tori internazionali, che, facendo ricorso a strumenti competitivi non convenzionali, tendono ad insidiare quote di mercato e know how pregiato della nostra industria.

In particolare, nell'aerospazio – segmento dalle enormi potenzialità anche in ragione del forte impegno italiano all'interno dei progetti della European Space Agency e nel campo delle esplorazioni lunari – sono emerse, confermando una tendenza consolidatasi negli ultimi anni, azioni di influenza e progettualità funzionali a marginalizzare i player nazionali.

Nel comparto della difesa, ove l'industria italiana è impegnata anche nel complesso sforzo di ammodernamento tecnologico in ambito UE e NATO, l'attività informativa è stata finalizzata a contenere – pur in un'ottica di collaborazione con gli alleati strategici – la penetrazione straniera e a sostenere la proiezione oltreconfine delle nostre aziende. Al riguardo, le evidenze raccolte hanno posto in luce iniziative di concorrenza sleale da parte dei concorrenti stranieri, azioni di lobbying e tentativi di ingerenza nella governance di joint venture.

Un altro ambito le cui dinamiche sono state sottoposte a costante scrutinio informativo è il settore delle **telecomunicazioni**, anche in ragione delle profonde trasformazioni tecnologiche e organizzative connesse all'introduzione della tecnologia 5G e al loro impatto sul sistema infrastrutturale nazionale. In tale scenario, le risultanze della ricerca hanno fatto emergere le articolate strategie di attori esteri interessati a penetrare e consolidare la propria presenza nel mercato italiano.

Nel contesto delle attività svolte a tutela degli assetti produttivi del Paese, mirato impegno informativo è stato riservato a quei settori capaci di svolgere una funzione di volano per l'intero sistema, tra cui **meccanica/meccatronica**, **automotive**, **biotech** e **made in Italy**, in grado di valorizzare i risultati della ricerca (di base e applicata), il patrimonio di conoscenze e il capitale reputazionale del Paese. In questi ambiti, sono emersi tentativi di sottrazione di know how strategico, anche attraverso mirate acquisizioni, e rischi di compromissione della catena del valore per quel che attiene alle forniture di prodotti industriali di base.

Pari attenzione è stata rivolta al settore della **logistica**, in particolare di quella **portuale**, di assoluta centralità in ragione della forte integrazione dell'economia italiana nei flussi commerciali internazionali. Al riguardo, nel corso dell'anno sono state raccolte indicazioni concernenti iniziative, di matrice estera, finalizzate sia a riorientare in modo strumentale i flussi di merci nel Mediterraneo sia a penetrare la filiera in territorio nazionale, anche per finalità extraeconomiche. Nello specifico, acquisizioni intelligence hanno posto in luce disegni espansivi di attori stranieri all'indirizzo non solo di aree portuali italiane, ma anche delle relative zone retroportuali.

Il monitoraggio dell'Intelligence non ha mancato di ricomprendere, inoltre, le dinamiche del **sistema finanziario nazionale**.

Nella congiuntura pandemica, nonostante il prolungato processo di rafforzamento patrimoniale e di riduzione dei crediti deteriorati (Non-Performing Loans-

NPL), il sistema bancario ha dovuto – e deve tuttora – misurarsi con la flessione economica connessa all'emergenza sanitaria mondiale e con la paventata prospettiva di un impatto della crisi, anche prolungato, su corsi azionari, insolvenze e redditività degli istituti bancari. In aderenza agli indirizzi del Governo, nonché in sintonia con le valutazioni espresse dal Copasir in novembre, a valle delle audizioni in materia di "Tutela degli asset strategici nazionali nei settori bancario e assicurativo", l'interesse informativo si è appuntato, tra l'altro, su talune progettualità estere suscettibili di ricadute anche sugli equilibri di finanziamento del debito pubblico italiano e sulle policy di erogazione di crediti alle nostre imprese. Ciò in quanto eventuali acquisizioni di player nazionali da parte di attori stranieri potrebbero determinare una vendita di titoli pubblici italiani e una contrazione dei finanziamenti a favore di aziende nazionali, con grave nocumento per il nostro sistema economico.

Costante vigilanza informativa è stata riservata, inoltre, alla **tecnologia fintech**, per i suoi effetti trasformativi sul settore finanziario nazionale, tanto più rilevanti in una fase che, alla luce dell'emergenza sanitaria, ha visto l'estensione e l'accelerazione dei processi di digitalizzazione anche in campo economico-finanziario.

## La sicurezza energetica

Le conseguenze depressive della crisi pandemica hanno riguardato, infine, anche l'**approvvigionamento energetico nazionale**, che, in ragione del rallentamento dell'economia, ha visto i consumi contrarsi in misura significativa. Particolarmente colpita è stata la domanda petrolifera, ridottasi di circa il 15% a causa delle misure di contenimento della mobilità, e quella di gas naturale, calata del 5% in ragione della parallela riduzione del fabbisogno elettrico.

Per quanto concerne i mercati internazionali di idrocarburi, da cui l'economia italiana dipende, il 2020 si è caratterizzato per un eccesso strutturale di offerta, che ha avuto il duplice effetto di contenere il costo delle materie prime, con ricadute positive sul saldo commerciale, e al contempo di aumentare la ridondanza delle forniture, comprimendo le potenziali implicazioni negative di qualunque interruzione dei flussi provenienti da un singolo fornitore.

All'aumento della capacità del Paese di accedere ai mercati internazionali hanno contribuito anche gli sviluppi infrastrutturali, soprattutto nel settore del gas. In questo senso, particolarmente significativa è stata l'entrata in funzione a fine anno del gasdotto TAP, tratto terminale del corridoio di trasporto che collega l'Azerbaigian con le coste pugliesi, attraversando l'Anatolia, la Grecia e l'Albania, e che consente, a regime, di fornire volumi pari al 10% del fabbisogno nazionale, contribuendo a diversificare le forniture.

