ATTI PARLAMENTARI

XVIII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **XXXIII**
n. **3**

RELAZIONE
SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA
(Anno 2020)

(Articolo 38 della legge 3 agosto 2007, n. 124)

Presentata dal Presidente del Consiglio dei ministri

(DRAGHI)

Trasmessa alla Presidenza il 26 febbraio 2021

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

PRESIDENZA DEL CONSIGLIO DEI MINISTRI

SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA

RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2020

PAGINA BIANCA

" O FRATI", DISSI, "CHE PER CENTO MILIA
PERIGLI SIETE GIUNTI ALL'OCCIDENTE,
A QUESTA TANTO PICCIOLA VIGILIA
DE' NOSTRI SENSI CH'È DEL RIMANENTE,
NON VOGLIATE NEGAR L'ESPERIENZA,
DI RETRO AL SOL, DEL MONDO SANZA GENTE.

CONSIDERATE LA VOSTRA SEMENZA:
FATTI NON FOSTE A VIVER COME BRUTI,
MA PER SEGUIR VIRTUTE E CANOSCENZA".

LI MIEI COMPAGNI FEC'IO SÌ AGUTI,
CON QUESTA ORAZION PICCIOLA, AL CAMMINO,
CHE A PENA POSCIA LI AVREI RITENUTI;
E, VOLTA NOSTRA POPPA NEL MATTINO,
DE' REMI FACEMMO ALI AL FOLLE VOLO,
SEMPRE ACQUISTANDO DAL LATO MANCINO.

Divina Commedia
Inferno, XXVI Canto

In concomitanza con le celebrazioni per i 700 anni dalla morte di Dante Alighieri, la Comunità intelligence nazionale ha inteso riservare un tributo al Sommo Poeta, intitolandogli la Sede del Comparto, che affaccia sull'omonima piazza capitolina.

PAGINA BIANCA

INDICE

INDICE DELLE TAVOLE

PAGINA BIANCA

PREMESSA

Nel 2020, l'emergenza sanitaria – ancora agli inizi quando, in febbraio, la scorsa Relazione annuale veniva data alle stampe – è inevitabilmente intervenuta, con la sua portata dirompente e planetaria, anche nel campo d'azione dell'Intelligence, rendendo il panorama della minaccia più ampio, fluido e complesso.

Nella prospettiva della sicurezza nazionale, la pandemia ha infatti agito su più piani: abbattendosi sulle economie e sul commercio internazionale, condizionando dinamiche geopolitiche e sviluppi d'area, aggravando vulnerabilità sistemiche e tensioni sociali, dilatando gli spazi per manovre ostili ed inserimenti strumentali di vario segno e matrice.

Il dato emerso con maggiore evidenza è, peraltro, quello di un'accelerazione di alcune linee di tendenza, sovente interagenti, che da tempo marcano l'orizzonte dell'Intelligence, quali il cronicizzarsi di conflitti e contenziosi, anche a causa delle proiezioni d'influenza da parte di Stati terzi, le difficoltà della mediazione multilaterale, l'antagonismo tra attori globali e la corsa alla primazia sul versante tecnologico, la regionalizzazione delle filiere produttive ed il riposizionamento di attori e operatori nelle catene globali del valore, la crescente aggressività della competizione economica e il consolidamento di strategie d'ingerenza articolate e multiformi.

Nel contempo, l'emergenza pandemica ha chiamato il Comparto Intelligence a nuove prove, connesse all'esigenza di assicurare ogni supporto informativo e d'analisi nel contesto dello sforzo corale che ha visto ogni componente dello Stato chiamata a fare la sua parte per fronteggiare una crisi senza precedenti nella storia recente. Mirate attivazioni hanno riguardato, tra l'altro, la rafforzata tutela di centri e strutture sanitarie, nonchè il rischio di iniziative e scalate ostili tese a sfruttare la difficile congiuntura economica a detrimento di assetti strategici nazionali.

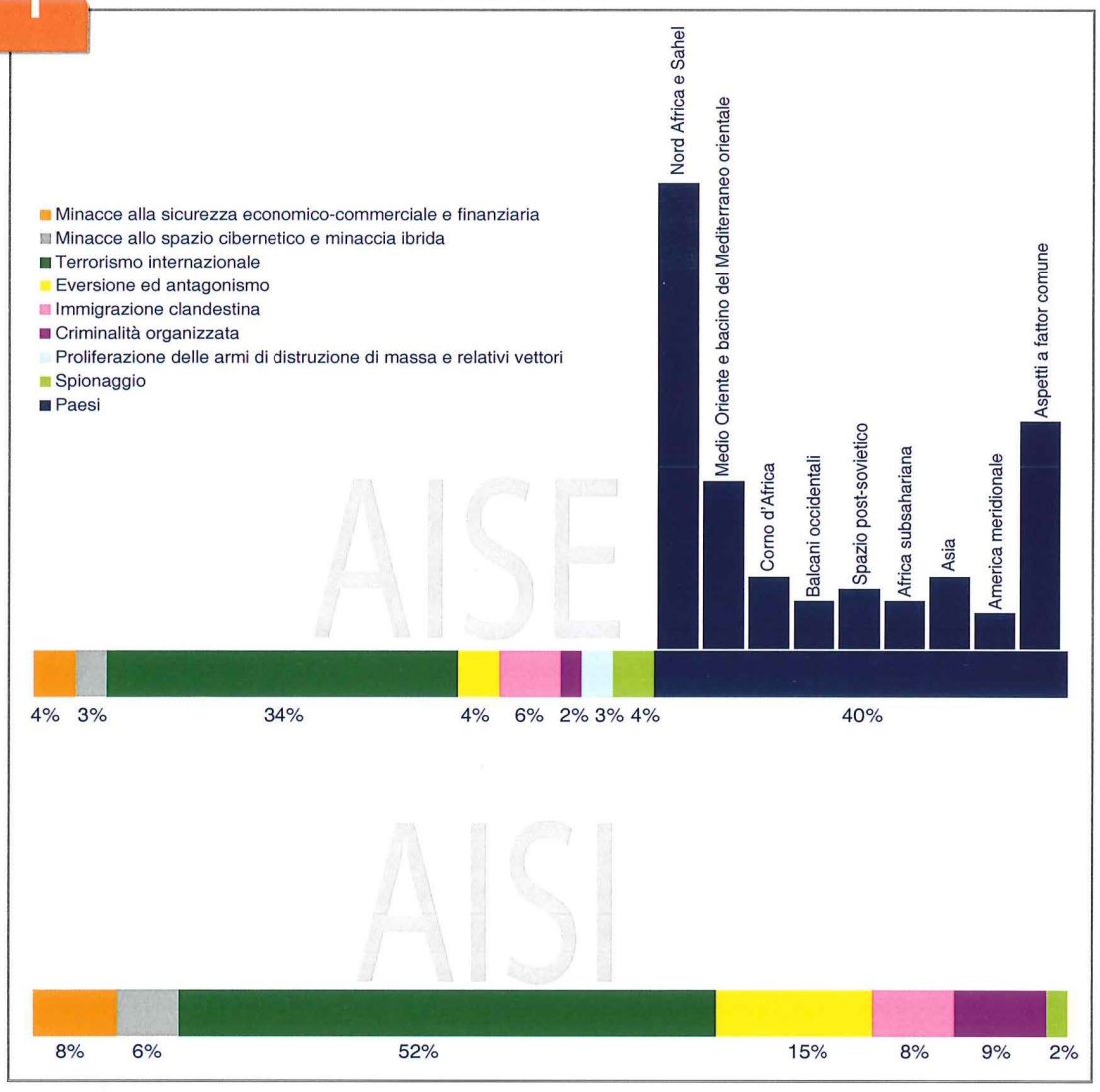
Il complesso delle evidenze raccolte è valso a ribadire, inoltre, come le accentuate interconnessioni tra gli eventi abbiano concorso a determinare rapidi mutamenti nel contesto e negli ambiti operativi dell'Intelligence, laddove profili inediti o emergenti della minaccia sono andati ad integrare il novero di fenomeni più risalenti e conosciuti, anch'essi peraltro in continua evoluzione. Ciò ha sollecitato il costante affinamento della ricerca informativa, l'acquisizione di nuove competenze e l'aggiornamento di chiavi di lettura e paradigmi interpretativi, anche a fronte di progressioni tecnologiche che, rimarchevoli per caratura e velocità, stanno ridise-

gnando forme e contenuti di minacce, rischi e opportunità.

L'incessante e coordinata attività operativa svolta dalle Agenzie in aderenza agli indirizzi del Governo, testimoniata dall'output info-analitico a beneficio di Enti istituzionali e Forze di polizia (vds. tavola n. 1), si è quindi accompagnata ad interventi di carattere organizzativo – volti a rendere ancora più performante la "macchina informativa" – e ad iniziative di/in raccordo con altre Amministrazioni dello Stato, con la Comunità accademica e della ricerca, nonché con il mondo imprenditoriale.

INFORMATIVE/ANALISI
INVIATE A ENTI ISTITUZIONALI E FORZE DI POLIZIA NEL 2020
(dati percentuali)

1

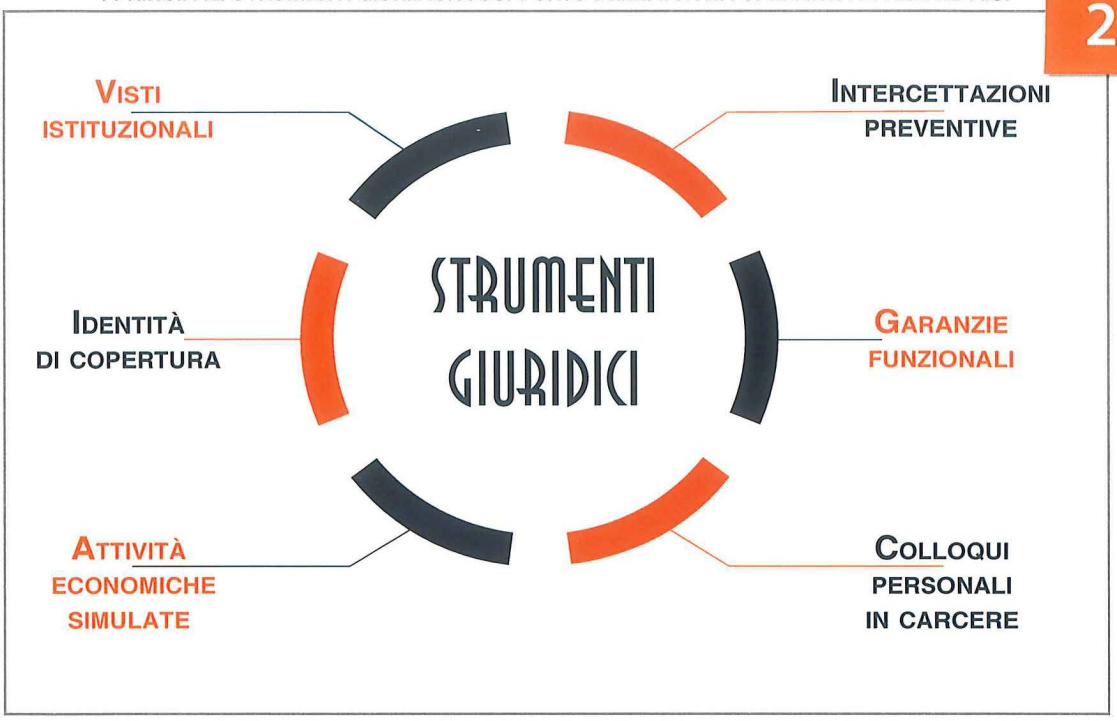


Tutto questo, in coerenza con la logica "di sistema" a suo tempo introdotta dalla legge 124/2007, che, tra i punti di forza dell'architettura a presidio della sicurezza nazionale, ha previsto il coordinamento tra le Agenzie, mirati strumenti giuridici a supporto e garanzia delle attività operative (vds. tavola n. 2), solidi meccanismi di cooperazione interistituzionale e la promozione della cultura della sicurezza.

Nel contesto descritto hanno così trovato spazio, nel 2020, il ruolo pro-attivo assicurato dal Comparto – anche sul piano degli aggiornamenti normativi – sia in tema di tutela degli assetti strategici e del correlato esercizio del cd. Golden Power sia con riguardo all'attuazione del perimetro di sicurezza nazionale cibernetica, nonché le assidue interlocuzioni con enti pubblici e privati finalizzate ad accrescerne il livello di consapevolezza sul versante della minaccia.

I PRINCIPALI STRUMENTI GIURIDICI A SUPPORTO DELL'ATTIVITÀ OPERATIVA DI AISE ED AISI

2

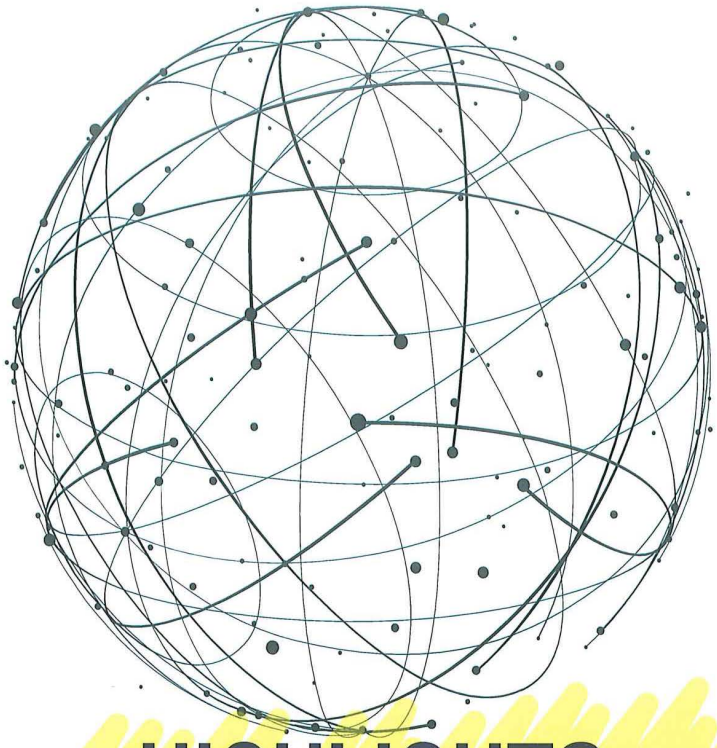


Nella medesima cornice si collocano gli avanzamenti nel progetto evolutivo della Scuola di Comparto, sempre più un vero e proprio Campus, ove la formazione, sulla scorta di programmi in costante aggiornamento, si coniuga con una pronunciata proiezione esterna, funzionale a supportarne la vocazione di centro irradiatore di cultura della sicurezza, alveo privilegiato per la condivisione di saperi e laboratorio per lo sviluppo di capacità previsionali e pensiero strategico. Obiettivo, quest'ultimo, perseguito con attività formative e seminariali anche a livello europeo, nell'ambito dell'Intelligence College in Europe – piattaforma di riflessione congiunta ed outreach cui hanno sinora aderito 23 Paesi del Vecchio

Continente – e che riflette l'avvertita percezione di come la valenza del prodotto a beneficio del decisore politico si misuri in modo crescente con la capacità di estendere lo sguardo. Del resto, la prevedibile onda lunga del Covid-19, nella sua incidenza pervasiva e globale, va ora ad aggiungersi alle sfide di scenario destinate a rappresentare, seppure con diverso peso e raggio temporale, altrettante variabili, se non vere e proprie ipoteche, sulla sicurezza dei cittadini e sugli interessi nazionali: dai cambiamenti climatici agli squilibri demografici, dalla transizione energetica all'esigenza, ineludibile, di perseguire nuovi modelli di sviluppo sostenibile, dai piani di ripresa mondiale ed europea alle frontiere possibili dell'Intelligenza Artificiale, dalle implicazioni della Brexit al posizionamento della UE sulla scena globale. Temi, questi, che dal dicembre 2020 vedono l'ingaggio del nostro Paese anche quale presidente di turno del G20.

La presente Relazione, che si rende al Parlamento ai sensi dell'art. 38 della citata legge 124/2007, si apre – come nelle ultime edizioni – con uno sguardo sullo scenario internazionale, focalizzato su quadranti e attori di prioritario interesse informativo, per poi soffermarsi sulle principali minacce al Sistema Paese, nella dimensione economico-finanziaria, cyber ed ibrida, sul terrorismo jihadista, su immigrazione clandestina e criminalità organizzata, nonché sull'estremismo endogeno. In allegato, come previsto dalla norma, il "Documento di sicurezza nazionale", in materia di protezione cibernetica.

Attesa la natura pubblica e non classificata della Relazione, i suoi contenuti devono intendersi quale panoramica di sintesi, fermo restando che una più dettagliata rendicontazione delle attività dei Servizi di informazione per la sicurezza è contenuta nella Relazione che semestralmente il Presidente del Consiglio trasmette, ai sensi dell'art. 33, comma 1, della stessa legge 124/2007, al Comitato parlamentare per la sicurezza della Repubblica, Organo di cui va qui richiamata l'azione di orientamento e stimolo svolta in quest'anno difficile.



HIGHLIGHTS

Nella prospettiva Intelligence, l'emergenza pandemica ha reso più articolato e complesso il quadro della minaccia, abbattendosi sulle economie, condizionando sviluppi geopolitici e relazioni internazionali, aggravando vulnerabilità strutturali e tensioni sociali, inasprendo la competizione, specie per il dominio tecnologico, e accrescendo gli spazi per manovre ostili e tentativi d'ingerenza di diversa matrice e portata.

In questo contesto, il Comparto ha assicurato il massimo impegno informativo e d'analisi – riorientando, all'occorrenza, direttrici e target della ricerca – e messo in campo iniziative di carattere sistemico, intese ad acquisire nuove competenze e capacità previsionali, nonché ad alimentare le migliori sinergie con le altre Amministrazioni dello Stato, con la Comunità accademica e con il mondo imprenditoriale, pure in ottica di promozione e diffusione della cultura della sicurezza.

Sul **VERSANTE ESTERO**, prioritaria attenzione informativa è stata riservata alla **regione mediterranea**, che a 10 anni dalle cc.dd. primavere arabe è ancora affetta da instabilità diffusa.

Nella fascia nordafricana, cruciale per gli interessi nazionali, il focus sulla **Libia** ha guardato agli sviluppi del confronto tra le componenti dell'Ovest e dell'Est e al profilarsi di una nuova fase negoziale, peraltro insidiata dal persistere, in quel teatro, di linee di faglia ed interessi contrapposti, locali e di sponsor esteri.

Il protrarsi della crisi ha continuato a riflettersi sulla sicurezza regionale, alimentando traffici illeciti e circuiti di sostegno all'estremismo jihadista, in un con-

testo di vulnerabilità socio-economiche reso ancora più fragile dall'impatto della pandemia. La grave congiuntura si è accompagnata: in **Tunisia**, a un'ondata di proteste e alla perdurante esposizione alla minaccia terroristica; in **Algeria**, alla ridefinizione degli equilibri interni; in **Egitto**, ad un'allerta elevatissima nei riguardi di frange qaidiste e filo-DAESH.

Anche per i loro riflessi sul Nord Africa, hanno rivestito specifico interesse informativo le dinamiche della fascia subsahariana.

La **regione del Sahel**, ove il nostro Paese sta assumendo un ruolo più profilato, ha conosciuto un accentuato dinamismo politico, ma anche un nuovo incremento della violenza, soprattutto di matrice jihadista, dovuto pure all'emergente, agguerrita competizione tra i gruppi qaidisti e quelli afferenti a DAESH. Il quadrante – segnato, altresì, da cronici conflitti settari – ha registrato cruente azioni terroristiche in **Niger**, **Mali** e **Burkina Faso**, nonché, più a Est, in **Nigeria** e nell'area del **Bacino del Lago Ciad**.

Segnali di scadimento dei livelli securitari sono stati colti anche nel **Corno d'Africa**, ove fragilità istituzionali e vulnerabilità economiche si sono accompagnate al pervasivo attivismo della formazione qaidista somala al Shabaab. Di rilievo, nel contesto, la contrapposizione tra Autorità centrali e Stati federati in **Somalia**, nonché la conflittualità e le tensioni interetniche in **Etiopia**.

Nel quadro delle dinamiche incidenti nell'area del Mediterraneo, specifico interesse informativo ha rivestito l'accresciuta competizione tra diversi attori per lo sfruttamento delle risorse energetiche off-shore nel **Bacino del Levante**, assurto a teatro di rivalità tra player rivieraschi ed extraregionali.

Articolato impegno informativo ha continuato ad essere rivolto al **quadrante mediorientale**, ove la pandemia ha di fatto contribuito a congelare le tensioni nell'area, dopo l'apice del confronto tra USA e Iran agli inizi del 2020, esacerbando, peraltro, vulnerabilità sociali e criticità politiche.

Quanto alle singole realtà nazionali, sono emerse in evidenza, tra l'altro: in **Siria**, le rimodulazioni interne all'establishment e la vitalità di sigle terroristiche; in **Libano**, la gravissima situazione finanziaria; in **Giordania**, le difficoltà, aggravate dalla crisi sanitaria, nella gestione dei rifugiati; nei **Territori Palestinesi**, i tentativi di ricomposizione della frattura interna; in **Iraq** (ove l'Italia è direttamente ingaggiata nella stabilità del Paese), la crescita delle capacità offensive di DAESH; in **Iran**, l'affermazione elettorale della componente conservatrice e l'evoluzione dei rapporti con gli USA e la Comunità internazionale.

Le dinamiche nel **Golfo** sono state dominate dalla normalizzazione dei rapporti diplomatici tra **Israele**, da un lato, ed **Emirati Arabi Uniti** e **Bahrain**, dall'altro, nonché dalle iniziative politiche volte a superate la spaccatura interna al Consiglio di Cooperazione del Golfo. Ancora senza esito i tentativi di mediazione nello **Yemen**, dove sei anni di ininterrotta ostilità hanno provocato una delle più gravi crisi umanitarie al mondo, acuita dall'arrivo del Covid-19.

HIGHLIGHTS

Anche a supporto del contingente italiano, costante monitoraggio informativo è stato dedicato alla situazione in **Afghanistan**, ove lo storico accordo tra Stati Uniti e Taliban non ha ancora permesso un'effettiva pacificazione del Paese, teatro, anche nel 2020, di cruenti attentati. Persistente dinamismo di gruppi insorgenti e frange terroristiche si è registrato, altresì, in **Pakistan**.

Lo sguardo analitico del Comparto ha visto la **Russia** confrontarsi con importanti dossier di politica interna ed economica, dal referendum costituzionale al severo impatto della pandemia, ma anche con crisi, emergenti o rivitalizzate, nello spazio post-sovietico. È il caso del confronto tra **Armenia** e **Azerbaigian** (sia nel confine settentrionale che nel Nagorno-Karabakh), delle proteste in **Bielorussia** e delle tensioni in **Kyrgyzstan**. Nel contempo, la visione strategica di Mosca ha conosciuto diverse declinazioni, inclusa la produzione di linee di policy sull'Artico e sulla deterrenza nucleare. Quanto alle relazioni internazionali, il Cremlino ha rafforzato la cooperazione bilaterale nel settore sanitario con numerosi Paesi, mentre, per altro verso, si è confermato articolato e complesso il dialogo con l'Occidente.

Postura e proiezioni della **Cina** sulla scena globale hanno continuato a rappresentare ambito rilevante di impegno per l'Intelligence. Muovendo dalla pandemia Pechino ha, sul fronte interno, implementato un più stringente sistema di controllo sociale, mentre all'estero ha potenziato la collaborazione internazionale anche in ambito sanitario, in coerenza con un dinamismo giocato su più piani (diplomatico, degli investimenti infrastrutturali e del commercio) e in direzione di un esteso novero di Paesi, nonché sullo sfondo di una strategia espansiva che ha fatto registrare, tra l'altro, significative progressioni nel campo dello Spazio, il quarto dominio. L'emergenza pandemica ha concorso, pure, a spiralizzare il confronto con gli Stati Uniti, inserendosi in un contesto che vede Pechino da tempo accusata di condotte scorrette sul mercato e violazione dei diritti umani, temi in evidenza anche in ambito UE.

L'incidenza della crisi sanitaria sul panorama della minaccia è emersa con particolare evidenza nell'attività informativa a **PRESIDIO DELL'ECONOMIA NAZIONALE**. Le difficoltà della congiuntura hanno contribuito a rendere più concreto il rischio di azioni di tipo predatorio/speculativo nei confronti di asset pregiati in Italia.

Al riguardo, l'Intelligence ha intensificato l'attività di ricerca ed analisi a supporto del decisore politico, anche ai fini dell'esercizio dei poteri speciali (cd. Golden Power) e dell'implementazione della normativa di riferimento.

La raccolta informativa a tutela degli assetti strategici si è focalizzata innanzi tutto sulla **filiera sanitaria**, anche con riferimento a possibili ingerenze esterne in danno di strutture emergenziali, centri di ricerca ed aziende. Alla prioritaria attenzione, inoltre, i settori: **aerospazio**, **difesa** e **sicurezza**, atteso l'appetibile know how della nostra industria; **telecomunicazioni**, anche in ragione delle profonde trasformazioni tecnologiche e organizzative connesse all'introduzione

della tecnologia 5G; **meccanica/meccatronica**, **automotive**, **biotech** e **made in Italy**, in grado di valorizzare i risultati della ricerca; **logistica**, in particolare quella **portuale**, di assoluta centralità in ragione della forte integrazione dell'economia italiana nei flussi commerciali internazionali.

Il monitoraggio dell'Intelligence non ha mancato di ricomprendere, inoltre, le dinamiche del **sistema finanziario** nazionale, specie in relazione a progettualità estere suscettibili di ricadute anche sugli equilibri di finanziamento del debito pubblico italiano e sulle policy di erogazione di crediti alle nostre imprese, come quelle afferenti la **sicurezza energetica** nazionale, con riguardo sia alla continuità degli approvvigionamenti, sia alle prospettive connesse al processo di decarbonizzazione dell'economia europea.

Come altri fronti, anche quello della **MINACCIA CIBERNETICA** è stato significativamente condizionato dall'emergenza pandemica, chiamando il Comparto a orientare una parte rilevante degli sforzi verso il contenimento di **progettualità ostili** (di matrice statuale, hacktivista o criminale): miranti a sfruttare il massiccio ricorso al lavoro agile in danno di operatori pubblici e privati, ovvero tese ad esfiltrare dati sensibili da strutture ospedaliere, centri di ricerca e realtà impegnate nello sviluppo di vaccini e terapie contro il Covid-19. In generale, gli attacchi "censiti" dall'Intelligence hanno fatto emergere: un complessivo incremento degli episodi; la prevalenza di target pubblici, specie Amministrazioni locali; la persistente, maggior ricorrenza della matrice hacktivista ed una contrazione dei casi di matrice statuale, a fronte peraltro di un aumento di azioni dalla matrice non identificabile, che potrebbe sottendere un'accresciuta capacità di operare senza lasciare traccia.

Una mirata e coordinata azione informativa ha interessato pure la **MINACCIA IBRIDA** – per definizione veicolata su diversi domini (quello diplomatico, militare, economico/finanziario, intelligence, etc.) – che, in concomitanza con il dispiegarsi della crisi sanitaria, è stata caratterizzata da costanti tentativi di intossicazione del dibattito pubblico attraverso campagne di disinformazione e/o di influenza.

È proseguita serrata e ininterrotta, in Italia e all'estero, l'attività informativa in direzione del **TERRORISMO JIHADISTA**, nel contesto di un dispositivo di prevenzione integrato che ha continuato a trovare punto di forza nelle consolidate sinergie tra Intelligence e Forze di polizia, specie nell'ambito del Comitato Analisi Strategica Antiterrorismo, e nell'assidua cooperazione con i Servizi esteri collegati.

Il 2020 ha visto la strategia di **DAESH** dipanarsi lungo tre principali direttrici: rivitalizzazione dell'attività insorgente in Iraq e Siria; decentralizzazione in

favore delle articolazioni regionali in Africa e in Asia; rilancio del conflitto asimmetrico in crisi d'area e teatri di jihad. La formazione ha mostrato, inoltre, un rinnovato attivismo mediatico.

Al Qaida, dal canto suo, ha proseguito la lotta contro i "nemici dell'Islam", declinandola in agende regionali focalizzate sulle istanze delle popolazioni, tra le quali si è nel tempo accreditata, ma anche adottando una strategia comunicativa in grado di garantire unitarietà tra obiettivi locali e globali.

Per quanto concerne l'**Europa**, gli attentati compiuti nel corso dell'anno hanno confermato i tratti prevalentemente endogeni e destrutturati della minaccia jihadista sul nostro Continente, tradottasi in attivazioni autonome ad opera di soggetti per lo più privi di legami con gruppi terroristici, ma da questi (specialmente DAESH) influenzati o ispirati. A una progettualità pianificata parrebbe ricondurre, peraltro, l'azione di Vienna del 2 novembre, alla luce di risultanze (su contatti e collegamenti dell'attentatore) valse anche a ribadire il ruolo della **regione balcanica** quale potenziale incubatore della minaccia terroristica in direzione di Paesi europei. Significativi indicatori della minaccia provengono anche dalle operazioni di controterrorismo condotte nell'anno, che attestano il persistente rischio di attivazioni da parte di ex combattenti e frustrated travellers, gli spostamenti di foreign fighters che decidono in autonomia di lasciare il Medio Oriente e ripiegare in suolo europeo, nonché la mai sopita ambizione di DAESH di colpire l'Europa. Profilo, quest'ultimo, richiamato anche nei warning condivisi in ambito di collaborazione internazionale.

L'impegno informativo in **territorio nazionale** ha continuato a focalizzarsi, in via prioritaria, sui processi di radicalizzazione, innescati o alimentati soprattutto sul web, ove vengono diffusi articoli, video di propaganda, istruzioni per la fabbricazione di ordigni e messaggi istigatori in lingua italiana; nelle carceri, come confermato, tra l'altro, dalle espulsioni a fine pena di soggetti detenuti per reati comuni che hanno aderito alla causa jihadista durante la reclusione; in luoghi di aggregazione, ove è emersa la pervasiva opera di proselitismo svolta da individui attestati su posizioni radicali.

L'emergenza pandemica ha parzialmente influito sull'andamento dei **FLUSSI MIGRATORI CLANDESTINI** in direzione dell'Europa e dell'Italia, che nelle rotte via mare, dopo la contrazione durante la primavera, hanno ripreso il trend incrementale mostrato all'inizio dell'anno. La ricerca intelligence ha riguardato prioritariamente la gestione criminale del fenomeno e segnatamente: gruppi tunisini e libici, ingaggiati lungo la direttrice del Mediterraneo centrale; strutturate reti – con sodali in territorio nazionale – attive nei trasferimenti via mare dalla Turchia alle coste greche e italiane; compagini afghane, pakistane e irachene, anch'esse con referenti in Italia, operanti sulla rotta balcanica terrestre.

Gli arrivi parcellizzati attraverso la frontiera terrestre, così come gli sbarchi

fantasma dal Nord Africa o dalle sponde turco-elleniche, restano, sul piano della sicurezza, le modalità d'ingresso più critiche, rispetto alle quali i rischi sanitari connessi alla possibile dispersione sul territorio nazionale di soggetti positivi al virus sono andati ad aggiungersi al pericolo di infiltrazioni terroristiche. Su quest'ultimo versante, peraltro, le risultanze della serrata attività d'intelligence fanno ancora escludere un ricorso sistematico ai canali dell'immigrazione clandestina per la movimentazione di jihadisti, mentre il "falso documentale" si è confermato insidioso ambito di interazione tra circuiti criminali e terroristici.

I tratti distintivi della **CRIMINALITÀ ORGANIZZATA**, così come ribaditi dalle acquisizioni intelligence, nonché dalle risultanze investigative e giudiziarie, valgono da sé a profilare l'interesse delle **mafie nostrane** a trarre profitto dall'impatto dell'emergenza pandemica e, segnatamente, a condizionare gli operatori economici in difficoltà e a tentare di intercettare i finanziamenti, nazionali ed europei, connessi ai piani di rilancio.

Fattore cruciale di alimentazione della capacità pervasiva dei sodalizi, anche in termini di alterazione della concorrenza e del corretto funzionamento del mercato, resta la disponibilità di denaro assicurata dai traffici illeciti più remunerativi. I sodalizi mafiosi, grazie anche alle saldature con professionisti e imprenditori collusi, hanno ulteriormente affinato le capacità di reinvestimento dei proventi illeciti, ma anche di occultamento e di movimentazione dei capitali a fini di evasione ed elusione fiscale.

Caratteristiche comuni alle singole matrici mafiose ('ndrangheta, Cosa nostra, camorra e aggregazioni pugliesi) sono risultate la pronunciata fluidità degli assetti, dovuta all'incessante azione di contrasto, e la sempre più marcata differenziazione tra componenti di profilo affaristico-strategico e formazioni di minor spessore, maggiormente esposte alla competizione interclanica.

All'attenzione informativa anche le **compagini straniere**, la cui crescita organizzativa, specie con riguardo ai gruppi nigeriani, è testimoniata dal crescente coinvolgimento in attività di riciclaggio e in articolate frodi informatiche.

L'emergenza pandemica ha inciso pure sul versante dell'**EVERSIONE INTERNA**: da un lato, limitando le potenzialità mobilitative dell'estremismo politico, dall'altro, facendo da volano, in concomitanza con il ruolo aggregante e amplificatore del web, a una montante effervescenza propagandistica, trasversalmente orientata a strumentalizzare la crisi sanitaria per rilanciare progettualità conflittuali e istanze antisistema.

L'**anarco-insurrezionalismo** resta la componente eversiva endogena più vitale, che alle campagne online (contro "repressione", tecnologie e misure di contenimento del contagio) ha visto corrispondere sortite operative, consistenti per lo più in atti vandalici e/o incendiari e sabotaggi, ai danni soprattutto di infrastrutture delle telecomunicazioni.

HIGHLIGHTS

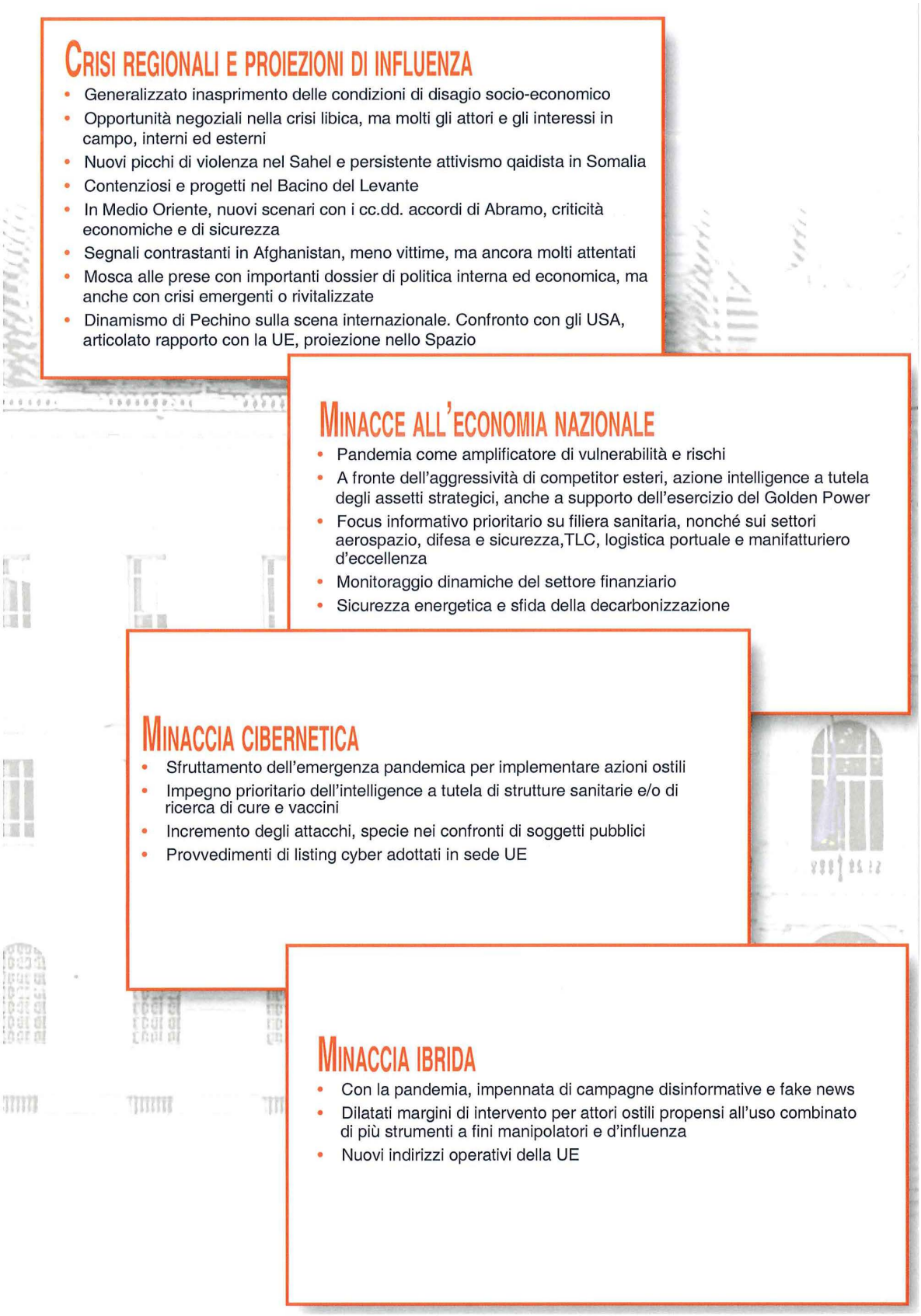
L'attività dei ristretti **circuiti marxisti-leninisti** è parsa ancora improntata alla tradizionale opera di recupero della memoria brigatista, unita ad interventi volti ad attualizzarne il messaggio, anche attraverso l'analisi, in ottica di "contrapposizione di classe", delle ricadute socio-economiche dell'emergenza sanitaria, oltre che delle dinamiche del mondo del lavoro.

