SCENARI E TENDENZE: UNA SINTESI

Il 2016 ha rappresentato un anno di rilevanti evoluzioni ed accelerazioni geopolitiche, economiche e nel settore della sicurezza, ponendo le premesse per un 2017 che si prospetta denso di opportunità ma anche di grandi sfide, complesse e tra loro interconnesse, con dinamiche passibili di alterare nel tempo, in modo anche significativo, lo scenario internazionale e interno che abbiamo conosciuto negli ultimi anni. La sempre maggiore presa di coscienza della portata di tali sfide e una accresciuta percezione da parte dei cittadini delle immediate ricadute di fenomeni esogeni e globali nella loro vita quotidiana, comporteranno per la Comunità intelligence un impegno crescente, e la ricerca di metodi e strumenti analitici ed operativi di sempre maggiore efficacia.

Il terrorismo internazionale jihadista, nelle sue variegate manifestazioni, continuerà ad avere centrale rilevanza. Una sconfitta militare di DAESH – che ha dato peraltro prova di feroce determinazione e efficace resistenza – non comporterà una rapida eliminazione dell'organizzazione ma una sua parziale mutazione, per perseguire con forme diverse i suoi obiettivi di destabilizzazione e dominio. Se privata dell'attuale territorialità o di gran parte di essa, l'organizzazione di al Baghdadi potrebbe da un lato accentuare ulteriormente la risposta asimmetrica, dall'altro assumere in modo crescente le modalità di radicamento che da tempo caratterizzano *al Qaida*, ancora attiva e vitale su molteplici scenari. Quest'ultima, in virtù delle difficoltà in cui versa la formazione concorrente, ha dato segnali di voler rilanciare la propria azione in una sorta di competizione con DAESH per la *leadership* sul *jihad* mondiale. Entrambe le organizzazioni continueranno a promuovere il proprio messaggio proselitista ed azioni impattanti, quali attentati su vasta scala da parte dei propri esponenti o attacchi di va-

ria natura ad opera dei cd. *lupi solitari* o di microcellule. Peraltro, se in alcuni scenari il terrorismo jihadista appare in affanno, esso continua ad espandersi e a rafforzarsi in modo preoccupante in altri quadranti, quali il Sud-Est asiatico, l'Afghanistan e l'Africa subsahariana e in quello limitrofo dei Balcani. Rileva inoltre come il jihadismo abbia tratto incoraggiamento e visibilità, e quindi accresciuto la possibilità di attivare in futuro seguaci e imitatori, dal fatto di avere intensificato con successo, nel 2016, i propri attacchi nel cuore stesso di molte Capitali, occidentali e mediorientali, ed esteso timore e apprensione nel quotidiano a crescenti porzioni della popolazione, la quale, legittimamente, richiede accresciute misure di tutela.

Le sempre più raffinate tecniche messe a punto dal terrorismo, come testimoniato ad esempio dall'affinamento delle modalità per promuovere tramite internet iniziative individuali, renderanno necessario un continuo perfezionamento delle modalità operative volte a prevenire e reprimere l'azione jihadista, nei vari settori del proselitismo, della propaganda, della promozione di azioni violente e nella dimensione di confronto aperto. Ciò comporterà anche un accresciuto ricorso alla collaborazione delle comunità straniere residenti nei vari Paesi ed interessate a dissociarsi e distanziarsi da fenomeni estremisti e violenti di cui sono anch'esse sovente vittime.

Tela di fondo della lotta al terrorismo sarà una sempre maggiore collaborazione internazionale anche nel settore intelligence, tendenza risalente già ulteriormente stressata nel 2016 e che dovrà necessariamente crescere negli anni a venire, arricchendosi di nuove modalità e strumentazioni.

Parallelamente, in linea con una visione condivisa nei più qualificati consessi multilaterali, anche a livello nazionale la strategia di prevenzione, con il concorso del Comparto informativo, dovrà sempre più articolarsi in misure funzionalmente interconnesse, quali: il dispiegamento di una controarrativa rivolta soprattutto ad un uditorio giovanile; l'attuazione di programmi di assistenza per soggetti esposti a rischio di radicalizzazione; la previsione di percorsi di de-radicalizzazione nei confronti di coloro che rientrano dai teatri di *jihad*.

