FSC.EMI/147/21/Rev.1
14 May 2021

ITALIAN only

Permanent Mission of Italy
OSCE

Prot. n. 111
Vienna, 14/05/2021

NOTE VERBALE

The Permanent Mission of Italy to the Organization for Security and Cooperation in Europe presents its compliments to all of the other Delegations and Permanent Missions to the Organization for Security and Cooperation in Europe, the Forum for Security Cooperation, and the Conflict Prevention Centre, and with reference to the Note Verbale n. 97 of May 5, 2021, has the honor to distribute a revised version of Italy's OSCE Questionnaire on the Code of Conduct on Politico-Military Aspects of Security, valid as of 15 April 2021.

The Permanent Mission of Italy to the Organization for Security and Cooperation in Europe avails itself of this opportunity to renew to all Delegations and Permanent Missions to the OSCE, the Forum for Security Cooperation, and the Conflict Prevention Centre the assurances of its highest consideration.

To all Permanent Missions and Delegations to the OSCE
OSCE- Conflict Prevention Centre
VIENNA

ITALIA

SCAMBIO DI INFORMAZIONI SUL CODICE DI CONDOTTA RELATIVO AGLI ASPETTI POLITICO-MILITARI DELLA SICUREZZA

APRILE 2021

SEZIONE I: ELEMENTI INTRASTATALI

1. Misure per prevenire e combattere il terrorismo

1.1 A quali accordi o convenzioni (universali, regionali, sub-regionali e bilaterali) relative alla prevenzione ed al contrasto del terrorismo ha aderito il vostro Stato?

CONVENZIONI DELLE NAZIONI UNITE

Convenzione sui reati commessi a bordo di aeromobili	Tokyo, 14 settembre 1963
Convenzione per la repressione della cattura illecita di aeromobili	L'Aia, 16 dicembre 1970
Convenzione per la repressione degli atti illeciti rivolti contro la sicurezza dell'aviazione civile	Montreal, 23 settembre 1971
Convenzione sulla prevenzione e repressione dei reati contro persone internazionalmente protette, compresi gli agenti diplomatici	New York, 14 dicembre 1973
Convenzione contro la cattura degli ostaggi	New York, 17 dicembre 1979
Convenzione sulla protezione fisica dei materiali nucleari	Vienna, 3 marzo 1980
Protocollo per la repressione degli atti illeciti di violenza negli aeroporti adibiti all'aviazione civile interazionale	Montreal, 24 febbraio 1988
Convenzione per la repressione dei reati diretti contro la sicurezza della navigazione marittima	Roma, 10 marzo 1988
Protocollo per la repressione di atti illeciti contro la sicurezza delle piattaforme fisse situate sulla piattaforma continentale	Roma, 10 marzo 1988
Convenzione sulla marcatura di esplosivi plastici e in foglie ai fini di identificazione	Montreal, 1 marzo 1991
Convenzione per la repressione degli attentati terroristici mediante utilizzo di esplosivo	New York, 15 dicembre 1997
Convenzione per la soppressione del finanziamento del terrorismo	New York, 9 dicembre 1999
Convenzione e Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale.	Palermo, 15 novembre 2000 e 31 maggio 2001.
Convenzione sulla repressione degli atti di terrorismo nucleare	New York, 13 aprile 2005

ALTRE CONVENZIONI INTERNAZIONALI

Convenzione europea per la repressione del terrorismo	Strasburgo, 27 gennaio 1977
Convenzione sulla criminalità informatica	Budapest, 23 novembre 2001
Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo	Varsavia, 16 maggio 2005
Protocollo addizionale alla Convenzione del Consiglio d'Europa sulla prevenzione del terrorismo	Riga, 22 ottobre 2015

ACCORDI BILATERALI

ALBANIA
Protocollo tra il Ministero dell'Interno della Repubblica Italiana e il Ministero dell'Interno della Repubblica di Albania per il rafforzamento della collaborazione bilaterale nel contrasto al terrorismo e alla tratta di esseri umani; Tirana, 3 novembre 2017.

ALGERIA
Accordo in materia di terrorismo, criminalità organizzata, traffico illecito di sostanze stupefacenti e psicotrope e immigrazione illegale; Algeri, 22 novembre 1999 – in vigore dal 28 gennaio 2008.