Complessivamente, dunque, la debolezza dei consumi finali e l'abbondanza dell'offerta hanno significativamente attenuato i rischi per la sicurezza energetica nazionale, pur in un contesto nel quale l'attenzione dell'Intelligence ha continuato a riguardare sia l'integrità delle infrastrutture di produzione, trasporto e

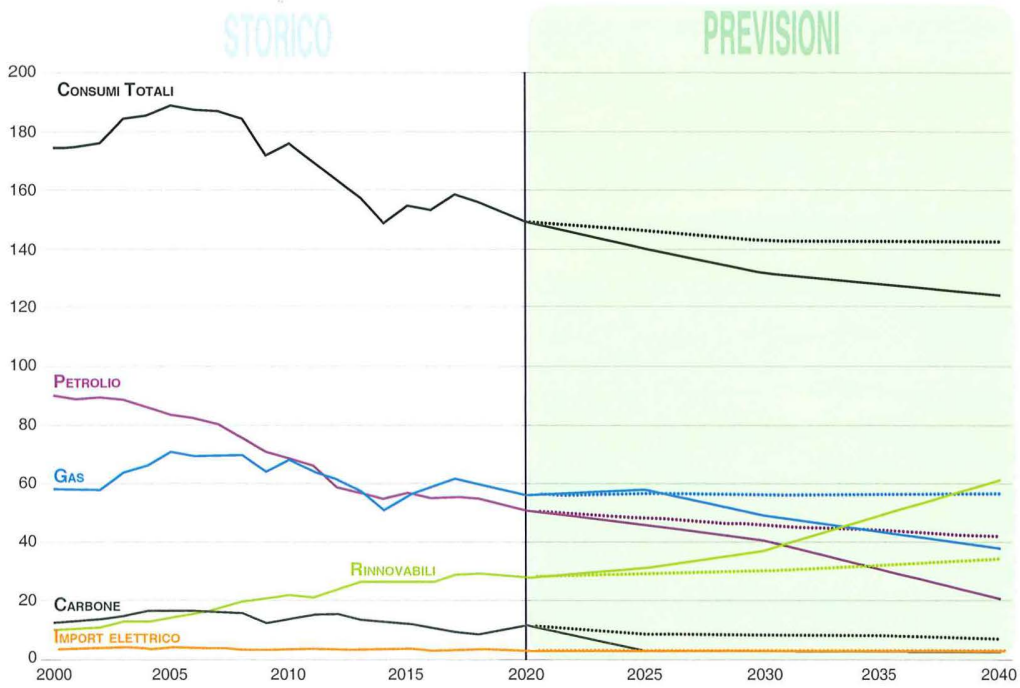
distribuzione, sia la stabilità geopolitica nei Paesi fornitori e di transito dei flussi diretti in Italia, nella prospettiva di verificarne l'adeguatezza per gli anni a venire, quando la ripresa delle domanda globale nel contesto post-pandemico modificherà l'attuale congiuntura.

L'azione informativa ha riguardato, altresì, in una prospettiva di più lungo periodo e in continuità con il passato, il monitoraggio dei possibili impatti sulla sicurezza nazionale del processo di decarbonizzazione dell'economia europea, sia sotto il profilo della stabilità e affidabilità dell'approvvigionamento energetico (vds. tavola n. 18), sia con riferimento alle sfide poste alla competitività del sistema produttivo, a fronte dei mutamenti nei paradigmi tecnologici dei principali comparti industriali nazionali.

**ANDAMENTO DEI CONSUMI ENERGETICI ITALIANI**

18

Il processo di decarbonizzazione dell'economia nazionale, in linea con gli obiettivi europei, prevede una forte riduzione dei consumi energetici rispetto allo scenario tendenziale (linea tratteggiata), con un deciso aumento delle fonti rinnovabili e un parallelo decremento delle fonti fossili.




*Unità: milioni di tonnellate equivalenti di petrolio (Mtep)

Fonte MISE, Piano nazionale integrato per l'energia e il clima (PNIEC)

PAGINA BIANCA

# MINACCIA CIBERNETICA

**in breve**

- Sfruttamento dell'emergenza pandemica per implementare azioni ostili
- Impegno prioritario dell'intelligence a tutela di strutture sanitarie e/o di ricerca di cure e vaccini
- Incremento degli attacchi, specie nei confronti di soggetti pubblici
- Provvedimenti di listing cyber adottati in sede UE

Al pari di quanto avvenuto in altri ambiti all'attenzione dell'Intelligence, anche il dominio cibernetico è stato significativamente condizionato dalla congiuntura pandemica, chiamando il Comparto ad orientare una parte rilevante degli sforzi verso il contenimento di progettualità che hanno tentato di sfruttare l'emergenza epidemiologica per condurre azioni ostili in danno di varie tipologie di target, a partire da quelli del settore sanitario.

La pandemia è stata un evento determinante anche in termini di impatto sulla società, sulle tecnologie in uso alla popolazione, sulla digitalizzazione di attività e servizi nonché sul conseguente ampliarsi della superficie di rischio cibernetico per l'individuo e per l'intero Sistema Paese. Hanno quindi acquisito maggiore attualità e concretezza le minacce alla sicurezza e al funzionamento delle reti e degli impianti, nonché alla continuità degli approvvigionamenti.

Nel complesso si è evidenziato come gli attori ostili abbiano sfruttato, nel periodo pandemico, il massiccio ricorso al lavoro agile e la conseguente accessibilità da internet, tramite collegamenti VPN (Virtual Private Network), di risorse digitali di Ministeri, aziende di profilo strategico e infrastrutture critiche, divenuti ancor più bersaglio di campagne ostili di matrice statuale, criminale o hacktivista.

Il Comparto, al fine di prevenire, mitigare e contrastare le diverse espressioni della minaccia cibernetica, ha garantito un'assidua produzione informativa su attori (statuali, strutturati, non statuali ma con sponsorizzazione statuale, criminali), vettori tecnologici, Indicatori di Compromissione (IoC), Tattiche, Tecniche e Procedure (TTP), target (istituzionali, infrastrutturali, critici e strategici), finalità (pianificate o in itinere) e azioni digitali offensive.