Pure il fenomeno – che sta assumendo valenza strutturale – rappresentato dalle grandi migrazioni comporterà nel 2017 un crescente impegno di intelligence, anche per quanto attiene alla raccolta informativa necessaria per contrastare adeguatamente le organizzazioni criminali di trafficanti di esseri umani, e ciò in tutti i teatri in cui esse operano con sempre maggiore sistematicità ed efficacia in un'ottica di *learning by doing*, tanto più in considerazione di crescenti contaminazioni, soprattutto nel Sahel e nel Sud della Libia, tra *network* criminali e terrorismo. Con il crescere, nella criminalità transazionale, del livello di specializzazione, delle modalità di finanziamento, di trasporto e nei falsi documentali,

in un giro d'affari ormai dell'ordine di miliardi di Euro, l'impegno dei Servizi di Informazione sarà sempre più articolato e complesso, anche perché determina la necessità di proiettarsi ed operare anche in scenari nuovi ed inediti ove andranno stabilite sempre più strette collaborazioni intergovernative e anche azioni di formazione e prevenzione *in loco*.

L'attività di monitoraggio continuerà a vedere fortemente impegnate le Agenzie in relazione alle crisi geopolitiche che ci lambiscono e che sono passibili di avere nel nostro Paese dirette e indirette ricadute, anche in virtù della partecipazione dell'Italia a coalizioni internazionali e della nostra perdurante attiva presenza su numerosi scenari. Tutto il bacino del Mediterraneo – di cui siamo al centro – e l'area intera del Medio Oriente allargato continuerà ad essere sotto pressione per le varie crisi aperte, la cui soluzione si presenta complessa quanto complesso è lo scenario che vi fa da sfondo. Quella di più immediato impatto, che riguarda la Libia, richiederà crescente impegno stabilizzante che faccia prevalere l'interesse comune del Paese su divisioni, tribalismo e personalismi, fattori che permeano fortemente quella realtà; ma il radicamento di tali fenomeni – rafforzato dal recente conflitto interno – lascia intravedere anche per l'anno a venire una situazione precaria, passibile finanche di deteriorare. Non si intravedono, poi, le premesse per una riduzione – a breve – dell'incalzante azione offensiva del terrorismo all'interno del territorio egiziano o turco, condotta con consapevole volontà destabilizzante. Il conflitto in Siria ha portato il Paese allo stremo e ciò fa intravedere crescente stanchezza nella popolazione, ma l'eredità di odio e rancori accumulatasi (e la percezione di alcune componenti di combattere uno scontro esistenziale) renderà comunque difficili e lunghe una effettiva pacificazione sul terreno e la necessaria, costosa ricostruzione, stante anche la vitalità di cui DAESH continua a dar prova in quel quadrante. In Iraq la resistenza della formazione di al Baghdadi, pur in arretramento, resta rilevante mentre, sul più generale piano politico interno, permangono ostacoli alla realizzazione di quella coesione nazionale, infra ed inter-settaria, che sarebbe necessaria premessa per una normalizzazione della situazione. Lo Yemen vede una resistenza della componente Houti molto determinata ed un crescente attivismo di DAESH ed *al Qaida,* acuito nello scorso anno dalle difficoltà di controllo del territorio da parte delle Autorità; si prospetta pertanto una situazione anch'essa di non facile e vicina soluzione, pur nella prostrazione dei vari contendenti. Anche l'azione di *Boko Haram* in Nigeria e Africa centrale continua a produrre instabilità in numerose aree, mettendo seriamente in difficoltà i locali governi. Ad alimentare la percezione di incertezza, questa volta nel Continente europeo, concorre anche la cronicizzazione della crisi ucraina e la contestuale determinazione delle parti in causa a tutela dei rispettivi obiettivi di lungo periodo. Anche scenari più lontani, in un mondo ormai globalizzato, continueranno ad essere oggetto di attenzione in relazione

al fenomeno jihadista, come l'Afghanistan e l'Asia centrale, ricca di risorse, nonché il Sud-Est asiatico.

