramenti contrapposti.

I MILIZIANI ITALIANI IN DONBASS

L'operazione "Ottantotto" del luglio 2018 coordinata dalla Procura della Repubblica di Genova, che ha coinvolto diversi soggetti accusati di "associazione a delinquere, aggravata dalla transnazionalità, finalizzata al reclutamento di mercenari e al combattimento in un conflitto in un territorio controllato da uno Stato estero", ha riportato all'attenzione generale il tema della presenza nel teatro di crisi ucraino di cittadini italiani o di stranieri residenti in Italia.

Sin dal principio, infatti, la crisi ucraina ha suscitato l'interesse dell'estrema destra, scatenando però un vivace dibattito interno che ha determinato il formarsi di due fronti: l'uno, favorevole alle istanze nazionaliste di Kiev; l'altro, solidale con gli indipendentisti delle regioni orientali dell'Ucraina, sostenuti da Mosca. Tale contrapposizione si è tradotta nella rilevata presenza in entrambi gli schieramenti di militanti dell'ultra-destra italiana, spinti da motivazioni tanto ideologiche quanto economiche. Più nel dettaglio, mirati approfondimenti informativi hanno rilevato che:

- a favore dei lealisti ucraini si è mobilitata una parte della destra radicale nazionale, in considerazione del ruolo di rilievo ricoperto dai movimenti ultranazionalisti nel corso delle note proteste di piazza del novembre 2013 (cd. Euromaidan);
- a sostegno dei separatisti si è invece schierata una componente di estrema destra più numerosa, d'impronta più propriamente identitaria, che sostiene le posizioni russe in chiave anti-USA e anti-UE.

Accanto ai filo-russi, peraltro, si è registrata anche una non irrilevante presenza di militanti dell'antagonismo di sinistra che, dal canto loro, interpretano la resistenza contro il Governo di Kiev in chiave antifascista e antimperialista.

Nella maggior parte dei casi, i soggetti spinti da motivazioni politico-ideologiche si sono recati nel Donbass per iniziative propagandistiche, allo scopo dichiarato di documentare quella "esperienza di lotta" e portare sostegno alla popolazione locale, mentre solo una parte, più consistente per gli elementi di destra, risulta coinvolta nei combattimenti. Accanto ai soggetti caratterizzati politicamente, figurano poi quei profili "ibridi" che vantano anche esperienze nel circuito dei contractors.

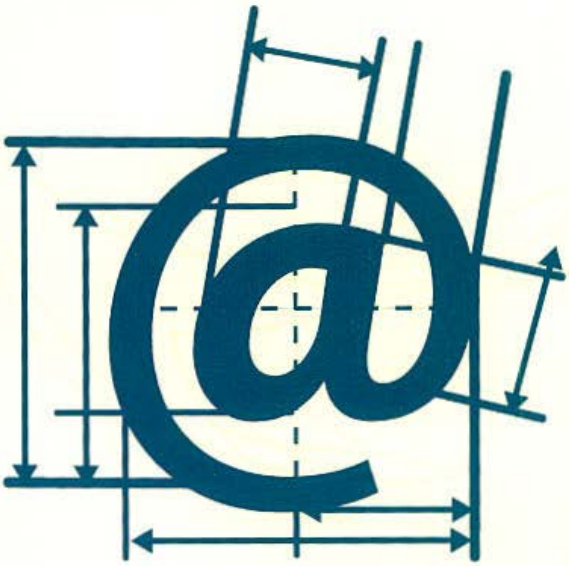
Come per analoghe mobilitazioni, anche in questo caso il web si è rivelato uno strumento di comunicazione e propaganda in grado di favorire contatti e adesioni.

Sebbene il fenomeno risulti numericamente contenuto e, per evidenti ragioni, non paragonabile a quello dei foreign fighters jihadisti, esso presenta comunque potenziali criticità, correlate soprattutto all'esperienza e alle competenze di natura militare che, al rientro in territorio nazionale, potrebbero essere riversate negli ambienti di riferimento.