## Il settore sanitario

L'impegno informativo ha mirato in via prioritaria a tutelare strutture ospedaliere e centri di ricerca nazionali, nonché le principali realtà attive nello sviluppo e nella sperimentazione di vaccini e terapie contro il Covid-19.

In questo contesto, è emerso come attori statuali abbiano tentato di sfruttare le debolezze connesse all'ondata pandemica per porre in atto attacchi sofisticati miranti ad esfiltrare informazioni sensibili su terapie e stato della ricerca.

L'azione intelligence ha consentito inoltre di rilevare, sul fronte hacktivista, la ricerca di vulnerabilità e tentativi di violazione di portali web e, sul versante del cybercrime, lo sfruttamento di vulnerabilità note, attività di phishing, nonché la registrazione di domini malevoli allo scopo di ingannare gli utenti – anche attraverso la creazione di portali fittizi – nel contesto delle procedure di erogazione dei contributi economici previsti dai provvedimenti introdotti con la crisi pandemica.

Le intrusioni hanno riguardato in particolare:

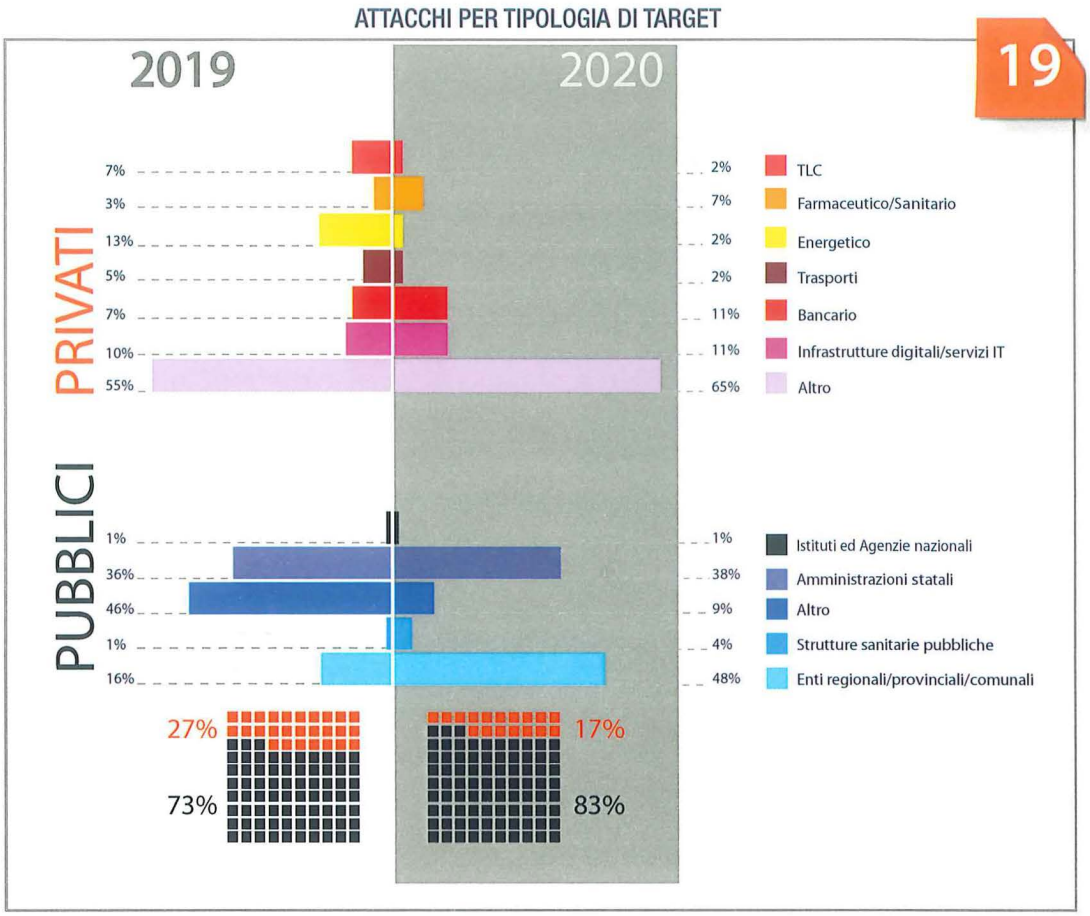
- enti/operatori afferenti al settore della sanità e della ricerca, in direzione dei quali sono state effettuate compromissioni informatiche attraverso l'acquisizione di credenziali amministrative ovvero l'inoculazione di malware;
- Dicasteri ed altre Amministrazioni dello Stato, nei cui confronti si è registrata una intensa campagna di diffusione di malware.

A rafforzamento del dispositivo di protezione, il Comparto ha posto in essere iniziative di monitoraggio preventivo a tutela di infrastrutture critiche e assetti strategici, al fine di individuare vulnerabilità informatiche riferibili a risorse web in uso a primarie realtà operanti nel settore e ad apparati diagnostici esposti in rete, instaurando all'occorrenza relazioni dirette con i potenziali target in un'ottica di mitigazione del rischio.

## Trend generale della minaccia

Per quel che attiene, più in generale, alle attività ostili perpetrate, attraverso il dominio cibernetico, in danno degli assetti informatici rilevanti per la sicurezza nazionale, il complesso dei dati raccolti dall'Intelligence – di cui si riportano di seguito le più significative elaborazioni statistiche – ha fatto emergere un generale incremento delle aggressioni (+20%), che, quanto alla **tipologia di target** (vds. tavola n. 19), hanno riguardato per lo più, a conferma di una tendenza già rilevata negli ultimi anni, sistemi IT di soggetti pubblici (83%, in aumento di 10 punti percentuali rispetto al 2019). Tra questi ultimi, quelli maggiormente interessati dagli eventi risultano le Amministrazioni locali (48%, valore in aumento di oltre 30 punti percentuali rispetto all'anno precedente), unitamente ai Ministeri titolari di funzioni critiche (+ 2% nel confronto anno su anno).