ANGOLA
Accordo di cooperazione in materia di sicurezza e ordine pubblico; Luanda, 19 aprile 2012; non ancora vigente sul piano internazionale.

ARABIA SAUDITA
- Verbale di incontro tra Ministri dell'Interno; Riyadh, 15 febbraio 2005.
- Accordo di cooperazione in materia di lotta alla criminalità; Roma, 6 novembre 2007 – in vigore dal 14 ottobre 2009.

ARGENTINA
- Accordo terrorismo, traffico illecito di stupefacenti e criminalità organizzata; Roma, 6 ottobre 1992 – in vigore dal 3 aprile 1996.
- Memorandum d'intesa per la lotta alla criminalità organizzata, ai traffici illeciti ed al terrorismo internazionale; Buenos Aires, 6 ottobre 1999; non ancora vigente sul piano internazionale.
- Accordo di cooperazione in materia di sicurezza; Buenos Aires, 8 maggio 2017.

ARMENIA
Accordo in materia di cooperazione di polizia; Roma, 23 aprile 2010 – in vigore dal 25 ottobre 2010.

AUSTRIA
- Memorandum d'intesa per conferire seguiti concreti agli accordi presi a Roma dai Ministri dell'Interno italiano ed austriaco ed individuare ulteriori materie di collaborazione; Vienna, 1° ottobre 2002.
- Accordo fra il Governo della Repubblica Italiana e il Governo della Repubblica d'Austria in materia di cooperazione di polizia; Vienna, 11 luglio 2014 – in vigore dal 1° aprile 2017.

AZERBAIJAN
Accordo di cooperazione tra il Ministero dell'Interno della Repubblica Italiana e il Ministero degli Affari Interni della Repubblica di Azerbaijan; Roma, 5 novembre 2012 – in vigore dal 22 giugno 2017.

BELGIO
Intesa tecnica fra il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno della Repubblica Italiana e la Polizia Federale Belga; Roma, 2 febbraio 2017.

BOSNIA ERZEGOVINA
Accordo contro la criminalità organizzata e il traffico di droga; Sarajevo, 28 gennaio 2002 – in vigore dal 26 ottobre 2007.

BULGARIA
Accordo di cooperazione di polizia in materia di lotta alla criminalità organizzata; Roma, 12 aprile 1999 – in vigore dal 16 febbraio 2001

CAPO VERDE
Accordo di cooperazione di polizia; Praia, 8 luglio 2013; non ancora vigente sul piano internazionale.

CILE
Accordo contro il terrorismo, la criminalità organizzata e il traffico di droga; Roma, 16 ottobre 1992; in vigore dal 26 dicembre 1995.

CINA
- Accordo in materia di lotta alla criminalità; Roma, 4 aprile 2001; in vigore dal 27 settembre 2004.
- Protocollo di cooperazione tra il Ministero dell'Interno della Repubblica Italiana e il Ministero della Pubblica Sicurezza della Repubblica Popolare Cinese; Roma, 24 luglio 2017.

CIPRO
Accordo di cooperazione su criminalità organizzata ed altre forme di criminalità; Nicosia, 28 giugno 2002; in vigore dal 27 luglio 2006.

COLOMBIA
Accordo in materia di cooperazione di polizia; Roma, 28 maggio 2013-in vigore dal 1° febbraio 2018.

COREA DEL SUD
Memorandum d'intesa in materia di cooperazione di polizia; Seoul, 7 maggio 2010.

COSTA D'AVORIO
Dichiarazione di Intenti del Ministro dell'Interno della Repubblica Italiana e del Ministro dell'Interno e della Sicurezza della Repubblica della Costa D'Avorio per il rafforzamento della cooperazione in materia di migrazione e sicurezza; Roma, 31 gennaio 2020.

CROAZIA
Dichiarazione congiunta (*Joint Declaration*, firmata dal Ministro Di Maio); Zagabria, 30 novembre 2020.

CUBA
Accordo in materia di cooperazione di polizia; L'Avana, 16 settembre 2014; non ancora vigente sul piano internazionale:

ECUADOR
Accordo in materia di cooperazione di polizia; Quito, 21 luglio 2016; non ancora vigente sul piano internazionale.