PAGINA BIANCA

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

PAGINA BIANCA

INDICE

PAGINA BIANCA

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 info-operative 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 é 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.

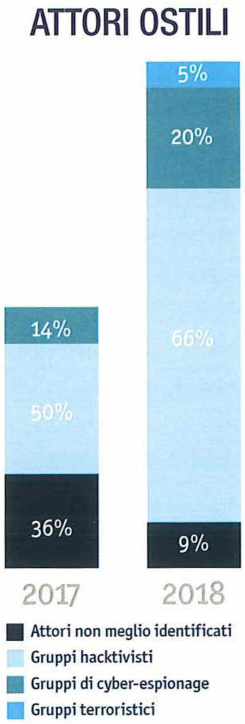
A tali formazioni vanno attribuiti anche gli attacchi contro risorse web e social media delle principali forze politiche nazionali (assimilate, ai fini della presente rilevazione, ai "soggetti pubblici" ed inserite nella categoria "Altro", di cui rappresentano circa un quarto del totale), impiegati per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

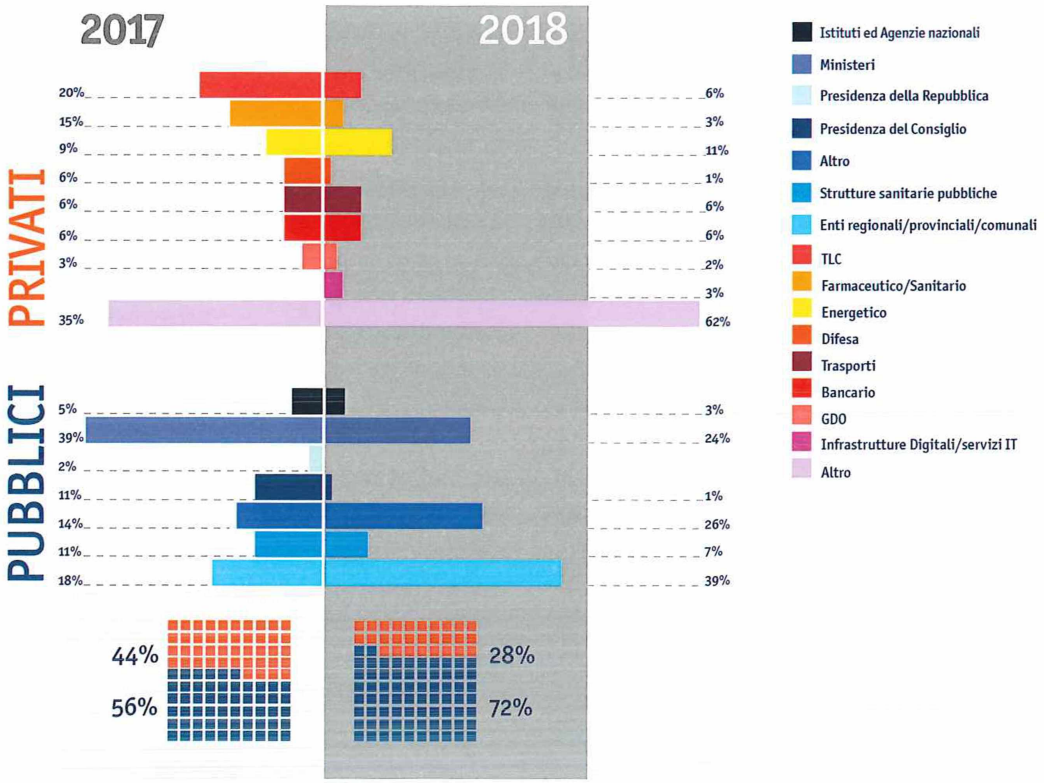
Per ciò che concerne gli attori ostili, il trend del 2018, in linea di continuità con quello degli ultimi anni e in coerenza con quanto appena descritto, ha identificato l'hacktivismo come la minaccia più consistente (66%), almeno in termini numerici. Tale dato va ascritto alla fase di particolare fermento 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