Le azioni digitali ostili perpetrate nei confronti dei soggetti privati hanno interessato prevalentemente il settore bancario (11%, in aumento di 4 punti percentuali rispetto al 2019), quello farmaceutico/sanitario (7%, in sensibile incre-

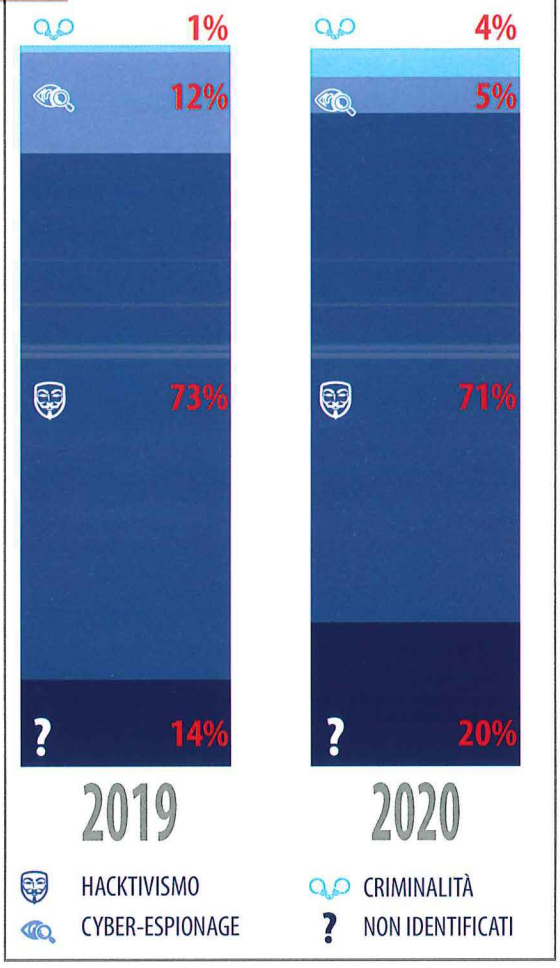



mento rispetto allo scorso anno) e dei servizi IT (11%, dato pressoché stabile).

Quanto alla **tipologia di attori ostili** (vds. tavola n. 20), occorre richiamare la complessità del processo di attribuzione delle loro azioni offensive, che spesso non risulta praticabile in virtù delle caratteristiche stesse del dominio cibernetico, nonché del sofisticato livello tecnologico raggiunto da alcune campagne cibernetiche, specialmente di matrice statuale. Di contro, si rileva come attacchi di stampo hacktivista abbiano una attribuzione ben specifica collegata alla rivendicazione e alla "pubblicità" posta in essere dagli attaccanti stessi, interessati ad ottenere risalto mediatico. Il complesso degli attacchi cibernetici rilevati nel 2020 ha confermato, in linea con quanto emerso nell'ultimo biennio, l'hacktivismo come matrice più ricorrente (71%), sebbene non si siano registrati, rispetto al 2019, significativi scostamenti nel numero di azioni condotte dal collettivo Anonymous Italia, sotto la cui egida operano, con sempre crescente autonomia, singole crew (AnonPlus ITA, AntiSec ITA e Lulzsec ITA).

Tale autonomia operativa ha trovato significativi riflessi anche nelle rivendicazioni degli attacchi, effettuate principalmente su blog e profili Twitter riconducibili alle singole cellule, rilanciate successivamente attraverso i canali digitali "ufficiali" di Anonymous Italia.

20 ATTACCHI PER TIPOLOGIA DI ATTORI




All'hacktivismo sono state ascritte anche le incursioni digitali nei confronti di operatori privati impegnati, a vario titolo, nel processo di estrazione e raffinazione degli idrocarburi, poste in essere nell'ambito della mobilitazione "OpLucania", nonché quelle in danno di numerose concerie campane, prese di mira nel contesto dell'iniziativa "OpSarno", in quanto ritenute responsabili dell'inquinamento dell'omonimo fiume.

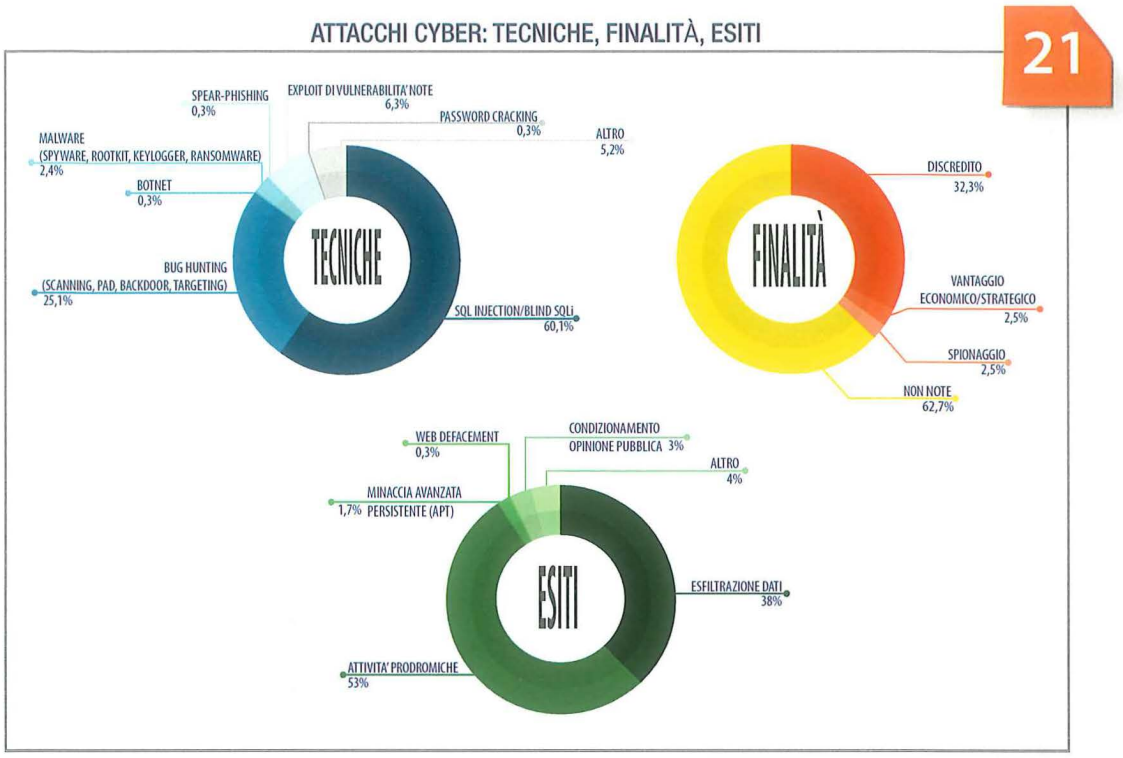
È stata registrata una significativa contrazione (-7%) nel numero delle proiezioni digitali di matrice statuale, a fronte, peraltro, di un nuovo, consistente incremento di episodi dalla matrice non identificabile (+ 6% rispetto al 2019), verosimilmente in ragione dell'accuratezza dimostrata, in più occasioni, dagli attori dotati di maggiori capacità, nella rimozione delle tracce digitali al fine di occultare il proprio operato.