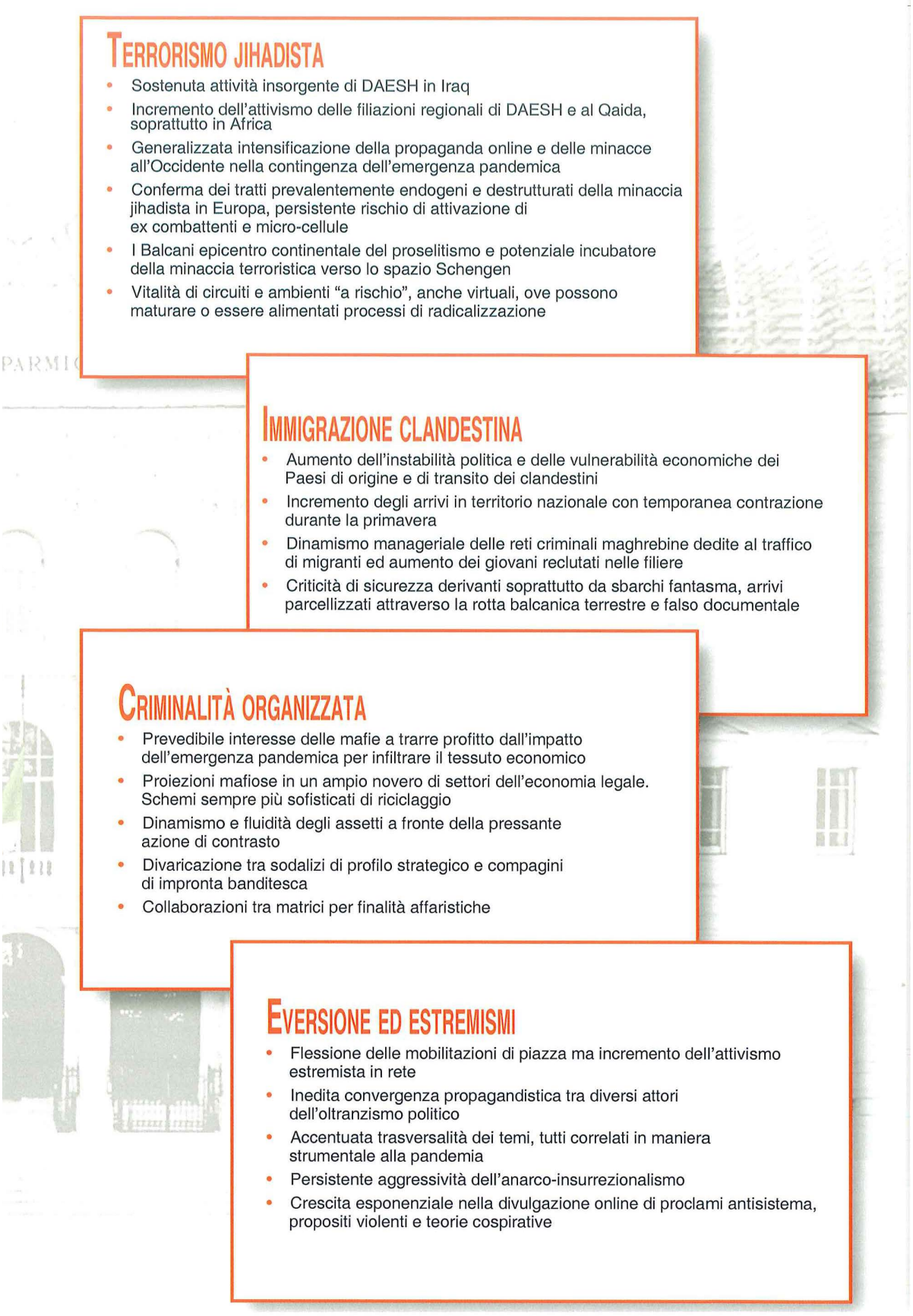
La crisi sanitaria e la sua gestione da parte del Governo hanno costituito temi centrali del dibattito che ha coinvolto le diverse "anime" del **movimento antagonista**, impegnato a rilanciare progettualità aggregative attorno a tradizionali campagne di lotta (a partire dal filone ambientalista), anche attraverso una propaganda d'area che ha, tra l'altro, strumentalmente connesso la diffusione del virus con il progresso tecnologico e i cambiamenti climatici.

Massima attenzione informativa, sul piano della ricerca e dell'analisi, è stata riservata agli ambienti della **destra radicale**, anche nella dimensione virtuale, nel cui ambito, in relazione alla pandemia, sono proliferate campagne di disinformazione e teorie cospirative, accompagnatesi a retoriche ultranazionaliste, xenofobe e razziste, nonché ad interventi propagandistici dagli accesi toni antisistema.

Importanti avanzamenti ha fatto registrare, nel 2020, il processo di rafforzamento dell'**ARCHITETTURA NAZIONALE DI SICUREZZA CIBERNETICA**, specie per quel che concerne: l'elaborazione dei decreti attuativi delle norme sul "Perimetro di sicurezza nazionale cibernetica"; l'implementazione della Direttiva europea NIS; la sicurezza delle reti 5G (con riguardo all'inserimento, nella disciplina nazionale sul Golden Power, di un richiamo anche alle linee guida europee in tema di notifiche relative all'acquisto di tecnologia 5G da fornitori extraeuropei); le attività del Nucleo di Sicurezza Cibernetica e dello CSIRT (Computer Security Incident Response Team) italiano, divenuto operativo presso il DIS in maggio.

Nel novero delle iniziative intese a rafforzare la resilienza cyber del Paese vanno richiamate, infine, quelle di carattere formativo e divulgativo, per una più diffusa consapevolezza e conoscenza di rischi e contromisure.


CRISI REGIONALI E PROIEZIONI DI INFLUENZA
• Generalizzato inasprimento delle condizioni di disagio socio-economico
• Opportunità negoziali nella crisi libica, ma molti gli attori e gli interessi in campo, interni ed esterni
• Nuovi picchi di violenza nel Sahel e persistente attivismo qaidista in Somalia
• Contenziosi e progetti nel Bacino del Levante
• In Medio Oriente, nuovi scenari con i cc.dd. accordi di Abramo, criticità economiche e di sicurezza
• Segnali contrastanti in Afghanistan, meno vittime, ma ancora molti attentati
• Mosca alle prese con importanti dossier di politica interna ed economica, ma anche con crisi emergenti o rivitalizzate
• Dinamismo di Pechino sulla scena internazionale. Confronto con gli USA, articolato rapporto con la UE, proiezione nello Spazio
MINACCE ALL'ECONOMIA NAZIONALE
• Pandemia come amplificatore di vulnerabilità e rischi
• A fronte dell'aggressività di competitor esteri, azione intelligence a tutela degli assetti strategici, anche a supporto dell'esercizio del Golden Power
• Focus informativo prioritario su filiera sanitaria, nonché sui settori aerospazio, difesa e sicurezza,TLC, logistica portuale e manifatturiero d'eccellenza
• Monitoraggio dinamiche del settore finanziario
• Sicurezza energetica e sfida della decarbonizzazione
MINACCIA CIBERNETICA
• 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
MINACCIA IBRIDA
• 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


TERRORISMO JIHADISTA
• 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
IMMIGRAZIONE CLANDESTINA
• Aumento dell'instabilità politica e delle vulnerabilità economiche dei Paesi di origine e di transito dei clandestini
• Incremento degli arrivi in territorio nazionale con temporanea contrazione durante la primavera
• Dinamismo manageriale delle reti criminali maghrebine dedite al traffico di migranti ed aumento dei giovani reclutati nelle filiere
• Criticità di sicurezza derivanti soprattutto da sbarchi fantasma, arrivi parcellizzati attraverso la rotta balcanica terrestre e falso documentale
CRIMINALITÀ ORGANIZZATA
• Prevedibile interesse delle mafie a trarre profitto dall'impatto dell'emergenza pandemica per infiltrare il tessuto economico
• Proiezioni mafiose in un ampio novero di settori dell'economia legale. Schemi sempre più sofisticati di riciclaggio
• Dinamismo e fluidità degli assetti a fronte della pressante azione di contrasto
• Divaricazione tra sodalizi di profilo strategico e compagini di impronta banditesca
• Collaborazioni tra matrici per finalità affaristiche
EVERSIONE ED ESTREMISMI
• Flessione delle mobilitazioni di piazza ma incremento dell'attivismo estremista in rete
• Inedita convergenza propagandistica tra diversi attori dell'oltranzismo politico
• Accentuata trasversalità dei temi, tutti correlati in maniera strumentale alla pandemia
• Persistente aggressività dell'anarco-insurrezionalismo
• Crescita esponenziale nella divulgazione online di proclami antisistema, propositi violenti e teorie cospirative

PAGINA BIANCA

CRISI REGIONALI E PROIEZIONI DI INFLUENZA

in breve

- Generalizzato inasprimento delle condizioni di disagio socio-economico
- Opportunità negoziali nella crisi libica, ma molti gli attori e gli interessi in campo, interni ed esterni
- Nuovi picchi di violenza nel Sahel e persistente attivismo qaidista in Somalia
- Contenziosi e progetti nel Bacino del Levante
- In Medio Oriente, nuovi scenari con i cc.dd. accordi di Abramo, criticità economiche e di sicurezza
- Segnali contrastanti in Afghanistan, meno vittime, ma ancora molti attentati
- Mosca alle prese con importanti dossier di politica interna ed economica, ma anche con crisi emergenti o rivitalizzate
- Dinamismo di Pechino sulla scena internazionale. Confronto con gli USA, articolato rapporto con la UE, proiezione nello Spazio

L'attività informativa e d'analisi sul versante estero, necessariamente dinamica e multidisciplinare a fronte di fenomeni sempre più mutevoli, trasversali e interconnessi, ha visto l'emergenza pandemica agire quale fattore di condizionamento globale e pervasivo, seppure variamente declinato per effetti e profondità, con riguardo non solo a crisi d'area – conflagrate, endemiche o in divenire – ma anche ad equilibri politici, disegni geostrategici e relazioni internazionali.

Nell'ottica della sicurezza nazionale e della tutela di cittadini ed interessi italiani all'estero, la ricerca, sostenuta dal costante monitoraggio informativo su un esteso novero di ambiti territoriali e tematici, si è focalizzata su contesti e attori di maggior rilevanza per il nostro Paese, per prossimità geografica, valenza strategica o potenziale impatto delle minacce ad essi riferibili.

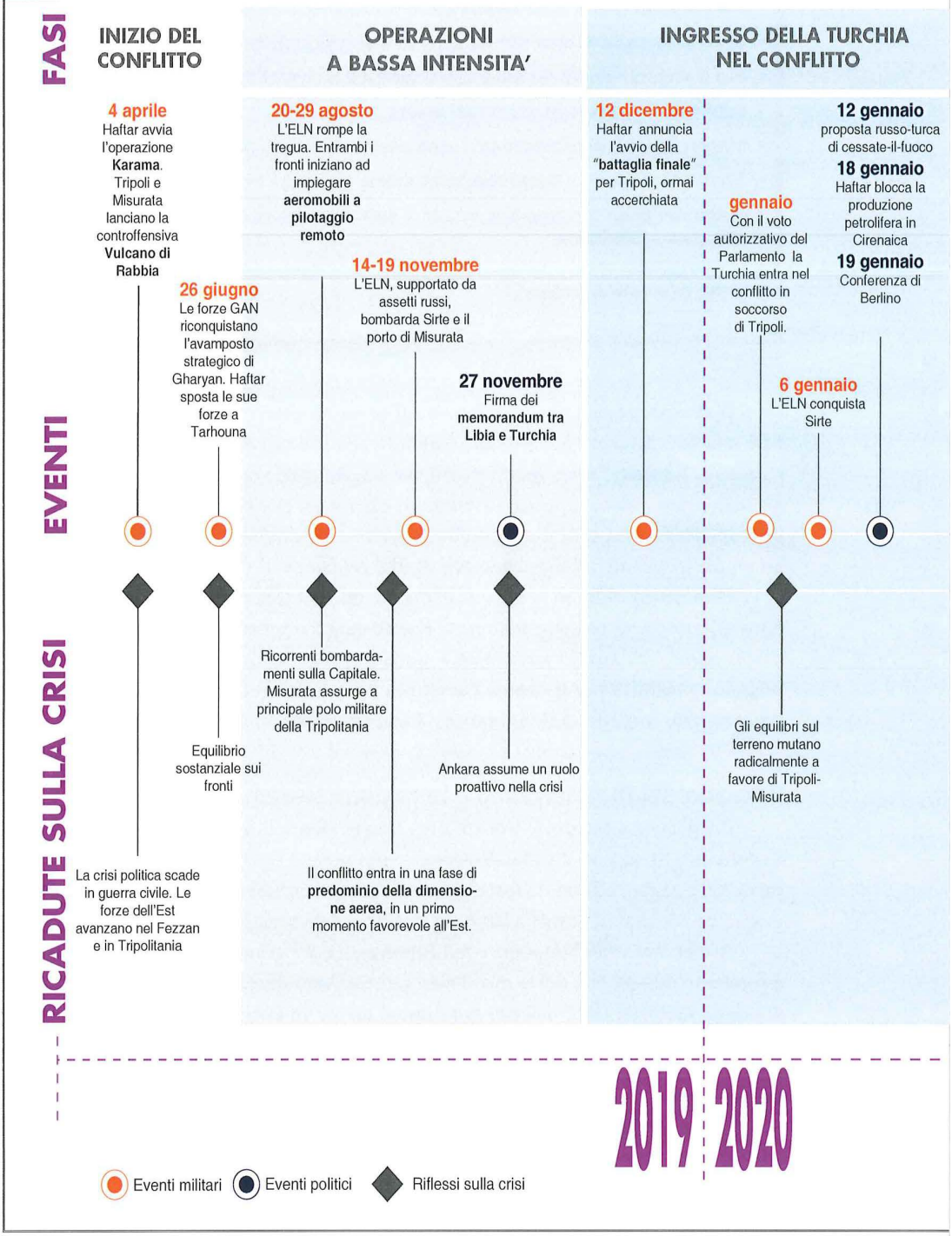
Il bacino del Mediterraneo e la regione subsahariana

Prioritaria attenzione informativa è stata riservata alla regione mediterranea, ancora alle prese con il radicale riassetto dei propri equilibri a 10 anni dalle cc.dd. primavere arabe, affetta da instabilità diffusa e attraversata da criticità di varia natura che ne frenano il consolidamento in senso democratico e la ripresa economica.

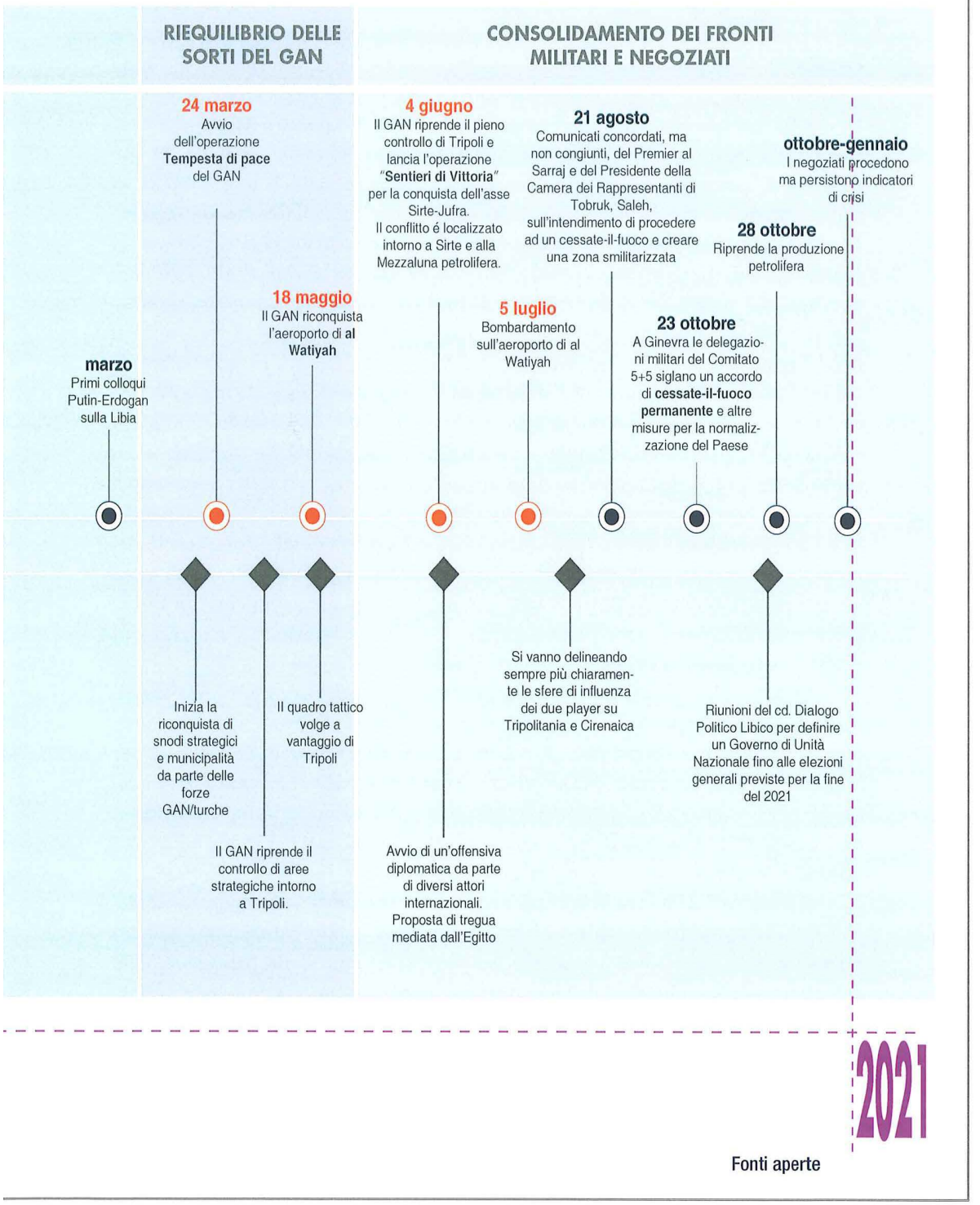
Anche nel 2020 l'impegno dell'Intelligence si è concentrato sulla crisi in **Libia**, a supporto dell'azione del nostro Paese per una stabilizzazione inclusiva, a salvaguardia degli interessi nazionali nel quadrante, anche in termini di garanzia dei rifornimenti energetici, nonché in chiave di presidio avanzato sul versante del contrasto alla minaccia terroristica e all'immigrazione clandestina. In tale quadro, specifica attenzione è stata riservata agli sviluppi delle relazioni tra le diverse componenti libiche, dell'Ovest e dell'Est, che, dalla seconda metà dell'anno – con l'interruzione delle ostilità seguita al raggiungimento del cessate-il-fuoco – hanno fatto registrare l'apertura di un'importante finestra di opportunità negoziale (vds. tavola n. 3).

3

TIMELINE DEI PRINCIPALI EVENTI DELLA CRISI LIBICA



CRISI REGIONALI E PROIEZIONI DI INFLUENZA



Da un lato, l'intervento turco a favore di Tripoli (avviato all'inizio del 2020) e il contestuale disimpegno delle forze cirenaiche dalle aree a sud della Capitale hanno riequilibrato i rapporti di forza sul campo, dall'altro, il Governo di Accordo Nazionale-GAN, dopo circa un anno di conflitto, ha riguadagnato terreno e credibilità diplomatica nei confronti di altri player, libici e internazionali. A tali sviluppi hanno corrisposto diverse iniziative – specie sotto egida ONU, attraverso UNSMIL, nel quadro dei 3 track negoziali (securitario, politico ed economico) – volte ad elaborare un meccanismo di monitoraggio del cessate-il-fuoco che potrebbe prevedere anche l'invio di osservatori internazionali. Il fine è quello di stabilizzare le dinamiche intra-libiche fino alla costituzione di un nuovo Esecutivo di unità nazionale in grado di traghettare il Paese verso le elezioni parlamentari e presidenziali previste entro il 2021. Si tratta di un obiettivo cruciale, insidiato, peraltro, dal riaffiorare delle tradizionali linee di conflittualità – politica, ideologica e tribale – che dal 2011 caratterizzano lo scenario libico. A ostacolare il raggiungimento di intese significative potrebbero concorrere, in particolare, la ripresa delle ostilità tra i gruppi armati tripolini, con l'insoluto nodo del reintegro dei miliziani in apparati di difesa e sicurezza "nazionali", la presenza di migliaia di mercenari (specie siriani, sudanesi e ciadiani) al servizio delle due parti e, su tutto, la pletora di veti incrociati da parte dei principali attori libici interessati a proteggere i propri interessi e quelli dei rispettivi sponsor esteri. Più in generale, le evidenze dell'intelligence fanno stato della delicatezza e della complessità del contesto, caratterizzato da equilibri altalenanti e da forti interessi, locali e di sponsor esteri, nell'ambito della ormai conclamata guerra per procura che contraddistingue quello scontro (con Turchia e Qatar al fianco di Tripoli ed Egitto, Emirati Arabi Uniti e Russia a sostegno della Cirenaica).

Quanto alle condizioni socio-economiche, si è assistito in autunno alla ripresa operativa dei siti petroliferi che, se da un lato ha riattivato la produzione, bloccata da circa un anno, dall'altro non si è ancora tradotta in benefici né per la popolazione, già provata dall'impatto del conflitto e dell'emergenza pandemica, né per le casse dello Stato, poiché gli introiti sono rimasti "congelati" presso una banca terza, in attesa di un accordo tra le Autorità dell'Est e dell'Ovest per un'equa ripartizione di quelle risorse finanziarie.

Il protrarsi della crisi libica ha continuato a riflettersi sulla sicurezza regionale, alimentando traffici illeciti e circuiti di sostegno al terrorismo jihadista, in un contesto di vulnerabilità reso più critico dall'impatto della pandemia, che, nell'aggravare le condizioni di disagio economico, ha ulteriormente inasprito divari e malesseri sociali.

Indicatori in tal senso sono emersi in **Tunisia**, dove le misure di contenimento adottate per fronteggiare la crisi sanitaria hanno colpito settori fondamentali, a partire dal turismo, contribuendo all'aumento della disoccupazione e alla contrazione dell'economia. Le difficoltà socio-economiche e il diffuso malcontento

hanno alimentato un'ondata di proteste su scala nazionale. Il Paese, inoltre, é rimasto esposto alla minaccia terroristica endogena legata all'attivismo di formazioni qaidiste e filo-DAESH che, seppur ridimensionate, hanno evidenziato persistenti capacità operative.

In **Algeria**, le ricadute delle misure di contenimento al Covid-19 si sono associate ad un processo di ridefinizione degli equilibri politici interni dopo le grandi mobilitazioni di piazza del 2019 e la fine dell'era Bouteflika, a fronte di una cornice securitaria rimasta stabile grazie all'efficacia di quel Comparto difesa e sicurezza, impegnato in costanti attività di monitoraggio e contrasto ai gruppi terroristici.

Altra realtà che sul piano economico ha risentito fortemente dell'emergenza Covid-19 è l'**Egitto**, che ha peraltro mantenuto un'allerta elevatissima nei confronti della minaccia terroristica e di un fronte jihadista particolarmente vitale, ove alla mai sopita operatività di cellule qaidiste ha continuato ad affiancarsi l'attivismo della branca filo-DAESH Wilayat-Sinai-WS. L'esigenza di rafforzare il controllo delle frontiere con Libia e Sudan, specie per prevenire il transito di foreign fighters, ha indotto Il Cairo ad inaugurare la base militare di Berenice, al confine con il Sudan.

Anche per i loro riflessi sul Nord Africa, hanno rivestito specifico interesse informativo le dinamiche della fascia subsahariana, segnatamente del Sahel e del Corno d'Africa, entrambi all'attenzione anche per il sequestro di nostri connazionali (Nicola Chiacchio, Padre Pierluigi Maccalli, Silvia Costanza Romano, Luca Tacchetto), tutti liberati nel 2020.

Proprio nella consapevolezza dell'importanza che la **regione del Sahel** riveste sotto il profilo securitario e quale hub di passaggio dei flussi di migranti clandestini verso la rotta del Mediterraneo centrale, l'Italia sta assumendo un ruolo più profilato, come dimostrano, tra l'altro, la nostra partecipazione al Gruppo Ristretto d'indirizzo politico della Coalizione per il Sahel, promossa dalla Francia, nell'ambito della quale a luglio è stata attivata, a sostegno delle Forze armate di Mali e Niger, la Task Force Takuba, nonché, sul piano bilaterale, la Missione di assistenza e supporto in Niger-MISIN e l'apertura di nuove Rappresentanze diplomatiche.

Accanto ad un accentuato e per certi versi inedito dinamismo politico, segnato dalla fase pre-elettorale in Burkina Faso e Niger e dalla transizione in Mali (vds. tavola n. 4), nel 2020 i Paesi saheliani hanno registrato un nuovo incremento della violenza. Si è trattato di eventi di diversa natura: etnico-tribale, anti-occidentale e, soprattutto, di matrice jihadista (più del 60% rispetto al 2019, con circa 4.300 vittime, secondo l'Armed Conflict Location and Event Data Project-ACLED). L'irrompere della pandemia ha poi, anche qui, alimentato tutte le preesistenti criticità sanitarie e sociali, favorendo pure l'azione di attori esterni interessati a guadagnare spazi d'influenza.

4

IL COLPO DI STATO IN MALI

Il 18 agosto un colpo di Stato di matrice militare e incruento nelle modalità ha portato in Mali alla rimozione dell'anziano Presidente Keita e allo scioglimento dell'Assemblea Nazionale e del Governo.

Le contestazioni alla Presidenza erano iniziate già all'indomani delle elezioni del 2018, per le condizioni economiche e sociali critiche, la dilagante corruzione, l'assenza dello Stato in talune regioni del Paese e per una cornice di sicurezza sempre più caratterizzata dalla recrudescenza della violenza interclanica e di matrice jihadista. Diversi schieramenti dell'opposizione avevano istituito un'alleanza (il Mouvement 5 Juin – Rassémblement Force Patriotique-M5-RFP) che si è resa protagonista di animate proteste, più volte sfociate in scontri con le forze dell'ordine e in temporanee paralisi delle istituzioni. Dopo vari tentativi di dialogo, risultati vani, con il golpe di agosto è stato istituito un Consiglio Nazionale per la Salvezza del Popolo, incaricato della gestione della transizione politica.

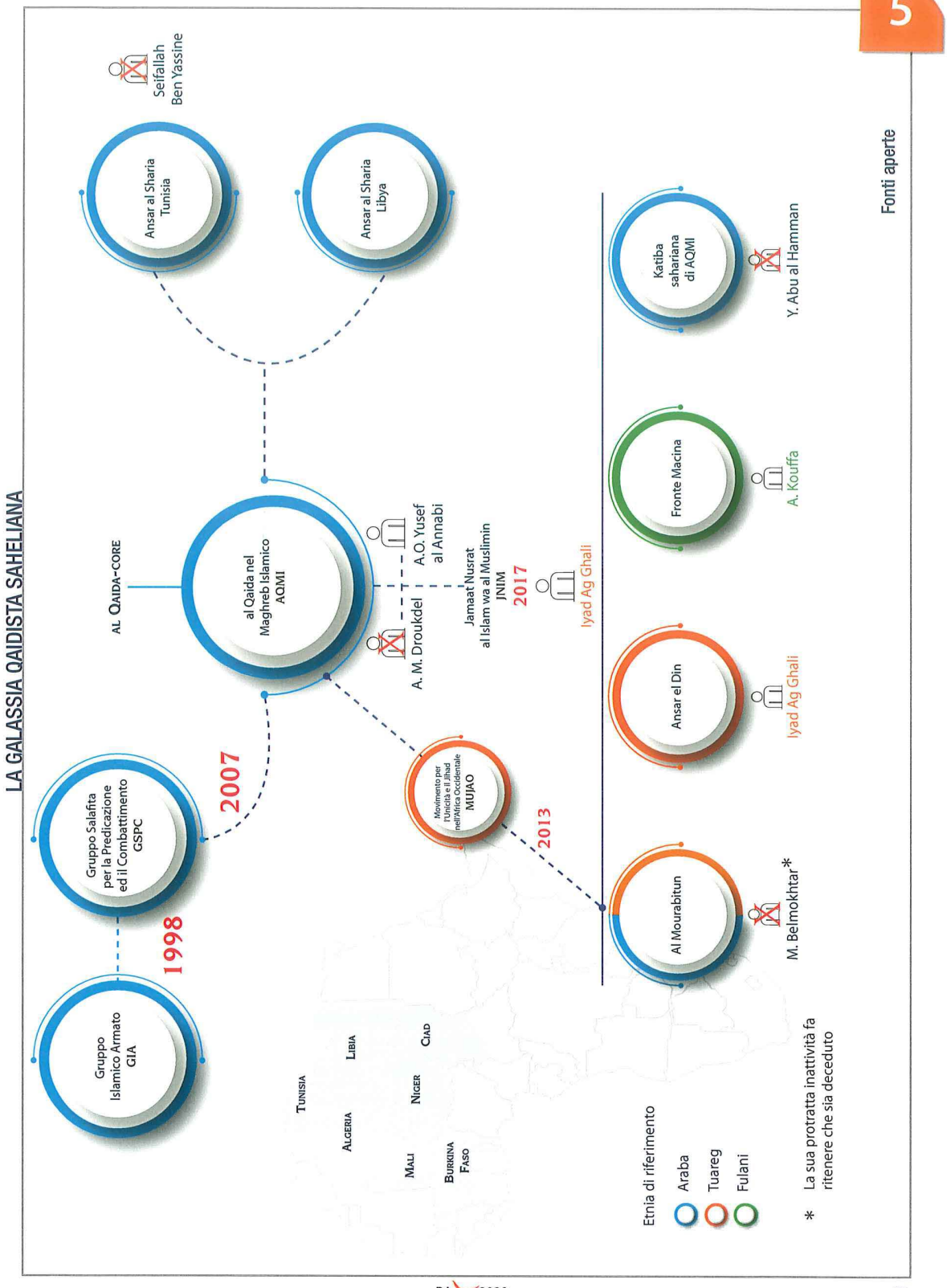
Nonostante i ripetuti appelli delle Nazioni Unite, della CEDEAO (la Comunità Economica degli Stati dell'Africa Occidentale, che ha imposto anche sanzioni, poi ritirate ad ottobre) e dell'Unione Africana, la giunta golpista si è mostrata determinata a portare avanti il proprio progetto, finalizzato alla ricostruzione di uno Stato coeso e al ripristino delle istituzioni e della legalità.

Sul terreno dell'attivismo terroristico, il principale elemento di novità emerso dal monitoraggio informativo riguarda il venir meno dell'"anomalia saheliana", che negli anni passati, in controtendenza rispetto agli altri teatri di jihad, aveva registrato sinergie logistico-operative tra formazioni terroristiche di stampo qaidista (in particolare il cartello Jamaa Nusrat al Islam wa al Muslimin-JNIM e la fazione "storica" della formazione nigeriana Boko Haram-BH) e quelle afferenti a DAESH (Islamic State in Greater Sahara-ISGS e Islamic State in West Africa Province-ISWAP). Il 2020 ha infatti osservato un'agguerrita competizione, sul piano sia ideologico-propagandistico che dell'espansionismo sul territorio, tra gruppi di diversa affiliazione, con accesi scontri specie nella regione triconfinaria tra Mali, Burkina Faso e Niger, nonché intorno al bacino del Lago Ciad. In quest'area, peraltro, l'attivismo jihadista è risultato ancora strettamente connesso alle conflittualità interetniche – alimentate dai cronici contrasti tra agricoltori stanziali e allevatori nomadi – tradottesi, fra l'altro, nelle ripetute violenze tra Fulani e Dogon e nella distruzione di interi villaggi (vds. tavola n. 5).

È questo il quadro che ha fatto da sfondo alle ricorrenti azioni terroristiche, anche ad alto impatto mediatico, contro postazioni di polizia, avamposti militari e obiettivi stranieri, anche dopo la neutralizzazione a giugno, in Mali, dell'emiro di al Qaida nel Maghreb Islamico-AQMI Abdelmalek Droukdel da parte delle Forze speciali francesi (vds. più avanti, capitolo terrorismo jihadista). Significativi, in **Niger**, l'attacco del 9 agosto contro 9 cooperanti di una OnG francese e 2 operatori locali e, in **Mali**, gli attentati condotti da JNIM e ISGS con modalità operative sofisticate nella regione triconfinaria del Liptako Gourma, snodo di passaggio di lucrosi traffici di esseri umani, armi, stupefacenti e minerali preziosi.

CRISI REGIONALI E PROIEZIONI DI INFLUENZA

5



Anche il **Burkina Faso** ha patito l'incremento di attacchi riconducibili a JNIM, segnatamente nelle regioni a Nord e Nord-Est, al confine con il Mali ed il Niger, a Sud tra Ghana e Costa d'Avorio e al confine con il Benin. Nel Paese sono risultate in aumento pure le azioni di matrice marcatamente settaria, specie in danno delle comunità cristiane del Nord, nonché le aggressioni armate contro i civili, le uccisioni mirate di capi villaggio, gli attacchi a installazioni minerarie e alle rotte di trasporto merci su strada, secondo un'articolata strategia jihadista intesa ad acuire le divisioni etniche e sociali nel Paese delegittimando le tradizionali autorità locali.

Spostando lo sguardo verso Est, il monitoraggio intelligence ha continuato ad appuntarsi sulla **Nigeria**, ove – segnatamente sulle regioni nord-orientali che si affacciano sull'area quadriconfinaria (con Camerun, Niger e Ciad) del Bacino del Lago Ciad – entrambe le fazioni (qaidista e filo-DAESH) di Boko Haram-BH hanno intensificato il proprio attivismo sia contro le locali Forze di sicurezza, sia contro la popolazione civile e i numerosi rifugiati stanziati in quelle aree. Più a Sud, indicatori critici sui livelli attuali e potenziali della violenza sono stati raccolti con riguardo al **Mozambico** e alla **Repubblica Democratica del Congo**.