Per il 2017 si ravvisano anche le premesse per l'avvio di possibili cambiamenti, anche significativi, nel complessivo andamento del commercio internazionale e nei flussi di investimenti finanziari, in un contesto che potrebbe conoscere una acuita competizione tra attori statuali e tra imprese di vari Paesi, a volte spregiudicata e senza esclusione di colpi. Ciò richiederà, specie nel caso italiano dove la struttura produttiva fatta in prevalenza da piccole e medie imprese rende le stesse più vulnerabili, un accresciuto impegno per la nostra intelligence – a sostegno dell'azione del Governo e del Sistema Paese – in tre sensi. *In primis*, per una interpretazione delle tendenze macroeconomiche in evoluzione discernendo, nel contesto delle stesse, opportunità e minacce. In secondo luogo, per favorire e stimolare le dinamiche virtuose e confacenti ai nostri interessi, come – ad esempio – la promozione di investimenti produttivi che arricchiscano il territorio in termini di competenze e occupazione. In terzo luogo, per prevenire nella misura del possibile i danni derivanti da azioni perniciose ed ostili, come gli investimenti speculativi o miranti a indebolire il nostro sistema (tramite sottrazione di *know-how* tecnologico e industriale), oppure la diffusione di notizie fuorvianti, o da ogni altra iniziativa pregiudizievole. La crescita, in numerosi Paesi, di ampie fasce di disagio e bisogno ed il ridimensionamento di molti sistemi di *welfare* renderanno peraltro la competizione economica sempre più vitale anche tra Stati tradizionalmente allineati e membri degli stessi consessi internazionali. Anche la tutela degli *asset* nazionali di pubblico interesse ha assunto ulteriore valenza negli ultimi anni e si consoliderà nel tempo, in quanto la crescente circolazione di flussi finanziari rende più difficile distinguere tra investimenti strettamente finanziari ed azioni ostili come acquisizioni di controllo con finalità strategiche. Di assoluto rilievo per l'anno a venire è anche l'azione informativa a tutela del sistema bancario e finanziario. Andranno inoltre seguite con immutata attenzione le tematiche attinenti ai mercati internazionali dell'energia, fondamentali per la stabilità stessa del nostro Paese.

Sul piano più strettamente interno, inoltre, si ravvisa una persistente estensione dell'influenza della grande criminalità organizzata sul tessuto imprenditoriale, anche al fine di riciclare gli ingenti proventi derivanti da traffici illeciti, soprattutto di stupefacenti, influenza resa più perniciosa dalla accresciuta vulnerabilità di molti operatori a causa di un più selettivo accesso al credito e della tendenza delle organizzazioni di stampo mafioso a fomentare la corruzione. L'attività informativa su tale versante sarà dunque anche per l'anno a venire un impegno rilevante per il Comparto, specie se si tiene conto della improrogabile necessità di ricostruzione delle aree colpite da terremoti e della conseguente importanza di una vigilanza attenta e approfondita.

Anche l'Italia, come molti Paesi, continuerà nel 2017, nonostante l'avviata ripresa, a risentire delle conseguenze della lunga crisi iniziata nel 2008. È un clima economico che molte famiglie vivono con difficoltà e disagio, che potrebbe favorire l'insorgere di una maggiore conflittualità sociale a sua volta alimentata e strumentalizzata da parte di componenti antagoniste per riportare attenzione e attualità alle loro istanze, di cui potrebbe essere corollario una accresciuta mobilitazione di frange estremiste di opposto orientamento. Sono fenomeni da monitorare anche a fini preventivi nelle loro varie espressioni e manifestazioni, tenuto anche conto del fatto che l'Italia ospiterà numerosi eventi internazionali di rilievo, tra cui quelli legati alla Presidenza di turno del G7. Parallelamente, ristretti circuiti che si richiamano all'esperienza degli "anni di piombo" continuano a ricercare spunti teorici per attualizzare il messaggio rivoluzionario.

Un macrosettore che sta conoscendo un'importanza esponenzialmente crescente per le attività di intelligence – come più estesamente evidenziato nell'apposito annesso – è poi quello, in tumultuosa evoluzione, del *cyber*. L'opinione pubblica sta acquisendo crescente consapevolezza delle grandi opportunità derivanti dallo sviluppo tecnologico, ma anche delle crescenti sfide securitarie e delle minacce che esso determina. Il funzionamento delle moderne società è divenuto, mai come in passato, completamente dipendente dalla tecnologia senza che, in molti casi, si siano in parallelo sviluppate adeguate difese. Strutture di governo, banche, borsa, *asset* strategici e quant'altro sono oggi più che mai esposti. Viviamo una fase in cui attori statali ostili ma anche organizzazioni criminali, gruppi terroristi o antagonisti, fanatici di varia natura o anche singoli individui, beneficiano sovente nel *cyberspace* di un *gap* securitario che deve essere, in larga misura, rapidamente colmato, e che comunque sarà in futuro oggetto di una continua evoluzione, con forme di aggressione sempre più sofisticate. Il Comparto sarà pertanto chiamato a dare il suo fondamentale contributo accentuando ulteriormente la sua pianificazione strategica nel *cyberspace*, e le sue capacità operative a tutela non solo degli obiettivi istituzionali ma anche del mondo imprenditoriale, per cui, nel caso italiano – in un contesto di assenza di materie prime – il differenziale di *know-how* trasformativo è di vitale importanza per la stessa competitività internazionale, e quindi per la sopravvivenza del Paese.