I dati sulle **tipologie di attacco** rilevate nel corso del 2020 (vds. tavola n. 21) hanno confermato il preponderante ricorso a tecniche di SQL Injection per violare le infrastrutture informatiche delle vittime (60% del totale), dopo una prima fase di osservazione delle vulnerabilità tecniche del target grazie ad attività di scansione di reti e sistemi (cd. Bug Hunting, 25%). Si è fatto ricorso anche a campagne di spear-phishing (0,3%), quale utile strumento per veicolare impianti malevoli, tra cui web-shell e Remote Access Trojan-RAT, impiegati per acquisire il controllo remoto delle risorse compromesse. Inoltre, attacchi Ransomware hanno coinvolto soggetti di rilievo nazionale, sia del settore sanitario che dell'industria del Made in Italy, sfruttando per l'infezione nuove modalità di collegamento attivate per lo smartworking.

In termini di esiti, il 2020, in linea di continuità con l'anno precedente, ha fatto registrare la preminenza di azioni prodromiche a potenziali attacchi (circa il 53% del totale, stabile rispetto al 2019), seguite da quelle tese alla sottrazione di informazioni da assetti effettivamente compromessi (38%, in crescita di 4 punti percentuali).

In ultima analisi, si ritiene che l'incremento di tali azioni propedeutiche possa essere collegato a quelle iniziative cui non è stato possibile attribuire una chiara

MINACCIA CIBERNETICA




finalità (62,7%) confermatesi, anche per il 2020, numericamente più consistenti.

In tale contesto – e al netto delle numerose campagne disinformative online – si è evidenziato un sostanziale azzeramento degli attacchi cyber per fini propagandistici, a fronte di un deciso incremento delle incursioni digitali tese a minare credibilità e reputazione dei target (32%), come diretta conseguenza della dichiarata ostilità delle frange hacktiviste nei confronti di imprese private ed istituti sanitari impegnati nel contrasto alla pandemia.

È stata e resta elevata l'attenzione del Comparto in direzione delle campagne con finalità di spionaggio. Pur permanendo marginali sul piano quantitativo (2,5%), queste forme di aggressione, definite Advancend Persistent Threat (APT) e caratterizzate dalla difficile individuazione per la natura volutamente occulta dell'azione ostile, rappresentano le più insidiose per il Sistema Paese, in termini di informazioni esfiltrate, perdita di operatività e competitività, nonché dispendio di risorse economiche per la loro mitigazione. In quest'ambito, sono parse di assoluto rilievo le campagne indirizzate verso Ministeri e primari fornitori nazionali di servizi di comunicazione elettronica, condotte attraverso azioni digitali altamente strutturate e con l'impiego di tecniche e strumenti sofisticati. Considerevole, altresì, l'impegno profuso dall'Intelligence nel contrasto di eventi che hanno interessato operatori di servizi essenziali del settore energetico, nonché in occasione dell'attacco digitale emerso in dicembre ai danni della società texana SolarWinds, per il potenziale impatto su reti e sistemi nazionali.

## Listing cyber in sede UE

Da richiamare, infine, il contributo assicurato dal Comparto a supporto della definizione della posizione nazionale in seno al Consiglio dell'Unione Europea con riguardo alle proposte, formulate da alcuni Stati Membri, finalizzate a sottoporre a misure restrittive – ai sensi del Regolamento del Consiglio Europeo 2019/796 e della Decisione del Consiglio 2019/797 del 17 maggio 2019 – soggetti e/o entità ritenuti responsabili di avere supportato, partecipato o condotto attacchi cyber in danno di target europei.

Il listing – le cui procedure istruttorie sono affidate all'Horizontal Working Party on Cyber Issues – esprime funzione duplice: di risposta univoca e collettiva all'attacco cyber e quale fattore deterrente, utile a scoraggiare tentativi di azioni ostili (vds. tavola n. 22).

22

### PROCEDURA DI LISTING

La proposta di introdurre soggetti e/o entità all'interno del regime di sanzioni, che dev'essere effettuata da uno Stato Membro e può essere sottoscritta da altri Paesi dell'Unione, prevede che gli attacchi informatici costituenti minaccia esterna:

- abbiano avuto effetti significativi;
- provengano o siano sferrati dall'esterno dell'UE;
- impieghino infrastrutture esterne all'UE;
- siano compiuti da una persona fisica o giuridica, da un'entità o da un organismo stabile od operante al di fuori della UE, oppure siano commessi con il sostegno, controllo o direzione di una persona fisica o giuridica, entità o organismo operante al di fuori dei confini dell'Unione.