EGITTO
Accordo di cooperazione di polizia; Il Cairo, 18 giugno 2000; in vigore dal 18 gennaio 2005.

EL SALVADOR
Accordo di cooperazione in materia di lotta alla criminalità organizzata; San Salvador, 12 dicembre 2006; in vigore dal 12 febbraio 2010.

EMIRATI ARABI UNITI
Accordo in materia di sicurezza; Abu Dhabi, 14 novembre 2005; in vigore dal 24 maggio 2007.

ESTONIA
Accordo di cooperazione sulla lotta contro la criminalità organizzata, il terrorismo e il traffico illecito di droga; Tallinn, 8 settembre 200; in vigore dal 9 marzo 2015.

FRANCIA

- Accordo contro il terrorismo, la criminalità organizzata e il traffico di droga; Parigi, 13 ottobre 1986.
- Dichiarazione congiunta tra i Ministri dell'Interno in materia migratoria; Imperia, 1° luglio 2002.
- Protocollo operativo fra il Dipartimento della P.S. e la Direzione Centrale della polizia giudiziaria del Ministero dell'Interno della Repubblica Francese finalizzato al rafforzamento della cooperazione in materia di lotta alla criminalità organizzata; Parigi, 17 gennaio 2012.
- Accordo tra i Ministri dell'Interno in materia di cooperazione bilaterale per l'esecuzione di operazioni congiunte di polizia; Lione, 3 dicembre 2012; in vigore dal 1° aprile 2016.
- Dichiarazione congiunta (XXX Vertice italo-francese); Lione, 3 dicembre 2012.
- Dichiarazione congiunta (XXXI Vertice italo-francese); Roma, 20 novembre 2013.
- Dichiarazione congiunta (XXXII Vertice italo-francese); Parigi, 24 febbraio 2015.
- Dichiarazione d'intenti fra il Capo della Polizia e il Direttore Generale della Polizia Nazionale francese per il rafforzamento della cooperazione di polizia; Roma, 3 marzo 2015.
- Dichiarazione congiunta (XXXIII Vertice italo-francese); Venezia, 8 marzo 2016.
- Dichiarazione comune tra il Capo della Polizia – Direttore Generale della Pubblica Sicurezza italiano e il Direttore Generale della Polizia Nazionale francese per lo scambio di informazioni ed il coordinamento operativo fra le rispettive reti di ufficiali di collegamento; Parigi, 14 febbraio 2017.

GEORGIA

Accordo di cooperazione in materia di lotta alla criminalità; Roma, 11 marzo 2010; in vigore dal 28 maggio 2010.

GERMANIA

Accordo sulla collaborazione tra le Polizie dei due Paesi; Bonn, 22 ottobre 1993.

GHANA

Accordo di cooperazione in materia di sicurezza; Accra, 8 febbraio 2010; non ancora vigente sul piano internazionale.

GIORDANIA

Accordo di cooperazione in materia di lotta alla criminalità; Amman, 27 giugno 2011; in vigore dal 21 dicembre 2016.

GRECIA

- Accordo contro il terrorismo, la criminalità organizzata e il traffico di droga; Atene, 23 settembre 1986.
- Accordo di cooperazione di polizia; Roma, 10 gennaio 2000; in vigore dal 1° settembre 2003.

INDIA

Accordo contro il terrorismo, la droga e la criminalità organizzata; Nuova Delhi, 6 gennaio 1998; in vigore dal 21 gennaio 2000.

IRAN

Accordo di cooperazione di polizia in materia di sicurezza; Roma, 31 ottobre 2002; in vigore dal 9 giugno 2004.

IRAQ

Memorandum in materia di cooperazione di polizia; Roma, 30 settembre 2009.

ISRAELE

- Dichiarazione congiunta cooperazione internazionale di polizia; Gerusalemme, 20 luglio 2004.
- Accordo in materia di pubblica sicurezza; Roma, 2 dicembre 2013; in vigore dal 1° gennaio 2018.