Come negli ultimi anni, segnali di scadimento dei livelli di sicurezza sono stati colti anche nella regione del **Corno d'Africa**, dove il nostro Paese è impegnato in numerose attività di capacity building sia multilaterali che bilaterali. Il quadrante ha continuato a registrare fragilità istituzionali e vulnerabilità economiche, in un contesto influenzato dal pervasivo attivismo della formazione qaidista somala al Shabaab-AS – proiettata pure in realtà limitrofe, sopratutto in Kenya – oltre che della locale branca di DAESH. Si tratta di un quadrante sempre più al centro dell'attenzione di attori regionali ed internazionali, specie del Golfo e della Turchia, ma anche di Cina e Russia, attive, la prima, nel consolidamento di partnership commerciali in ambito finanziario ed infrastrutturale e, la seconda, nel settore energetico.

Particolare attenzione è stata rivolta alla **Somalia**, che ha visto slittare al 2021 le previste elezioni generali a causa della permanente contrapposizione tra Mogadiscio e Stati federati. Al riguardo, nonostante in estate sia stato registrato un rilancio dello strumento negoziale nella dialettica centro-periferia (cd. Processo di Dhusamareb) per individuare un accordo su tempi e modalità elettorali, il percorso di institution building del Paese non ha fatto registrare significativi avanzamenti. Si è mantenuto elevato il livello della minaccia terroristica riferibile ad al Shabaab. Al pari degli anni scorsi, la formazione si è infatti dimostrata in grado di organizzare e mettere a segno attentati particolarmente cruenti e con modalità complesse contro target ad alta visibilità (sedi e obiettivi istituzionali, infrastrutture strategiche, esercizi pubblici, interessi stranieri, omicidi mirati), quali l'azione condotta in prossimità della base turca di Mogadiscio (23 aprile) e l'attacco con presa di ostaggi all'Elite Hotel, sempre nella Capitale (16 agosto).

L'analisi intelligence ha poi guardato ai combattimenti che, dall'inizio di novembre, hanno visto contrapposte in **Etiopia**, in particolare nella regione nord del Tigray, le Forze federali di Addis Abeba e quelle del Tigray People Liberation Front-TPLF di Makallè. La caduta della Capitale tigrina in mano alle Forze governative (28 novembre) ha permesso l'istituzione di un'Amministrazione ad interim del Tigray. Il conflitto nell'Etiopia settentrionale ha contribuito a rinfocolare le tensioni interetniche di un Paese che, peraltro, ha mostrato di voler preservare il suo ruolo stabilizzatore in ambito regionale. Significativa, al riguardo, l'attenzione del Premier etiope su importanti dossier (contenzioso marittimo fra Kenya e Somalia e dialogo fra le Autorità della Somalia e del Somaliland), anche in relazione alla questione della Grand Ethiopian Renaissance Dam-GERD, la cui costruzione è terminata nel 2020 (vds. tavola n. 6).

6

LA GERD

La Grand Ethiopian Renaissance Dam riveste rilevanza strategica per l'Etiopia, che ambisce a divenire hub regionale per la produzione di energia elettrica ed entrare così nel novero delle principali potenze energetiche del Continente. Si tratta della più grande diga africana, i cui lavori sono iniziati nel 2011 e che assegna all'Etiopia un ruolo sempre più rilevante tra i Paesi cc.dd. upstream del Nilo. Il completamento dell'opera e la conclusione, lo scorso luglio, della prima fase di riempimento dell'invaso hanno acuito le tensioni tra Addis Abeba e Il Cairo.

Nel 2020, il contenzioso ha visto due tentativi di mediazione di alto profilo: il primo, a febbraio, sponsorizzato dagli USA e il secondo, sotto l'egida dell'Unione Africana. Tali tentativi hanno portato ad una serie di negoziati rimasti senza seguito, attesa la persistente distanza tra le parti. L'Etiopia sembra infatti disposta a trovare un compromesso solo sugli aspetti tecnici che potrà gestire direttamente e che non pregiudicheranno l'operatività complessiva del progetto, mentre l'Egitto, che identifica nelle risorse idriche del Nilo una questione di orgoglio e di sicurezza nazionale, continuerà a perseguire i propri interessi.

Nel contesto delle dinamiche incidenti nell'area del Mediterraneo, specifico interesse informativo ha rivestito l'accresciuta competizione tra diversi attori in merito soprattutto alla questione dello sfruttamento delle risorse energetiche off-shore nel **Bacino del Levante**, assurto a teatro di rivalità tra player rivieraschi ed extraregionali, tutti attivamente impegnati nel perseguimento dei propri interessi, tattici e strategici, in un'area che appare ormai ridefinita da logiche di agguerrito antagonismo. Il confronto, intrecciato alle storiche tensioni sull'Egeo e caratterizzato dalla pronunciata assertività dei diversi attori, è parso riflettere l'intenzione di ridisegnare spazi e linee di giurisdizione marittima. Si è evidenziato, in particolare, l'attivismo della Turchia, che ha contestato i criteri internazionali di ripartizione delle Zone Economiche Esclusive dell'area, anche alla luce del rinvenimento di importanti giacimenti gasiferi nelle acque di Egitto, Israele e Cipro. Tali sviluppi hanno di fatto stimolato l'elaborazione di progetti potenzialmente finalizzati anche all'esportazione dei prodotti energetici verso l'Unione Europea.

Nel medesimo contesto – e ad ulteriore attestazione della rilevanza strategica del dossier – si colloca la creazione, nel gennaio 2020, dell'East Mediterranean Gas Forum, organizzazione regionale (alla quale partecipano, oltre all'Italia, Cipro, Egitto, Grecia, Israele, Giordania e Autorità Nazionale Palestinese) intesa a promuovere la cooperazione nel settore del gas tra i Paesi che affacciano sul Mediterraneo Orientale.

Il Medio Oriente allargato

In continuità con gli anni precedenti, articolato impegno informativo è stato rivolto al quadrante mediorientale – area tradizionalmente influenzata da tensioni tra attori regionali e internazionali e da profonde instabilità intra-statuali – dove l'Italia è presente in missioni di stabilizzazione, formazione e addestramento.

Sul piano delle macro-dinamiche, l'apice del confronto tra Iran e Stati Uniti, concretizzatosi – come già richiamato nella precedente Relazione – nell'eliminazione in Iraq del Generale iraniano Soleimani (avvenuta agli inizi del 2020 per opera di un raid statunitense), ha significativamente influenzato, per i primi mesi dell'anno, gli sviluppi politici e securitari della regione. In tale scenario si è poi innestata la pandemia, che ha esacerbato vulnerabilità sociali e criticità politiche, ma ha anche contribuito a congelare le tensioni dell'area in quanto, a livello globale e regionale, le agende dei Governi hanno attribuito priorità al contenimento dell'emergenza sanitaria e alla gestione delle connesse ricadute economiche. Nel contempo, tuttavia, il contesto securitario è rimasto significativamente influenzato dalla minaccia espressa dai gruppi jihadisti, sia filo-DAESH che qaidisti, con elevate capacità operative soprattutto nel teatro siro-iracheno.

Altro evento che ha inciso in modo importante sugli assetti dell'area è stato quello della normalizzazione dei rapporti politici tra lo Stato di Israele e alcuni Paesi arabi del Medio Oriente e dell'Africa (Emirati Arabi Uniti e Bahrain a settembre, Sudan a ottobre e Marocco a dicembre) avvenuta con i cosiddetti Accordi di Abramo. Tale convergenza, suscettibile di rimodulare in maniera profonda e permanente i tradizionali equilibri regionali, ha potenzialmente aperto, infatti, ad una nuova fase della presenza dello Stato ebraico in Medio Oriente, una presenza finora caratterizzata dal confronto, seppur con gradi diversi di sfumature, con i vari attori del mondo arabo (come noto, solo Egitto e Giordania avevano riconosciuto Israele). Si tratta di sviluppi – fortemente sostenuti da Washington – che hanno profilato la realizzazione di un solido fronte regionale, trasversale e alleato, in chiave di contenimento dell'Iran, unendo Paesi avversari, ma aggregati da una comune percezione della minaccia di matrice sciita e da una condivisa ostilità nei confronti della Fratellanza Musulmana.

Su tale sfondo, gli Stati dell'area, alla costante attenzione dell'Intelligence, hanno mantenuto tutte le loro criticità interne. In **Siria**, sul piano militare, nell'area di Idlib sono proseguite le violazioni del cessate-il-fuoco tra le Forze di

Damasco e i ribelli, nonostante l'accordo siglato tra Russia e Turchia a marzo. A fronte di un sostanziale consolidamento delle posizioni del regime – che, grazie al supporto russo e iraniano, ha ripreso il controllo di gran parte del Paese – sono state significative le difficoltà affrontate dall'entourage damasceno: la diffusione della pandemia, l'inefficienza del sistema sanitario e l'entrata in vigore delle nuove sanzioni USA (Caesar Act) hanno infatti ulteriormente aggravato un quadro già segnato da 10 anni di conflitto e da endemica instabilità, andando a rivitalizzare talune forme di protesta popolare anche nelle zone controllate da Damasco. Si è assistito, inoltre, a rimodulazioni interne all'establishment, presentate all'opinione pubblica come frutto di una vasta campagna anti-corruzione, ma verosimilmente funzionali a rinsaldare la posizione del Presidente Assad in vista delle elezioni presidenziali (previste tra aprile e maggio 2021). Tali criticità hanno pesato sui lavori del Comitato Costituzionale Siriano – consesso delle Nazioni Unite che riunisce rappresentanti governativi, dell'opposizione e della società civile – i cui lavori hanno subìto un significativo stallo. È restata alta l'attenzione informativa anche sulle attività delle numerose sigle terroristiche attive in territorio siriano. Oltre ad una cospicua galassia di formazioni di matrice qaidista operative soprattutto nell'area di Idlib, si è mantenuta significativa la minaccia posta da DAESH, che ha operato come gruppo insorgente clandestino, attivo soprattutto nel Centro e nell'Est del Paese. Nel contesto, le evidenze raccolte hanno fatto stato di una pronunciata fluidità nei rapporti tra le diverse componenti, suscettibile di tradursi in alleanze inedite e convergenze operative.

L'Intelligence ha poi svolto un attento monitoraggio della complessa situazione in **Libano**, realtà di primario interesse informativo per la presenza del Contingente UNIFIL (United Nations Interim Force in Lebanon), sotto comando italiano, e della Missione Militare Bilaterale in Libano-MIBIL per la formazione del personale militare locale. Il Paese dei cedri, già duramente gravato dai riflessi del conflitto in Siria, ha affrontato un anno denso di criticità economico-finanziarie, sociali, securitarie e sanitarie. L'impasse governativa ha aggravato ultreriormente lo scenario interno. Il negoziato sui confini marittimi tra Tel Aviv e Beirut, iniziato a ottobre, è stato cristallizzato dopo circa un mese dal suo inizio a causa di divergenze tra le parti.

L'emergenza pandemica ha concorso ad aggravare, in **Giordania**, le difficoltà connesse alla gestione dei rifugiati (oltre 650mila quelli affluiti nel tempo a seguito della crisi siriana), in una realtà in cui la minaccia terroristica connessa alla radicalizzazione delle fasce giovanili è un tema alla costante evidenza di quelle Autorità.

Il monitoraggio informativo ha riguardato inoltre le complesse dinamiche **intra-palestinesi**, le cui due leadership (Autorità Nazionale Palestinese-ANP e Hamas), alle prese con la difficile gestione del Covid-19 e di fatto marginalizzate dalle normalizzazioni tra Israele e Paesi arabi, hanno avviato tentativi di ricom-

posizione della frattura e hanno inteso rilanciare il processo democratico per trasmettere un chiaro segnale di rinnovamento, credibilità e legittimità politica agli occhi dei Palestinesi e della Comunità Internazionale. A tal proposito, il Presidente dell'ANP, Mahmoud Abbas, ha annunciato nel gennaio 2021 le date delle elezioni politiche nei Territori Palestinesi (West Bank, Striscia di Gaza e Gerusalemme Est) per il rinnovo del Consiglio Legislativo Palestinese dell'ANP, di quelle presidenziali, nonché per il Consiglio Nazionale Palestinese, l'organo legislativo dell'OLP, rispettivamente calendarizzate per il 22 maggio, 31 luglio e 31 agosto 2021.

Elevata attenzione intelligence è stata rivolta all'**Iraq**, ove l'impegno italiano a favore della stabilità del Paese è testimoniato, tra l'altro, dalla presenza in loco di un cospicuo Contingente nazionale inquadrato nelle missioni internazionali della NATO e nella Coalizione anti-DAESH con compiti di supporto alle attività di controterrorismo e di addestramento delle locali Forze di sicurezza. La prima parte dell'anno è stata influenzata dalle tensioni interne connesse alla citata eliminazione del Generale Soleimani (evento nel quale è deceduto anche un elemento di Vertice delle locali milizie sciite), cui hanno fatto seguito l'attacco missilistico di Teheran contro alcune basi irachene dove erano presenti militari statunitensi, ripetuti lanci di razzi da parte delle stesse milizie locali contro gli assetti USA in quel Paese ed un acceso dibattito, nell'arena politica irachena, sull'opportunità di mantenere una così elevata presenza militare straniera entro i propri confini. Il quadro interno ha risentito anche delle proteste popolari, che hanno interessato specialmente la Capitale, e dell'incertezza istituzionale, superata solo a maggio con la formazione del nuovo Governo. La fase di maggiore stabilità si è accompagnata ad un crescente dinamismo di Baghdad sul piano internazionale – specie con l'avvio, nell'estate, del Dialogo Strategico con gli Stati Uniti – nel tentativo di trovare una posizione di equilibrio tra Washington e Teheran e di ridurre le ricadute interne di un confronto potenzialmente destabilizzante per il Paese. Tra le più insidiose ipoteche sotto il profilo securitario resta DAESH, che ha mostrato un sostenuto attivismo ed una crescita delle proprie capacità offensive, con cellule attive soprattutto nelle aree centrali e occidentali.

Complesso e articolato è il quadro emerso con riferimento all'**Iran**. Sotto il profilo interno, si è evidenziata la netta affermazione delle componenti conservatrici alle elezioni parlamentari di febbraio, tanto più rilevante in vista delle presidenziali in agenda per giugno 2021, alle quali Rohani non potrà ricandidarsi essendo al secondo mandato. A fronte di sporadiche forme di protesta contro l'establishment, l'opposizione e le spinte autonomiste sono risultate frammentate e non in grado di insidiare la stabilità del regime. Nel contempo, il Paese è parso in affanno per le difficoltà socio-economiche, acuite dalle sanzioni USA e dall'impatto della pandemia che, proprio nella Repubblica Islamica, ha mostrato particolare virulenza. Sul piano delle relazioni regionali e internazionali, Tehe-

ran, accusata soprattutto di sponsorizzare attività destabilizzanti nel quadrante, è stata interessata da dinamiche di teso confronto non solo con Washington, ma anche con Tel Aviv, subendo altresì l'isolamento diplomatico conseguente ai citati Accordi di Abramo. Anche in quest'ottica va letto il rafforzamento delle partnership con altri attori, quali Russia e Cina. Per quel che attiene al dossier nucleare, l'Iran ha disapplicato nel 2020 alcune clausole del Joint Comprehensive Plan of Action-JCPOA, continuando peraltro a permettere le ispezioni di monitoraggio dell'Agenzia Internazionale per l'Energia Atomica-AIEA. A fine anno, tuttavia, in risposta all'eliminazione in novembre del fisico Fakhrizadeh, figura di spicco del programma nucleare iraniano, il regime ha annunciato di voler avviare l'arricchimento dell'uranio al 20% e limitare le attività di verifica dell'Agenzia onusiana.

Quanto alle realtà sunnite del **Golfo**, le dinamiche regionali dell'anno in esame sono state dominate dalla richiamata normalizzazione dei rapporti diplomatici tra Israele, Emirati Arabi Uniti e Bahrain e dalle iniziative politiche volte a giungere ad una ricomposizione della frattura all'interno del Consiglio di Cooperazione del Golfo tra il Qatar e gli altri membri del consesso, tra tutti Arabia Saudita ed Emirati Arabi Uniti (avvenuta nei primi giorni del 2021). La necessità di rafforzare la cooperazione tra i Paesi dell'area è stata d'altronde motivata anche dall'esigenza di superare le comuni difficoltà economiche legate alla diffusione della pandemia e al connesso calo della domanda (e del già basso prezzo) di idrocarburi, che ha ridotto le rendite dei Paesi produttori. Sul versante securitario, nel corso del 2020 è stato registrato un sostanziale miglioramento del quadro generale, specie rispetto ai numerosi incidenti che l'anno prima, nel vivo del confronto con l'Iran, avevano coinvolto l'area dello Stretto di Hormuz. È verosimile che le iniziative di sicurezza marittima, come le missioni a guida statunitense (International Maritime Security Construct-IMSC) ed europea (European Maritime Awareness in the Strait of Hormuz-EMASoH), abbiano di fatto favorito un maggiore controllo sulle rotte navali nell'area riducendo il rischio di incidenti.

L'Intelligence ha continuato a monitorare anche la situazione in **Yemen**, dove sei anni di ininterrotta ostilità hanno provocato una delle più gravi crisi umanitarie al mondo, acuita dall'arrivo del Covid-19 (vds. tavola n. 7).

Costante focus informativo è stato dedicato alla situazione in **Afghanistan**, anche a supporto del Contingente italiano (circa 900 militari) operante nella missione NATO Resolute Support-RS, impegnato nel Train Advise Assist Command-West e nel quartier generale di RS a Kabul. Il Paese ha visto importanti avanzamenti sul piano negoziale, con la storica firma dell'accordo bilaterale tra Stati Uniti e Taliban (Doha, 29 febbraio), che ha definito i tempi del ritiro delle forze internazionali in cambio di garanzie, da parte insorgente, sul contrasto ai gruppi terroristici (AQ e DAESH in primis) e sull'avvio di colloqui intra-afghani. L'intesa, che nel 2020 ha portato al massiccio ritiro delle forze USA da quel teatro, ridotte dalle 13.000 unità di febbraio alle 4.500 di novembre, non ha ancora permesso

una effettiva pacificazione del Paese, il cui quadro securitario ha restituito segnali contrastanti. Da una parte, è diminuito il numero delle vittime civili per terrorismo (del 30% rispetto all'anno precedente: 5.939 quelle censite dalla UN Assistance Mission in Afghanistan nei primi 9 mesi del 2020, il numero più basso in

7

SVILUPPI DELLA CRISI IN YEMEN

A ormai sei anni dall'inizio di un conflitto cruento tra i ribelli Houthi (clan tribale sciita zaydita operante nel Nord del Paese, di cui il partito Ansarallah è espressione) e il Governo internazionalmente riconosciuto del Presidente Mansour Hadi, i tentativi di mediazione non hanno avuto esito positivo. Gli accordi di pace di Stoccolma del dicembre 2018 sono infatti rimasti in gran parte lettera morta e non ha retto neppure la tregua unilaterale della Coalizione militare a guida saudita, in vigore dal 9 aprile, che avrebbe dovuto consentire l'apertura di corridoi umanitari e agevolare il percorso verso una soluzione politica della crisi.

Nel Nord del Paese è continuata l'avanzata degli Houthi/Ansarallah verso le coste del Mar Rosso, mentre nelle province meridionali sono ripresi gli scontri tra le forze fedeli al Presidente e i secessionisti del Consiglio di Transizione del Sud (STC), sostenuti informalmente dagli Emirati Arabi Uniti, che hanno proclamato ad Aden l'Amministrazione autonoma delle regioni del Sud (25 aprile).

Per scongiurare una spaccatura all'interno del fronte anti-Houthi, nonché tra Abu Dhabi e Riyadh, quest'ultima ha esercitato forti pressioni su Hadi e sui gruppi separatisti per porre fine alle tensioni. Gli sforzi hanno portato all'intesa, annunciata il 10 dicembre, con cui Hadi ha acconsentito alla formazione di un nuovo Esecutivo composto da 24 ministri, inclusivo delle diverse componenti politiche yemenite, compresi elementi del STC, i cui membri sono peraltro scampati ad un attentato all'aeroporto di Aden il 30 dicembre.

Quanto alle iniziative sotto egida ONU, ha trovato applicazione l'intesa (Ginevra, 27 settembre) relativa al rilascio dei prigionieri, in virtù della quale nella metà di ottobre sono stati liberati più di 600 Houthi e 400 ostaggi filo-governativi, nonché due statunitensi catturati da Ansarallah ad ottobre. Il Palazzo di vetro ha inoltre proposto una bozza di accordo contemplante misure umanitarie, l'interruzione delle operazioni militari e l'impegno da parte Houthi a porre fine a ogni offensiva diretta contro il Regno saudita. Riyadh si è dichiarata pronta ad accettare l'intesa in cambio di alcune garanzie, tra cui la creazione di una "zona cuscinetto" ai propri confini. In tale contesto, è intervenuta, peraltro, la designazione degli Houthi e di Ansarallah a organizzazione terroristica straniera, annunciata dal Segretario di Stato USA il 10 gennaio 2021.

assoluto dal 2012). Dall'altra, sono proseguiti gli attacchi, anche ad alto impatto mediatico, riferibili alle componenti Taliban e all'Islamic State Khorasan Province, condotti spesso a danno delle minoranze – come le azioni a Kabul contro le comunità Hazara (6 marzo) e Sikh (25 marzo) – o in danno di obiettivi di specifico significato politico (come il reparto di maternità dell'ospedale di Kabul, assaltato il 12 maggio, o l'Università della Capitale, al cui interno, il 2 novembre, in pieno giorno, hanno fatto irruzione tre terroristi). Inoltre, sono aumentate le uccisioni mirate ai danni di membri governativi, Forze di sicurezza e leader tribali e religiosi, verosimilmente in connessione con le forti difficoltà che le Autorità di Kabul

incontrano nel processo di normalizzazione istituzionale, in un contesto che vede ormai i Taliban protagonisti anche politici di quel variegato campo etnico-tribale.

Hanno continuato ad incidere sul quadro afghano anche l'attivismo su quel territorio di formazioni tradizionalmente operanti nel Jammu e Kashmir (quali Jaish-e-Mohammad e Lashkar-e-Tayba) e la situazione di sicurezza del **Pakistan**, specie nelle aree tribali, dove si è registrato il persistente dinamismo di gruppi insorgenti. Sempre in suolo pakistano, sono parse altrettanto vitali le formazioni di matrice separatista, attive soprattutto nella provincia del Baluchistan, ove più marcate risultano le contaminazioni con frange d'ispirazione islamista.

La Russia e lo spazio post-sovietico

Nella prospettiva analitica dell'Intelligence, la **Russia,** nel 2020, si è misurata con importanti dossier di politica interna ed economica, ma anche relativi a crisi, emergenti o rivitalizzate, in diversi quadranti dello spazio post-sovietico (vds. tavola n. 8).

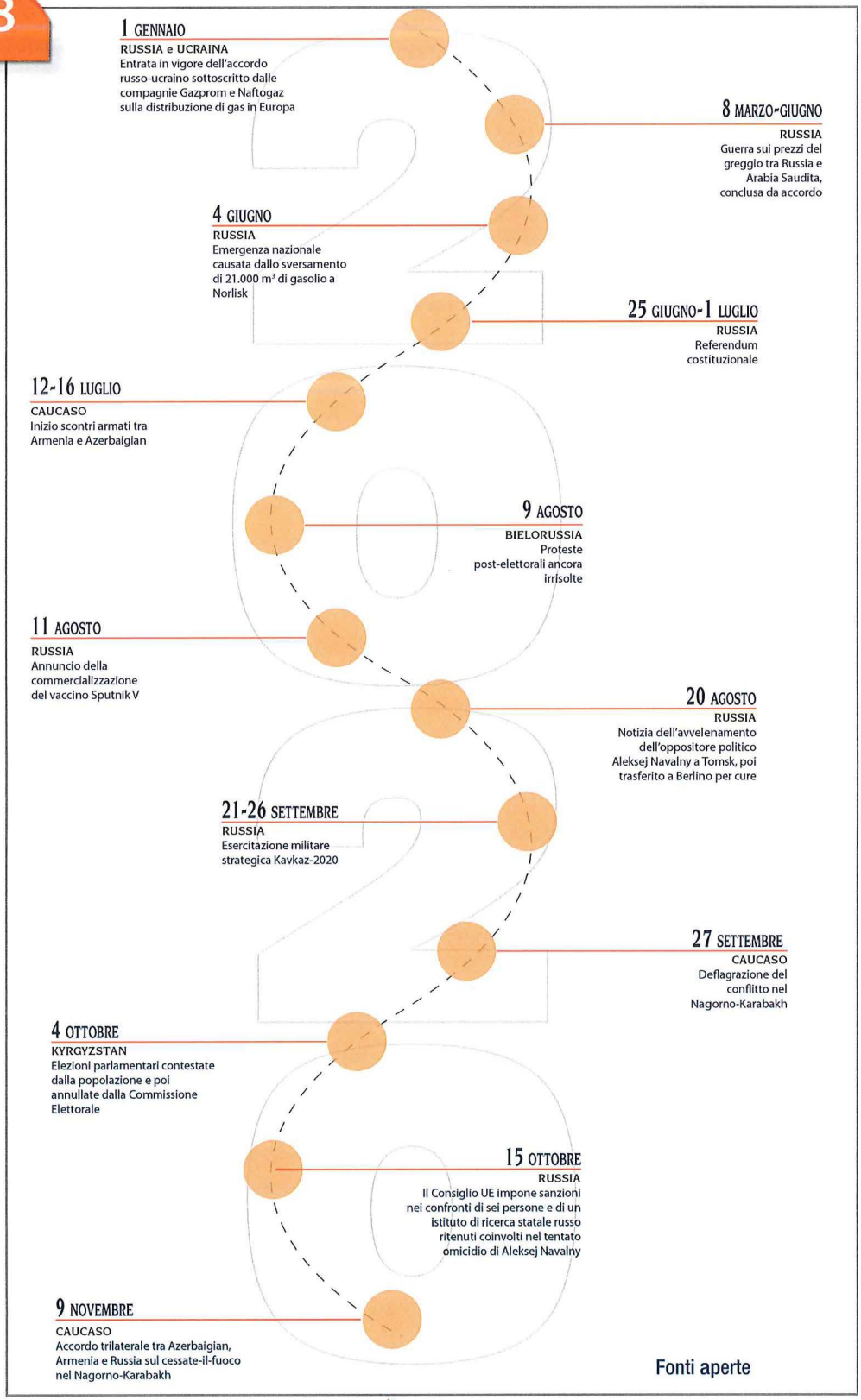
Sul piano interno, un passaggio di particolare rilevanza è stato rappresentato dalla riforma costituzionale, annunciata dal Presidente Putin il 15 gennaio e conclusasi con il referendum del 1° luglio.

Al contempo, il Paese ha dovuto confrontarsi con il severo impatto della pandemia, che ha richiesto considerevoli misure economiche a sostegno della popolazione, tali da determinare, per la prima volta dal 2014, una riduzione nei prossimi tre anni delle spese per la difesa. Per altro verso, Mosca ha rafforzato la cooperazione bilaterale nel settore sanitario con numerosi Paesi, inclusi quelli dell'area del MENA.

Agli effetti della pandemia sono connessi, inoltre, gli accordi raggiunti (in aprile e in giugno) in seno all'OPEC+ sul taglio della produzione di petrolio (poi lievemente ridimensionato nell'intesa raggiunta a dicembre), che ha messo fine alla guerra dei prezzi allo scopo di risollevare i mercati dopo il crollo della domanda. Russia e Arabia Saudita sono risultati i Paesi impegnati in più significativi tagli di produzione, con i connessi costi, ma al contempo, in quanto principali fornitori internazionali, ne sono stati anche i principali beneficiari, sia per l'effettiva stabilizzazione dei prezzi sia per il successo d'immagine, avendo potuto dimostrare ai mercati di essere in grado di cooperare efficacemente in congiunture particolarmente negative.

Sul versante geostrategico, è intervenuta la produzione di importanti linee di policy relative all'Artico (vds. tavola n. 9) valse a ribadire la valenza prioritaria ad esso assegnata dal Cremlino, specie in ottica di rilancio produttivo infrastrutturale. Pur determinata a riaffermare la leadership regionale e a difendere la propria agenda economica, Mosca – che dal maggio 2021 sarà Presidente di turno del Consiglio Artico, ove l'Italia siede come Paese osservatore – si è mostrata propensa ad innescare, tra i Paesi rivieraschi, dinamiche di positiva interazione per

8 2020: CRONOLOGIA DEI PRINCIPALI AVVENIMENTI NELLO SPAZIO POST-SOVIETICO



9

LA PROIEZIONE RUSSA NELL'ARTICO

L'interesse russo verso la regione artica si è tradotto, in marzo e ottobre, nell'approvazione dei "Principi fondamentali della politica statale nell'Artico fino al 2035" e della "Strategia per lo sviluppo della regione artica russa e per la protezione della sicurezza nazionale fino al 2035", dai quali emergono:

- l'eccezionale rilevanza che l'Artico riveste per l'economia del Paese. All'area è riconducibile il 10% circa del PIL russo e il 20% dell'export. Di qui, la determinazione di Mosca a promuovere una profonda e complessiva modernizzazione di tutte le maggiori infrastrutture critiche presenti nella regione (ferrovie, strade e vie d'acqua, sistemi portuali ed apparato militare);
- la gravità delle sfide interne, dai paventati mutamenti del "permafrost" (suolo perennemente ghiacciato, che in conseguenza del riscaldamento globale potrebbe liberare grandi quantità di metano e anidride carbonica, dunque gas serra) alla continua riduzione della popolazione (oggi vicina ai 2 milioni e mezzo di abitanti, con un'emorragia annua stimata in 15-20.000 unità), dovuta allo scadimento del livello dei servizi pubblici ed al peggioramento delle condizioni di vita;
- l'importanza, per Mosca, di esercitare un fattivo controllo dei 5.500 km circa lungo cui si sviluppa (dallo Stretto di Bering al Mar di Kara) la cd. Northern Sea Route-NSR, candidata a imporsi nei prossimi decenni come una delle principali arterie mondiali per il traffico commerciale tra il Pacifico e l'Europa Occidentale. Per tenere aperta e vigilare sulla NSR, considerata dal Cremlino una "via d'acqua interna", Mosca dispone della più cospicua flotta di rompighiaccio al mondo (oltre 40 navi di classe variabile, alcune delle quali armate con sistemi missilistici avanzati) e fissa l'obiettivo di vararne da qui al 2035 altre 8 (di cui 5 a propulsione nucleare) per assicurare, nei prossimi 15 anni, la quadruplicazione del volume dei trasporti commerciali lungo la Route, attestato oggi a circa 30 milioni di tonnellate annue. Per raggiungere tale scopo potrebbe risultare fondamentale l'interesse sviluppato da Pechino, che collega la NSR alla Belt and Road Initiative, attraverso la "Polar Silk Road", o Via della Seta Artica, che da parte cinese si vorrebbe utilizzare, in prospettiva, quale via di approvvigionamento alternativa a quella meridionale dello Stretto di Malacca.

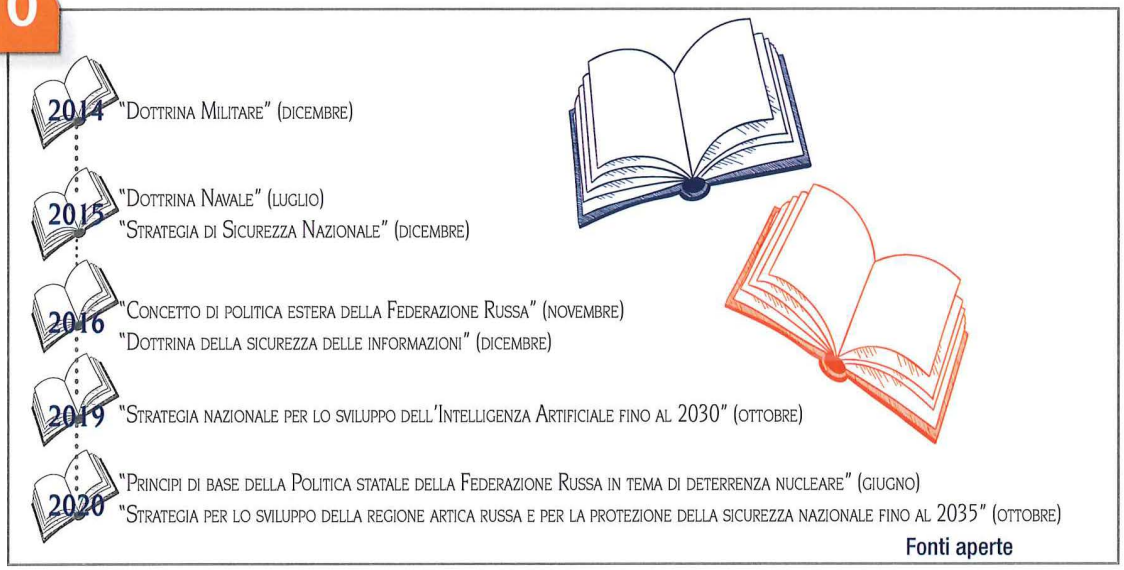
proteggere il fragile eco-ambiente artico, aprendo un dialogo sulla promozione di modelli di sviluppo sostenibile.

Sul piano securitario, il rilievo attribuito da Mosca, anche sotto il profilo simbolico-dimostrativo, al grado di efficienza, modernizzazione e prontezza operativa delle proprie Forze Armate ha trovato espressione nello svolgimento, in settembre, dell'esercitazione multinazionale di livello strategico "Kavkaz-2020", nella quale sono state impegnate unità militari russe e reparti provenienti da Armenia, Bielorussia, Cina, Myanmar e Pakistan, sulla scia degli analoghi eventi ciclicamente proposti da oltre un decennio, aperti ai membri dell'Organizzazione per la Cooperazione di Shanghai-SCO (importante asset nel rapporto con la Cina) e ad alcuni partner regionali.

Sul versante della deterrenza nucleare, il Cremlino ha reso pubblici, in giugno, i principi ai quali Mosca intende ispirare la propria azione in tema di difesa globale. La sortita si pone a sviluppo di un'evoluzione dottrinaria sulle strategie di difesa e sicurezza in corso dal 2014 (vds. tavola n. 10).

Articolato e complesso si è confermato il dialogo con i Paesi occidentali, anche alla luce del tentato omicidio con avvelenamento, in agosto, dell'oppositore politico Aleksej Navalny, a seguito del quale il Consiglio UE, in ottobre, ha impo-

10 **EVOLUZIONI DOTTRINARIE RUSSE SULLE STRATEGIE DI DIFESA E SICUREZZA**



sto sanzioni mirate nel quadro delle misure restrittive contro la proliferazione e l'uso delle armi chimiche.

Nello **spazio post-sovietico**, lo scoppio del conflitto del Nagorno-Karabakh e una rapida successione di movimenti di protesta hanno impegnato il Cremlino proprio in quei Paesi (Armenia, Bielorussia, Kyrgyzstan) che – unitamente al Kazakhstan – sono stati eretti a perni della politica russa di integrazione nello spazio eurasiatico.

Nella porzione più occidentale del quadrante, ove la crisi nella regione ucraina del Donbass non ha fatto registrare significativi progressi nel processo di pace, gli sviluppi più rilevanti hanno riguardato la **Bielorussia**, dove il regime si è dovuto confrontare con le proteste sorte dalla contestazione delle elezioni presidenziali di agosto (vds. tavola n. 11).

Sul fronte caucasico, l'attenzione del Comparto si è rivolta al riaccendersi delle tensioni tra **Armenia** e **Azerbaigian**, dapprima negli scontri di luglio al confine settentrionale tra i due Paesi, poi con la guerra per il controllo del **Nagorno–Karabakh** (vds. tavola n. 12), il più risalente "frozen conflict" dello spazio post-sovietico, che dalla fine degli anni '80 vede opposti i due Paesi. L'Azerbaigian, sostenuto dalla Turchia, è uscito vincitore dal conflitto, riconquistando militarmente l'antica città di Shusha (da cui originano gran parte degli sfollati azeri) e i sette distretti occupati intorno al Nagorno-Karabakh. Sul piano geopolitico, la Federazione Russa rimane legata all'Armenia (ove la sconfitta ha, tra l'altro, inaugurato una stagione di forti proteste anti-governative) da una solida alleanza militare, sancita dalla comune appartenenza all'Organizzazione del Trattato di Sicurezza Collettiva e dalla presenza in territorio armeno dell'unica struttura

11

GLI SVILUPPI IN BIELORUSSIA

La riconferma, con oltre l'80% dei voti, di Aleksandr Lukashenko (Capo di Stato dal 1994) alla Presidenza della Bielorussia nelle elezioni del 9 agosto ha innescato proteste popolari senza precedenti, che hanno coinvolto larghe componenti del Paese, anche nelle zone rurali, compresi dipendenti di aziende statali e giornalisti della radio e della TV di Stato.