Emerge, alla luce di quanto sopra, un quadro dinamico e complesso, denso di opportunità ma nel contempo di incognite e difficoltà che richiederà, anche nel 2017, alle donne e gli uomini dell'intelligence italiana uno straordinario impegno, l'adozione di conoscenze e metodi in continua ed incessante evoluzione ed un grande sforzo di integrazione con gli altri Organismi dello Stato, in un'azione sistemica a tutela della sicurezza che è per il cittadino bene primario e presupposto necessario e imprescindibile della libertà individuale.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

ai sensi dell'art. 38, co. 1 bis, legge 124/07

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

ai sensi dell'art. 38, co. 1 bis, legge 124/07

Premessa

In linea con l'approccio redazionale adottato per il 2015, anche quest'anno il Documento di Sicurezza Nazionale-DSN è stato sviluppato lungo due direttrici: quella relativa alle evoluzioni architetturali, dedicata al potenziamento delle capacità cibernetiche del nostro Paese; quella di natura fenomenologica, incentrata sulla minaccia *cyber* che ha interessato soggetti rilevanti sotto il profilo della sicurezza nazionale.

Il primo filone ha risentito di alcuni importanti "fattori di spinta" sia endogeni che esogeni al sistema-Paese. Tra i primi va annoverata l'esperienza maturata a partire dal 2013, anno di adozione del provvedimento che ha delineato l'architettura nazionale *cyber* dell'Italia, grazie alla quale è stata acquisita una maggiore conoscenza sia dei punti di forza e di debolezza del nostro sistema, sia della mutevolezza senza precedenti assunta dalla minaccia cibernetica. Tale accresciuta consapevolezza ha costituito il punto di partenza di una riflessione volta ad individuare soluzioni in grado di assicurare il costante adeguamento degli strumenti di risposta rispetto alla minaccia ed alla naturale evoluzione degli scenari.

A rendere effettiva tale riflessione ha contribuito, poi, lo stanziamento straordinario operato dal Governo nell'ambito della legge di stabilità 2016, volto a garantire un significativo incremento delle capacità cibernetiche del Paese e ad assicurare, attraverso lo sviluppo di progettualità di sistema, il potenziamento della sicurezza informatica nazionale.

Tra i fattori esogeni, il dato di rilievo è stato l'adozione, il 6 luglio 2016, della Direttiva UE 2016/1148, recante *"misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"* (c.d. Direttiva NIS - *Network and Information Systems*). L'approvazione di tale Direttiva – che dovrà essere recepita nell'ordinamento nazionale entro il maggio 2018 – ha rappresentato l'occasione per l'assunzione di più mirate azioni di manutenzione delle strutture poste a presidio dello spazio cibernetico, parte delle quali già previste dall'esercizio di revisione che ha interessato gli atti di indirizzo strategico (il Quadro Strategico Nazionale) ed operativo (il Piano Nazionale).

La seconda direttrice del presente Documento rimanda alle funzioni proprie dell'intelligence, strettamente correlate allo stato della minaccia cibernetica in Italia e alle sue possibili evoluzioni. In tale ambito, il Comparto ha continuato a sviluppare strumenti per rendere più efficace la prevenzione della minaccia. Quest'ultima, in particolare, è risultata caratterizzata da un elevato grado di eterogeneità e dinamismo tecnologico e da una diversificazione degli obiettivi, delle modalità attuative e delle finalità di attacco in base alle differenti matrici: si è passati da quelle più rilevanti in termini di rischi per gli *asset* critici e strategici nazionali a quelle connesse al *cybercrime,* al *cyber-espionage* ed alla *cyberwarfare,* il cui confine distintivo appare sempre più sfumato, sino a quella hacktivista e all'uso, da parte di gruppi terroristici, di risorse informatiche per finalità di proselitismo e propaganda.