KAZAKHSTAN
Accordo in materia di lotta alla criminalità organizzata, al traffico illecito di stupefacenti, al terrorismo e ad altre forme di criminalità; Roma, 5 novembre 2009; in vigore dal 9 febbraio 2016.

KOSOVO
Accordo tra il Governo della Repubblica Italiana e il Governo della Repubblica del Kosovo sulla cooperazione di polizia; Roma, 12 novembre 2020; non ancora vigente sul piano internazionale

LIBIA
- Accordo contro il terrorismo, la criminalità organizzata, il traffico illegale di stupefacenti e sostanze psicotrope e l'immigrazione clandestina; Roma, 13 dicembre 2000; in vigore dal 22 dicembre 2002.
- Protocollo di cooperazione per fronteggiare il fenomeno dell'immigrazione clandestina; Tripoli, 29 dicembre 2007.
- Protocollo concernente l'aggiunta di un articolo al Protocollo firmato il 29.12.2007; Tripoli, 4 febbraio 2009.
- Trattato di amicizia, partenariato e cooperazione (l'art. 19 detta regole per la cooperazione di polizia); Bengasi, 30 agosto 2008; in vigore dal 2 marzo 2009.
- Nuovo Protocollo tecnico operativo per fronteggiare il fenomeno dell'immigrazione clandestina; Roma, 7 dicembre 2010; in vigore dal 1° gennaio 2011.
- Memorandum d'intesa sulla cooperazione nel campo dello sviluppo, del contrasto all'immigrazione illegale, al traffico di esseri umani, al contrabbando e sul rafforzamento della sicurezza delle frontiere tra lo Stato della Libia e la Repubblica Italiana; Roma, 2 febbraio 2017.

MACEDONIA DEL NORD
Accordo in materia di cooperazione di polizia; Roma, 1° dicembre 2014; in vigore dal 29 maggio 2018.

MALTA
Memorandum d'intesa tecnico-operativa tra il Dipartimento della Pubblica Sicurezza Italiano e la Polizia di Malta per il rafforzamento della cooperazione di polizia, nella lotta contro la tratta di esseri umani, l'immigrazione illegale, la criminalità organizzata e il terrorismo; Roma e La Valletta, 4 ottobre 2012.

MAROCCO
- Accordo contro il terrorismo, la criminalità organizzata e il traffico di droga; Rabat, 16 gennaio 1987.
- Protocollo aggiuntivo all'Accordo del 16 gennaio 1987; Roma, 16 dicembre 1996.
- Dichiarazione congiunta per l'istituzione di un partenariato strategico multidimensionale; Rabat, 1 novembre 2019.

MOLDAVIA
- Accordo contro la criminalità organizzata; Roma, 3 luglio 2002; in vigore dal 5 maggio 2004.
- Protocollo di cooperazione; Chisinau, 15 dicembre 2006.

MONTENEGRO
- Accordo di cooperazione contro la criminalità organizzata; Roma, 25 luglio 2007; in vigore dal 22 novembre 2011.
- Accordo di collaborazione strategica tra il Governo della Repubblica Italiana ed il Governo del Montenegro; Roma, 6 febbraio 2010; in vigore dal 25 maggio 2015.

NIGER
Accordo di cooperazione in materia di sicurezza; Niamey, 9 febbraio 2010: in vigore dal 14 dicembre 2016.

PANAMA
Accordo contro la criminalità organizzata; Roma, 12 settembre 2000; in vigore dal 5 febbraio 2003.

PARAGUAY
Accordo contro la criminalità organizzata; Roma, 24 ottobre 2002; in vigore dal 23 agosto 2010.

POLONIA
Accordo lotta criminalità; Varsavia, 4 giugno 2007; in vigore dal 25 giugno 2009.

QATAR
Memorandum d'intesa sulla lotta alla criminalità tra il Governo della Repubblica Italiana ed il Governo dello Stato del Qatar; Roma, 16 aprile 201;2 in vigore dal 5 febbraio 2018.

REGNO UNITO DI GRAN BRETAGNA E IRLANDA DEL NORD
Accordo contro il terrorismo, la criminalità organizzata e il traffico di droga; Roma, 11 gennaio 1989.