Il fronte del dissenso – raccolto intorno alla principale candidata dell'opposizione Svetlana Tikhanovskaya, riparata all'estero per sfuggire alle minacce degli apparati statali – ha peraltro mostrato difficoltà a mantenere, nel corso dei mesi, lo slancio iniziale, scontando, verosimilmente, l'assenza in loco di un leader carismatico, nonché la pressione delle intimidazioni e degli arresti di manifestanti e giornalisti.

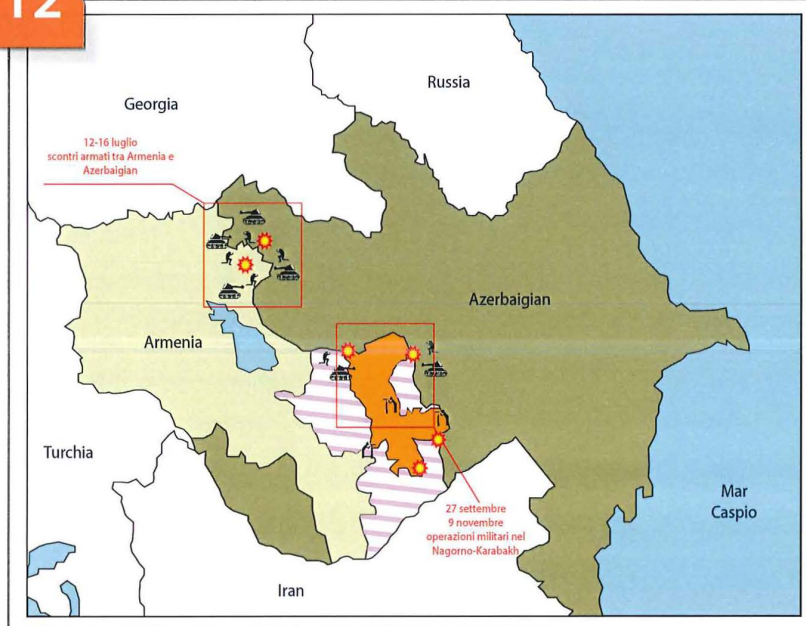
Le proteste bielorusse non possono inquadrarsi nel solco delle cc.dd. "rivoluzioni colorate", di segno filo-occidentale, prodottesi negli ultimi anni nello spazio post-sovietico, caratterizzandosi per una dimensione spiccatamente interna, focalizzata sui temi dell'autoritarismo e delle difficoltà economiche, mentre la questione di un possibile riposizionamento del Paese (alleato collaborativo del Cremlino, sia a livello bilaterale che nell'ambito dell' Organizzazione del Trattato di Sicurezza Collettiva-OTSC e dell'Unione Economica Eurasiatica-UEE) non è mai emersa tra le richieste dei manifestanti.

militare controllata da Mosca nel sud del Caucaso. La mediazione tripartita tra Erevan, Baku e Mosca, che ha portato al cessate-il-fuoco del 10 novembre, è stata condotta dal Cremlino, che ha anche ottenuto il dispiegamento di quasi 2.000 peacekeepers per il monitoraggio post-accordo nell'area.

Nel quadrante centrasiatico, la crisi sanitaria si è accompagnata alle gravi ricadute economiche correlate al crollo del mercato degli idrocarburi e dei flussi di rimesse dall'estero, che rappresentano oltre un quarto del PIL di Tagikistan e **Kyrgyzstan**. Quest'ultimo Paese – attraversato da endemiche divisioni interetniche e interclaniche – ha fatto registrare violente manifestazioni di protesta contro gli esiti delle elezioni parlamentari di ottobre, annullate per presunti brogli, ed avvicendamenti al vertice di governo, con l'ascesa dell'ex leader dell'opposizione.

12

CONFRONTO TRA ARMENIA E AZERBAIGIAN



Cronologia della crisi

21 maggio:
giuramento del nuovo Presidente del NK e proposta di riunificazione con l'Armenia del Primo Ministro Harutyunyan.

12-16 luglio:
scontri armati tra Armenia e Azerbaigian al confine nord tra i due Paesi.

29 luglio-10 agosto:
esercitazione militare tra Forze Armate turche e azere in Azerbaigian.

19 settembre:
i Vertici del NK annunciano la decisione di spostare la capitale da Stepanakert a Susha nel 2022.

27 settembre:
inizio dell'attacco azero contro le truppe armene in diversi punti strategici lungo la linea del fronte nagorino.

27 settembre-9 novembre:
conflitto del Nagorno-Karabakh.

9 novembre:
accordo trilaterale per il cessate-il-fuoco tra Russia, Azerbaigian e Armenia. Dispiegamento di 1.960 peacekeepers russi. Ruolo di monitoraggio del cessate-il-fuoco per la Turchia.

Fonti aperte

La Cina

Postura e proiezioni della **Cina** sulla scena globale hanno continuato a rappresentare ambito rilevante di impegno per l'Intelligence. Se agli inizi del 2020 l'emergenza sanitaria da Coronavirus veniva qualificata, da taluni osservatori, come un "momento Chernobyl" in grado di minare la credibilità del gigante asiatico, le iniziative articolate messe in campo da Pechino ne hanno in realtà evidenziato la determinazione a gestire la fase trasformando in opportunità alcuni fattori di rischio direttamente correlati alla pandemia. A livello domestico, Pechino ha infatti implementato un più stringente sistema di controllo sociale, mentre all'estero ha potenziato la collaborazione internazionale anche in ambito sanitario.

In quest'ottica si pone l'azione delle Autorità cinesi nei confronti delle proprie periferie, a partire da Hong Kong (vds. tavola n. 13), nonchè dei Paesi confinanti con cui sussistono annose dispute territoriali, in primis l'India. Ciò, in linea con un'agenda che persegue su tutto interessi nazionali considerati non negoziabili: integrità territoriale, sovranità, sicurezza, stabilità politica ed economica, nonché salvaguardia del diritto del Partito Comunista a governare. Nella medesima cornice si inseriscono i provvedimenti varati sul fronte interno, quali quelli sullo sviluppo delle regioni occidentali del Paese e sulla promozione della domanda interna.

13

LE VICENDE DI HONG KONG

La Cina ha da tempo fissato quale priorità la "normalizzazione" delle sue province più problematiche, quali il Tibet, lo Xinjiang e, in maniera più evidente a partire dal cd. "Movimento degli ombrelli" del 2014, Hong Kong.

Nel maggio 2020 il Governo cinese ha introdotto la "Legge sulla Sicurezza Nazionale", che ha modificato la normativa fondamentale della Regione Amministrativa Speciale di Hong Kong, con l'intento dichiarato di prevenire e punire quelli che ritiene essere atti di sovversione, secessione, terrorismo, furto di segreti di Stato ed interferenze da parte di entità straniere.

I moti di protesta fino ad allora inscenati dalla popolazione hongkongina, specie dalle fasce più giovani, si sono presto ridotti drasticamente, anche a seguito dell'arresto (o della fuga all'estero) di molti leader delle manifestazioni. Ancora una volta il Partito Comunista Cinese si è dimostrato disposto a pagare un prezzo elevato pur di eliminare ogni percepita minaccia interna alla propria legittimità a governare. I costi della stretta operata sull'ex colonia britannica sono stati, infatti, molteplici, ingenti e dalle implicazioni di lungo periodo.

Sul piano economico e dell'immagine internazionale, in molti hanno percepito la vicenda come la fine dello status speciale di Hong Kong in termini di diritti civili e di rule of law, rendendo più difficile attrarre investimenti e capitale umano.

Sul piano politico, l'erosione del modello "un Paese, due sistemi", che era stato a suo tempo presentato quale chiave per il ricongiungimento alla madrepatria dell'ex colonia entro il 2047, appare destinato a rendere più complessa la riunificazione pacifica con Taiwan.

Per quanto riguarda la proiezione internazionale, Pechino ha giocato sui terreni del dinamismo diplomatico, degli investimenti infrastrutturali (sia pure, come già rilevato nella Relazione 2019, con un approccio più selettivo nel finanziamento dei progetti della Belt and Road Initiative) e del commercio (come testimoniato dalla Regional Comprehensive Economic Partnership siglata a novembre dalla Cina e da altri 14 Paesi dell'Asia-Pacifico).

Il 2020 si è caratterizzato, inoltre, per il confronto con gli Stati Uniti, che l'emergenza pandemica ha concorso a spiralizzare, innestandosi peraltro in un contesto che vede Pechino da tempo accusata di condotte scorrette sul piano commerciale, specie nel settore high tech, e di violazione dei diritti umani nei confronti della popolazione musulmana nello Xinjiang. Si tratta di questioni alla costante evidenza anche in ambito UE, ove il "dossier Cina" ha formato oggetto di vivace dibattito, pure in vista del Comprehensive Agreement on Investment-CAI siglato a fine dicembre.

Nel contempo, a testimonianza di quanto articolata sia la strategia d'espansione della Cina, sono intervenute talune significative progressioni nel campo dello Spazio, sempre più considerato da Pechino come un "domain" strategico di primaria importanza (vds. tavola n. 14).

Altrettanto emblematica dell'ampiezza del raggio d'azione di Pechino è la sua crescente proiezione nel continente latino-americano (vds. tavola n. 15) che si aggiunge alle numerose iniziative indirizzate all'Africa, al Medio Oriente e ai Balcani.

14

LE POLITICHE SPAZIALI CINESI

Pechino ha investito con continuità nello sviluppo dei programmi spaziali e delle relative tecnologie, conseguendo importanti successi sia nel settore civile, con lo sviluppo e la promozione del sistema di posizionamento satellitare Beidou, sia in quello militare mediante, ad esempio, la formulazione di un framework concettuale per le operazioni e la creazione di una componente dedicata, costituita dalla "Forza di Supporto Strategico", posta alle dipendenze dell'Esercito Popolare di Liberazione.

In meno di due decenni, la Cina è passata dal lancio di un vettore missilistico con un astronauta alla pianificazione, per il 2021, della prima messa in orbita di una stazione spaziale permanente. Nel solo 2020, Pechino ha lanciato:

- una missione esplorativa su Marte (Tianwen-1), destinata a permettere, entro l'estate del 2021, l'atterraggio sul "pianeta rosso" di un veicolo mobile per la raccolta di elementi conoscitivi sulla struttura geologica del pianeta e sulla composizione della sua atmosfera;
- una missione lunare (Chang'e-5), che ha raccolto frammenti rocciosi da un'area della Luna geologicamente più giovane rispetto a quelle studiate fin qui;
- il primo satellite sperimentale per il 6G, Tianyan-5, volto a testare lo spettro elettromagnetico dei Terahertz per la trasmissione dei dati.

La Cina ha inoltre pianificato un incremento del processo di esplorazione del sistema solare, con l'obiettivo di raggiungere Giove entro il 2029, traguardo che ne farebbe una potenza spaziale d'avanguardia.

15

L'AZIONE CINESE IN AMERICA LATINA

Negli ultimi due decenni la Cina è diventata un partner economico e politico di primaria importanza per il continente latino-americano. Gli obiettivi cinesi nella regione sono anzitutto economici: l'approvvigionamento di risorse minerarie, energetiche ed alimentari, l'inserimento nei sistemi bancari locali e l'accesso a un vasto mercato di sbocco per il proprio surplus produttivo in beni industriali e di consumo. Secondo il Congressional Research Service statunitense, nel 2002 l'interscambio dell'America Latina con la Cina era pari a 17 miliardi di dollari, mentre nel 2019 aveva raggiunto i 315 miliardi, superando gli USA, fermi a 270 miliardi. Parallelamente, anche gli investimenti cinesi sono cresciuti: i dati del China Global Investment Tracker dell'American Enterprise Institute mostrano come, dal 2005 ad oggi, essi ammontino a quasi 200 miliardi di dollari, 100 dei quali in progetti energetici e 36 nel settore minerario, con il Brasile quale destinatario principale. Due banche cinesi (la China Development Bank e la China Export-Import Bank) sono divenute le prime fonti di prestiti per il Continente, ancorché, negli ultimi tre anni, su livelli di capitale fortemente contratti.

Anche sul piano politico, Pechino ha ottenuto importanti risultati, tra i quali il rinnovo, in agosto, dell'accordo con cui l'Argentina ha conferito alla China Satellite Launch and Tracking Control General il controllo per 50 anni della stazione satellitare di Neuquen, in Patagonia, e le decisioni (nel 2017-2018) di Panama, Repubblica Dominicana ed El Salvador di interrompere i rapporti diplomatici con Taiwan e di riconoscere la Repubblica Popolare Cinese.

Tali successi sono anche l'esito degli sforzi diplomatici espressi in ambito multilaterale. Pechino ha organizzato due summit, nel 2015 e nel 2018, con la Community of Latin American and Caribbean States (CELAC), l'unica organizzazione continentale a non comprendere gli Stati Uniti. I summit sono stati utilizzati per convincere i Governi della regione a far parte della Belt and Road Initiative (BRI) e dell'Asian Infrastructure Investment Bank (AIIB), riscuotendo l'adesione di 19 Paesi alla BRI e di 5 alla AIIB.

MINACCE ALL'ECONOMIA NAZIONALE

in breve

- Pandemia come amplificatore di vulnerabilità e rischi
- A fronte dell'aggressività di competitor esteri, azione intelligence a tutela degli assetti strategici, anche a supporto dell'esercizio del Golden Power
- Focus informativo prioritario su filiera sanitaria, nonché sui settori aerospazio, difesa e sicurezza,TLC, logistica portuale e manifatturiero d'eccellenza
- Monitoraggio dinamiche del settore finanziario
- Sicurezza energetica e sfida della decarbonizzazione

L'emergenza pandemica ha colpito pesantemente i bilanci di tutti i Paesi, sia pure con intensità diversa, condizionandone le politiche economiche. Stime dell'OCSE indicano che nel 2020 il prodotto mondiale si è contratto di oltre il 4%, la recessione più profonda dalla fine della seconda guerra mondiale. Le conseguenze sugli scambi internazionali sono state dirompenti, soprattutto nel secondo trimestre dell'anno, quando si è registrata una contrazione del 45% su base annua.

A livello europeo, di fronte alle conseguenze economiche dell'emergenza sanitaria, le reazioni dei Governi nazionali e della Banca Centrale Europea-BCE sono state rapide e di eccezionale entità, come mai nella storia. Sul fronte monetario, la BCE, per contrastare le tensioni sui mercati finanziari e sostenere l'erogazione dei prestiti alle famiglie e alle imprese, è intervenuta con tagli dei tassi di interesse, acquisti di titoli pubblici e privati (Pandemic Emergency Purchase Programme, PEPP) e misure a sostegno del credito attraverso abbondante liquidità. Le istituzioni europee hanno velocemente reso più flessibili le regole sugli aiuti di Stato e attivato la clausola di salvaguardia generale del Patto di stabilità e crescita. Inoltre, il raggiungimento dell'accordo in Consiglio europeo sul piano Next Generation EU ha permesso di delineare una storica strategia comune di uscita dalla crisi per gli anni a venire, con lo stanziamento di ingenti risorse da investire, in particolare, in settori ritenuti strategici nel medio e lungo periodo.

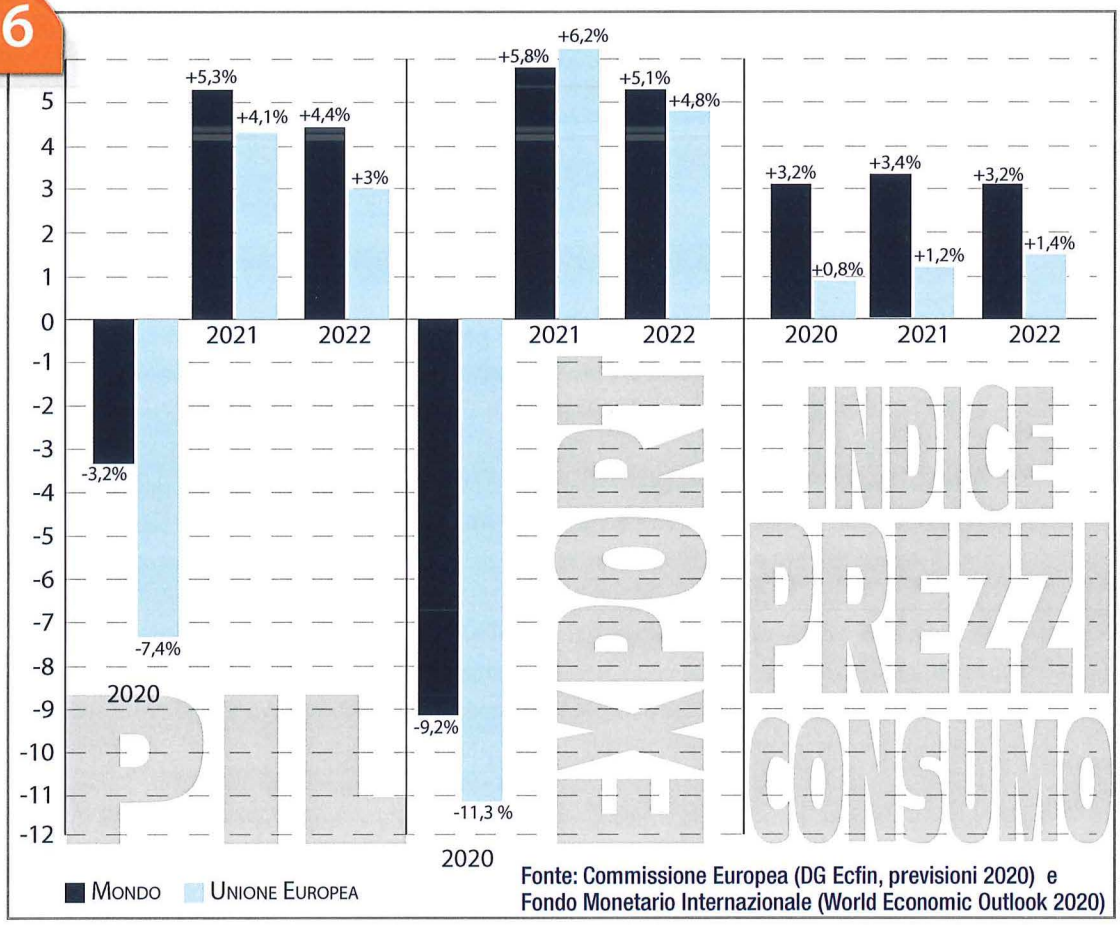
Nel contempo, quanto alle politiche di bilancio dei singoli Stati, sono stati disposti aumenti di spesa, riduzioni del prelievo fiscale e ampi trasferimenti pubblici.

L'insieme di questi provvedimenti ha consentito, fin da subito, di contenere l'impatto della crisi. Ciononostante, l'incertezza per il futuro, i vincoli alla mobilità e la diminuzione dei redditi hanno compresso in maniera sostanziale i consumi interni, portando, parallelamente, ad un aumento della propensione al risparmio delle famiglie.

La situazione ha assunto una fisionomia critica per quanto riguarda i servizi, soprattutto in quei settori più esposti agli effetti della pandemia, quali il commercio al dettaglio, i trasporti, il turismo e la ristorazione. Nel complesso, come evidenziato dalle previsioni in ambito UE, un completo recupero dei livelli di PIL pre-crisi avverrà non prima della seconda metà del 2023 (vds. tavola n. 16).

16

CRISI PANDEMICA - INDICATORI MACROECONOMICI



Fonte: Commissione Europea (DG Ecfin, previsioni 2020) e Fondo Monetario Internazionale (World Economic Outlook 2020)

La tutela degli assetti strategici

I profondi e inattesi sconvolgimenti dell'economia globale del 2020 hanno costituito un catalizzatore del rischio per il Sistema Paese. Le realtà produttive nazionali si sono dovute misurare con la contrazione non solo della domanda interna, ma anche di quella estera e con le conseguenti difficoltà di carattere finanziario, che sono andate a sommarsi alle sfide epocali derivanti dal rapido mutamento tecnologico e dalla crescente concorrenza internazionale.

In questo senso, la crisi sanitaria ha messo in luce in modo ancora più marcato la postura aggressiva di attori esteri, determinati a conseguire posizioni di leadership commerciale e tecnologica in aderenza ad obiettivi ed indirizzi di carattere geopolitico.

Tali sviluppi sono andati profilando un aumento del rischio di azioni di tipo predatorio/speculativo in direzione degli assetti proprietari di imprese che, pur dotate di un patrimonio di know how produttivo e di un portafoglio clienti significativo, hanno conosciuto una prolungata fase di difficoltà connessa alle conseguenze economiche della pandemia. Una vulnerabilità tanto più pronunciata per le aziende di piccole e medie dimensioni, anche con riguardo alla loro capacità di proiezione sui mercati esteri, in presenza, oltretutto, di player stranieri non sempre vincolati a condizioni di leale concorrenza.

La congiuntura ha quindi reso più concreto il pericolo che attori esteri, favoriti anche dall'accesso a forme di finanziamento con finalità extraeconomiche, si ponessero quali acquirenti di asset pregiati in Italia, con prospettive di spostamento dei centri decisionali e produttivi al di fuori dei nostri confini e/o di perdita di know how, a detrimento della competitività del tessuto economico nazionale.

In questo contesto – ove lo screening in ottica securitaria vale a dilatare gli spazi per investimenti "sani", portatori di sviluppo e occupazione – il Comparto ha intensificato l'azione di ricerca e d'analisi a supporto del decisore politico, anche ai fini dell'esercizio dei poteri speciali (cd. Golden Power) e dell'implementazione della normativa di riferimento, il cui ambito di applicazione è stato ulteriormente esteso, nel 2020, proprio per garantire una maggiore protezione dell'economia nazionale (vds. tavola n. 17).

17

IL GOLDEN POWER NEL 2020

L'esigenza di assicurare ogni possibile tutela agli assetti strategici nazionali ha indotto il Governo a operare, dopo gli aggiornamenti del 2019, nuovi, mirati interventi normativi intesi a rafforzare il dispositivo.

Sul piano legislativo, il riferimento è alle modifiche al D.L. n. 21/2012 introdotte dagli artt. 15 e 16 del D.L. 8 aprile 2020, n. 23 – convertito, con modificazioni, dalla Legge 5 giugno 2020, n. 40 (cd. Decreto "Liquidità") – che hanno ampliato gli strumenti a disposizione del decisore politico per contrastare il rischio di acquisizioni predatorie od opportunistiche di aziende e di asset strategici per il Paese da parte di investitori esteri. Tra le principali novità apportate dal decreto si segnala, in particolare, l'introduzione di un regime temporaneo, che ha esteso (inizialmente fino al 31 dicembre 2020, poi fino al 30 giugno 2021) l'ambito di applicazione della disciplina Golden Power rispetto al regime ordinario (ad es. sottoponendo a scrutinio anche gli acquisti, da parte di investitori europei, di partecipazioni di controllo in società che detengono asset di rilevanza strategica). Inoltre, il Legislatore ha previsto, inter alia: il rafforzamento della tutela Golden Power nell'ambito finanziario (incluso quello creditizio e assicurativo); l'introduzione di norme che prevedono e disciplinano il potere della Presidenza del Consiglio di avviare d'ufficio il procedimento per l'esercizio dei poteri speciali, nei casi in cui sia stata accertata una violazione dell'obbligo di notifica; in tema 5G, l'inserimento, tra i criteri guida dello scrutinio operato ai sensi dell'art. 1-bis, D.L. n. 21/2012, di un riferimento esplicito ai principi e agli indirizzi elaborati a livello internazionale e dell'Unione europea.

Sul piano regolamentare, sono stati varati, tra l'altro, il nuovo decreto attuativo dell'art. 2, comma 1, del D.L. 21/2012 (DPCM 23 dicembre 2020, n. 180, sostitutivo del DPR 85/2014), nonché il DPCM attuativo dell'art. 2, comma 1-ter del D.L. 21/2012 (DPCM 18 dicembre 2020, n. 179). Particolare attenzione, al riguardo, è stata rivolta alla tutela degli attivi di rilevanza strategica nel settore finanziario, creditizio e assicurativo, in quello del trattamento e dell'archiviazione dei dati, nonché dell'accesso e controllo di dati e informazioni sensibili, avendo a mente l'esigenza di adeguare le strategie di risposta all'evoluzione della minaccia (richiamata anche dal Comitato parlamentare per la sicurezza della Repubblica nella Relazione del 12 dicembre 2019 "sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale").

L'estensione del perimetro di tutela ha concorso ad incrementare il numero delle notifiche pervenute al Gruppo di Coordinamento interministeriale operante a Palazzo Chigi, più che quadruplicate rispetto al 2019 (fig. A). L'unica decisione di veto rispetto alle operazioni notificate ha riguardato l'ambito del 5G; in un'ottica di mitigazione dei rischi, invece, si è fatto perno sull'imposizione di prescrizioni/condizioni in 37 procedimenti, più 2, avviati nel 2019 e conclusi nel 2020 (figg. B e C).

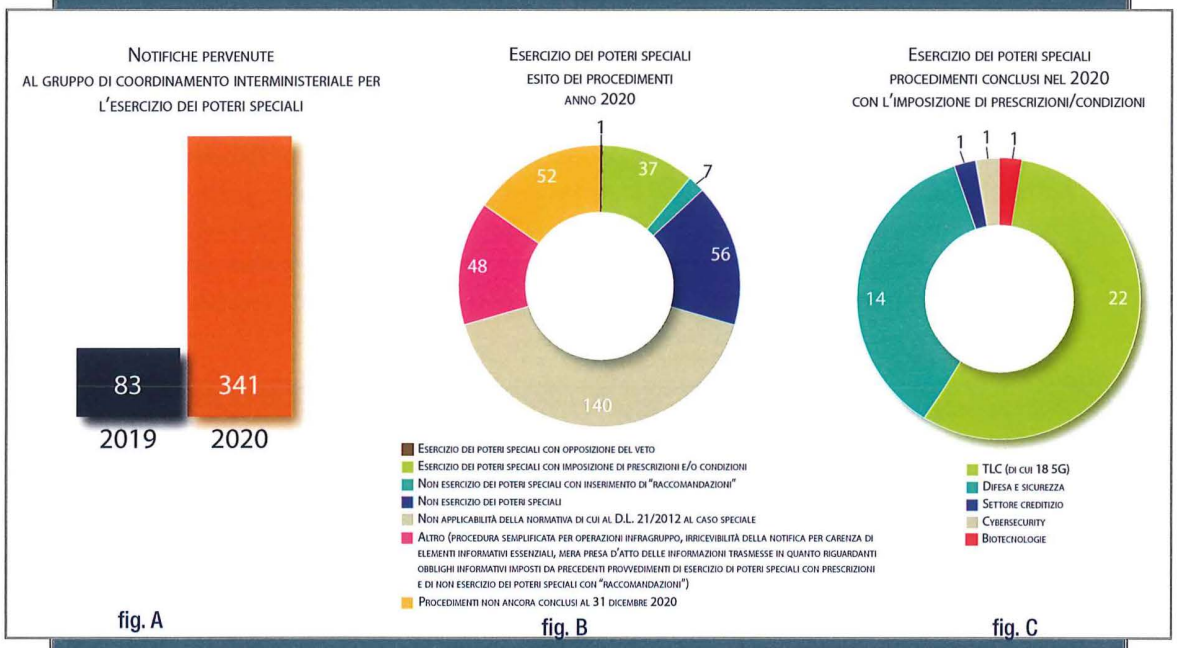


fig. A fig. B fig. C

A fronte dell'emergenza pandemica, un particolare focus informativo si è concentrato sulla **filiera sanitaria**, sia per quanto concerne il monitoraggio degli impatti della pandemia a livello internazionale e le conseguenti ricadute negative per gli interessi industriali e scientifici dell'Italia, sia con riferimento alle possibili ingerenze estere in danno di strutture sanitarie ed emergenziali, centri di ricerca e aziende di settore.

Considerevole impegno informativo ha poi riguardato, in continuità col passato, il **settore aerospazio**, **difesa** e **sicurezza**, al fine di tutelare i grandi player nazionali e le filiere produttive ad essi collegate rispetto alle manovre aggressive di at-

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

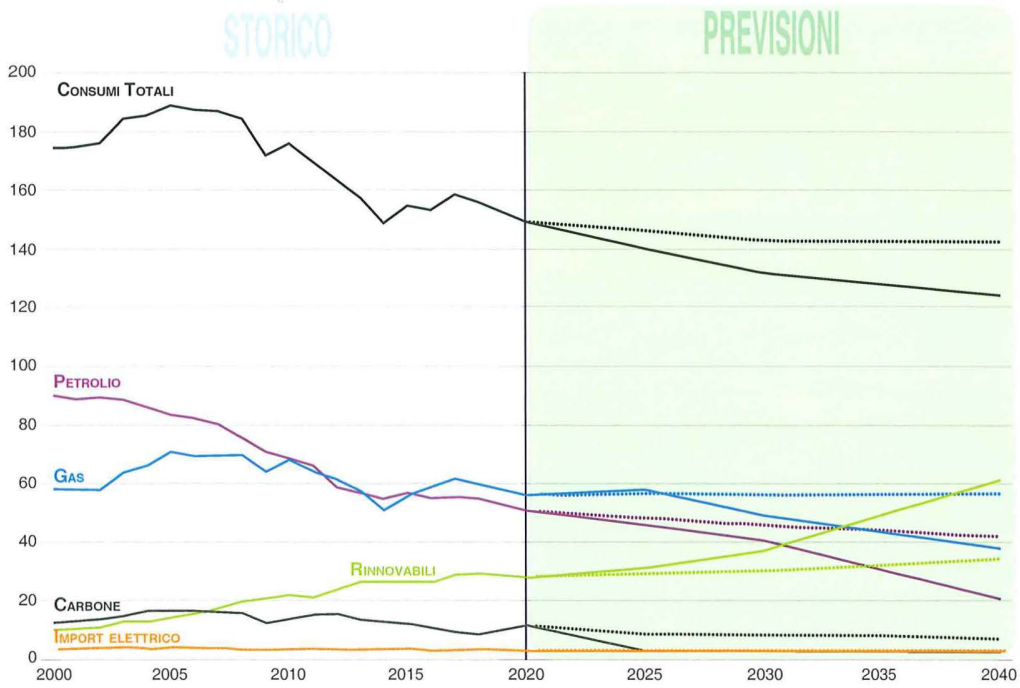
distribuzione, sia la stabilità geopolitica nei Paesi fornitori e di transito dei flussi diretti in Italia, nella prospettiva di verificarne l'adeguatezza per gli anni a venire, quando la ripresa delle domanda globale nel contesto post-pandemico modificherà l'attuale congiuntura.

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:

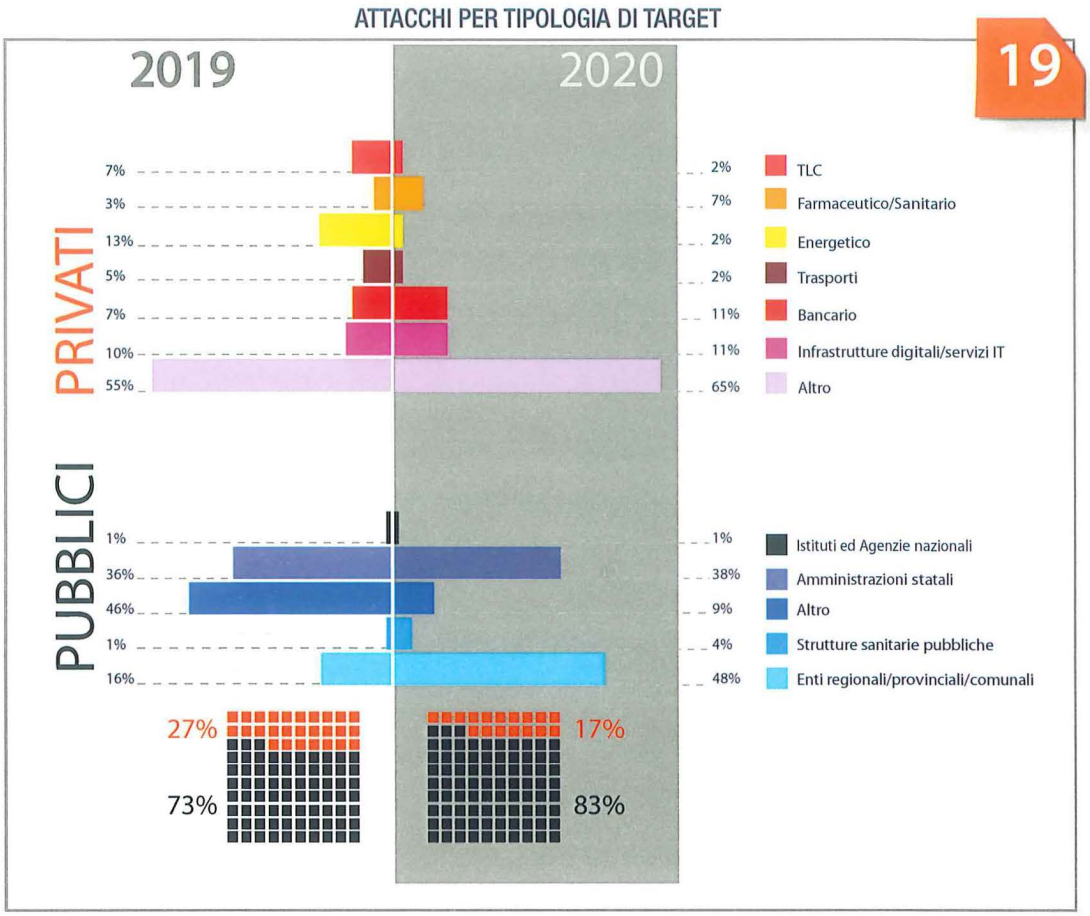
- enti/operatori afferenti al settore della sanità e della ricerca, in direzione dei quali sono state effettuate compromissioni informatiche attraverso l'acquisizione di credenziali amministrative ovvero l'inoculazione di malware;
- Dicasteri ed altre Amministrazioni dello Stato, nei cui confronti si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

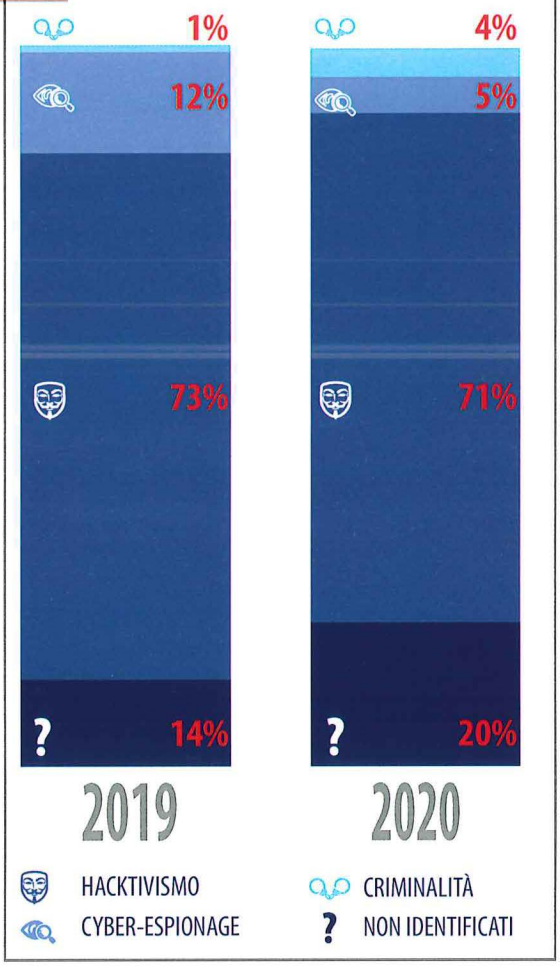


mento rispetto allo scorso anno) e dei servizi IT (11%, dato pressoché stabile).