Le misure restrittive applicabili possono includere divieti di circolazione per le persone fisiche verso l'UE e congelamento di beni sia di individui che entità. A queste ultime, inoltre, una volta applicato il regime sanzionatorio, è fatto divieto di ricevere fondi da parte di persone ed entità UE.

# MINACCIA IBRIDA

**in breve**

- Con la pandemia, impennata di campagne disinformative e fake news
- Dilatati margini di intervento per attori ostili propensi all'uso combinato di più strumenti a fini manipolatori e d'influenza
- Nuovi indirizzi operativi della UE

Mirata e coordinata azione intelligence è stata riservata alla cd. minaccia ibrida – per definizione veicolata su diversi domini (quello diplomatico, militare, economico/finanziario, intelligence, etc.) – che, in concomitanza con il dispiegarsi dell'emergenza sanitaria, è stata caratterizzata da costanti tentativi di intossicazione del dibattito pubblico attraverso attività di disinformazione e/o di influenza, nel contesto di più ampie campagne ibride. Al riguardo, è stata registrata una elevatissima produzione di fake news e narrazioni allarmistiche, sfociate in un surplus informativo (cd. infodemia) di difficile discernimento per la collettività. Fattore di rischio intrinseco al fenomeno della disinformazione online ha continuato a risiedere nelle logiche e negli algoritmi alla base dello stesso funzionamento dei social media, tendenti a creare un ambiente autoreferenziale ed autoalimentante, fondato sulla condivisione dei contenuti e delle relazioni di interesse che, polarizzando l'informazione disponibile, ne alimenta quindi la percezione parziale e faziosa.

In tale contesto, alla luce della particolare attenzione riservata al tema anche in ambito UE (vds. tavola n. 23), la ricerca informativa ha consentito di rilevare il

**23**

## LA POSIZIONE DELL'UNIONE EUROPEA

A fronte dell'accresciuta portata del fenomeno della disinformazione sulla pandemia da Coronavirus, l'impegno delle Istituzioni europee si è tradotto, tra l'altro, nella pubblicazione, in giugno, di una Comunicazione congiunta della Commissione e dell'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza dal titolo "Tackling Covid-19 disinformation: getting the facts right".

L'intervento, nel quadro di un'attenzione risalente che ha visto anche il varo, nel 2018, di un "Piano d'azione contro la disinformazione", ha proposto una serie di indirizzi operativi funzionali ad incrementare la resilienza della UE: rafforzamento delle capacità di comunicazione strategica; potenziamento della cooperazione tra Stati Membri e UE, nonché tra questa e i Partner internazionali; maggiore trasparenza da parte delle piattaforme online (coinvolgimento nella gestione delle crisi e sostegno a fact-checkers/ricercatori); tutela della libertà di espressione e del dibattito pluralistico; promozione della consapevolezza dei cittadini.

In tale contesto, non va trascurato il lavoro svolto dall'ECDC (European Centre for Disease Prevention and Control) attraverso report periodici, risk assessment e puntuali aggiornamenti sull'evoluzione dei vaccini.

ricorso all'utilizzo combinato, da parte dei principali attori ostili di matrice statuale, di campagne disinformative e attacchi cibernetici, volti a sfruttare l'onda emotiva provocata dalla crisi sanitaria, nel tentativo di trasformare la pandemia in un vantaggio strategico di lungo termine: ciò, anche attraverso manovre miranti ad influenzare l'opinione pubblica ed i processi decisionali nazionali, nonché a danneggiare i nostri assetti economici.

Sullo sfondo di un dibattito internazionale in costante evoluzione, il Comparto ha inoltre continuato a promuovere iniziative di raccordo e interscambio volte a consolidare la definizione del perimetro della minaccia e a rafforzare le capacità nazionali di prevenzione e contrasto anche attraverso le sinergie tra gli attori istituzionali (in primis MAECI, Interno e Difesa) e la cooperazione con i principali Partner internazionali.

# TERRORISMO JIHADISTA

**in breve**

- Sostenuta attività insorgente di DAESH in Iraq
- Incremento dell'attivismo delle filiazioni regionali di DAESH e al Qaida, soprattutto in Africa
- Generalizzata intensificazione della propaganda online e delle minacce all'Occidente nella contingenza dell'emergenza pandemica
- Conferma dei tratti prevalentemente endogeni e destrutturati della minaccia jihadista in Europa, persistente rischio di attivazione di ex combattenti e micro-cellule
- I Balcani epicentro continentale del proselitismo e potenziale incubatore della minaccia terroristica verso lo spazio Schengen
- Vitalità di circuiti e ambienti "a rischio", anche virtuali, ove possono maturare o essere alimentati processi di radicalizzazione

L'attività informativa svolta in direzione del terrorismo di matrice jihadista è proseguita serrata e ininterrotta, in Italia e all'estero, modulandosi su contesti e tratti evolutivi di un fenomeno sempre più dinamico e polimorfo quanto ad attori, ambiti operativi e strategie offensive.

## Tendenze e proiezioni del jihad globale

Il 2020 ha coinciso, per **DAESH**, con una fase di riorganizzazione – dopo l'"annus horribilis" segnato dal collasso territoriale e dalla scomparsa del leader storico al Baghdadi – che ha visto la strategia della formazione dipanarsi lungo tre principali direttrici: rivitalizzazione dell'attività insorgente in Iraq e Siria, decentralizzazione in favore delle articolazioni regionali, rilancio del conflitto asimmetrico in crisi d'area e teatri di jihad.

Per quanto riguarda la Siria e l'Iraq, la sconfitta dello Stato Islamico ne ha ridotto in maniera determinante le capacità operative in quei territori, dove il gruppo, dopo essersi assicurato nel tempo bastioni in aree rurali e desertiche, ha proseguito ad adattare tattica e postura alle contingenze e ad incunearsi nei vuoti di potere creatisi sul terreno. Seppur indebolito, DAESH è parso ancora in grado di:

- muovere i propri combattenti dal territorio siriano a quello iracheno, grazie alla porosità di quelle frontiere;
- sostenere finanziariamente le attività insorgenti e la riorganizzazione in atto, sia con i profitti di attività criminali a livello locale (estorsioni, rapimenti e traffici illeciti) sia reimpiegando fondi raccolti attraverso il contrabbando di merci, petrolio, armi e droga;
- reclutare nuove leve, specie tra le fasce più giovani della popolazione locale e all'interno dei campi profughi.