REPUBBLICA CECA
Accordo contro il terrorismo, la criminalità organizzata e il traffico di sostanze stupefacenti; Praga, 22 marzo 1999; in vigore dal 15 dicembre 1999.

REPUBBLICA DI SAN MARINO
Accordo sulla cooperazione per la prevenzione e la repressione della criminalità tra l'Italia e la Repubblica di San Marino; Roma, 29 febbraio 201; in vigore dal 4 febbraio 2015.

RUSSIA
- Accordo sulla cooperazione nella lotta alla criminalità; Roma, 5 novembre 2003; in vigore dal 17 settembre 2009.
- Protocollo di cooperazione; Roma, 20 gennaio 2006.
- Piano d'Azione; Trieste, 26 novembre 2013.

SERBIA
- Accordo di cooperazione in materia di lotta alla criminalità organizzata, al narcotraffico e al terrorismo internazionale tra il Governo della Repubblica Italiana e il Governo della Repubblica di Serbia; Roma, 18 dicembre 2008; in vigore dal 6 novembre 2009.
- Dichiarazione congiunta in materia di polizia; Belgrado, 8 marzo 2012.

SLOVACCHIA
Accordo contro il terrorismo, il traffico di sostanze stupefacenti e la criminalità organizzata; Bratislava, 19 aprile 2002; in vigore dal 6 novembre 2002.

SPAGNA
- Accordo contro il terrorismo e la criminalità organizzata; Madrid, 12 maggio 1987
- Dichiarazione congiunta; La Moncloa, 29 ottobre 2012.

SUD AFRICA
Accordo di cooperazione in materia di sicurezza; Città del Capo, 17 aprile 2012; in vigore dal 30 gennaio 2015.

SUDAN
Memorandum d'Intesa per la lotta alla criminalità, gestione delle frontiere e dei flussi migratori ed in materia di rimpatrio; Roma, 3 agosto 2016.

SVIZZERA
Accordo sulla cooperazione di polizia e doganale; Roma, 14 ottobre 2013; in vigore dal 1° novembre 2016.

TUNISIA

- Accordo contro la criminalità organizzata; Tunisi, 13 dicembre 2003; in vigore dal 21 dicembre 2005.
- Protocollo d'intesa tra il C.A.S.A. e il *Pole Securitaire pour la Lutte contre le Terrorisme et le Crime Organisè* tunisino; Tunisi, 10 maggio 2018.

TURCHIA

Accordo di cooperazione sulla lotta ai reati gravi, in particolare contro il terrorismo e la criminalità organizzata; Roma, 8 maggio 2012; in vigore dal 1° aprile 2018

UNGHERIA

Accordo contro il terrorismo, la criminalità organizzata, il traffico stupefacenti e sostanze psicotrope; Roma, 13 maggio 1997; in vigore dal 17 aprile 1998.

U.S.A.

- Accordo per la collaborazione nella lotta al terrorismo; Roma, 24 giugno 1986.
- Memorandum in materia di cooperazione nella lotta al terrorismo; Washington, 4 dicembre 2007.
- Procedure operative per lo scambio di informazioni relative al monitoraggio antiterrorismo; Roma, 28 gennaio 2009.
- Accordo tra Italia e USA sul rafforzamento della cooperazione nella prevenzione e lotta alle forme gravi di criminalità; Roma, 28 maggio 2009; in vigore dal 03 ottobre 2014.
- Intesa di attuazione dell'accordo fra il Governo della Repubblica Italiana e il Governo degli Stati Uniti d'America sul rafforzamento della cooperazione nella prevenzione e nella lotta alle forme gravi di criminalità fatto a Roma il 28 maggio 2009; Ischia, 20 ottobre 2017 (acquisterà efficacia al ricevimento, da parte dei punti di contatto italiano e statunitense, della notifica dell'avvenuto perfezionamento degli aspetti tecnici necessari per l'attuazione dell'Intesa); non ancora vigente sul piano internazionale.

UZBEKISTAN

Accordo contro la criminalità organizzata, il terrorismo e il traffico illecito di droga; Roma, 21 novembre 2000; in vigore dal 17 agosto 2001.