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.

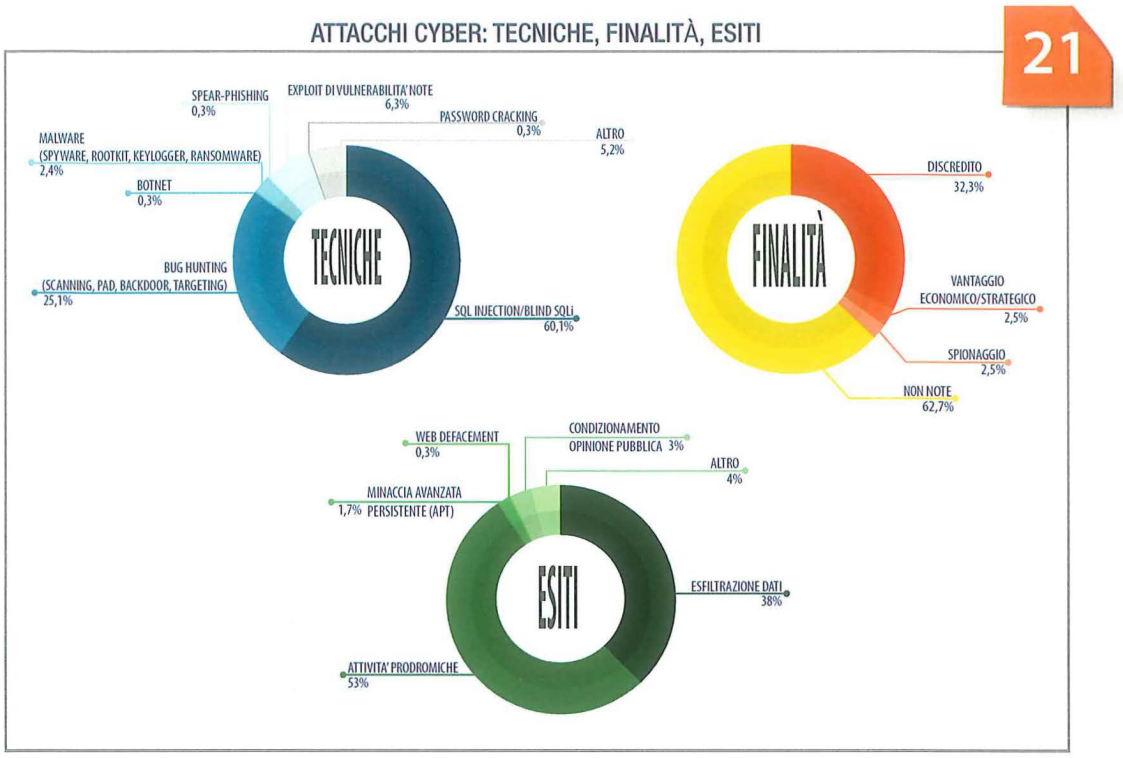
È stata registrata una significativa contrazione (-7%) nel numero delle proiezioni digitali di matrice statuale, a fronte, peraltro, di un nuovo, consistente incremento di episodi dalla matrice non identificabile (+ 6% rispetto al 2019), verosimilmente in ragione dell'accuratezza dimostrata, in più occasioni, 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

produzione mediatica e l'attivismo operativo delle articolazioni regionali e, al contempo, rilanciare campagne di "respiro" globale, come la nota "Jerusalem shall never be judaized", nel cui nome sono state, tra l'altro, rivendicate cruente azioni (da parte di AS in Somalia e di JNIM nel Sahel) contro obiettivi/interessi internazionali. Con ciò, a voler diffondere, tanto tra i propri attivisti quanto tra le file "nemiche", la percezione di compattezza del fronte qaidista, di raccordo sinergico tra centro e periferia, nonché della capacità di portare il jihad anche Oltreatlantico, come dimostrato dalla rivendicazione in febbraio, da parte di AQAP, dell'attacco compiuto il 6 dicembre 2019 da un soldato saudita nella base della marina militare USA di Pensacola in Florida.

La realtà europea e la scena nazionale

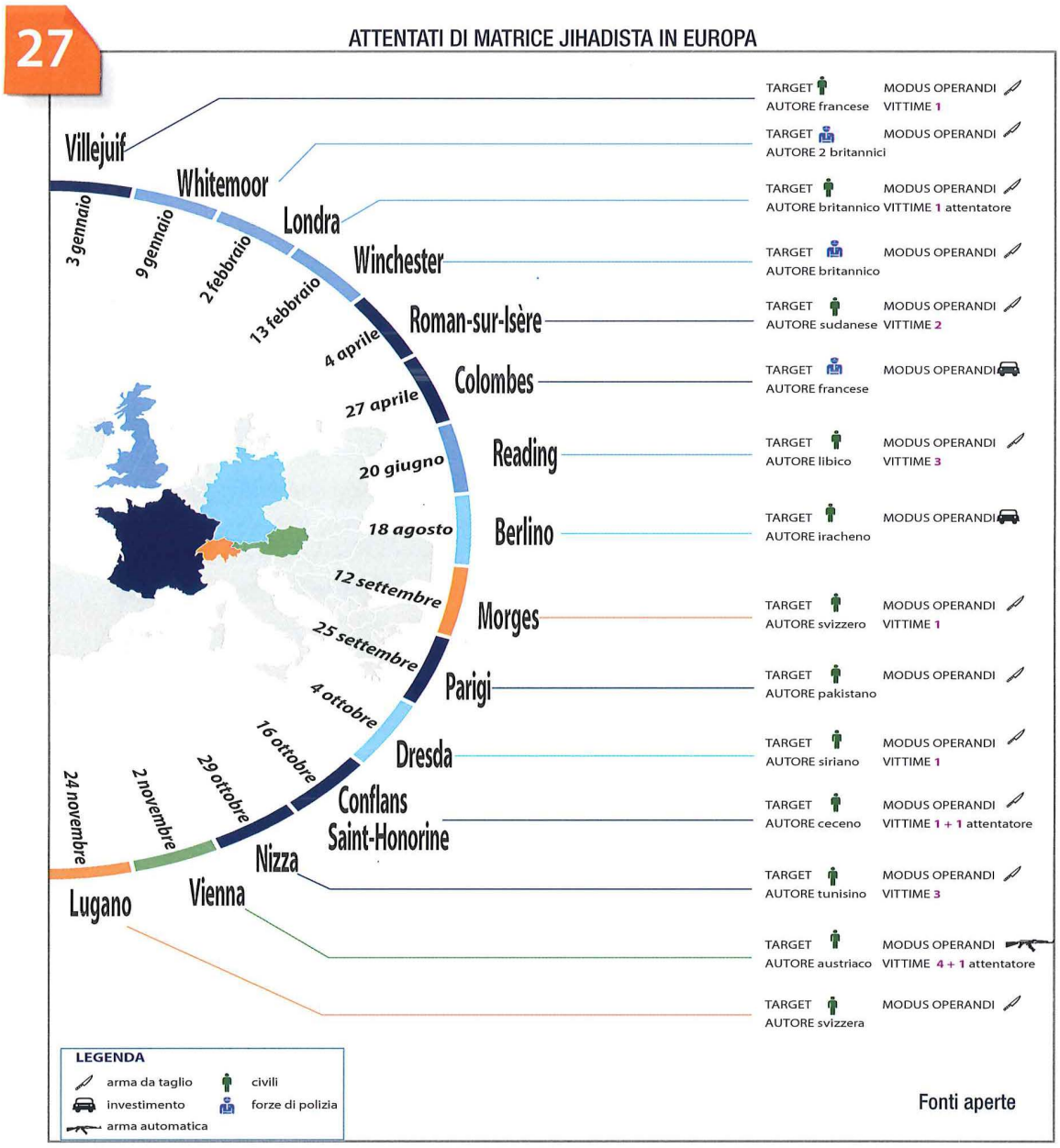
Gli attentati compiuti in Europa nel 2020 hanno confermato i tratti prevalentemente endogeni e destrutturati della minaccia jihadista sul nostro Continente, tradottasi in attivazioni autonome ad opera di soggetti nella maggioranza dei casi privi di legami con gruppi terroristici, ma da questi influenzati o ispirati (vds. tavola n. 27).

Le azioni, in aumento rispetto all'anno precedente, sebbene con un numero di vittime sensibilmente inferiore, sono quasi tutte riconducibili a soggetti filo-DAESH, a riprova della persistente capacità istigatoria della formazione, nonostante la morte del leader al Baghdadi e la sconfitta territoriale del Califfato. La propaganda jihadista e le minacce all'Occidente, ripostate e condivise sulle piattaforme social, non hanno infatti conosciuto battute d'arresto e DAESH, servendosi del consueto mix di richiami emotivi, teologici ed ideologici, ha continuato ad incoraggiare il jihad, nonché a fornire istruzioni per la realizzazione di attacchi, reclutare/addestrare seguaci e talvolta dirigere da remoto i propri adepti. Costante è stato pure il ricorso a campagne propagandistiche contro gli Stati "infedeli", al fine di perpetuare lo "scontro" con l'Occidente e incitare alla "vendetta".

Il profilo degli attentatori si identifica per lo più con quello di "attori solitari", passati all'azione con modalità operative assai semplici, come attesta l'elevato numero di aggressioni all'arma bianca registrato in Francia, che ha visto il 2020 chiudersi con una rapida successione di attacchi culminata, il 29 ottobre, con l'uccisione di 3 persone a Nizza, nella Basilica di Notre Dame de l'Assomption.

Gli autori di alcuni degli attentati realizzati in Europa erano peraltro già noti alle Autorità di sicurezza. È il caso, tra l'altro, dell'azione compiuta il 2 febbraio, a Londra, da parte di un britannico già condannato per attività di propaganda di stampo jihadista, nonché dell'accoltellamento di due turisti tedeschi, il 4 ottobre a Dresda, in Germania, per mano di un pakistano già detenuto per reati di terrorismo.

Emblematico delle difficoltà di cogliere e anticipare i segnali del passaggio all'azione è l'attentato di Vienna del 2 novembre, il cui responsabile, all'attenzione dal 2018 dei Servizi di sicurezza austriaci per le sue simpatie pro-DAESH, era



stato condannato per aver tentato di unirsi all'organizzazione terroristica e poi rimesso in libertà, dopo essere stato sottoposto a un programma di de-radicalizzazione. Le risultanze degli approfondimenti sull'azione condotta nella capitale austriaca, l'unica del 2020 che ha visto l'impiego di armi da fuoco, suggeriscono anche l'ipotesi di una progettualità pianificata e connotata da alcuni dei tratti latenti della minaccia jihadista in Europa, specie per quel che attiene alle con-

vergenze tra circuiti terroristici e criminali e all'attivismo di elementi dal "profilo ibrido", a cavallo tra radicalità e delinquenza, in grado di facilitare il reperimento di documenti falsi, armi e finanziamenti anche per la realizzazione di piani terroristici. Sono emersi, infatti, contatti tra l'attentatore di Vienna (un cittadino austriaco di origini nord-macedoni), elementi radicali di origine balcanica residenti in Europa ed esponenti dell'estremismo violento basati Oltreadriatico in collegamento con membri di DAESH. Tali risultanze hanno trovato significativi punti di tangenza con un consolidato patrimonio informativo che da tempo fa guardare al contesto balcanico quale potenziale incubatore della minaccia terroristica in direzione dello spazio Schengen. Rilevano, nel senso, le indicazioni concernenti l'elevata presenza di returnees, la diffusione del fenomeno della radicalizzazione in alcuni Paesi della regione e il possibile utilizzo del territorio balcanico per il passaggio o il temporaneo rifugio di estremisti con contatti in Europa, grazie a partnership di "convenienza" tra terroristi e criminali (vds. tavola n. 28).

Le evidenze raccolte hanno riguardato altresì imam radicali e predicatori carismatici di origine balcanica operanti in Europa (Italia inclusa), in grado di spostarsi e mantenere contatti con estremisti e soggetti radicalizzati presenti in territorio europeo e nazionale.

28

BALCANI OCCIDENTALI

Il ricorrere della regione balcanica quale epicentro continentale delle attività di proselitismo jihadista e di supporto logistico a estremisti in transito si conferma elemento ancora caratterizzante di un quadrante strategico per la nostra sicurezza e per gli interessi nazionali.

La pandemia ha inciso in misura non omogenea sul composito contesto, determinando peraltro, a fattor comune, effetti recessivi sull'economia, solo in parte mitigati da misure fiscali espansive, e un aumento della polarizzazione sul piano politico, con formazioni contrapposte poco propense al reciproco riconoscimento e istituzioni non sempre in grado di contenere le tensioni.

Le criticità economiche e sanitarie hanno inoltre accresciuto il bisogno di assistenza e, quindi, la potenziale permeabilità dell'area all'influenza esterna di attori extra-UE, che approfittano della stagnazione nel processo di integrazione europea. Quest'ultimo ha continuato ad incontrare numerosi ostacoli, quali il rallentamento dei negoziati di adesione con Serbia e Montenegro e il rinvio dell'apertura di quelli con Macedonia del Nord e Albania.

Ad integrare il quadro descritto, intervengono le operazioni di controterrorismo condotte nell'anno, che mostrano come il Vecchio Continente continui ad essere esposto al rischio sia di attivazioni da parte di ex combattenti e frustrated travellers – come dimostra lo smantellamento in Francia, a gennaio, di una cellula di sette componenti (tre francesi, un tunisino, un marocchino, un siriano e un franco-algerino) che pianificava attentati in territorio transalpino – sia di progettualità coordinate da parte di piccoli gruppi/micro-cellule, come emerso in Spagna

con l'arresto, a maggio, di quattro cittadini marocchini, uno dei quali già noto per la vicinanza ad ambienti riconducibili a DAESH, accusati di voler realizzare attacchi nel Paese iberico. Connessioni internazionali tra sostenitori di DAESH sono emerse, altresì, dall'arresto a maggio, in Polonia, di 4 tagiki legati all'organizzazione e sospettati di reclutare convertiti per condurre attacchi in quel territorio. Dell'operatività di reti di trasferimento di denaro con finalità terroristiche ha fatto stato, invece, il fermo in Norvegia, sempre nel mese di maggio, di un siriano che avrebbe agito da tramite per transazioni in favore di un combattente in Siria.

Non sarebbero mancati, poi, tentativi direttamente ascrivibili alla leadership di DAESH di colpire l'Europa, a conferma della mai sopita ambizione dell'organizzazione terroristica a condurre attentati più strutturati, anche per mantenere la leadership nel panorama del jihad globale e motivare i propri sostenitori. In tal senso può essere letta la pianificazione di un attentato contro installazioni militari statunitensi in Germania, sventata grazie ad una operazione di controterrorismo condotta, nel mese di aprile, nel land Nord Reno-Vestfalia (vds tavola n. 29).

Di una minaccia in suolo europeo riferibile a preordinate pianificazioni da parte dei vertici di DAESH hanno continuato a far stato, d'altro canto, numerose segnalazioni, condivise in ambito di collaborazione internazionale, concernenti il possibile invio, nel Vecchio Continente, di combattenti incaricati di realizzare attentati, nonché il trasferimento di membri dell'organizzazione – anche di figure apicali – al di fuori del quadrante siro-iracheno.

Alla costante attenzione dell'Intelligence, inoltre, il fenomeno degli spostamenti di foreign fighters di DAESH che decidono autonomamente di lasciare il

29

LA CELLULA TAGIKA IN GERMANIA

Sul piano fenomenico, l'operazione Takim, che ha portato, il 15 aprile, all'arresto di 5 tagiki richiedenti asilo, ha fornito alcune significative conferme alle evidenze raccolte nel tempo dall'Intelligence.

Per quanto riguarda gli arrestati, i 5 soggetti, inizialmente intenzionati a recarsi in Tajikistan per unirsi alla locale militanza filo-DAESH, avrebbero in seguito deciso, sotto la direzione da remoto di due handlers dell'organizzazione, basati in Siria e in Afghanistan, di re-indirizzare i loro progetti sul territorio tedesco.

L'ampiezza dei collegamenti emersa dalle indagini sembra profilare l'esistenza in Europa di connessioni interetniche in supporto a DAESH e testimonia, nel contempo, la mobilità dei militanti e la transnazionalità dei loro legami. Accanto alla tradizionale tendenza aggregativa degli estremisti balcanici, caucasici e centroasiatici, che ha favorito la creazione di reti basate su legami familiari, amicali e clanici, si sono registrati, più di recente, segnali che attestano il coinvolgimento in pianificazioni terroristiche di estremisti centroasiatici basati nei Balcani. Tali convergenze sarebbero favorite dalla presenza di tratti condivisi: forte senso di appartenenza al gruppo, background criminale e propensione alla costituzione di network altamente fidelizzati, nonché esperienze operative acquisite in conflitti etnico-nazionalisti e/o nella militanza nelle file di al Qaida e/o DAESH.

teatro mediorientale e ripiegare in Europa. In tal senso rileva l'operazione condotta il 14 aprile in Spagna, ad Almeria, che ha portato all'arresto di tre returnees, tra cui Abdel Majed Abdel Bary, ex rapper egiziano naturalizzato britannico, unitosi a DAESH nel 2014, "volto noto" della propaganda del gruppo in quanto apparso in numerosi video di minaccia contro l'Occidente.

In tale contesto, l'**Italia**, al pari di altri Paesi europei, risulta esposta ad un utilizzo del territorio quale via d'ingresso e ponte verso altre aree del Continente. Sebbene i casi ad oggi emersi non siano riferibili a strutturate strategie per il trasferimento di jihadisti in Europa, rappresenta da tempo una sfida, sul piano informativo, la presenza illegale entro i nostri confini di soggetti "a rischio", che spesso si rendono difficilmente identificabili attraverso l'utilizzo di molteplici alias e che, non di rado, risultano essere stati già più volte espulsi dalle nostre Autorità.

Pur a fronte della sospensione dei rimpatri da marzo a giugno, dovuta all'emergenza epidemiologica, sono stati adottati nell'anno – in buona parte grazie al contributo dell'Intelligence – n. 59 provvedimenti di espulsione (vds. tavola n. 30), a corredo di un dispositivo di prevenzione integrato che ha continuato a trovare punto di forza nelle consolidate sinergie tra Intelligence e Forze di polizia, specie nell'ambito del Comitato Analisi Strategica Antiterrorismo, e nell'assidua cooperazione con i Servizi esteri collegati.

L'impegno informativo entro i nostri confini è rimasto prioritariamente focalizzato sull'eterogeneo bacino di soggetti esposti a/coinvolti in processi di radicalizzazione, sovente rapidi e invisibili, che maturano sul web, nelle carceri e in luoghi di aggregazione.

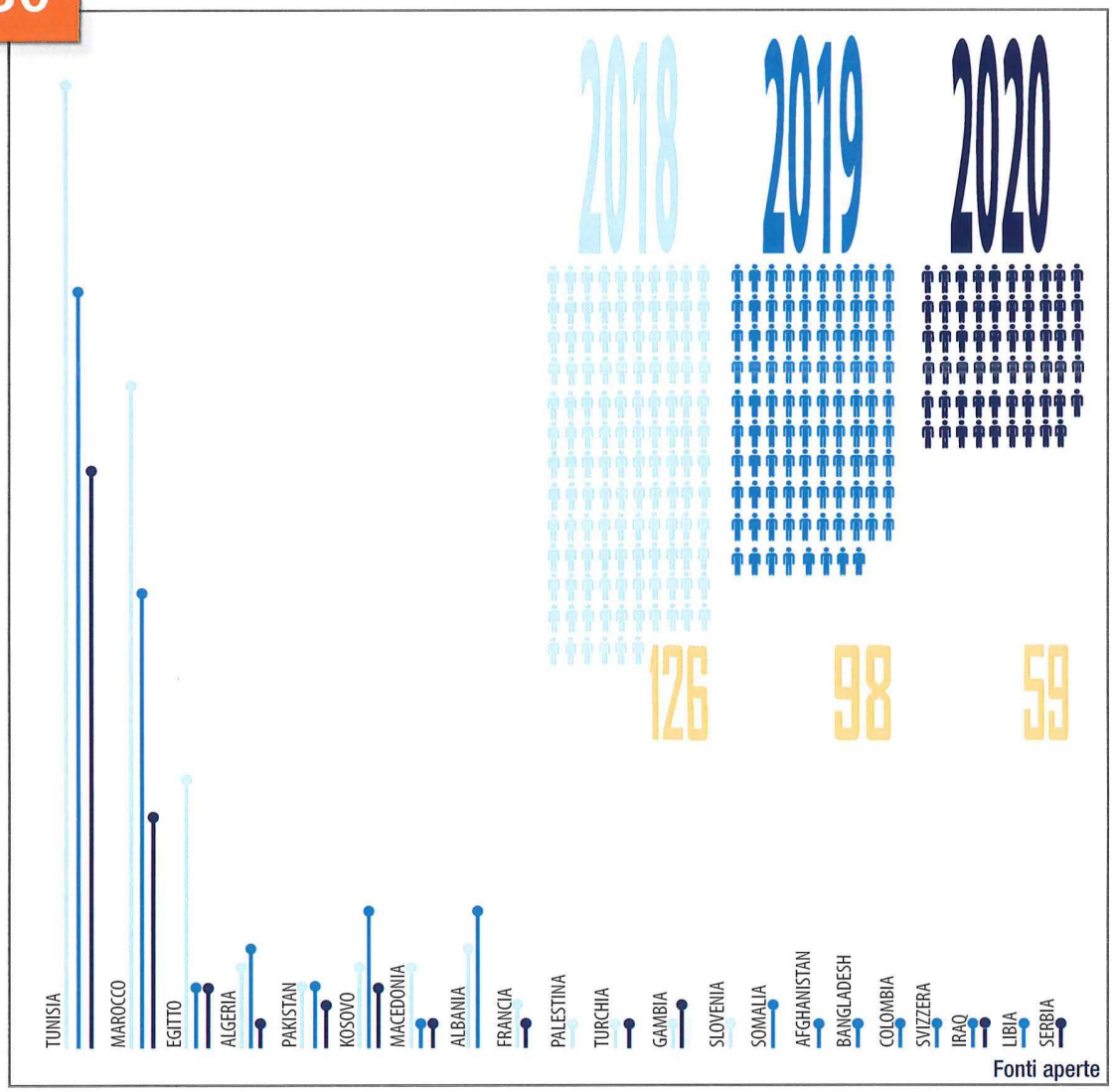
Come nel resto d'Europa, in Italia ha continuato a registrarsi una certa adesione al jihadismo attraverso il web, dove vengono diffusi articoli, infografiche, video di propaganda in lingua italiana, condiviso materiale teso a veicolare istanze anti-occidentali e diramate immagini minatorie di monumenti simbolo del nostro Paese e del Cristianesimo. All'attenzione, in questo contesto, il rischio legato all'effetto istigatorio che tale messaggistica potrebbe esercitare su soggetti particolarmente influenzabili, siano essi residenti (homegrown/di recente immigrazione) o in transito, orientandoli verso estemporanei gesti dimostrativi/provocatori, anche con esiti violenti, se non motivandoli a veri e propri atti premeditati e organizzati di jihad individuale.

Anche nel corso del 2020, sebbene non sia stata rilevata una produzione originale di propaganda jihadista in italiano, materiale tradotto o sottotitolato nella nostra lingua a uso di utenti italofoni è stato condiviso online, utilizzando soprattutto social network e piattaforme di messaggistica protette da crittografia end-to-end.

A tal proposito, appare significativa l'emissione nel novembre 2020 di un provvedimento di custodia cautelare in carcere nei confronti di un 42enne italiano accusato di auto-addestramento con finalità terroristiche, il quale scaricava materiale jihadista anche riferibile a DAESH.

30

ESPULSI: NUMERI E NAZIONALITÀ



In generale, l'opera di replicazione si è concentrata perlopiù su locandine, estratti di audio-messaggi, parti di newsletter e rivendicazioni di attività militari di DAESH. È stato inoltre rilevato il rilancio di contributi già diffusi, come un video sottotitolato del 2016, nel quale si invitano i lupi solitari a colpire i "miscredenti", fornendo indicazioni sull'uso di armi da taglio e TATP (perossido di acetone), nonché un documento distribuito nel 2019, che riporta nozioni indirizzate ai mujahidin per difendersi da "attacchi mediatici" e "guerre psicologiche dei miscredenti".

È stata riscontrata anche la circolazione di manualistica contenente istruzioni per la produzione di ordigni di tipo artigianale, talvolta tramite la sintesi di sostanze esplodenti.

Rileva, poi, l'azione di da'wa radicale condotta in italiano da alcuni internauti, anche convertiti, dotati di particolare carisma e residenti nel nostro Paese o all'estero. Il loro attivismo si è concentrato generalmente su utenti carenti di adeguata preparazione religiosa e più facilmente plasmabili, i quali, una volta attratti nell'alveo di questa forma di "proselitismo sistematico", possono contribuire a diffondere i principi propri dell'Islam radicale e militante, in particolare la tipica visione conflittuale Islam/Occidente. Rappresentativo, al riguardo, è il caso di un 38enne italiano, arrestato a Milano nel luglio scorso con l'accusa di apologia di DAESH e istigazione ad aderire a tale organizzazione terroristica.

Contesto sensibile resta quello carcerario, come testimoniato dalle espulsioni a fine pena di estremisti o altri soggetti ristretti per reati comuni che, durante la detenzione, hanno confermato o manifestato per la prima volta la propria adesione all'ideologia jihadista, rendendosi responsabili di manifestazioni apologetiche, atteggiamenti rivoltosi e reazioni violente contro il personale penitenziario e correligionari ritenuti non "in linea". In prospettiva, le principali incognite riguardano coloro che, pur avendo scontato la propria pena, conservano un forte risentimento e propositi ritorsivi nei confronti dell'Italia e quanti, una volta tornati in libertà, tendono a recuperare contatti con ambienti criminali/radicali.

Il monitoraggio informativo ha riguardato, infine, l'attivismo di soggetti attestati su posizioni radicali impegnati nell'opera di indottrinamento/proselitismo anche in luoghi di aggregazione islamici. In talune realtà territoriali, essi hanno mostrato di esercitare forme di condizionamento ideologico rispetto a componenti moderate, cercando di orientare l'uditorio verso posizioni oltranziste. Indicativo, nel senso, il caso di un cittadino egiziano, espulso dall'Italia per motivi di sicurezza, già imam presso luoghi di culto del Nord d'Italia e in contatto con soggetti – presenti anche in altri Stati europei – gravitanti in ambienti islamisti e dediti a condotte criminali.

PAGINA BIANCA

IMMIGRAZIONE CLANDESTINA

in breve

- Aumento dell'instabilità politica e delle vulnerabilità economiche dei Paesi di origine e transito dei clandestini
- Incremento degli arrivi in territorio nazionale con temporanea contrazione durante la primavera
- Dinamismo manageriale delle reti criminali maghrebine dedite al traffico di migranti ed aumento dei giovani reclutati nelle filiere
- Criticità di sicurezza derivanti soprattutto da sbarchi fantasma, arrivi parcellizzati attraverso la rotta balcanica terrestre e falso documentale

Trend

L'emergenza pandemica ha parzialmente influito sull'andamento del fenomeno migratorio irregolare in direzione dell'Europa e dell'Italia. A gennaio/febbraio, il trend degli arrivi via mare sul territorio nazionale era incrementale rispetto al medesimo periodo del 2019. I flussi hanno poi subìto una sensibile contrazione nei mesi primaverili per riprendere vigore già a partire da maggio.

L'aggravamento, per effetto della crisi sanitaria, delle condizioni socio-economiche dei Paesi di origine e transito dei clandestini potrebbe peraltro costituire ulteriore fattore di spinta del fenomeno.

Organizzazioni criminali

La gestione criminale dei flussi migratori irregolari e del lucroso giro di affari connesso al trasferimento dei migranti dalle aree d'origine a quelle di destinazione ha continuato a rappresentare obiettivo prioritario dell'Intelligence. Una copiosa produzione informativa, puntualmente condivisa con le Forze di polizia, ha infatti riguardato modus operandi e assetti delle organizzazioni criminali coinvolte nel traffico.

Il quadro emerso fa stato dell'attivismo di sodalizi dinamici, in grado di rimodulare rotte, relazioni e partnership per sfuggire all'azione di contrasto e caratterizzati da una spiccata "managerialità", che ha consentito loro di cogliere le opportunità offerte dalla crisi sanitaria anche sul piano del reclutamento, con riguardo ad un bacino di manovalanza reso più ampio dall'accresciuto degrado delle condizioni economiche. Significativo quanto emerso in Tunisia, ove la logistica del traffico e il relativo indotto illecito – che da tempo registrano l'ingaggio di pescatori locali in qualità di scafisti, operanti in connessione con facilitatori, mediatori

e proprietari di safe house – hanno rappresentato fattore di attrazione, ambito di impiego e fonte di sostentamento per giovani tunisini, sempre più impiegati nella fase "promozionale" dei viaggi, grazie anche alla loro dimestichezza con l'utilizzo dei social media.

Non sono emerse nuove evidenze di network strutturati e ramificati dediti alla facilitazione della migrazione clandestina dalla Tunisia verso l'Italia. Sono state invece acquisite indicazioni sull'attivismo, specie nell'area di Sfax, di consorterie criminali "indipendenti" composte da soggetti di nazionalità tunisina. Seppur in misura minore, è emerso il dinamismo di gruppi criminali anche nelle zone confinarie con la Libia, soprattutto per le partenze verso la Sicilia sud-occidentale. Le sinergie tra reti di trafficanti operanti nei due Paesi hanno concorso ad alimentare la direttrice che vede il trasferimento di migranti dalla Libia, via terra, verso le località marittime della Tunisia ed il successivo imbarco in direzione delle nostre coste.

Le acquisizioni hanno confermato l'utilizzo di imbarcazioni di piccole dimensioni – consentito dalla prossimità delle coste tunisine a quelle italiane – che ha alimentato il fenomeno dei cc.dd. sbarchi autonomi (o fantasma).

Analoghe modalità occulte di ingresso hanno interessato, con numeri più esigui, gli arrivi dall'Algeria sulle coste sarde, con l'impiego di gommoni semirigidi idonei a coprire la distanza in poche ore. In altri casi, è stato rilevato il trasporto dei migranti, a cura di facilitatori algerini e tunisini, dall'area nord-orientale dell'Algeria alla Tunisia, da dove intraprendere il viaggio via mare verso l'Italia.

Le reti criminali dedite al traffico di migranti dalla Libia si sono confermate tra le più flessibili e capaci di adattarsi alle circostanze contingenti. Negli ultimi mesi del 2019 si era assistito ad arrivi da quel Paese con l'impiego di navi "madri", mentre nell'anno appena trascorso le consorterie criminali sono tornate ad utilizzare soprattutto natanti più piccoli, da affidare a migranti opportunamente "indottrinati" sulle rotte da seguire.

La ricerca intelligence ha fatto emergere un uso sempre più frequente dei social network da parte dei trafficanti libici per la promozione delle traversate, anche con la diffusione di notizie false, quale la possibilità di ottenere facilmente permessi di soggiorno e sanatorie.

In linea generale, le località della fascia costiera ad ovest di Tripoli (Zawiya, Sabrata e Zuwara sino a quelle a ridosso del confine tunisino) sono rimaste le principali aree di imbarco.

I flussi che alimentano la rotta del Mediterraneo orientale e che, via mare, muovono dalla Turchia in direzione della Grecia e dell'Italia hanno registrato il perdurante protagonismo di gruppi criminali operanti in stretto collegamento con sodali attivi in territorio nazionale. L'attività informativa ha confermato, altresì, l'utilizzo di barche a vela, condotte da skipper russofoni, per effettuare la traversata dalle coste turche a quelle italiane con approdi in elusione dei con-

trolli. Un inedito modus operandi consisterebbe, secondo le evidenze raccolte, nel dichiarare, all'atto della partenza dai porti anatolici, una falsa destinazione, segnatamente i Paesi africani in regime di facilitazione o esenzione visti, per poi dirigersi alla volta delle coste greche o italiane.

Lungo la rotta balcanica terrestre, la Bosnia Erzegovina si è confermata hub dei flussi che raggiungono l'Italia, in prossimità di Trieste, attraverso la Slovenia. Particolarmente sensibile la situazione dei campi di accoglienza presenti in territorio bosniaco, a rischio per quel che attiene alla diffusione dei contagi da Covid-19, oltre che potenziali catalizzatori di attività criminali e proselitismo estremista.

La produzione informativa ha messo in evidenza la proliferazione nella regione di realtà delinquenziali eterogenee e parcellizzate, composte da microgruppi e singoli passeur, maggiormente competitive nell'offrire, rispetto a quelle operanti lungo la rotta del Mediterraneo, opzioni diverse in base alle differenti capacità economiche dei migranti. In questo contesto, ha trovato conferma la primazia dei gruppi criminali pakistani, afghani e siriani, unitamente alla presenza di loro referenti in varie città italiane per facilitare gli spostamenti dei migranti nelle ulteriori tappe del viaggio.

Come già emerso nel 2019, questa direttrice – prevalentemente impiegata da migranti asiatici – ha visto il transito, altresì, di irregolari maghrebini, che trovano nella rotta balcanica terrestre una via alternativa (e più sicura rispetto a quella del Mediterraneo centrale) per raggiungere il territorio della UE.

Gli arrivi parcellizzati attraverso la frontiera terrestre, così come gli sbarchi fantasma dal Nordafrica o dalle sponde turco-elleniche, restano, sul piano della sicurezza, le modalità d'ingresso più critiche, rispetto alle quali i rischi sanitari connessi alla possibile dispersione sul territorio nazionale di soggetti positivi al virus sono andati ad aggiungersi al pericolo di infiltrazioni terroristiche. Su quest'ultimo versante, le risultanze della serrata attività d'intelligence, condotta in raccordo con le Forze di polizia e in collaborazione con i Servizi collegati esteri, fanno ancora escludere un ricorso sistematico ai canali dell'immigrazione clandestina per la movimentazione di jihadisti, ribadendo peraltro la sussistenza di rischi connessi all'eventualità che nei centri di confluenza/accoglienza dei migranti possano maturare processi di radicalizzazione islamista. Del pari, mirata attenzione informativa è stata riservata al settore del falso documentale, che vede spesso l'interazione tra circuiti criminali e terroristici.