In tale quadro, il Comparto ha incentrato l'attenzione sul monitoraggio e sulla ricerca di indicatori della minaccia, specie quella di natura avanzata e persistente, così da individuarne principali direttrici e paradigmi comportamentali.

Anche nel 2016 il Comparto ha continuato ad accrescere le proprie capacità di *detection, response* ed *attribution*, moltiplicando gli sforzi per far fronte ad una minaccia che ha continuato a far registrare una crescita non solo in termini quantitativi ma anche qualitativi, soprattutto nel caso delle minacce di tipo avanzato e persistente. Le difficoltà insite nella loro rilevazione e attribuzione continuano a rendere pagante il ricorso ad attività malevole nello spazio cibernetico.

Potenziamento delle capacità cibernetiche nazionali

In linea di continuità con gli esercizi avviati nel 2013, il DIS ha operato attraverso due strumenti: il TAVOLO TECNICO *CYBER*-TTC per garantire le attività di raccordo inter-istituzionale; il TAVOLO TECNICO IMPRESE-TTI per rafforzare il Partenariato Pubblico-Privato (PPP).

Il 2016 ha costituito per il TTC un significativo punto di svolta. Gli esiti della verifica dell'attuazione del Piano Nazionale riferito al 2014-2015 – che hanno consentito di rilevare il livello di crescita degli assetti *cyber* nazionali e la loro capacità di rispondere alle sfide/opportunità offerte dallo spazio cibernetico – sono stati il punto di partenza del processo di revisione dello nuovo Piano, valido per il 2016-2018.

Tale processo ha interessato, oltre al Piano Nazionale, anche il Quadro Strategico, al fine di verificarne l'attualità e di procedere al loro

MEMBRI DEL TTC

1. Ministero degli Affari Esteri e della Cooperazione Internazionale;
2. Ministero dell'Interno;
3. Ministero della Giustizia;
4. Ministero della Difesa;
5. Ministero dell'Economia e delle Finanze;
6. Ministero dello Sviluppo Economico;
7. Agenzia per l'Italia Digitale;
8. Nucleo per la Sicurezza Cibernetica;
9. Comparto intelligence.

aggiornamento in ragione del mutato scenario di riferimento, specie avuto riguardo alla richiamata Direttiva UE in materia di sicurezza di *Network and Information Systems* (NIS). L'obiettivo più significativo di tale revisione è stato quello di pervenire alla definizione di strumenti per rendere più efficace l'attuazione degli indirizzi strategici e operativi fissati nei predetti documenti e più misurabili le azioni progettuali che da essi scaturiscono.

Sotto il profilo del metodo, la revisione è stata posta in essere secondo un articolato e ben definito processo di lavoro (vds. *Figura 1*) che, grazie allo sviluppo di una dinamica sinergica in sede di TTC, non si è limitato ad operare un mero aggiornamento dei richiamati documenti, ma ha preso in considerazione differenti piani – giuridico-normativo, organizzativo e finanziario – attraverso cui sviluppare l'azione di potenziamento delle capacità cibernetiche del Paese.

Le direttrici che hanno inciso sul processo di revisione hanno riguardato lo sviluppo delle capacità di prevenzione e reazione ad eventi cibernetici, ambito nel quale si sono evidenziate nel biennio concluso le più rilevanti criticità, e l'indispensabile coinvolgimento del

Figura 1 –Revisione del Quadro Strategico Nazionale e del Piano Nazionale 2016-2018

settore privato ai fini della protezione delle infrastrutture critiche/strategiche nazionali e dell'erogazione di servizi essenziali. Aspetti, questi, sui quali si focalizza con rinnovata attenzione la citata Direttiva NIS. Per un approfondimento sulle novità introdotte dalla stessa, si veda la scheda nel *box 1*.