VIETNAM

Accordo fra il Governo della Repubblica Italiana e il Governo della Repubblica Socialista del Vietnam di cooperazione nella lotta alla criminalità; Roma, 9 luglio 2014; in vigore dal 30 novembre 2016.

YEMEN

Accordo contro la criminalità; Roma, 26 novembre 2004 –in vigore dal 15 giugno 2007.

UNOCT

United Nations Office of Counter-Terrorism (UNOCT) ed il Corpo della Guardia di Finanza hanno sottoscritto, in data 28 marzo 2019, un *Memorandum* d'Intesa in materia di contrasto al finanziamento del terrorismo.

A livello globale, le **Nazioni Unite** costituiscono il principale foro di riferimento per la cooperazione multilaterale in materia di prevenzione e lotta al terrorismo. Il quadro giuridico disegnato dalla "Strategia Globale per la lotta al terrorismo" (adottata l'8 settembre 2006) rappresenta il terreno comune per l'azione di settore. In conformità ai principi in essa contenuti, l'Italia ha aderito a numerose convenzioni internazionali contro il terrorismo. Ha inoltre adeguato la sua legislazione in materia con l'adozione di altri provvedimenti legislativi approvati tra il 2004 e il 2018 e che, in linea con le risoluzioni del Consiglio di Sicurezza delle Nazioni Unite, hanno consentito di adattare la risposta investigativa e giudiziaria alle dinamiche evolutive della minaccia terroristica. Ci si riferisce anche a quei dati veicolati dal "Comitato Sanzioni" del Consiglio di Sicurezza agli Stati membri concernenti i soggetti tacciati di appartenere a reti terroristiche ed

inseriti nelle c.d. "liste consolidate". Una volta attivato per mezzo del MAECI, il Dipartimento della Pubblica Sicurezza provvede ad alimentare gli inserimenti e le cancellazioni nell'apposita banca dati delle Forze di Polizia. Tale attività discende dalla Risoluzione n. 1267/1999 con cui il Consiglio di Sicurezza ha introdotto una misura, specifica per la lotta al terrorismo, volta ad innescare una procedura di "congelamento" dei fondi e delle risorse economiche detenuti da persone fisiche e giuridiche, gruppi ed entità specificatamente individuate dal Consiglio di Sicurezza ONU collegate alla rete terroristica Al-Qaeda, sulla base di una black-list gestita da un apposito comitato (Comitato per le Sanzioni).
Nell'ambito del contrasto al terrorismo, un ruolo di primo piano, a livello nazionale, è svolto dal Comitato di Analisi Strategica Antiterrorismo (cd. C.A.S.A., best practice nazionale di coordinamento delle forze di law enforcement e delle agenzie di intelligence) e dal Comitato di Sicurezza Finanziaria (organismo interministeriale costituito presso il Ministero Economia e Finanze), e dalla sottesa "rete esperti".
Il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, per tramite delle competenti articolazioni, partecipa con regolarità alle annuali sessioni della Commissione ONU sulla Prevenzione del Crimine e la Giustizia Penale, che normalmente si tengono a Vienna nel mese di maggio.
In tale foro viene svolto un esame dello stato di ratifica e applicazione delle convenzioni delle Nazioni Unite in materia di crimine organizzato transnazionale, corruzione e terrorismo ed affrontata una discussione tematica che varia ad ogni edizione.
La XXIX sessione, che si sarebbe dovuta svolgere a Vienna dal 18 al 22 maggio 2020, è tuttavia stata posticipata e svolta in formato ridotto il 3 e 4 dicembre 2020, a causa della pandemia. La trattazione dei temi in agenda, ivi inclusa la discussione tematica sulle misure efficaci per la prevenzione ed il contrasto al traffico di migranti, è pertanto stata rinviata alla prossima edizione, che avrà luogo a Vienna dal 17 al 21 maggio 2021.