PAGINA BIANCA

CRIMINALITA' ORGANIZZATA

in breve

- Prevedibile interesse delle mafie a trarre profitto dall'impatto dell'emergenza pandemica per infiltrare il tessuto economico
- Proiezioni mafiose in un ampio novero di settori dell'economia legale. Schemi sempre più sofisticati di riciclaggio
- Dinamismo e fluidità degli assetti a fronte della pressante azione di contrasto
- Divaricazione tra sodalizi di profilo strategico e compagini di impronta banditesca
- Collaborazioni tra matrici per finalità affaristiche

Le mafie autoctone

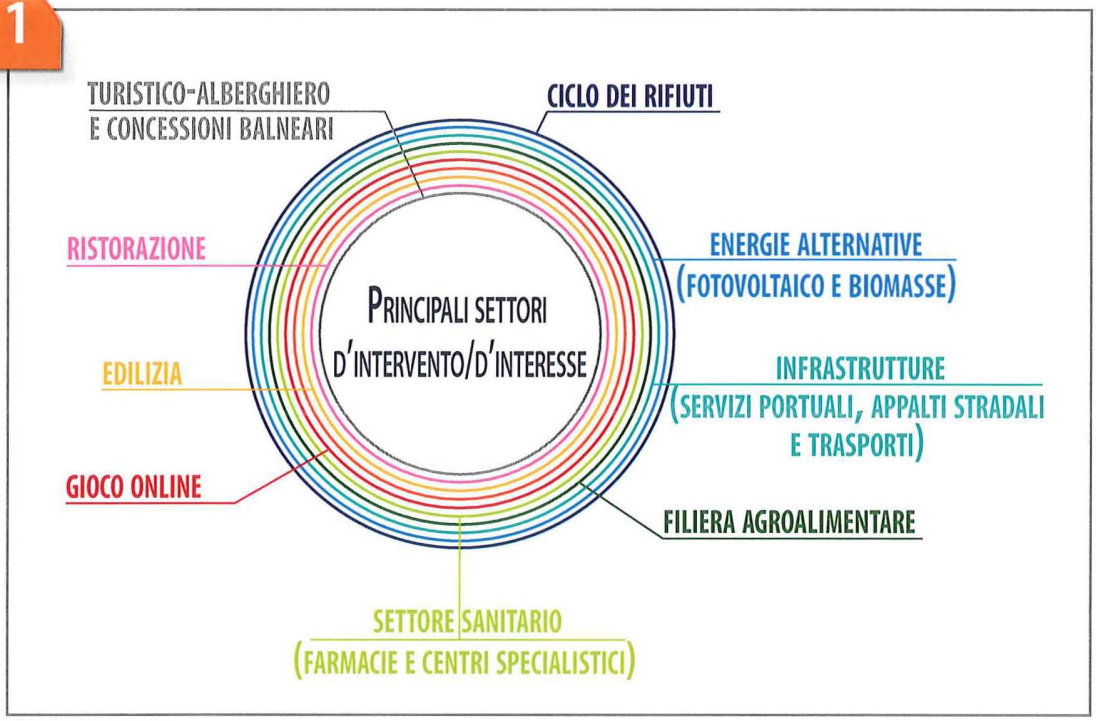
I tratti distintivi della criminalità organizzata, così come ribaditi dalle acquisizioni intelligence, nonché dalle risultanze investigative e giudiziarie, valgono da sé a profilare l'interesse delle mafie a trarre profitto dall'impatto dell'emergenza pandemica e, segnatamente, a condizionare gli operatori economici in difficoltà e a tentare di intercettare i finanziamenti, nazionali ed europei, connessi ai piani di rilancio.

Al netto delle implicazioni della crisi sanitaria, le evidenze raccolte nel 2020 hanno infatti confermato la propensione delle organizzazioni criminali più competitive a consolidare ed espandere gli spazi di inserimento nel tessuto economico, reinvestendo nei circuiti legali i proventi delle attività illecite, sfruttando inefficienze e vulnerabilità gestionali a livello locale e sviluppando reti collusive e corruttive funzionali all'inquinamento dei processi decisionali pubblici (vds. tavola n. 31).

Fattore cruciale di alimentazione della capacità pervasiva dei sodalizi, anche in termini di alterazione della concorrenza e del corretto funzionamento del mercato, resta la disponibilità di denaro assicurata dai traffici illeciti più remunerativi, rispetto ai quali hanno continuato a registrarsi cointeressenze tra diverse matrici mafiose. È il caso non solo del traffico di stupefacenti, ma anche del contrabbando internazionale di prodotti petroliferi, realizzato con il coinvolgimento di studi professionali e società di comodo, attestate in Italia e all'estero, e utilizzato anche a fini di riciclaggio. Altrettanto "ambivalente", quale fonte di introiti e vettore di reinvestimento dei capitali, si è confermato, altresì, l'attivismo criminale nel setto-

31

IL PROFILO AFFARISTICO DELLE MAFIE



re dei giochi e delle scommesse, che coniuga l'infiltrazione nel gioco lecito, pure mediante pressione estorsiva sui concessionari, con la gestione di circuiti, anche online, del gioco clandestino (vds. tavola n. 32).

Seppure protagonisti non esclusivi nel panorama internazionale della criminalità economica, che comprende un ampio e diversificato novero di attori e matrici, i sodalizi mafiosi, grazie anche alle saldature con professionisti e im-

32

INFILTRAZIONI DELLA CRIMINALITÀ ORGANIZZATA NEL SETTORE DEI GIOCHI E DELLE SCOMMESSE

Il settore dei giochi e delle scommesse ha da tempo attirato l'attenzione della criminalità organizzata, nazionale e straniera, interessata a strumentalizzarne le potenzialità a fini di arricchimento e riciclaggio, anche con il ricorso ad articolati schemi societari con ramificazioni all'estero.

Le numerose operazioni di polizia realizzate nel corso del 2020 hanno confermato ricorrenza e varietà delle pratiche adottate dai gruppi criminali, tra le quali la manomissione delle apparecchiature di gioco, finalizzata alla trasmissione di informazioni non veritiere sui relativi flussi di denaro, in violazione della normativa fiscale, e la raccolta illegale delle scommesse – anche mediante lo schermo di agenzie regolarmente abilitate all'esercizio dell'attività e intestate a prestanome – i cui importi in denaro vengono convogliati su piattaforme con sede all'estero. Proprio al di fuori dei confini nazionali, infatti, trovano spesso dimora i server, i conti di gioco e le relative piattaforme digitali, circostanza che consente agli operatori criminali di eludere la tracciabilità dei flussi finanziari illegali, potendo beneficiare di ordinamenti legislativi meno rigorosi in materia di contrasto al riciclaggio e al crimine organizzato.

prenditori collusi, hanno ulteriormente affinato le capacità di reinvestimento dei proventi illeciti, ma anche di occultamento e movimentazione dei capitali a fini di evasione ed elusione fiscale, attraverso sistemi articolati, operanti soprattutto nella dimensione virtuale e/o con sponde in Paesi nei quali risulti più debole il presidio antiriciclaggio. Si tratta di un contesto nel quale le opacità garantiscono margini di operatività non solo ad attori criminali, ma anche ad organizzazioni terroristiche e che – nonostante l'attivismo anche normativo dei principali consessi multilaterali – reclama ancora, a livello internazionale, la realizzazione di stabili ed efficaci meccanismi di collaborazione e di interscambio informativo. In quest'ottica è intervenuto a luglio, in ambito UE, il "Piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo" (vds. tavola n. 33).

33

PIANO D'AZIONE PER UNA POLITICA INTEGRATA DELL'UNIONE IN MATERIA DI PREVENZIONE DEL RICICLAGGIO DI DENARO E DEL FINANZIAMENTO DEL TERRORISMO

Il Piano d'azione della Commissione UE, adottato il 10 luglio dal Parlamento Europeo, propone un ambizioso potenziamento del dispositivo, attraverso i seguenti interventi:

- effettiva attuazione del quadro normativo vigente da parte degli Stati Membri, delle Autorità competenti e dei cc.dd. soggetti obbligati. In particolare, a fronte di rilevate inadempienze a livello dei singoli Paesi, la Commissione ha più volte avviato procedure d'infrazione volte a sollecitare il pieno recepimento della IV e V direttiva antiriciclaggio che, tra le misure di rafforzamento del sistema finanziario comune, prevedono l'istituzione dei registri centralizzati dei conti bancari e dei registri sui cc.dd. titolari effettivi;
- istituzione di un corpus normativo unico, con l'obiettivo, tra l'altro, di evitare asimmetrie legislative in grado di favorire la canalizzazione di attività di impresa e dei relativi flussi finanziari all'interno di Paesi nei quali le politiche di contrasto risultino meno rigide (cd. shopping normativo);
- realizzazione di una vigilanza europea integrata, a complemento delle funzioni svolte dalle Autorità competenti dei singoli Paesi, le cui eventuali carenze sul piano operativo e gestionale – riconducibili anche a deficit di risorse umane e finanziarie o di competenze tecniche – appaiono suscettibili di riflettersi sull'intero sistema europeo;
- istituzione di un meccanismo di supporto alle Unità di Informazione Finanziaria (UIF) nazionali, funzionale al superamento di asimmetrie operative a livello europeo o di eventuali criticità nello scambio informativo tra UIF e Autorità competenti. Ciò, con particolare riferimento ai casi in cui le cc.dd. Segnalazioni di Operazioni Sospette (SOS) abbiano una dimensione transfrontaliera;
- omogeneizzazione delle disposizioni di diritto penale e miglioramento dello scambio informativo a livello europeo, con l'obiettivo, da un lato, di colmare le lacune normative degli ordinamenti nazionali in merito alla definizione della fattispecie di riciclaggio e, dall'altro, di agevolare la cooperazione giudiziaria e di polizia, anche attraverso l'interconnessione dei cc.dd. registri centrali dei conti correnti;
- rafforzamento della dimensione internazionale del quadro normativo di riferimento, con l'ingaggio di rappresentanti delle Istituzioni europee nei lavori del Gruppo d'Azione Finanziaria Internazionale-GAFI, anche mediante la previsione di un maggior coordinamento tra Commissione e Stati Membri.

Per quel che attiene alle singole matrici mafiose del panorama nazionale, l'attività informativa ha rilevato, a fattor comune, una pronunciata fluidità degli assetti, dovuta all'incessante azione di contrasto, unitamente ad una sempre più marcata differenziazione tra le componenti di profilo affaristico-strategico, più vocate all'infiltrazione nei circuiti legali, e le formazioni di minor spessore, maggiormente esposte alla competizione interclanica.

La **'ndrangheta** si conferma l'espressione mafiosa più dinamica che, al persistente e diffuso attivismo nella regione di origine, associa una radicata presenza, nel resto del territorio nazionale, di propaggini – sovente con solide basi all'estero – proiettate nel traffico di stupefacenti e nella penetrazione dei circuiti imprenditoriali e amministrativi. Alla costante ricerca di spazi di intervento negli ambiti più remunerativi, le famiglie calabresi hanno mantenuto forza espansiva e pronunciata capacità relazionale, che ne hanno sostenuto, tra l'altro, l'interesse – oltre che verso il citato settore del gioco – in direzione del ciclo dei rifiuti, del settore sanitario (specie con riguardo alla gestione di farmacie e centri specialistici) e della cd. green economy, segnatamente nel campo delle cc.dd. bioenergie, rispetto al quale i sodalizi mirerebbero ad acquisire il controllo della relativa filiera, seguendo schemi di ingerenza consolidati che assicurano ingenti profitti a fronte di un minore rischio repressivo.

È rimasta elevata, inoltre, l'attenzione delle 'ndrine sui traffici di merci sviluppati negli scali portuali calabresi, snodi strategici per importanti famiglie, che, in ragione del volume degli interessi in gioco, specie per il narcotraffico, tenderebbero qui a non esasperare la conflittualità interclanica. In altre realtà territoriali, peraltro, sono emerse dinamiche associative contrassegnate da dispute suscettibili di innescare contrapposizioni anche violente.

Sul piano organizzativo, **Cosa nostra** palermitana ha risentito delle difficoltà di ripianare le posizioni di vertice rese vacanti dall'azione di contrasto, della mancata ricostituzione di un coordinamento unitario a livello provinciale e di talune tensioni interne. Cionondimeno, i clan hanno mostrato persistente vitalità, grazie alla loro capacità di adattarsi ai mutamenti di contesto e all'approccio pragmatico al "business" finalizzato al riciclaggio e alla creazione di imprese "pulite" da impiegare nella gestione manageriale degli interessi criminali, tanto in territorio siciliano quanto nei contesti di proiezione extra-regionale. L'attivismo dei sodalizi ha riguardato, oltre ai tradizionali affari illeciti, quali il traffico di sostanze stupefacenti, il gioco online, il racket delle estorsioni e il contrabbando di idrocarburi, anche i settori immobiliare, dei trasporti, delle assicurazioni, della ristorazione e dell'abbigliamento. Del pari, sono stati rilevati tentativi di penetrazione nelle procedure di assegnazione di appalti pubblici e fondi europei. Quanto alle famiglie della Sicilia orientale, l'azione intelligence ha evidenziato un particolare dinamismo nel narcotraffico e nell'infiltrazione della filiera della raccolta agrumicola, anche secondo accordi interclanici di tipo spartitorio (vds. tavola n. 34).

34

LO SFRUTTAMENTO DELLA MANODOPERA NEL SETTORE DELLA RACCOLTA AGRUMICOLA

Il cd. caporalato, reato sanzionato dall'articolo 603 bis del codice penale, è un sistema illecito di intermediazione e sfruttamento del lavoro da parte di intermediari illegali, i cc.dd. caporali, che arruolano manodopera da impiegare in alcuni settori economici.

La consolidata presenza della criminalità organizzata, sia endogena che straniera, nelle aree in cui si concentra la raccolta stagionale in agricoltura ha concorso, da un lato, ad inquinare un settore già condizionato dal lavoro irregolare e da una forte competitività dei mercati esteri, dall'altro, allo sviluppo di relazioni affaristico-criminali connesse ai cicli della stagionalità, finalizzate anche ad assicurare il tempestivo spostamento dei migranti all'interno del territorio nazionale per corrispondere alle contingenti richieste di manodopera.

Per contrastare il fenomeno, il "Tavolo caporalato" (operante presso il Ministero del Lavoro e delle Politiche Sociali con la partecipazione di Enti istituzionali, parti sociali e rappresentanti del Terzo settore) ha varato in febbraio il "Piano triennale 2020-2022 di contrasto allo sfruttamento lavorativo in agricoltura e al caporalato". Il documento programmatico, tra l'altro, nell'individuare talune vulnerabilità sistemiche (eccessiva stratificazione normativa, nazionale e sovranazionale, sovrapposizione di competenze tra Enti pubblici centrali e periferici, etc.), che verosimilmente hanno di fatto dilatato gli spazi di intervento della criminalità organizzata, ha delineato priorità strategiche quali:

- vigilanza e ispezione nelle realtà locali interessate dal lavoro stagionale;
- efficaci servizi pubblici di intermediazione tra domanda e offerta di lavoro;
- idonei mezzi di trasporto per il raggiungimento delle aree di coltivazione/raccolta;
- realizzazione di alloggi e foresterie in luogo delle attuali baraccopoli, al cui interno si sviluppano derive criminogene legate allo sfruttamento della prostituzione e al traffico di stupefacenti.

Le formazioni catanesi, i cui equilibri associativi sono rimasti precari, hanno mantenuto la loro presenza, altresì, nei settori degli autotrasporti e della logistica.

Le **organizzazioni criminali campane** sono parse ancora contrassegnate da dinamiche associative fluide, influenzate da flebili alleanze mirate alla gestione delle principali piazze di spaccio e delle attività sul territorio di natura predatoria ed estorsiva. Lo scenario partenopeo è quello in cui si è colta con particolare nettezza la compresenza di sodalizi meno qualificati, duramente colpiti dall'azione di contrasto e alla costante ricerca di opportunità di affermazione criminale, e formazioni più strutturate, che beneficiano di risalente expertise nella penetrazione del tessuto socio-economico. A queste ultime le evidenze informative hanno ricondotto tentativi di infiltrazione nei settori immobiliare, della grande distribuzione e dell'edilizia, con riferimento agli appalti, pubblici e privati, in territorio nazionale e all'estero, specie in Europa orientale. Il carattere transnazionale dell'attivismo camorrista, evidenziatosi anche in relazione al business del gioco e delle scommesse, è emerso pure per trasferimenti all'estero di quote societarie o di cariche sociali a favore di prestanome, unitamente alla realizzazione per fini illeciti, con l'aiuto di professionisti compiacenti, di articolati schemi finanziari. Sul

fronte casalese, i sodalizi, malgrado la costante azione di contrasto e il deficit di legittimazione causato dalla collaborazione con la giustizia di esponenti di vertice del clan, hanno mostrato persistenti, significative capacità criminali, specie sul versante delle proiezioni in attività economiche, in territorio nazionale ed estero. Le indicazioni raccolte ne hanno confermato, in particolare, l'interesse verso i settori agroalimentare e dei trasporti.

Eterogeneità strutturale, spinte espansive e propensione alle derive violente sono gli aspetti emersi con maggiore evidenza dalle acquisizioni intelligence sulla **criminalità organizzata pugliese** e dalle importanti operazioni di polizia condotte nell'anno, valse a ribadire, specie con riguardo alla cd. società foggiana (vds. tavola n. 35), la persistente pressione estorsiva esercitata sul territorio e gli intrecci collusivi finalizzati all'indebita acquisizione di finanziamenti pubblici, anche europei.

35

PECULIARITÀ ORGANIZZATIVE DELLA CD. SOCIETÀ FOGGIANA

A sviluppo delle numerose operazioni di contrasto in direzione della criminalità organizzata pugliese, tra cui quella denominata "Decima Azione", che a fine 2018 ha portato all'arresto di numerosi esponenti di clan attivi nella provincia di Foggia, il 16 novembre ha avuto luogo l'operazione "Decima Bis", in direzione delle "batterie" della cd. società foggiana Moretti-Pellegrino-Lanza, Sinesi-Francavilla e Trisciuoglio-Tolonese-Prencipe.

L'azione investigativa ha posto in evidenza dinamiche e modus operandi tipici delle compagini foggiane, dedite ad una ampia gamma di attività illecite, tra cui il traffico di sostanze stupefacenti, il riciclaggio e, soprattutto, le estorsioni in danno delle locali realtà economico-imprenditoriali.

Nel contesto delineato è altresì emersa l'operatività di una "cassa comune", utilizzata dai sodalizi foggiani per far fronte alle esigenze di liquidità connesse al cd. welfare mafioso, specie per quanto attiene alle spese legali e al mantenimento delle famiglie dei detenuti. La cassa verrebbe alimentata, tra l'altro, con i proventi delle citate attività estorsive, nonché con le risorse derivanti da una "contribuzione" imposta anche ai gruppi criminali minori, presenti nel contesto territoriale in parola.

Inoltre, per la sua posizione a ridosso della sponda balcanica, la regione ha continuato a rappresentare snodo strategico per le organizzazioni criminali impegnate nei traffici via mare, siano esse le consorterie "storiche" dedite al narcotraffico così come le aggregazioni di più recente emersione, specializzatesi nel settore dell'immigrazione clandestina.

Nel contempo, non sono mancate indicazioni concernenti fattispecie di riciclaggio e reimpiego dei capitali illeciti, anche in contesti di proiezione extraregionale, nonché sinergie con altri sodalizi, specie riconducibili alla criminalità organizzata calabrese ed albanese, funzionali al traffico di sostanze stupefacenti.

Le matrici criminali straniere

Il monitoraggio informativo non ha mancato di riguardare, altresì, le organizzazioni criminali di matrice etnica attive in territorio nazionale in un ampio novero di settori dell'illecito. Le più ricorrenti acquisizioni hanno riguardato le **formazioni nigeriane** che, fortemente incise dall'azione di contrasto, restano la componente criminale straniera più strutturata, ramificata e pervasiva.

Attraversati da processi di riorganizzazione interna e momenti di aspra contrapposizione per la ripartizione degli ambiti operativi, i sodalizi nigeriani hanno conservato pronunciato dinamismo in contesti "tradizionali", quali il traffico internazionale di stupefacenti e il favoreggiamento dell'immigrazione clandestina, ivi comprese le connesse fattispecie di falso documentale e sfruttamento della prostituzione. Nel contempo, a testimonianza della loro crescita organizzativa, si sono evidenziati sempre più per il coinvolgimento in pratiche di evasione fiscale e riciclaggio, articolate frodi informatiche e per il trasferimento, attraverso piattaforme finanziarie online, di ingenti somme nei Paesi di origine, in alternativa ai più tradizionali metodi basati su money transfer informali gestiti all'interno dei cc.dd. african shop.

I **sodalizi cinesi**, inclini al compimento di reati ai danni dell'erario e al reinvestimento di proventi illeciti nei circuiti legali, hanno continuato a mostrare una significativa presenza nei settori della logistica e dei trasporti, della ristorazione etnica, del gioco e delle scommesse, nonché della ricezione alberghiera, quest'ultima con l'obiettivo di sfruttare, in prospettiva, le opportunità offerte dalla domanda turistica proveniente dalla Cina in direzione del nostro Paese.

Le **organizzazioni criminali dell'Est Europa** si sono evidenziate, tra l'altro, per operazioni di riciclaggio internazionale, con particolare predilezione per il settore del gioco. Traffico di sostanze stupefacenti, favoreggiamento dell'immigrazione clandestina e furti in appartamento sono rimasti, inoltre, ambiti prioritari d'intervento per agguerriti sodalizi albanesi.

Le **aggregazioni delinquenziali sudamericane**, dal marcato profilo gangsteristico, hanno fatto registrare accesi contrasti interni per il controllo delle piazze di spaccio e tentativi di riorganizzazione, a seguito di operazioni di polizia che ne hanno scompaginato gli assetti.

PAGINA BIANCA

EVERSIONE ED ESTREMISMI

in breve

- Flessione delle mobilitazioni di piazza ma incremento dell'attivismo estremista in rete
- Inedita convergenza propagandistica tra diversi attori dell'oltranzismo politico
- Accentuata trasversalità dei temi, tutti correlati in maniera strumentale alla pandemia
- Persistente aggressività dell'anarco-insurrezionalismo
- Crescita esponenziale nella divulgazione online di proclami antisistema, propositi violenti e teorie cospirative

L'attività informativa, che nel contesto della minaccia eversiva trova un ambito "tradizionale" di impegno, ha dovuto misurarsi con uno scenario inedito e in rapidissima evoluzione, che ha richiesto costanti e tempestivi aggiornamenti sul piano della ricerca e dell'analisi.

Se, da un lato, l'emergenza pandemica ha limitato le potenzialità mobilitative dell'estremismo politico, dall'altro ha fatto da volano, in concomitanza con il ruolo aggregante e amplificatorio del web, ad una montante effervescenza propagandistica, che ha trasversalmente interessato anarco-insurrezionalisti, marxisti-leninisti, realtà del movimento antagonista e circuiti della destra radicale impegnati, pur con intensità variabile e nelle diverse, specifiche prospettive, a strumentalizzare la crisi sanitaria – e segnatamente il suo impatto emotivo, sociale ed economico – per rilanciare progettualità conflittuali e istanze antisistema.

Nel vivo di una fase che in molti Paesi europei ha fatto registrare proteste – talvolta sfociate in incidenti ed episodi di guerriglia urbana – contro le misure di contenimento del virus adottate dai Governi, anche l'Italia è stata interessata, in ottobre, da manifestazioni con derive violente, che hanno visto una partecipazione eterogenea. Si sono infatti evidenziati negli scontri, oltre che militanti di matrice oltranzista, anche frange ed individualità non connotate ideologicamente – inclusi giovani contigui alla criminalità comune – prive, secondo quanto emerso sul piano informativo, di una regia unitaria, ma accomunate da slanci ribellistici condivisi e alimentati online.

L'anarco-insurrezionalismo

Le evidenze raccolte dall'Intelligence nel 2020, sistematicamente condivise con le Forze di polizia, fanno stato di come l'anarco-insurrezionalismo resti la com-

ponente eversiva endogena più vitale.

Le misure governative di contenimento del contagio – che limitando gli spostamenti hanno verosimilmente concorso alla flessione nel numero complessivo delle "azioni dirette" di matrice anarchica – hanno rappresentato per l'area spunto ulteriore di attivazione, nel contesto di una propaganda geneticamente protesa ad alimentare spinte ribelliste ed antiautoritarie.

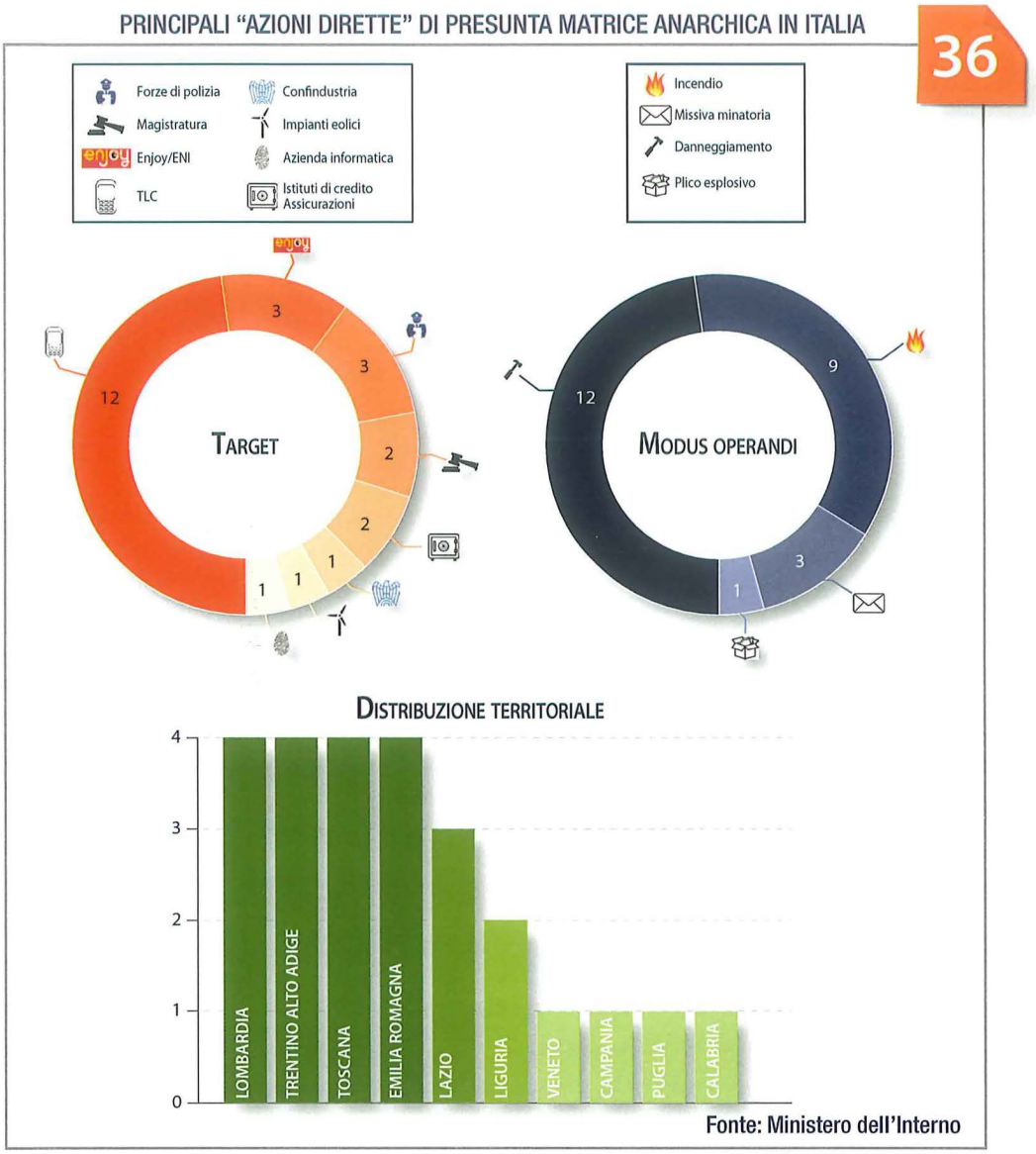
In questo senso, sono stati intensificati sul web i messaggi istigatori contro la "militarizzazione" del territorio e l'asserita volontà dello Stato di enfatizzare la pericolosità del virus per promuovere il "controllo sociale". Sono nati nuovi siti, attraverso i quali incitare alla "rivolta" e alla violazione dei divieti imposti dalle Autorità, fornire suggerimenti operativi e lanciare attacchi alle Forze di polizia.

Il tema di fondo è rimasto la lotta alla "repressione" che – nella articolata interpretazione tipica dell'anarco-insurrezionalismo – non ha mancato di connettere l'emergenza pandemica all'era di un moderno "capitalismo della sorveglianza", coniugandosi con la campagna contro le tecnologie. Al riguardo, seppure in linea di continuità con il 2019, ha trovato nuova linfa, anche a livello internazionale, la mobilitazione contro la rete 5G, annoverando tra l'altro, in coerenza con la prassi insurrezionalista, documenti recanti circostanziate indicazioni anche per quel che attiene ai potenziali obiettivi, come la mappatura delle antenne 5G sul territorio nazionale. Tralicci e ripetitori, reti in fibra ottica, sistemi di videosorveglianza e aziende specializzate in tecnologie digitali sono diventati, quindi, target privilegiati della campagna contro il "capitalismo digitale" e le "nocività".

Alla propaganda hanno corrisposto sortite operative (vds. tavola n. 36), consistenti perlopiù in atti vandalici e/o incendiari e sabotaggi, ai danni soprattutto d'infrastrutture delle telecomunicazioni (come l'incendio, il 29 aprile a Roma, dei cavi di un'antenna di una compagnia telefonica nazionale e il sabotaggio, tra il 14 e il 15 maggio a Rovereto-TN, di centraline della fibra ottica che ha provocato il temporaneo blocco della rete). Nella medesima ottica antirepressiva si collocano i danneggiamenti di istituti bancari ed assicurativi, strutture o automezzi di Polizia locale e veicoli in car sharing riferibili all'ENI che, per la maggior parte, sono stati rivendicati, nel segno della lotta allo Stato e alle "tecnologie del controllo", in "solidarietà ai compagni prigionieri". Temi, questi, che sul versante estero hanno animato anche l'attivismo di componenti insurrezionaliste europee e sudamericane, specie messicane e cilene, di cui l'attività informativa ha confermato i legami con le compagini nazionali.

Entro i nostri confini, il sostegno agli anarchici inquisiti o processati ha, del resto, continuato a rappresentare motivo ricorrente di mobilitazioni e "azioni dirette", a fronte di un'attività di contrasto che anche nel 2020 ha fatto registrare importanti operazioni di polizia e sviluppi giudiziari, tra i quali l'emissione, in novembre, della sentenza di condanna a conclusione del processo d'appello a carico di alcuni militanti riferibili alla Federazione Anarchica Informale/Fronte

EVERSIONE ED ESTREMISMI



Rivoluzionario Internazionale - FAI/FRI (vds. tavola n. 37).

Proprio l'insurrezionalismo a marchio FAI/FRI, con la sigla "Nucleo Mikhail Zhlobitsky" (giovane anarchico russo responsabile, nell'ottobre 2018, di un'azione esplosiva suicida all'interno di una sede dell'Intelligence russa) ha rivendicato, con uno scritto diffuso su siti d'area, l'invio, a settembre, di due plichi esplosivi: l'uno, aperto, ma non deflagrato, ai danni del Presidente dell'Associazione Industriale Bresciana; l'altro, mai giunto a destinazione, al Sindacato Autonomo della Polizia Penitenziaria di Modena. Il gesto ha dichiaratamente inteso colpire il "sindacato dei padroni" e sostenere le agitazioni della popolazione carceraria connesse all'emergenza pandemica.

37

LE OPERAZIONI "RITROVO" E "BIALYSTOK"

L'attività di contrasto nei confronti dell'anarco-insurrezionalismo ha fatto registrare due importanti operazioni di polizia giudiziaria: la prima, denominata "Ritrovo", del 13 maggio, ha colpito alcuni anarchici del circuito bolognese, accusati, tra l'altro, di aver incendiato un ponte ripetitore di reti televisive; la seconda, "Bialystok", del 12 giugno, ha portato all'esecuzione di alcune misure cautelari nei confronti di militanti riconducibili all'area libertaria romana più radicale, ritenuti responsabili di partecipazione ad un'associazione con finalità di terrorismo o di eversione dell'ordine democratico nonché di varie "azioni dirette", tra cui quella perpetrata, il 7 dicembre 2017, ai danni di una stazione dei Carabinieri di Roma con l'utilizzo di un ordigno esplosivo ad alto potenziale. Attentato, quest'ultimo, rivendicato con la sigla "FAI/FRI - Cellula Santiago Maldonado", riferibile al cartello terroristico/eversivo "Federazione Anarchica Informale", il cui ideologo – già detenuto per il ferimento, nel 2012, dell'allora AD di Ansaldo Nucleare – il 24 novembre è stato condannato a 20 anni di reclusione all'esito del processo d'appello "Scripta Manent", per essere stato riconosciuto tra i promotori della predetta organizzazione, oltre che responsabile di alcuni attentati effettuati con più ordigni esplosivi a deflagrazione differita.

Anche nella sua dimensione movimentista, l'area ha trovato occasioni d'intervento sul tema anticarcerario, organizzando presidii di protesta in occasione dei tumulti che sono esplosi in marzo all'interno di diversi penitenziari nazionali. Analoghe iniziative sono state poi intraprese nei pressi di vari Centri di Permanenza per il Rimpatrio-CPR, in solidarietà con gli stranieri irregolari colà trattenuti. Inoltre, soggetti riferibili all'area anarco-insurrezionalista hanno partecipato ad alcune manifestazioni di protesta, anche violente, svoltesi in ottobre in varie città italiane, contro le misure anti-contagio adottate dal Governo.

È proseguito, altresì, l'impegno delle frange libertarie sul tema dell'antimilitarismo, con campagne contro aziende del settore della difesa e nei confronti di taluni istituti bancari ritenuti colpevoli di finanziare l'"industria delle armi", nonché su quello dell'opposizione alle cc.dd. grandi opere, con rinnovati tentativi d'infiltrazione nelle proteste ambientaliste, come testimoniato dalla diffusione online, in ottobre, di un documento volto a rilanciare la mobilitazione contro la costruzione del gasdotto SNAM lungo la dorsale adriatica, prosecuzione del progetto salentino TAP.

I circuiti marxisti-leninisti

La propensione a sfruttare la sensibile congiuntura a fini propagandistici ha caratterizzato anche i ristretti ambienti dell'oltranzismo marxista-leninista, che hanno intensificato le attività di divulgazione delle teorie rivoluzionarie.

Con l'intento di far proseliti, tali circuiti si sono infatti impegnati tanto nella tradizionale opera di recupero della memoria brigatista, mediante pubblicazioni e documenti redatti da ex militanti, quanto in interventi tesi ad attualizzarne il messaggio attraverso l'analisi, in ottica di "contrapposizione di classe", delle ricadute socio-economiche dell'emergenza pandemica. Ricadute che, nella visione

che contraddistingue il settore in parola, sarebbero da imputare unicamente ad una crisi sistemica del "potere capitalista" e "imperialista".

Nella medesima chiave, l'interesse dell'area ha continuato ad appuntarsi sul mondo del lavoro e segnatamente su quei settori occupazionali maggiormente gravati da precarietà e tensioni, con l'obiettivo, velleitario, di conferire alle contingenti rivendicazioni delle maestranze una valenza politico-ideologica di più lungo periodo. Analoghi tentativi di strumentalizzazione in chiave oltranzista, anch'essi rimasti senza seguito, sono stati rilevati con riguardo a specifiche istanze relative alla questione della tutela della salute e della sicurezza sui luoghi di lavoro.

In linea con la tendenza degli ultimi anni, non sono mancati ambiti di tangenza con altre realtà oltranziste, in ragione del comune impegno su tematiche trasversali a diverse componenti del fronte antisistema.

È il caso della propaganda d'area contro la "repressione" e il cd. carcere duro, da tempo prioritariamente focalizzata sulla permanenza di ex brigatisti nel regime detentivo del 41 bis, che non ha mancato – in analogia con gli interventi dell'anarco-insurrezionalismo – di inneggiare alle citate rivolte che, nel vivo della prima ondata epidemica, hanno riguardato diversi istituti di pena.

Più sostanziali le "aperture" verso settori dell'antagonismo di sinistra. Al riguardo, oltre alle convergenze sul versante lavoristico, le evidenze informative hanno confermato come l'attivismo marxista-leninista abbia cercato di raggiungere un uditorio più vasto, promuovendo e sviluppando approfondimenti su temi ritenuti di forte presa, quali l'"antimilitarismo" e l'"antifascismo".

Sono poi proseguite, soprattutto sul web, le iniziative di sostegno ad omologhi circuiti esteri impegnati in iniziative di solidarietà ai "detenuti politici" ristretti in altri Paesi, alla "resistenza palestinese", alla "lotta del popolo curdo", nonché all'opposizione maoista in Turchia.

Da evidenziare, infine, come il brigatismo abbia continuato a rappresentare un riferimento di pronunciata valenza simbolica con riguardo a taluni episodi intimidatori registratisi nel corso dell'anno, in cui logo e lessico dell'area sono stati strumentalmente mutuati per conferire enfasi e risonanza mediatica a gesti di protesta contro le restrizioni anti-contagio imposte dalle Autorità nazionali e locali.

Il movimento antagonista

Il monitoraggio intelligence in direzione del composito fronte antagonista ha rilevato come l'emergenza pandemica e, più in particolare, la gestione della crisi da parte del Governo abbiano costituito i temi centrali di un ampio dibattito che ha coinvolto le diverse "anime" del dissenso, in un'ottica di rilancio delle tradizionali campagne di lotta e, nello stesso tempo, di superamento dell'endemica frammentazione che affligge da tempo il movimento.