Servendosi di queste linee d'azione, vitali per la sopravvivenza del gruppo,

DAESH ha quindi proseguito, e a tratti intensificato, l'attività insorgente in Iraq, con numerosi attacchi suicidi, omicidi e sequestri di persona, sfruttando anche il rientro nel Paese di suoi membri. L'attuale strategia di DAESH, tuttavia, non è parsa orientata a ricostituire uno Stato territoriale in area siro-irachena, bensì a mantenere una sostanziale decentralizzazione dell'organizzazione nei vari Paesi di interesse, lasciando a livello centrale la funzione di coordinamento e controllo delle articolazioni periferiche.

Fuori dalle roccaforti siro-irachene, l'attivismo delle filiazioni locali è stato particolarmente evidente in Africa con: l'affermazione dell'Islamic State West Africa Province-ISWAP e dell'Islamic State Greater Sahara-ISGS, entrambi capaci di mantenere alte frequenza e letalità degli attacchi in Nigeria, Niger, Mali, Burkina Faso e nella regione del Lago Ciad; l'avanzata in Mozambico dell'Islamic State Central Africa Province-ISCAP, che – dopo il significativo segnale di presenza nella Repubblica Popolare del Congo a partire dall'aprile 2019 – si è dimostrato in grado di conquistare, seppure brevemente, porzioni di territorio; la competizione con al Qaida-AQ nel Sahel, che ha concorso al deterioramento delle condizioni di sicurezza e ad un innalzamento della minaccia terroristica nell'area.

In un contesto che, per effetto dell'emergenza pandemica, ha registrato un generalizzato incremento dell'attivismo estremista online (vds. tavola n. 24), il fervore operativo dei gruppi regionali affiliati a DAESH, specie nel Sahel e nel Bacino del Lago Ciad, non ha mancato di essere celebrato dalla propaganda ufficiale del gruppo, che ne ha dato ampia eco e copertura mediatica, al fine di capitalizzare i "successi" ottenuti.

**24**

## 2020 VIRTUAL COUNTER-TERRORISM WEEK (6-10 LUGLIO, NEW YORK)

Si è tenuto in luglio, nell'ambito della "Virtual Counter-Terrorism Week 2020" promossa dalle Nazioni Unite, il seminario "Strategic and Practical Challenges of Countering Terrorism in a Global Pandemic Environment". L'evento, che ha visto la partecipazione da remoto di delegazioni di vari Paesi Membri, di rappresentanti di Organizzazioni internazionali e regionali, nonché del mondo imprenditoriale, ha evidenziato, tra l'altro, che:

- la grave crisi economico/occupazionale globale e le limitazioni di alcuni diritti e libertà imposte dai vari Governi per contrastare l'emergenza sanitaria hanno creato terreno fertile per la proliferazione di sentimenti d'odio e intolleranza che hanno agevolato processi di radicalizzazione, sia religiosa che politico/ideologica;
- DAESH e al Qaida hanno sapientemente sfruttato tale situazione per alimentare la propaganda online, guadagnare nuovi consensi e incitare una ripresa/intensificazione degli attacchi in alcuni teatri di crisi, approfittando delle vulnerabilità degli Stati impegnati ad affrontare l'emergenza sanitaria;
- gli spostamenti dei foreign fighters continuano ad essere monitorati, mentre resta aperta la questione del loro rimpatrio (e di quello dei familiari), all'esame nell'ambito del progetto Global Framework on United Nations Support to Member States. È stata valutata preoccupante, altresì, la situazione umanitaria e securitaria nei centri di detenzione in Siria e in Iraq, sia per le difficoltà gestionali, aggravate dalla crisi sanitaria, sia per gli aspetti legati al pericolo di radicalizzazione ed alla presenza di ex combattenti.

In Asia, DAESH ha conservato rilevanti capacità operative, in particolare in Afghanistan dove, attraverso l'Islamic State Khorasan Province-ISKP, è risultato capace di pianificare attacchi di elevato profilo nonostante le forti perdite inflitte dai Taliban e dalle Forze di sicurezza locali.

Il gruppo terroristico ha mostrato un rinnovato slancio mediatico, con un utilizzo più consapevole e strategico del proprio apparato propagandistico, evidenziando la chiara volontà di rafforzare la propria base di consensi, soprattutto nel subcontinente indiano. In questa cornice si inscrive la rivista online "Voice of Hind" che, per incitare al jihad, fa leva simultaneamente sulle dinamiche legate al conflitto in Kashmir e sulle condizioni dei musulmani in India (vds. tavola n. 25).

25

## "VOICE OF HIND"

Il 24 febbraio, al Qitaal Media Center, media outlet pro-DAESH, ha pubblicato – in concomitanza con le violente tensioni scoppiate in India tra hindu e musulmani a seguito dell'approvazione, nel dicembre 2019, della legge sulla cittadinanza, ritenuta discriminatoria nei confronti della minoranza musulmana – il primo numero di "Voice of Hind" (in arabo Sawt al Hind). La rivista, diffusa online nelle principali lingue locali (hindi, urdu, maldiviano, bengali, tamil) e in inglese, è considerata uno dei prodotti editoriali più innovativi dell'organizzazione, che punta, dopo l'annuncio (maggio 2019) della creazione della nuova provincia indiana, l'Islamic State of Hind, ad una più ampia visibilità della sua filiazione regionale, l'Islamic State Khorasan Province-ISKP, sia nel quadrante indiano che nell'intera area del subcontinente.