Gli esiti dell'esercizio di verifica hanno costituito un utile parametro di riferimento anche per l'enucleazione delle attività poste in essere dall'Italia ai fini dell'attuazione del primo e del secondo pacchetto delle misure OSCE (*Organization for Security and Co-operation in Europe*), le cd.

box 1

NOVITÀ INTRODOTTE DALLA DIRETTIVA NIS

La Direttiva NIS prevede:

- sul piano strategico: l'adozione di una strategia nazionale NIS, che contempli la fissazione di obiettivi e priorità, delinei l'architettura di governo (comprensiva di ruoli e responsabilità attribuite ai diversi soggetti), preveda programmi di sensibilizzazione (*awareness*), piani di ricerca e sviluppo, nonché renda operativo un piano di valutazione dei rischi;
- sul versante architetturale e operativo:
- l'istituzione di una (o più) Autorità nazionale NIS e di un punto unico di contatto nazionale per la ricezione delle notifiche di incidenti e la cooperazione alla loro risoluzione;
- la costituzione di uno o più *Computer Security Incident Response Teams* (CSIRTs), cui è – tra l'altro – attribuita la responsabilità della gestione degli incidenti e dei rischi, con specifico riferimento a quelli che dovessero interessare gli operatori di servizi essenziali, dovendo fornire loro supporto per la risoluzione degli incidenti di impatto significativo;
- specifici obblighi di sicurezza informatica per:
  - gli operatori di servizi essenziali (nei settori dell'energia, del trasporto, bancario e finanziario, sanitario, idrico e delle infrastrutture digitali);
  - i fornitori di servizi digitali (come i motori di ricerca *on-line*, i negozi *on-line*, i servizi di *cloud computing*),

  tra cui l'obbligo della tempestiva notifica all'Autorità nazionale NIS degli incidenti informatici subiti.

"Confidence Building Measures (CBMs) *to reduce the risks of conflict stemming from the use of information and communication technologies*", adottate dal Consiglio permanente di quella organizzazione mediante le Decisioni del 3 dicembre 2013 e del 10 marzo 2016.

Il TTC ha seguito anche gli sviluppi maturati sulla materia *cyber* in sede di Alleanza Atlantica. Sono stati oggetto di particolare attenzione il riconoscimento, nel corso del summit NATO tenutosi a Varsavia dall'8 al 9 luglio 2016, del *cyber*-spazio quale nuovo dominio operativo e della necessità che in esso la NATO debba *"defend itself as effectively as it does in the air, on land, and at sea"*. A dare concretezza a tale passaggio hanno contribuito, da una parte, gli Alleati con l'impegno a rafforzare, attraverso il "*Cyber Defence Pledge*", le rispettive difese cibernetiche e, dall'altro, l'adozione di un meccanismo di misurazione dell'attuazione di tali obiettivi da parte dell'Alleanza.

Il Tavolo Tecnico *Cyber*, inoltre, quale tavolo di raccordo inter-istituzionale, ha contribuito allo sviluppo dei lavori e delle azioni concertate di sicurezza cibernetica proposte nell'ambito dei *Cyber Expert Group Meeting* del G7 Finanza ed Energia, anche in vista della prossima presidenza italiana del "Gruppo dei sette".

Vale poi evidenziare le interlocuzioni tenute dal Comparto con Banca d'Italia sul fronte della costituzione di un CERT Finanziario che – istituito nel dicembre 2016 in seguito ad un accordo tra Banca d'Italia, Associazione Bancaria Italiana (ABI) e Consorzio ABI Lab – opera quale organismo altamente specializzato nella *cybersecurity* nel settore bancario e finanziario, con l'obiettivo di prevenire e contrastare le minacce informatiche legate allo sviluppo delle nuove tecnologie e dell'economia digitale. Sempre con riguardo all'Istituto centrale, l'intelligence ha collaborato nella predisposizione di un elaborato incentrato sulla sicurezza *cyber* delle imprese italiane, allo scopo di ottenere, per la prima volta in Italia, un quadro statisticamente rilevante dell'esposizione alla minaccia cibernetica del sistema produttivo.

Sul fronte della *partnership* pubblico-privato (PPP) come accennato, opera il TTI che, istituito nell'ambito del DIS, fonda la sua azione sulla

condivisione informativa, così da consentire alle infrastrutture critiche ed alle imprese strategiche convenzionate con il Dipartimento di arricchire le loro conoscenze e rafforzare le proprie capacità di difesa cibernetica.