La propaganda d'area ha cercato, dunque, di accreditare l'inedita contingenza quale occasione favorevole a progettualità aggregative, attraverso una nar-

razione antisistema che ha, tra l'altro, strumentalmente connesso la diffusione del virus con il progresso tecnologico e i cambiamenti climatici.

È in tale contesto che, all'indomani del primo lockdown nazionale, si è registrata una ripresa sul territorio delle iniziative che, muovendo dalla tematica ecologista, si sono progressivamente declinate, sulla scia di omologhe mobilitazioni internazionali, anche in chiave anticapitalista e no-global.

Direttamente collegate al filone ambientalista sono state anche le critiche al cd. decreto semplificazione, accusato dagli antagonisti di agevolare la realizzazione delle "grandi opere inutili e dannose". Tema, quest'ultimo, dalla persistente capacità propulsiva per frange di diversa matrice che, come di consueto specie nei mesi estivi, hanno rivitalizzato la campagna No TAV con assalti ai cantieri valsusini e scontri con le Forze dell'ordine.

È proseguito, inoltre, l'attivismo antimilitarista, nel cui ambito sono state riproposte le argomentazioni sulle asserite ricadute, in termini di tagli al welfare, degli investimenti pubblici destinati alla difesa, con l'organizzazione di iniziative di protesta, specie nei territori con una maggiore presenza di siti militari.

Non è mancato, infine, il tradizionale impegno antagonista sul terreno dell'"antifascismo militante" e dell'opposizione alla gestione della questione migratoria, nel tentativo di sfruttare, in funzione aggregante e con fini di proselitismo, l'impatto della mobilitazione statunitense contro il razzismo animata dal movimento Black Lives Matter.

La destra radicale

Massima attenzione informativa, sul piano della ricerca e dell'analisi, è stata riservata ai circuiti della destra radicale, anche nella dimensione virtuale, nel cui ambito, in relazione alla pandemia, sono proliferate campagne di disinformazione e teorie cospirative, accompagnatesi a retoriche ultranazionaliste, xenofobe e razziste, nonché ad interventi propagandistici dagli accesi toni antisistema.

Le principali formazioni dell'estrema destra, alle prese con i cronici dissidi interni e disegni evolutivi, hanno seguìto con interesse gli sviluppi dell'emergenza sanitaria, nel tentativo di sfruttare il tema del disagio economico correlato alla crisi e guadagnare consensi tra le categorie sociali più in difficoltà, con riguardo soprattutto ai cittadini delle periferie urbane.

Tali ambienti, particolarmente attivi nella promozione d'iniziative pubbliche contro il Governo, ritenuto colpevole di aver imposto alla popolazione una sorta di "dittatura sanitaria", hanno tentato di coinvolgere nelle mobilitazioni anche gruppi di protesta spontanei e realtà delle tifoserie ultras. Un fervore contestativo, questo, che ha concorso ad animare le richiamate manifestazioni di ottobre, caratterizzatesi per l'inedita commistione di istanze e pulsioni ribelliste di vario segno.

La propaganda delle compagini più strutturate ha, altresì, riproposto i tradizionali dogmi identitari, ribadendo indirizzi teorici di ferma opposizione alla UE e

alla NATO, evidenziando, nel contempo, accentuate posizioni anti-globalizzazione, come testimoniato dalla promozione, in occasione delle festività natalizie, di campagne di boicottaggio degli acquisti online e delle multinazionali dell'e-commerce.

Quanto al mondo skinhead, d'ispirazione marcatamente nazi-fascista e antisemita, si è continuato a registrare l'attivismo di formazioni interessate a perseguire un progetto aggregativo delle diverse e frammentate realtà d'area.

In linea di continuità con gli anni precedenti, l'Intelligence ha, inoltre, seguito con attenzione l'attivismo di componenti estere dell'ultradestra, in relazione ad un contesto nel quale la contingenza legata alla pandemia ha fatto registrare un rinnovato slancio dei circuiti suprematisti – attivi soprattutto negli USA, ma anche in Europa continentale – che propugnano, in chiave "accelerazionista", il collasso del sistema occidentale ritenuto corrotto.

L'intensificazione della propaganda di stampo razzista e xenofobo attraverso piattaforme online e social media, unitamente al proliferare di teorie complottiste e messaggi dal contenuto violento e nichilista, ha richiesto un mirato impegno informativo inteso a coglierne eventuali seguiti e proseliti in ambito nazionale (vds. tavola n. 38). Ciò, a fronte dei rischi connessi alla possibile influenza di tali teorie sulle progettualità di frange e micro-gruppi, ma anche sui più invisibili e imprevedibili processi individuali di radicalizzazione.

38

IL MEGAFONO VIRTUALE DELL'ESTREMA DESTRA

Come per il terrorismo jihadista, anche per l'ultradestra filo-nazista la propaganda circolante su web, social network, chat e piattaforme di messaggistica ha concorso ad alimentare il fenomeno dell'estremismo violento e a favorire percorsi di radicalizzazione tra comunità di utenti sempre più estese e meno relegabili agli specifici ambienti di riferimento.

Sono numerosi ed in continua evoluzione i contenitori online in cui anche soggetti privi di specifico background ideologico, tra cui molti giovani affascinati dalla "gaming culture", possono indottrinarsi ed attingere ad un coacervo di teorie e pseudo-ideologie, spesso interconnesse, che propugnano il ricorso alla violenza indiscriminata. In tali circuiti è possibile trovare, in maniera più o meno esplicita, narrative razziste, omofobe ed antisemite, ispirate al suprematismo bianco, all'esoterismo nazista e alle svariate teorie del complotto. Tra queste ultime, figura la statunitense "QAnon", assurta alla ribalta mediatica dopo la partecipazione di suoi seguaci all'assalto a Capitol Hill del 6 gennaio 2021.

PAGINA BIANCA

2020 DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO
AI SENSI DELL'ART. 38, COMMA 1 BIS, LEGGE 124/2007

DOCUMENTO DI SICUREZZA NAZIONALE

SOMMARIO

DOCUMENTO DI SICUREZZA NAZIONALE

INTRODUZIONE

Nel corso del 2020 l'ampio ricorso al telelavoro, dettato dall'insorgenza della pandemia, ha enfatizzato ancora di più l'importanza di poter contare su reti di informazione e comunicazione sicure quale prerequisito essenziale per la regolare fornitura dei servizi pubblici, nonché per lo svolgimento delle attività economiche fondamentali e della vita dei cittadini, già duramente impattate dalla situazione contingente.

In questo senso, il progressivo rafforzamento dell'architettura nazionale di sicurezza cibernetica perseguito dal 2018 ad oggi ha mirato ad accrescere la resilienza cyber del Paese, garantendo, al contempo, unicità di indirizzo e un alto livello di coordinamento attraverso un approccio univoco a una materia complessa e trasversale a diversi settori e realtà.

Al raggiungimento di tale traguardo hanno contribuito specifiche misure normative, che hanno attribuito al Comparto Intelligence un ruolo centrale nell'ecosistema cyber nazionale. Al netto dei profili strettamente intelligence – nel cui contesto è stato a suo tempo previsto il coordinamento delle attività di ricerca di AISE ed AISI (legge n. 133/2012) e per i quali si rimanda al corpo della Relazione, capitolo MINACCIA CIBERNETICA – vale ricordare l'istituzione, presso il DIS, del Nucleo per la Sicurezza Cibernetica-NSC (DPCM 17 febbraio 2017), del Computer Security Incident Response Team (CSIRT) italiano (DPCM 8 agosto 2019 in attuazione del decreto legislativo n. 65/2018 di recepimento della Direttiva UE NIS) e del punto di contatto unico NIS (il già citato D.Lgs. n. 65/2018). A ciò si è aggiunta, più di recente, l'assegnazione di funzioni di raccordo con le Autorità competenti e con i soggetti inclusi nel "Perimetro di sicurezza nazionale cibernetica", nonché di supporto al Presidente del Consiglio nell'implementazione di tale disciplina (D.L. n. 105/2019 convertito, con modificazioni, nella legge n. 133/2019).

Molteplici sono, pertanto, i compiti assegnati dal citato sostrato giuridico, con una conseguente proiezione delle attività in diversi ambiti di intervento che vanno – in sinergia con gli attori interessati dell'ecosistema nazionale cyber – dall'elaborazione delle policy in materia di cybersecurity e dei contributi per la definizione di atti sovranazionali alla gestione delle crisi cyber, dallo svolgimento delle attività dello CSIRT alla realizzazione di analisi tecniche a supporto della sua operatività, per concludere con la promozione di nuove progettualità in materia di innovazione digitale, volte a far sì che l'evoluzione tecnologica dell'Italia sia al passo con gli altri Paesi, in particolare europei, e tenga in debita considerazione gli aspetti di cybersecurity.

Al fine, pertanto, di fornire una compiuta panoramica delle iniziative e delle attività poste in essere in tema di protezione delle infrastrutture critiche, protezione cibernetica e sicurezza informatica, è stato elaborato il presente Documento di Sicurezza Nazionale (DSN), che – ai sensi dell'art. 38, comma 1 bis, della legge

Architettura nazionale di sicurezza cibernetica

Architettura nazionale cyber (DPCM 17.2.2017)

- NSC composizione ordinaria
- NSC composizione in caso di crisi
- Collaborazione funzionale

Direttiva NIS (D.Lvo 65/2018)

- Attori NIS
- OSE Comitato tecnico di raccordo
- FSD Operatori di Servizi Essenziali
- * Fornitori di Servizi Digitali
- Più regioni e province autonome di Trento e Bolzano

Decreto «Telco» (12.12.2018)

Decreto CSIRT (DPCM 8.8.2019)

L 133/2019 Perimetro di Sicurezza Nazionale Cibernetica

- Misure di sicurezza
- Notifiche incidenti
- Verifiche al procurement ICT

Per amministrazioni pubbliche, enti e operatori nazionali, pubblici e privati che esercitano funzioni/servizi essenziali per la sicurezza nazionale

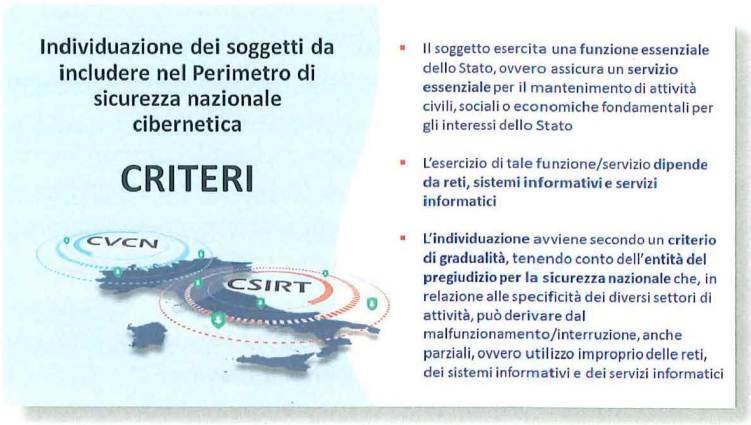
CISR - Comitato Interministeriale per la Sicurezza della Repubblica
CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
COR - Comando per le Operazioni in Rete
CSIRT - Computer Security Incident Response Team
CVCN - Centro di Valutazione e Certificazione Nazionale
NSC - Nucleo per la Sicurezza Cibernetica

n. 124/2007 – viene allegato alla Relazione sulla politica dell'informazione per la sicurezza, riferita al 2020.

EVOLUZIONE DELLE POLICY CYBER A LIVELLO NAZIONALE E INTERNAZIONALE

L'attuazione del Perimetro di sicurezza nazionale cibernetica

L'iniziativa, promossa dal Comparto, che meglio rappresenta gli sforzi profusi dal Paese sotto il profilo delle policy cyber, è sicuramente quella del "Perimetro di sicurezza nazionale cibernetica". Si tratta di un provvedimento che, è bene ricordare, prevede – per la prima volta – oltre a obblighi quali il rispetto di stringenti misure di sicurezza e la notifica degli incidenti, anche specifiche disposizioni in materia di forniture di beni, sistemi e servizi ICT, appartenenti a determinate categorie, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici utilizzati dai soggetti inclusi nel Perimetro per l'esercizio della funzione/servizio essenziale per la sicurezza nazionale ("beni ICT perimetro").



OBBLIGHI IN CAPO AI SOGGETTI PERIMETRO

- Notifica degli incidenti aventi impatto sui "beni ICT perimetro", così da assicurare un immediato flusso di informazioni a favore delle strutture deputate alla prevenzione, preparazione e gestione degli eventi cibernetici (in particolare NSC e CSIRT, entrambi incardinati nel DIS).
- Adozione di misure di sicurezza per i "beni ICT perimetro" relative a organizzazione, processi e procedure, anche in relazione al procurement ICT.
- Screening tecnologico degli approvvigionamenti ICT appartenenti a categorie specifiche, destinati ai "beni ICT perimetro". La procedura prevede che il soggetto che intenda procedere a tali acquisizioni ne dia comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN, operante presso il Ministero dello Sviluppo Economico) che, entro un massimo di 60 giorni, può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software (questi ultimi devono essere conclusi nel termine di ulteriori 60 giorni). Tali attività sono svolte dai Centri di Valutazione (CV) dei Ministeri dell'Interno e della Difesa – in stretta sinergia con il CVCN – per le forniture di beni, sistemi e servizi ICT da impiegare sulle rispettive reti, sistemi e servizi informatici.

Al riguardo, se il 2019 è stato caratterizzato dalla definizione dell'atto normativo e dal relativo iter parlamentare che ha condotto alla sua adozione, il 2020 si è connotato per l'elaborazione dei relativi decreti attuativi. Nel novembre 2019 il Comitato Interministeriale per la Sicurezza della Repubblica (CISR) aveva infatti assegnato al Comparto Intelligence il ruolo di coordinare l'implementazione del Perimetro, attraverso la costituzione di 6 gruppi di lavoro e relativi sottogruppi. Ciò ha portato, a seguito di una complessa e articolata attività di coordinamento interministeriale, con il determinante apporto del Dipartimento per gli Affari Giuridici e Legislativi della Presidenza del Consiglio, concretizzatasi in oltre 150 riunioni nell'arco del 2020: all'adozione del DPCM n. 131/2020 per la definizione dei criteri per l'identificazione dei soggetti da includere nel Perimetro e di quelli per l'individuazione dei relativi "beni ICT perimetro"; alla predisposizione del DPCM (in fase avanzata di approvazione) per la definizione delle modalità di notifica degli incidenti e delle misure di sicurezza, comprese quelle sul procurement ICT; all'elaborazione del Regolamento – approvato in via definitiva dal Consiglio dei Ministri il 29 gennaio 2021 – relativo alle ispezioni e alle modalità di scrutinio tecnologico da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei CV; alla stesura del DPCM contenente le categorie di prodotti ICT da sottoporre alle valutazioni del CVCN e dei CV in fase di procurement da parte dei soggetti perimetro, esaminato dal CISR a fine novembre 2020; alla definizione del DPCM relativo all'accreditamento e ai raccordi tra CVCN, CV e laboratori.

Nel citato DPCM n. 131/2020, in attuazione del criterio di gradualità contemplato dal D.L. n. 105/2019, sono stati definiti 11 settori di attività, all'interno dei quali devono essere poi individuati i soggetti da includere nel Perimetro. Il 25 novembre 2020, su proposta del CISR, previa indicazione da parte delle Amministrazioni competenti, è stato, pertanto, adottato dal Presidente del Consiglio dei Ministri l'atto – non soggetto a pubblicazione e per il quale è escluso il diritto di accesso – contenente l'elencazione dei soggetti inclusi nel Perimetro ai quali, come previsto, il DIS ha dato la relativa comunicazione, il 22 dicembre. Alla luce di quanto descritto, da giugno 2021 inizierà, quindi, l'operatività del "sistema Perimetro", specie in materia di notifiche di incidenti cibernetici.

L'implementazione della Direttiva NIS

Il DIS, in veste di punto di contatto unico NIS, ha assicurato gli opportuni raccordi con le Autorità competenti NIS, attraverso riunioni plenarie bimestrali

e costanti interazioni bilaterali. In queste occasioni sono state oggetto di esame tanto l'attuazione della Direttiva NIS in Italia (ad esempio per quel che concerne la definizione delle attività di ispezione e di verifica, nonché il livello di maturità raggiunto dagli operatori di servizi essenziali-OSE nell'applicazione delle misure di sicurezza), quanto le iniziative europee in materia, in particolare nell'ambito del Gruppo di Cooperazione NIS (NISCG), in cui i Paesi Membri si confrontano su aspetti concernenti l'implementazione della Direttiva. In questo contesto, sono state, altresì, assicurate sinergie con l'Ufficio del Consigliere Militare del Presidente del Consiglio dei Ministri, punto di contatto italiano del programma europeo di protezione delle infrastrutture critiche, nelle attività propedeutiche alla revisione della Direttiva UE 114/2008 sulle Infrastrutture Critiche Europee (ICE), al fine di garantire l'armonizzazione delle due normative, evitando in tal modo eventuali accresciuti oneri per gli operatori. Analogamente, di stretta intesa con il Ministero dell'Economia e delle Finanze, si è proceduto rispetto all'avvio delle negoziazioni a livello UE relative alla proposta di Regolamento sulla resilienza operativa digitale per il settore finanziario ("DORA").

Il DIS partecipa in rappresentanza del nostro Paese alle attività del NISCG, nel cui ambito nel corso dell'anno è stato, tra l'altro, affrontato l'avvio del processo di revisione della Direttiva NIS (la cd. NIS 2), rispetto alla quale, operando in stretto coordinamento con le Autorità NIS italiane, sono state presentate delle proposte volte ad incrementarne l'efficacia.

Autorità competenti NIS nazionali	Ambito di competenza
Ministero dello Sviluppo Economico	Settore energia
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle Infrastrutture e dei Trasporti	Settore trasporti
Ministero dell'Economia e delle Finanze in collaborazione con Banca d'Italia e Consob	Settore bancario
	Settore infrastrutture dei mercati finanziari
Ministero della Salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'Ambiente e della Tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore fornitura e distribuzione di acqua potabile

Il NISCG, sulla base del programma biennale di lavoro, attiva dei gruppi di lavoro (Work Stream) dedicati all'approfondimento di specifiche tematiche (seguiti direttamente dal DIS), ovvero concernenti i settori di attività sottoposti alla Direttiva NIS (ai quali partecipano le Autorità competenti NIS nazionali, in stretta intesa con il DIS).

Work Stream NIS Cooperation Group

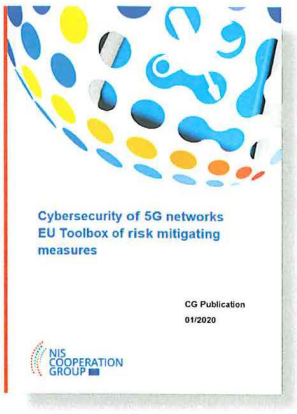
OGGETTO	AMMINISTRAZIONE NAZIONALE COINVOLTA	OBIETTIVI
Gestione incidenti e crisi cibernetiche su vasta scala a livello UE	DIS (co-leader)	Definizione e implementazione del progetto Cyber Crisis Liaison Organisation Network (CyCLONe) e delle relative procedure di funzionamento. 29 settembre 2020 lancio di CyCLONe
5G	DIS (co-leader) e Min. dello Sviluppo Economico	Implementazione della Raccomandazione della Commissione 2019/534 in materia di sicurezza cibernetica delle reti 5G. Predisposizione e implementazione del Toolbox europeo e stesura dei relativi report di attuazione
Misure di sicurezza per gli operatori di servizi essenziali	DIS	Aggiornamento delle linee guida sulle misure di sicurezza per gli operatori di servizi essenziali
Notifiche di incidente	DIS	Revisione del meccanismo di notifica degli incidenti NIS e predisposizione Annual Summary Report
Fornitori di Servizi Digitali	Min. Sviluppo Economico	Attività di implementazione della Direttiva NIS negli specifici settori e armonizzazione con le normative settoriali Condivisione di casi d'uso e best practice di cybersecurity Raffinamento dei criteri e delle soglie per la notifica degli incidenti e per l'identificazione degli operatori di servizi essenziali
Settore energetico		
Settore infrastrutture digitali		
Settore sanitario	Min. Salute	
Sotto-settore trasporto aereo - Aviazione civile	Min. Infrastrutture e Trasporti	

In particolare, é stata assunta la guida dei Work Stream su:

- "Gestione di incidenti e crisi cibernetiche su vasta scala a livello UE", in raccordo con l'Agenzia francese per la sicurezza dei sistemi informatici (ANSSI), nel cui contesto è stato definito il progetto Cyber Crisis Liaison Organisation Network (CyCLONe) di gestione degli incidenti e delle crisi cibernetiche su larga scala di cui alla Raccomandazione della Commissione 2017/1584 (cd. Blueprint);
- 5G, insieme a Belgio, Estonia, Francia, Olanda, Repubblica Ceca e Svezia, coadiuvati dalle Presidenze di turno del Consiglio dell'UE, per l'implementazione della Raccomandazione della Commissione 2019/534 in materia di sicurezza cibernetica delle reti 5G.

Nel NISCG è stata anche effettuata una disamina dei rischi cyber correlati alla pandemia e alle applicazioni di tracciamento dei contatti dei cittadini con soggetti risultati positivi al Covid-19 adottate dai diversi Stati Membri, al fine di assicurarne l'interoperabilità, la sicurezza cibernetica, nonché la protezione dei dati personali trattati.

Sviluppo delle reti di nuova generazione (5G)



Costante è stata, al riguardo, l'attenzione della Commissione europea rispetto alla sicurezza delle reti 5G degli Stati Membri. In tale ambito, in continuità con le iniziative avviate con la citata Raccomandazione del 26 marzo 2019, il NISCG ha adottato il Toolbox delle misure di sicurezza, pubblicato il 29 gennaio 2020.

Di concerto con il Ministero dello Sviluppo Economico (MiSE), sin dalle fasi preparatorie, sono stati forniti contributi determinanti alla stesura del documento. Il Toolbox contiene una serie di misure strategiche e tecniche, nonché azioni di supporto destinate, su base volontaria, agli Stati Membri al fine di promuovere un approccio armonizzato alla sicurezza delle reti 5G. Al riguardo, l'Italia non si è limitata ad uniformarsi alle citate linee guida, ma le ha recepite all'interno dell'ordinamento giuridico nazionale. Attraverso il cd. Decreto liquidità (D.L. n. 23/2020, convertito dalla legge n. 40/2020), la disciplina sul Golden Power (D.L. n. 21/2012 convertito, con modificazioni, dalla legge n. 56/2012) è stata, infatti, emendata prevedendo un richiamo alle linee guida europee, e quindi al Toolbox, quale riferimento per il processo istruttorio delle notifiche relative all'acquisto di tecnologia 5G da fornitori extra-europei.

Tale aspetto è stato evidenziato nel Report sull'implementazione del Toolbox da parte degli Stati Membri, pubblicato nell'ottobre 2020, nel quale l'Italia è stata citata quale esempio, insieme a pochi altri Paesi. In particolare, con rife-

rimento alla misura relativa alle restrizioni nei confronti dei fornitori "ad alto rischio", l'attuale impianto normativo (Golden Power, Perimetro di sicurezza nazionale cibernetica e Decreto MiSE del 12 dicembre 2018, cd. Decreto Telco) consente al nostro Paese di monitorare i contratti stipulati con fornitori extra-europei e, con il perfezionamento dei decreti attuativi del Perimetro, affiderà al CVCN il compito di condurre le opportune verifiche tecniche sulla presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano. Per quel che concerne, poi, la misura di cui al Toolbox sulla diversificazione dei fornitori di sistemi 5G, è stata in particolare richiamata l'applicazione della normativa sul Golden Power a casi specifici in cui, tra le prescrizioni imposte agli operatori, vi è quella relativa all'elaborazione di un piano di diversificazione delle piattaforme tecnologiche della componente "core" della rete 5G.

Sul fronte nazionale è, inoltre, proseguito lo sviluppo delle reti 5G italiane. Al riguardo, l'attenzione del Comparto Intelligence resta alta in merito ai profili di rischio che derivano dai nuovi scenari tecnologici, specie con l'avvento delle reti core 5G in configurazione Stand Alone, che, tramite l'attivazione delle funzioni più avanzate, come la suddivisione logica di risorse di rete fisiche (cd. network slicing), e lo spostamento delle infrastrutture di calcolo verso l'utente finale (cd. edge computing), abiliteranno applicazioni innovative quali le comunicazioni mobili a banda ultra larga, realtà aumentata, veicoli a guida autonoma, chirurgia da remoto, reti di sensori e smart cities e automazione industriale di nuova generazione.

Nel settore delle reti di accesso radio (RAN), il Comparto segue con particolare interesse lo sviluppo di architetture basate su tecnologie aperte, quali l'iniziativa Open RAN, uno standard industriale che definisce i componenti della parte radio e come comunicano tra loro, per favorire una maggiore trasparenza e una diversificazione dei fornitori.

Ulteriori attività in ambito internazionale

Il nostro Paese è coinvolto, specie con riguardo ai negoziati di documenti di policy e atti normativi, in ambito ONU, OSCE, UE, NATO, G7 e G20. Il DIS, in costante raccordo con il Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI), ha assicurato nel corso dell'anno la propria partecipazione a più di cento riunioni a livello multilaterale, dapprima in presenza poi, in ragione della pandemia, in videoconferenza. Al fine, poi, di definire una posizione nazionale condivisa e in grado di tutelare gli interessi dell'Italia, il Dipartimento ha continuato ad attuare, per i profili di diretta competenza, uno stretto coordinamento, oltre che con la Farnesina, con i Dicasteri interessati, in particolare, la Difesa (per i dossier NATO) e il MiSE (specie per i lavori dell'ITU, inclusa la predisposizione del relativo Global Cybersecurity Index).

In sede OSCE, invece, il DIS ha affiancato il MAECI nella conduzione del

periodico Communication Check, organizzato dal Segretariato di quell'organizzazione per accrescere il livello di prontezza dei punti di contatto degli Stati partecipanti, nonché nei costanti aggiornamenti sullo stato di implementazione delle misure di confidence building, volte a prevenire l'insorgenza di possibili conflitti derivanti dall'impiego delle tecnologie ICT.

Di tutto rilievo, inoltre, sono le attività svolte in ambito UE per definire una posizione comune dell'Unione da riversare nei lavori dell'Open Ended Working Group (OEWG) dell'ONU sulle questioni cyber, con l'obiettivo di fornire pieno sostegno ai risultati già conseguiti in materia, in particolare in seno allo UN Group of Governmental Experts (UN GGE), specie con riguardo all'applicabilità delle norme di diritto internazionale alle condotte degli Stati nello spazio cibernetico.

Sempre per quel che concerne gli sforzi profusi dall'UE per rafforzare la resilienza ad attacchi cyber, il DIS ha contribuito, per la parte di competenza, al negoziato, avviato nel 2018 e giunto a termine nel dicembre 2020, della "proposta di Regolamento per la creazione di un Centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di cybersecurity e della rete dei Centri di coordinamento nazionali"(vds. più avanti, riquadro di pag. 24), volta a promuovere la sovranità tecnologica e la leadership dell'UE (e dei suoi Stati Membri) e, conseguentemente, ad accrescerne l'autonomia strategica nel settore e la competitività industriale.

Nell'ambito dei tavoli europei un contributo è stato, altresì, fornito con riguardo a ruolo e funzioni che la futura Joint Cyber Unit – a suo tempo annunciata dal Presidente della Commissione europea von der Leyen e parte integrante della "Strategia dell'UE per la cybersecurity nel decennio digitale", varata il 16 dicembre – andrebbe a svolgere nell'ambito dell'ecosistema cyber dell'Unione, quale strumento volto a coordinare le diverse realtà europee competenti, a vario titolo, in materia di sicurezza cibernetica.

GESTIONE DELLE SITUAZIONI DI CRISI CIBERNETICA

Nucleo per la Sicurezza Cibernetica

A partire dal 2018, il NSC svolge le proprie funzioni riunendosi mensilmente per attività di prevenzione, preparazione, risposta e ripristino rispetto ad eventuali situazioni di crisi cibernetica, con l'obiettivo di rafforzare la resilienza cyber del Paese, con il determinante apporto di AISI, AISE, della Polizia Postale e, ove necessario, del Comando Operazioni in Rete della Difesa.

Oltre alle attività ordinarie, il NSC è stato attivato numerose volte anche nel 2020 per valutare possibili impatti di attacchi cyber sulla sicurezza nazionale e sulla protezione cibernetica – in particolare anche ai danni di strutture italiane di eccellenza impegnate nel fronteggiare l'emergenza pandemica da Covid-19 – e approntare opportune contromisure. Nell'occasione, gli esperti del NSC, avvalendosi delle strutture tecniche preposte, hanno valutato gli episodi registrati provve-

dendo ad allertare la rete sanitaria nazionale allo scopo di innalzare le difese cyber di tali infrastrutture.

Quanto alle attività di prevenzione e preparazione, il NSC ha:

- raccolto, analizzato e disseminato, attraverso lo CSIRT italiano, dati su incidenti e compromissioni di reti e sistemi delle Amministrazioni;
- studiato misure di coordinamento interministeriale;
- proseguito nella predisposizione di attività di formazione quali, ad esempio, i corsi destinati ai dirigenti delle Amministrazioni NSC, anche di fascia apicale;
- promosso e coordinato la partecipazione nazionale ad esercitazioni cyber, tra le quali meritano particolare menzione la pianificazione di esercizi multisettoriali in ambito UE (e.g. Cyber Europe) e NATO (e.g. Crisis Managament Exercise-CMX), nonché la Blueprint Operational Level Exercise (Blue OLEx).

Compiti del Nucleo per la Sicurezza Cibernetica

Cyber Crisis Liaison Organisation Network

Il lancio ufficiale della rete Cyber Crisis Liaison Organisation Network (CyCLONe) è un risultato conseguito grazie al lavoro svolto in particolare dall'Italia (attraverso il DIS) e dalla Francia (ANSSI), che hanno guidato i lavori in ambito europeo. CyCLONe è volto a garantire la preparazione, la conoscenza situazionale dell'Unione, nonché il raccordo nella gestione delle crisi ed il supporto al decisore politico sia nazionale che europeo. La rete si incardina nel framework delineato dal Blueprint per una risposta coordinata agli incidenti e alle crisi su larga scala organizzando la cooperazione transfrontaliera su tre piani: politico, rappresentato dai dispositivi integrati per la risposta politica alle crisi (IPCR) del Consiglio UE; operativo, da CyCLONe; e tecnico, dalla rete degli CSIRT. In questo contesto, CyCLONe rappresenta l'infrastruttura transfrontaliera utile ad un efficace coordinamento tra il Presidente del NSC e i suoi omologhi negli altri Stati Membri.

In seno a CyCLONe, con il supporto del NIS Cooperation Group, viene organizzato con cadenza annuale l'evento UE di alto livello Blue OLEx a cui partecipano gli Executive, ovvero i vertici delle Autorità cyber nazionali in Europa, nonché gli omologhi delle Istituzioni UE. Componente fondante è l'esercizio svolto dagli Executive stessi con lo scopo di testare e rafforzare le capacità degli Stati in caso di situazioni di crisi cibernetica in Europa, nell'ambito del Blueprint, al fine di migliorare la cooperazione tra Stati Membri e con le Istituzioni UE, sia sul versante della prevenzione e risposta alle minacce del cyberspazio, sia su quello della resilienza.

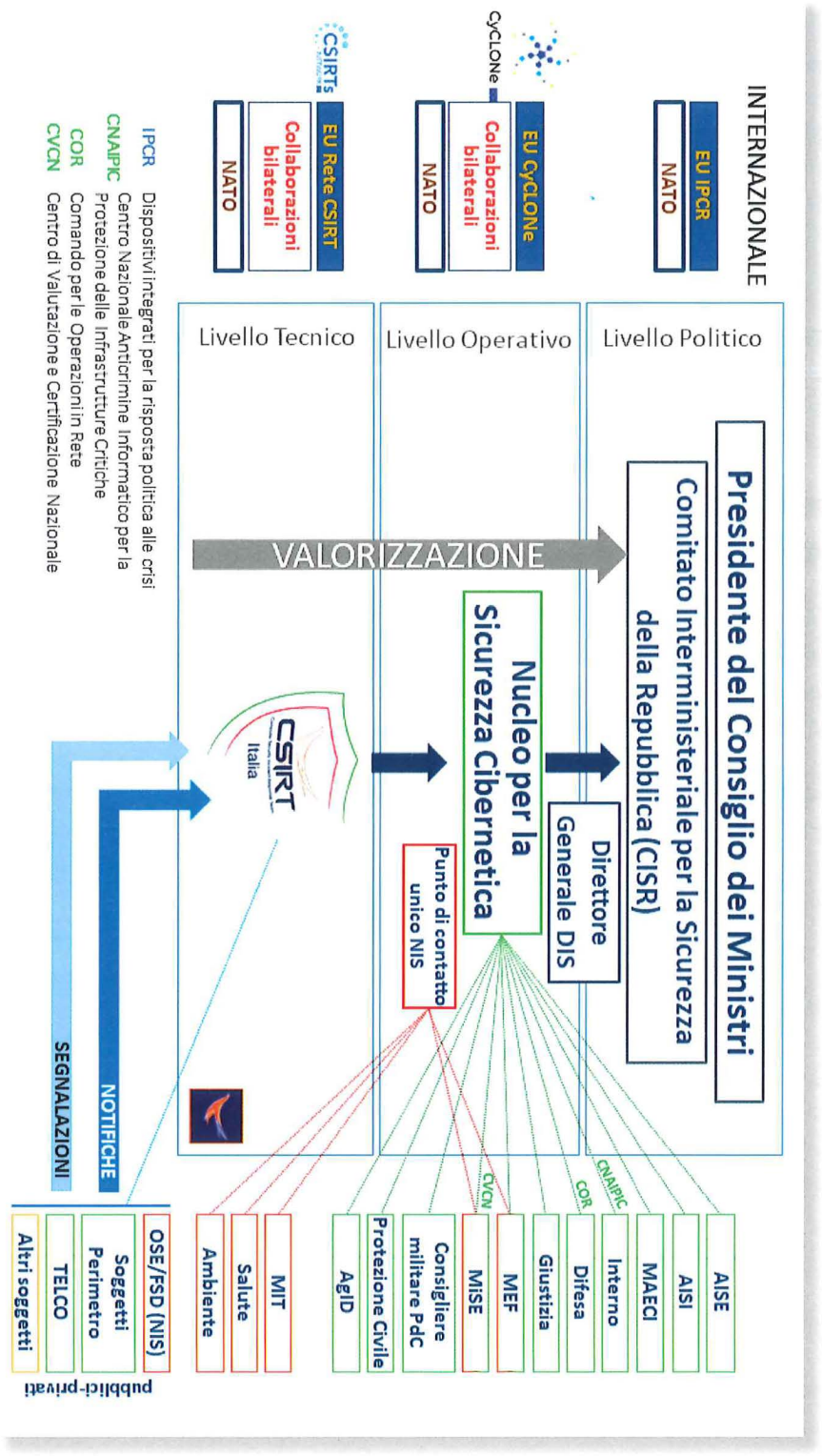
Ruolo di coordinamento nelle situazioni di crisi cibernetica

L'architettura nazionale di sicurezza cibernetica si incardina perfettamente nella piattaforma definita dal citato Blueprint, con il livello:

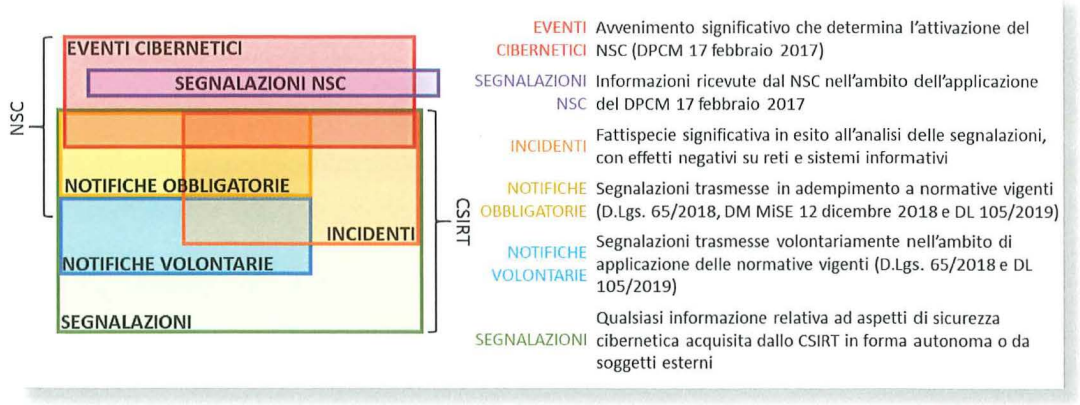
- politico, rappresentato dal Presidente del Consiglio dei Ministri e dal CISR;
- operativo, costituito dal NSC;
- tecnico, realizzato dallo CSIRT italiano.