Nonostante il focus del magazine riguardi prevalentemente questioni di rilevanza locale, come attesta l'ampio risalto dato all'attivismo anti-indiano nel Jammu Kashmir e in alcuni Stati della Federazione indiana (Kerala, Tamil Nadu, Maharashtra), "Voice of Hind" fa riferimento anche a temi del jihad globale. Ne sono riprova tanto gli appelli ai suoi simpatizzanti/attivisti a colpire l'Occidente, fiaccato dall'emergenza pandemica, quanto le "copertine" dedicate ad alcuni degli autori di attacchi condotti in Europa (come quella che ritrae il responsabile della strage di Vienna del 2 novembre scorso). Ricorre, anche in questo nuovo format di DAESH, il leitmotiv delle campagne di discredito contro i gruppi affiliati ad al Qaida e il movimento Taliban, a conferma di dinamiche di competizione mai sopite, anche nel quadrante afghano, tra i due maggiori attori del terrorismo jihadista.

Un ulteriore filone narrativo della rivista riguarda il territorio delle Maldive, mèta turistica frequentata anche da connazionali. Il richiamo negli editoriali ad alcuni attacchi terroristici perpetrati ai danni di stranieri ed infrastrutture turistiche (febbraio e aprile 2020) testimonia, infatti, la particolare attenzione della compagine islamista per il territorio maldiviano.

Analogamente, è significativo il risalto dato da "Amaq", agenzia mediatica centrale di DAESH, all'attentato del 25 marzo contro un tempio sikh a Kabul, successivamente rivendicato da ISKP in nome dei musulmani del Kashmir.

Per quanto riguarda al Qaida, il 2020 è stato caratterizzato dalla perdita di storici leader delle filiazioni regionali dell'organizzazione: da Droukdel, capo di al Qaida nel Maghreb Islamico-AQMI (vds. tavola n. 26), ad al Raymi, guida di al Qaida nella Penisola Arabica-AQAP.

26

## LA FINE DELL' ERA DROUKDEL

Il 3 giugno, Forze speciali francesi, con il supporto di assetti intelligence del Comando statunitense per l'Africa (AFRICOM), hanno neutralizzato, in Mali, l'emiro di al Qaida nel Maghreb Islamico-AQMI, Abdelmalek Droukdel, insieme ad alcuni suoi stretti collaboratori. L'azione ha avuto ampia eco nella propaganda qaidista a livello globale. Algerino, formatosi nel Gruppo Islamico Armato-GIA prima e a capo, poi, del Gruppo Salafita per la Predicazione e il Combattimento-GSPC, Droukdel è stato l'artefice dell'alleanza delle formazioni jihadiste maghrebine con al Qaida e quindi della nascita, nel 2006, di AQMI. Ormai il più anziano comandante militare della formazione, nel 2017 era stato nominato da al Zawahiri suo vice e costituiva uno dei principali anelli di congiunzione tra i qaidisti africani e il nucleo afghano-pakistano. Dopo la morte, nel 2019, di Seifallah Ben Yassine, leader di Ansar al Sharia Tunisia ed altro esponente storico della vecchia guardia qaidista in Africa, Droukdel era rimasto l'ultimo elemento in vita di AQMI all'interno della senior leadership di al Qaida.

L'emiro è stato pure ideatore dell'ampliamento operativo della formazione al di fuori dell'Algeria, a partire dal Mali, dove l'insurrezione tuareg dell'Azawad aveva costituito l'occasione favorevole all'apertura di nuovi fronti di lotta, secondo una "strategia" valsa pure a spostare l'epicentro del jihadismo dal Nord Africa al Sahel. La galassia qaidista d'area aveva così visto ridimensionata la sua storica anima algerina, da sempre in posizione di comando, a favore di più giovani e aggressive figure e sigle saheliane, non arabe – specie quelle confluite nel cartello qaidista Jamaa Nusrat al Islam wa al Muslimin-JNIM – che, seppure percepite dal mondo arabofono-qaidista come entità di "secondo livello", si sono rese operativamente più visibili e attive nella gestione dei dossier locali (secondo dati ACLED/Armed Conflict Location and Event Data Project, la sola JNIM è responsabile del 64% della violenza jihadista nel Sahel negli ultimi tre anni).

È in questo senso che la scelta di al Qaida di sostituire Droukdel con una figura algerina (Abu Obeida Yousef al Annabi, capo del Consiglio della Shura di AQMI e privo di un significativo passato operativo) evidenzia la volontà del "core" qaidista di garantire una "continuità di comando" che, tuttavia, potrebbe, nel medio termine, collidere con gli effettivi equilibri sul terreno, rischiando di condurre a scontri/scissioni tra le due anime di AQMI.

Tali eventi, tuttavia, non sembrerebbero essersi tradotti in un cambio di direzione, né in un indebolimento sostanziale di al Qaida, che ha continuato a perseguire la lotta contro i "nemici dell'Islam", declinandola in agende regionali basate sulle priorità delle popolazioni locali tra le quali si è nel tempo accreditata.

Sebbene la centrale di comando e controllo di al Qaida rimanga attestata nell'area compresa tra Iran, Afghanistan e Pakistan, il radicamento dell'organizzazione a livello territoriale trova emblematica espressione nel Corno d'Africa (dove al Shabaab-AS opera con un esteso network, che dalla Somalia si è proiettato nel tempo anche in Kenya, Etiopia, Gibuti, Uganda e Tanzania), nel Sahel (con Jamaa Nusrat al Islam wa al Muslimin-JNIM, la cui crescente capacità di espansione nelle aree limitrofe rappresenta un pericoloso fattore di destabilizzazione per tutta la fascia saheliana), in Nigeria (con la fazione filo-qaidista di Boko Haram) e nella Penisola arabica, ove la yemenita AQAP, pur ridimensionata territorialmente, ha conservato vocazione offensiva transnazionale.

L'unitarietà tra obiettivi globali e locali è stata garantita da una sapiente strategia comunicativa della leadership di al Qaida, che ha inteso valorizzare la