Il formato di collaborazione con gli operatori privati in sede di TTI ha continuato ad essere articolato su incontri di livello strategico, nel cui ambito vengono forniti aggiornati quadri sullo stato della minaccia *cyber* nel nostro Paese, e di livello tecnico, dedicati all'analisi di "casi studio", dei quali vengono condivisi i relativi indicatori di compromissione. Ciò per agevolare, da un lato, il rafforzamento delle misure di difesa cibernetica e consentire, dall'altro, in caso di presenza della minaccia, la sua rapida identificazione al fine di impedirne l'ulteriore propagazione.

In via più generale, lo scambio informativo tra intelligence e privati è assicurato da una piattaforma dedicata, il cui principale obiettivo è quello di porsi sempre più quale *"one-stop-shop"* per la fornitura di servizi informativi e di correlazione dati a supporto delle decisioni di sicurezza cibernetica che le aziende sono chiamate ad assumere.

Tra gli eventi internazionali che hanno coinvolto, su iniziativa dell'intelligence, gli operatori privati, oltre al *17th NATO Cyber Defence Workshop* di cui si è accennato nella premessa alla presente Relazione, va menzionato l'incontro relativo alla *"contractual Private-Public Partnership"* (cPPP) che, come parte integrante della strategia UE sul *Digital Single Market* per la *cyber security*, mira ad accrescere la competitività delle aziende attive nello specifico settore per favorire la produzione, in ambito europeo, di tecnologie affidabili sotto il profilo della sicurezza ed agevolarne altresì l'esportazione.

In ambito nazionale, poi, di rilievo è stata la terza edizione dell'ICT4INTEL 2020 dedicata al tema dei *Big Data* (BD), declinato, tenuto conto delle esigenze dell'intelligence, sulla base degli aspetti indicati in *Figura 2*.

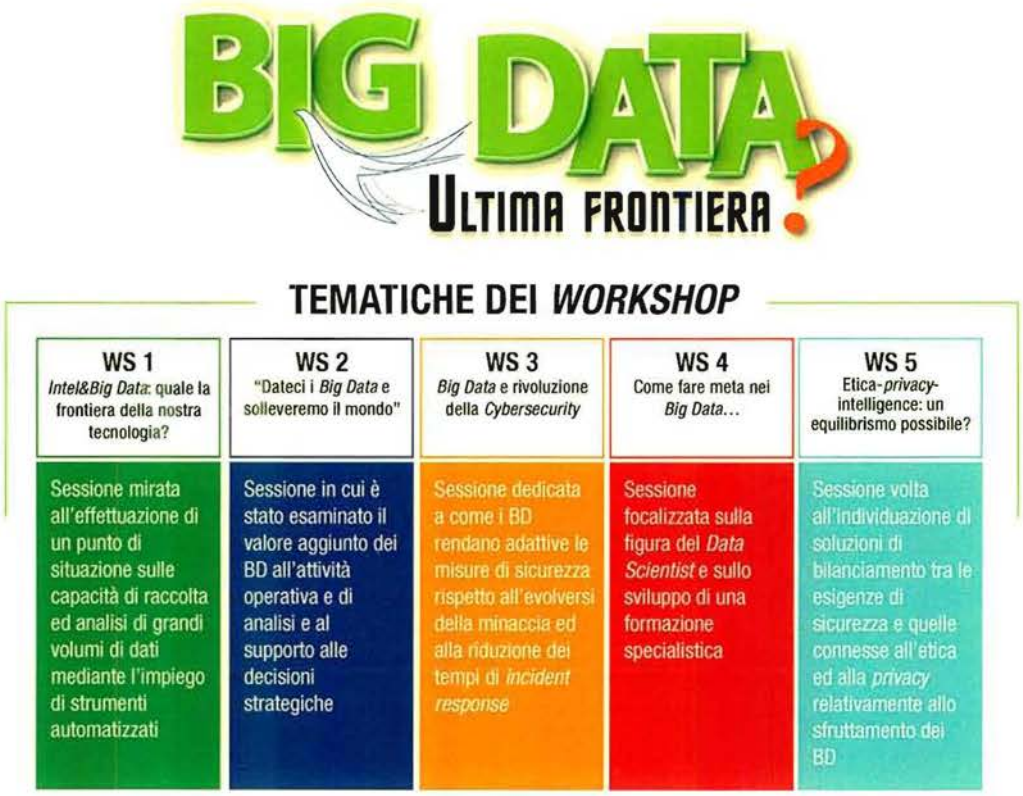

Figura 2 – Tematiche trattate in occasione dell'evento ICT 4INTEL 2020 edizione 2016