Avendo al suo interno lo CSIRT italiano, l'Unità per l'Allertamento (UdA), il Punto di contatto unico NIS (PoC) e il NSC, il DIS ricopre due dei tre livelli funzionali a consentire una prevenzione e risposta adeguata a potenziali attacchi cyber al Sistema Paese, fornendo altresì supporto al livello politico, quale coordinatore delle situazioni di crisi cibernetica. La struttura sinergica così definita determina un processo che, in pieno raccordo con le omologhe articolazioni europee e internazionali, vede la valorizzazione delle segnalazioni o notifiche acquisite dallo CSIRT in merito a possibili incidenti trattati a livello tecnico o in eventi cibernetici che necessitano dell'attivazione del NSC per la valutazione della sussistenza di situazioni di crisi.

Per quanto la maggior parte delle attività del NSC siano sensibili e protette, per adempiere alle sue funzioni istituzionali, alcune sono rese note al pubblico. Si fa riferimento, ad esempio, all'evento cibernetico relativo a SolarWinds Orion, per il quale, a seguito di interlocuzioni con gli omologhi europei tramite CyCLONe, è stata avviata – in piena sinergia con lo CSIRT italiano – una campagna pubblica di sensibilizzazione per mitigare i rischi, nonché di mappatura dell'esposizione potenziale dei soggetti preposti a gestire le funzioni ed i servizi essenziali per la sicurezza nazionale (inclusi nel Perimetro), gli OSE e gli enti della Pubblica Amministrazione. L'attività è ancora in corso al tempo della stesura di questo documento ed è stata oggetto di condivisione con i membri di CyCLONe.


INTERNAZIONALE
EU IPCR
NATO
CyCLONe
EU CyCLONe
Collaborazioni bilaterali
NATO
CSIRTs Network
EU Rete CSIRT
Collaborazioni bilaterali
NATO
Livello Politico
Livello Operativo
Livello Tecnico
Presidente del Consiglio dei Ministri
Comitato Interministeriale per la Sicurezza della Repubblica (CISR)
VALORIZZAZIONE
Direttore Generale DIS
Nucleo per la Sicurezza Cibernetica
Punto di contatto unico NIS
CSIRT Italia
IPCR Dispositivi integrati per la risposta politica alle crisi
CNAIPIC Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
COR Comando per le Operazioni in Rete
CVCN Centro di Valutazione e Certificazione Nazionale
SEGNALAZIONI
NOTIFICHE
AISE
AISI
MAECI
Interno
Difesa
Giustizia
MEF
MISE
CVCN
Consigliere militare PdC
Protezione Civile
AgID
MIT
Salute
Ambiente
OSE/FSD (NIS)
Soggetti Perimetro
TELCO
Altri soggetti
pubblici-privati

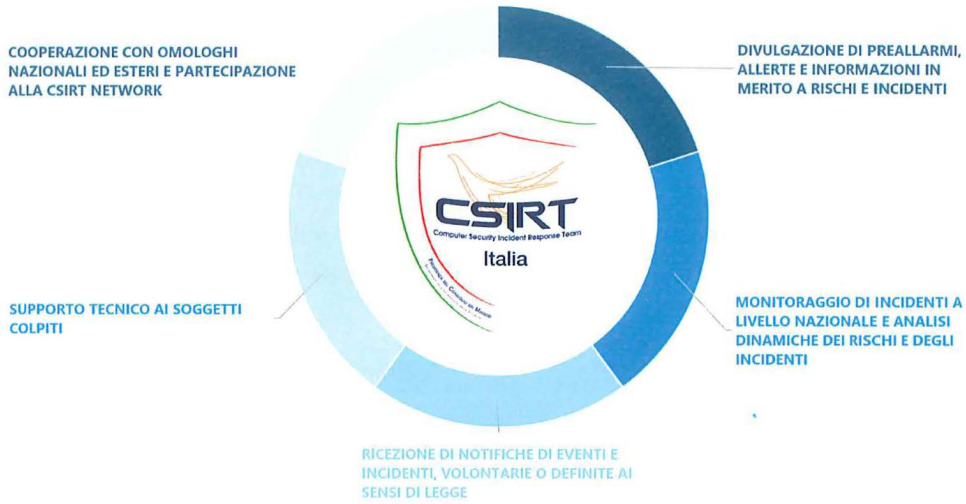
Terminologia: tassonomia degli eventi cibernetici e delle segnalazioni



ATTIVITA' DELLO CSIRT ITALIANO

Compiti dello CSIRT

Come anticipato nel Documento di Sicurezza Nazionale del 2019, a partire dal 6 maggio 2020 è divenuto operativo presso il DIS lo CSIRT italiano, assumendo i compiti fino a quel momento assolti dal CERT della Pubblica Amministrazione dell'Agenzia per l'Italia Digitale e dal CERT Nazionale del MiSE. Tale struttura tecnica, incaricata di svolgere attività di prevenzione e gestione degli incidenti informatici con impatto, effettivo o potenziale, sul territorio nazionale, è andata a rafforzare la governance unitaria della sicurezza cibernetica nazionale.



Tra i principali compiti svolti dallo CSIRT italiano, emergono: le attività di divulgazione, tramite preallarmi e allerte, di informazioni relative a rischi e incidenti cibernetici; il monitoraggio degli incidenti a livello nazionale; la ricezione delle notifiche di incidenti, volontarie o definite ai sensi di legge e l'eventuale, successivo inoltro al NSC; il supporto ai soggetti colpiti per facilitare la gestione

tecnica dell'evento cibernetico; le attività di cooperazione e collaborazione con altri omologhi esteri, inclusa la diffusione delle informazioni verso altri Stati eventualmente coinvolti da incidenti avvenuti in territorio nazionale.

Lo CSIRT partecipa attivamente alla rete UE degli CSIRT. Dalla sua attivazione, il Team italiano ha preso parte a numerosi meeting, side-meeting e conferenze ed eventi internazionali afferenti all'ambito della rete CSIRT, nell'ottica del potenziamento della proiezione internazionale.

RETE UE DEGLI CSIRT

La rete UE degli CSIRT è composta dagli CSIRT degli Stati Membri dell'Unione e dal CERT-UE, al fine di sviluppare la fiducia tra i Paesi europei e promuovere una cooperazione operativa rapida ed efficace. Tale rete è diventata uno dei principali punti di riferimento, grazie all'attivazione di piattaforme per la condivisione di informazioni e all'organizzazione di periodiche riunioni, volte anche allo scambio di esperienze e best practice per una risposta coordinata a specifici incidenti.

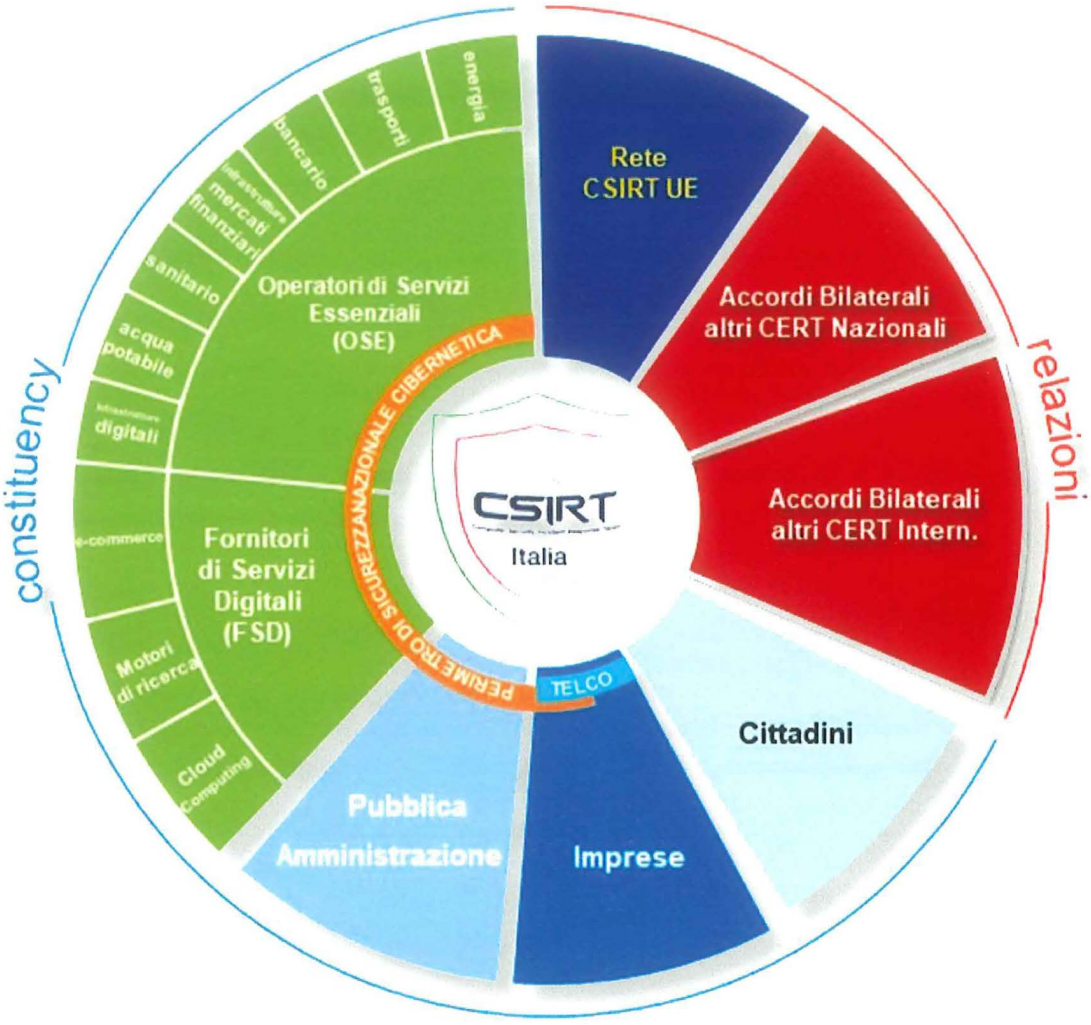
Sono stati molteplici anche gli incontri in conference call con l'intera rete nell'ottica di rafforzare i rapporti di collaborazione fra le parti e la condivisione di report tecnici, elaborati dallo CSIRT italiano, relativi a incidenti avvenuti ai danni di soggetti nazionali, ma con possibili implicazioni per gli altri Stati Membri.

Al riguardo, in ragione della natura tipicamente transnazionale degli eventi cibernetici, lo CSIRT, dalla sua nascita, ha costantemente interagito – a livello bilaterale – con gli omologhi organismi esteri, operanti in Stati sia europei che extra-europei.

Ciò ha permesso di mettere a sistema le rispettive competenze per l'effettuazione di analisi congiunte, consentendo di approfondire la conoscenza di vulnerabilità e di infrastrutture/servizi gestiti dai cyber-criminali, come nel caso della pubblicazione relativa a un framework di "Phishing-As-A-Service" realizzata insieme al CERT della Lettonia.

Canali di comunicazione

Sono stati predisposti e attivati diversi canali per la condivisione di informazioni con la constituency – composta da soggetti appartenenti alle Pubbliche Amministrazioni (centrali e locali) e al settore privato, come OSE, Fornitori di Servizi Digitali (FSD), soggetti inclusi nel "Perimetro di sicurezza nazionale cibernetica" e operatori di telecomunicazioni (cd. Telco) – che si differenziano in ragione del tipo di informazioni trattate e della loro sensibilità. Al riguardo, a partire dal mese di ottobre, è stato avviato un portale di "collaboration", riservato ai membri della constituency. Quest'ultimo rappresenta lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati.



Al fine di supportare i compiti di sensibilizzazione su tematiche di sicurezza informatica e disseminare contenuti di rilevanza pubblica, sin dall'avvio dei lavori dello CSIRT è stato realizzato un portale pubblicamente accessibile, disponibile all'indirizzo web https://csirt.gov.it, che offre anche ai cittadini la possibilità di segnalare eventi cibernetici significativi. In particolare, esso contiene notizie, allerte, bollettini di approfondimento, analisi, infografiche e pubblicazioni di interesse, suddivisi per tipologia e destinatari. Nell'ottica di promozione dei servizi offerti e di potenziamento delle attività di divulgazione dello CSIRT, è stato, anche, creato l'account ufficiale Twitter @CSIRT_it.

Portale pubblico

Portale di collaboration

Portale Twitter

Lo CSIRT ha, altresì, attivato numerosi contatti, in occasione di incidenti, con le strutture IT delle organizzazioni interessate, offrendo loro piena collaborazione anche al fine di individuare, in accordo con le controparti, opportune strategie di mitigazione dei relativi effetti e di risposta.

Infine, nel quadro del rapporto di collaborazione tra il DIS e il Garante per la protezione dei dati personali, si annovera la sottoscrizione, avvenuta il 1° dicembre 2020, di un Addendum per l'attuazione del "Protocollo d'intenti sulla protezione dei dati personali nelle attività di sicurezza cibernetica", rinnovato nel marzo 2019. Al riguardo, il documento attuativo mira a definire le modalità con cui lo CSIRT, in occasione di data-breach, possa ricevere gli elementi tecnici rilevanti sotto il profilo della cybersecurity, al fine di prevenire ulteriori simili incidenti.

Segnalazioni

Dall'avvio delle sue attività, lo CSIRT ha trattato oltre 25.000 segnalazioni provenienti sia da società di sicurezza ed omologhi esteri, sia da soggetti nazionali attraverso i canali messi a disposizione della constituency. Di questi, oltre 3.500, pari al 13,8% circa, sono stati classificati quali incidenti e conseguentemente gestiti nel dettaglio, nonché in buona parte inviati, per successiva valorizzazione, al NSC.

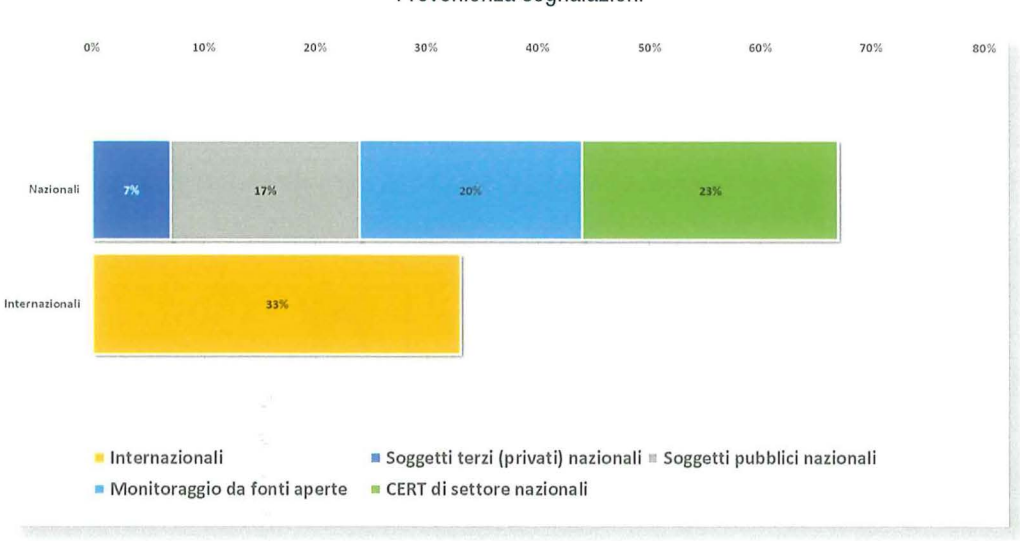
25.845 segnalazioni | **3.558** incidenti | **117** incidenti critici | **273** vulnerabilità critiche

Periodo 06/05/2020 - 31/12/2020

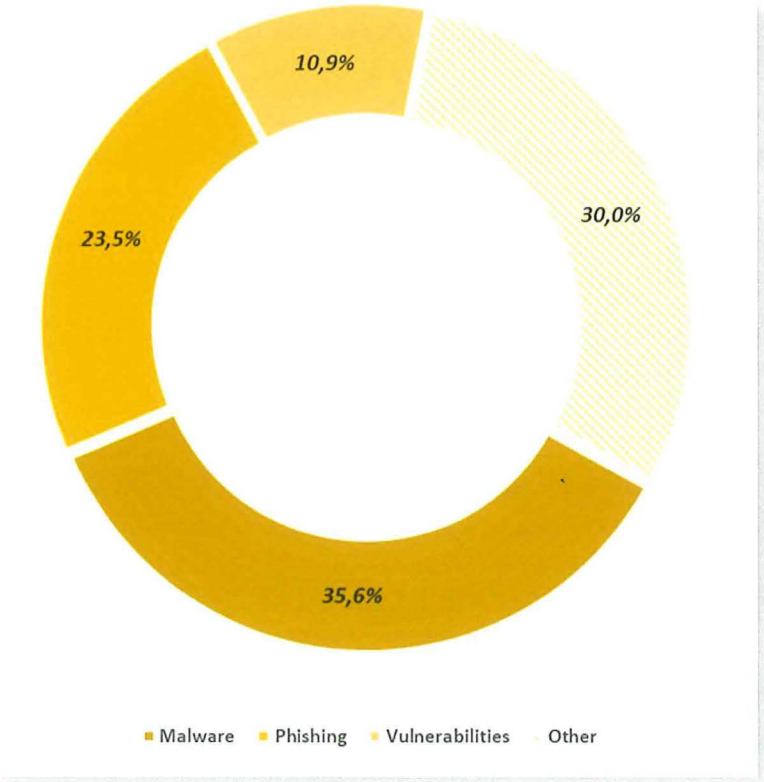
Le suddette attività sono state espletate nel rispetto delle best practice internazionali (e.g. Trusted Introducer, FIRST) e delle linee guida stabilite dall'Agenzia dell'UE per la Cybersercurity (ENISA), attraverso un processo di gestione delle segnalazioni opportunamente strutturato.

Con riferimento alla provenienza geografica delle segnalazioni, si rileva la preponderanza delle attivazioni originate in ambito nazionale. Al riguardo, dalla loro ripartizione effettuata sulla base dei soggetti segnalanti, emerge la prevalenza di quelle provenienti dai CERT di settore nazionali. Per quanto riguarda, invece, il

contesto internazionale, le segnalazioni pervengono principalmente da omologhe articolazioni governative e CERT commerciali, aderenti alla rete UE degli CSIRT.



Per quanto concerne le categorie di rischio, si evidenzia la prevalenza di malware e phishing, seguiti dalle vulnerabilità individuate in prodotti e sistemi e altre casistiche che includono ad esempio data-breach, DDoS, etc.



Con riferimento ai settori maggiormente colpiti, registrati nella prima fase di operatività dello CSIRT, emerge la prevalenza dei soggetti appartenenti alla Pubblica Amministrazione e al settore finanziario.

Nell'ambito della trattazione delle segnalazioni, sono stati emessi preallarmi, allerte, annunci e divulgate informazioni alle parti interessate in merito a rischi e incidenti. Le funzioni di allertamento e divulgazione a favore di singoli soggetti della constituency vengono effettuate attraverso comunicazioni dirette. Nello specifico, dall'avvio delle attività dello CSIRT al 31 dicembre 2020 sono state inviate oltre 3.000 comunicazioni ai soggetti a rischio interessati, tese alla loro sensibilizzazione o allertamento.

3.072 comunicazioni dirette | **379** comunicazioni sul portale pubblico | **79** comunicazioni sul portale di "collaboration"

Periodo 06/05/2020 - 31/12/2020

Analisi tecniche

Considerando gli incidenti legati ad agenti malevoli, lo CSIRT ha pubblicato le seguenti monografie tecniche, realizzate sulla base delle analisi esperite:

- Agent Tesla: nato come infostealer, ha aggiunto nel tempo capacità di injection e diffusione molto più avanzate oltre alla capacità di sottrarre dettagli delle reti e credenziali di accesso;

- Emotet: trojan modulare distribuito come first stage che, dopo aver infettato con successo un sistema, distribuisce infostealer o ransomware;
- Netwalker: ransomware as-a-service che usa tecniche di tipo fileless;
- ModiLoader: dropper multi-stage sfruttato per eseguire un Remote Access Tool (RAT, tool di accesso remoto) sulla macchina vittima;

- Sunburst: trojan osservato per la prima volta nel mese di dicembre 2020 a seguito dall'evento cibernetico che ha riguardato la piattaforma Solarwinds Orion.

ATTIVITA' DI FORMAZIONE E CONSAPEVOLEZZA

Il DIS, proseguendo le attività avviate dal 2018, continuerà a promuovere, nell'ambito del NSC, iniziative volte a favorire una maggiore consapevolezza dei rischi connessi alla cibersicurezza, il rispetto delle pratiche di cyber-hygiene e la formazione, a beneficio di target diversificati, operanti a diversi livelli, dalle Pubbliche

Amministrazioni al mondo dell'industria, dalla cittadinanza agli studenti. A quest'ultimo riguardo, il DIS ha patrocinato la "CyberChallenge.IT", organizzata dal Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica, finalizzata alla creazione della prossima generazione di professionisti dalla sicurezza informatica, composta da giovani talenti da formare e, successivamente, impiegare nelle realtà strategiche del Paese.

L'edizione 2020 ha registrato la partecipazione di oltre 4mila studenti suddivisi su 28 sedi (di cui 26 università) e ha visto la vittoria della squadra dell'Università di Udine.

Il DIS, inoltre, in ragione del diffuso impiego di modalità lavorative "agili", accresciuto dall'emergenza Covid-19, ha predisposto un "Vademecum delle policy di sicurezza per le organizzazioni", volto a sensibilizzare gli OSE in primis, ma anche per la più ampia diffusione a livello nazionale, contenente alcuni accorgimenti necessari alla riduzione del livello di esposizione al rischio cyber associato al telelavoro.

Nel medesimo contesto, si è proceduto, in fattivo raccordo con il Ministro per l'Innovazione tecnologica e la Digitalizzazione - Dipartimento per la Trasformazione Digitale, ad assicurare l'osservanza dei principi di cybersecurity, nonché la formazione del personale e la promozione della consapevolezza, nell'ambito della norma di impulso alla digitalizzazione della Pubblica Amministrazione (D.L. n. 76/2020, cd. Decreto "semplificazioni", convertito, con modificazioni, dalla legge n. 120/2020).

TRASFORMAZIONE DIGITALE E SICUREZZA CIBERNETICA

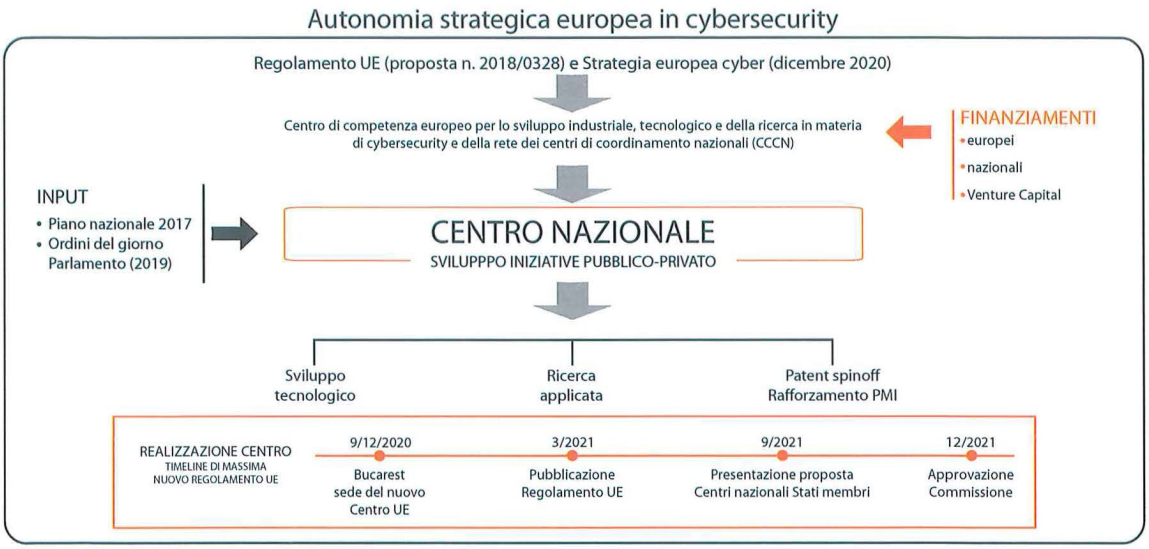
Dopo l'accelerazione del processo di trasformazione digitale imposto dalla pandemia Covid-19 che ha portato ad un sensibile aumento degli attacchi cibernetici, il programma di finanziamento "Next Generation EU" getta i presupposti per un'ulteriore fase di allargamento e velocizzazione di tale processo creando quindi contestualmente la necessità di aumentare la resilienza del Paese e dell'Europa rispetto agli attacchi. Il DIS ha mantenuto stretta sinergia con il Ministro per l'Innovazione tecnologica e la Digitalizzazione - Dipartimento per la Trasformazione Digitale, così da assicurare il rafforzamento degli investimenti in sicurezza cibernetica nel contesto delle attività di innovazione digitale della Pubblica Amministrazione e del settore produttivo, in coerenza con le normative nazionali in materia e con la "Strategia dell'UE per la cybersecurity nel decennio digitale". Tale Strategia invita gli Stati Membri ad allocare adeguate risorse del programma "Next Generation EU" per accrescere la resilienza delle infrastrutture e dei servizi critici, nonché la sovranità tecnologica e la leadership dell'Unione e dei suoi Stati Membri. Il perseguimento di tale scopo passa anche attraverso:

- la creazione di un "European Cyber Shield", ossia di una rete integrata di CSIRT nazionali, Security Operations Center (SOC) nazionali, Information Sharing and Analysis Centers (ISACs) settoriali, con le Autorità nazionali di cybersecurity;
- il supporto alla supply-chain industriale per garantire la sovranità tecnologica europea, avvalendosi di fondi, competenze, capacità tecnologiche e industriali. In tal senso, la Strategia assegna un ruolo chiave al Centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di cybersecurity e alla rete dei Centri di coordinamento nazionali;
- la creazione di un mercato del lavoro europeo attrattivo per i giovani talenti nel settore della sicurezza cibernetica e la promozione di mirati programmi di formazione di personale specializzato.

Le menzionate azioni sono già state al centro di diverse iniziative avviate dal Comparto Intelligence nel corso del 2020, e che proseguiranno nel 2021, per elevare i livelli di sicurezza cibernetica del Paese e le capacità di prevenzione e risposta agli eventi cibernetici, rafforzando, in particolare, lo scambio di informazioni e l'analisi degli elementi tecnici grazie agli strumenti normativi messi in campo dalla normativa sul Perimetro di sicurezza nazionale cibernetica, nonché lo sviluppo di modelli matematici funzionali alla modellazione delle interdipendenze tra le infrastrutture ICT dei soggetti pubblici e privati più rilevanti per la sicurezza nazionale, così da poter meglio definire, in ottica previsionale, l'impatto degli incidenti cibernetici significativi.

REGOLAMENTO UE PER LA CREAZIONE DI UN CENTRO DI COMPETENZA EUROPEO PER LO SVILUPPO INDUSTRIALE, TECNOLOGICO E DELLA RICERCA IN MATERIA DI CYBERSECURITY E DELLA RETE DEI CENTRI DI COORDINAMENTO NAZIONALI

Entro sei mesi dall'entrata in vigore del Regolamento, ogni Stato Membro è chiamato a costituire un proprio Centro di coordinamento nazionale da individuare in un ente pubblico, o a maggioranza pubblica, e che abbia la capacità di: supportare e relazionarsi con il citato Centro UE e la connessa rete dei diversi Centri nazionali di coordinamento; gestire fondi; possedere o avere accesso diretto a capacità tecniche e di ricerca in materia di cybersecurity; coinvolgere e coordinarsi con i settori pubblico (incluse le Autorità NIS) e privato, con l'accademia, il mondo della ricerca e la società civile. Il Centro nazionale, creato per potenziare la capacità domestica industriale, di competenze e di ricerca in cybersecurity, per poter accedere ai fondi europei, dovrà essere accreditato al Centro UE dallo Stato Membro e, in questo senso, la Commissione avrà tre mesi di tempo per esprimersi. Il Centro UE e il Centro nazionale dovrebbero essere operativi a partire dalla fine del 2021. L'importanza di tale Centro è di tutta evidenza solo considerando la circostanza che, durante i lavori parlamentari relativi al citato "Perimetro di sicurezza nazionale cibernetica", il Parlamento stesso ha ritenuto di impegnare il Governo con tre ordini del giorno alla creazione di un Centro nazionale di ricerca e sviluppo in cybersecurity, anche in relazione alle nuove tecnologie.

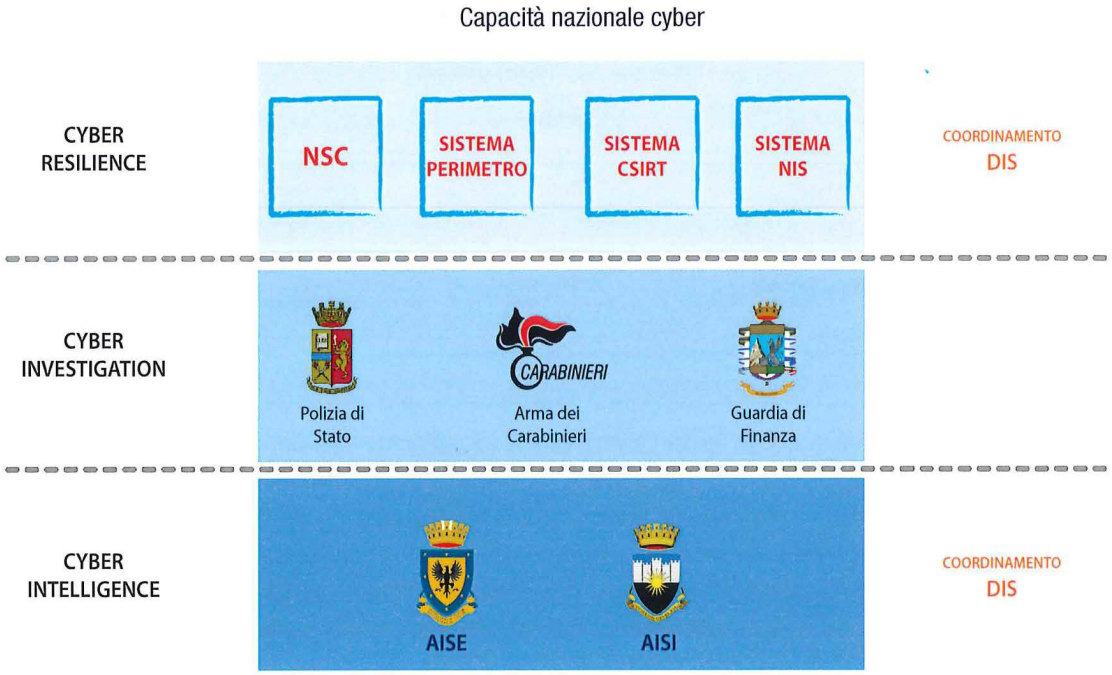


Sempre in questo contesto, inoltre, considerato che l'Italia sarà, in pochi mesi, chiamata a creare il proprio Centro di coordinamento nazionale, destinato ad operare in stretto raccordo con il sopra richiamato Centro europeo, il DIS ha condotto un approfondimento in merito all'organizzazione e alle funzioni che la nuova struttura sarà chiamata a svolgere, evidenziando l'esigenza che questo Ente assuma anche le funzioni di centro nazionale di ricerca e sviluppo in cybersecurity, in linea con quanto previsto dal Piano Nazionale per la protezione cibernetica e la sicurezza informatica (marzo 2017) e alla cui istituzione il Parlamento, come già accennato, ha impegnato il Governo, con tre ordini del giorno, in sede di conversione in legge del D.L. n. 105/2019 sul Perimetro di sicurezza nazionale cibernetica.

Il Centro avrebbe quindi l'obiettivo, da un lato, di favorire lo sviluppo e il potenziamento di una industria italiana ed europea competitiva, in grado di fornire tecnologie e servizi abilitanti ad elevato grado di sicurezza, con particolare riguardo all'ambito delle infrastrutture critiche digitali, alle principali filiere industriali nazionali e, dall'altro, di operare – in termini di supporto, studio e sviluppo – in stretta sinergia con i diversi soggetti che compongono l'architettura nazionale di sicurezza cibernetica.

La menzionata nuova struttura, inoltre, costituirebbe la naturale interfaccia dei Centri di competenza previsti dal Piano nazionale Impresa 4.0 – che fa seguito all'iniziativa della Commissione europea "Digitising European Industry" dell'aprile 2016, volta a promuovere la trasformazione digitale delle imprese, rafforzando i collegamenti tra ricerca e industria – oltre che dei Digital Innovation Hub, distribuiti sul territorio a supporto delle piccole e medie imprese e delle Pubbliche Amministrazioni locali per il relativo incremento delle capacità di prevenzione e di valutazione del livello di maturità digitale e tecnologica, nonché per l'accrescimento della consapevolezza.

In tal modo, si ritiene che possa essere definita l'architettura nazionale cyber per la parte connessa alla sicurezza nazionale, allo stato della vigente legislazione.



LISTA ACRONIMI

AgID – Agenzia per l'Italia Digitale
ANSSI – Agenzia nazionale francese per la sicurezza dei sistemi informatici
Blue OLEx – Blueprint Operational Exercise
CISR – Comitato Interministeriale per la Sicurezza della Repubblica
CMX – Crisis Management Exercise
CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
COR – Comando per le Operazioni in Rete
CERT – Computer Emergency Response Team
CSIRT – Computer Security Incident Response Team
CV – Centro di Valutazione
CVCN – Centro di Valutazione e Certificazione Nazionale
CyCLONe – Cyber Crisis Liaison Organisation Network
DDoS – Distributed Denial of Service
DORA – Digital Operational Resilience Act
DPCM – Decreto del Presidente del Consiglio dei Ministri
DSN – Documento di Sicurezza Nazionale
ENISA – Agenzia dell'Unione Europea per la cybersecurity
FIRST – Forum of Incident Response and Security Teams
FSD – Fornitori di Servizi Digitali
ICE – Infrastrutture Critiche Europee
ICT – Information and Communication Technology
IPCR – Integrated Political Crisis Response Arrangements
ISAC – Information Sharing and Analysis Center
ITU – International Telecommunication Union
MAECI – Ministero degli Affari Esteri e della Cooperazione Internazionale
MEF – Ministero dell'Economia e delle Finanze
MiSE – Ministero dello Sviluppo Economico
MIT – Ministero delle Infrastrutture e dei Trasporti
NATO – North Atlantic Treaty Organization
NIS – Network and Information Systems
NISCG – NIS Cooperation Group
NSC – Nucleo per la Sicurezza Cibernetica
OEWG – Open Ended Working Group
ONU – Organizzazione delle Nazioni Unite
OSE – Operatori di Servizi Essenziali
OSCE – Organizzazione per la Sicurezza e la Cooperazione in Europa
PoC – Punto di contatto unico NIS
PN – Piano Nazionale per la protezione cibernetica e la sicurezza informatica

RAN – Radio Access Network
RAT – Remote Access Tool
SOC – Security Operations Center
TELCO – Fornitori di reti e di servizi di comunicazione elettronica accessibili al pubblico
UdA – Unità per l'Allertamento
UE – Unione Europea
UN GGE – United Nations Group of Governmental Experts