Il **Gruppo Roma-Lione** (RLG), dedicato specificamente alla lotta al terrorismo, alla criminalità organizzata e ai traffici illeciti internazionali, è nato nell'ottobre 2001, dopo gli attentati dell'11 settembre, su impulso della Presidenza italiana dell'allora G8, dalla fusione del "Gruppo Roma" sul controterrorismo e del "Gruppo Lione" sul contrasto al crimine internazionale. L'Italia è stata quindi attore cruciale nel lancio del "Roma-Lione" e nel suo sviluppo. Esso si riunisce, per prassi, due volte all'anno in seduta plenaria sotto la Presidenza di turno G7. Nel corso del 2020, sotto presidenza statunitense, si sono tenute due riunioni, in formato virtuale a causa delle restrizioni dovute all'emergenza epidemiologica da Covid-19. Il Roma-Lione "costruisce" un approccio comune dei Paesi G7 in tema di lotta al terrorismo/criminalità organizzata, elaborando strumenti pratici condivisi di collaborazione e "best practices", in particolare nei settori: anti-terrorismo, sicurezza dei trasporti, migrazione, affari giuridici, "law enforcement", crimine ad elevata tecnologia (incluso cyber crime). A tali settori sono dedicati 6 sotto-gruppi tematici: CTPSG (Counter-Terrorism Practitioner Sub-Group); CLASG (Criminal Legal Affairs Sub-Group); HTCSG (High Technology Crime Sub-Group); LEPSG (Law Enforcement Projects Sub-Group); MESG (Migration Experts Sub-Group); TSSG (Transportation Security Sub-Group). Il valore aggiunto del Roma-Lione è di duplice natura, con una prevalente dimensione pratica, ma sempre inquadrata in un'ottica di collaborazione politica strategica e di discussione più ampia ed "informale". L'Italia mantiene uno specifico ruolo propositivo sia sul piano strategico e di "policy", sia su quello delle competenze specifiche. Nella riunione RLG di Londra sotto presidenza britannica (28-30 ottobre 2013), l'Italia ha ottenuto la Presidenza del Sotto-Gruppo Migrazione, che attualmente detiene, il quale, nel corso degli anni e col mutare degli scenari globali, ha assunto una connotazione orientata al contrasto del terrorismo in connessione con i fenomeni migratori.
Con particolare riferimento alle attività in seno al Counter-Terrorism Practitioners Sub-Group (CTPSG), coordinato dalla Presidenza statunitense del 2020, la delegazione italiana ha orientato la discussione su alcune specifiche tematiche quali: l'utilizzo di watchlist e di dati acquisiti nei campi di battaglia e il pieno utilizzo di tali dati per la prevenzione di possibili infiltrazioni di terroristi/estremisti violenti nei flussi migratori; lo sfruttamento dell'emergenza epidemiologica a fini di propaganda da parte dei gruppi terroristici islamici e sodalizi di estrema destra e sinistra; l'attualizzazione del documento sulla minaccia.

Il **Global Counter Terrorism Forum (GCTF)** è stato lanciato ufficialmente a New York, a livello di Ministri degli Esteri, il 22 settembre 2011.
È una piattaforma antiterrorismo (CT) informale, politica e multilaterale che ha rafforzato l'architettura internazionale per affrontare il terrorismo del XXI secolo. Il punto centrale della missione globale del Forum è la promozione di un approccio strategico a lungo termine per contrastare il terrorismo e le ideologie estremiste violente che ne sono alla base. Il GCTF sviluppa buone pratiche e strumenti per i responsabili politici e gli operatori, finalizzate a rafforzare le capacità civili di CT, le strategie nazionali, i piani d'azione e i moduli di formazione. Costituisce rilevante network per funzionari e operatori degli assetti CT nazionali, ove condividere esperienze, competenze, strategie, strumenti e programmi di sviluppo di capacità.
E' articolato, a livello strategico, su un Comitato di coordinamento (Coordinating Commitee) presieduto dal marzo 2019 da Canada e Marocco e su cinque Gruppi di lavoro, tre tematici e due geografici; i tematici si occupano di: contrasto all'estremismo violento (CVE), combattenti terroristi stranieri (FTF), cooperazione giudiziaria penale e rule of law (CJRL); i geografici si occupano di: rafforzamento delle capacità nella regione dell'Africa orientale; capacity-building nella regione dell'Africa occidentale.
I gruppi tematici sono co-presieduti rispettivamente da Australia/Indonesia (CVE), Giordania/USA (FTFs) e Nigeria/Svizzera (CJRL), mentre quelli regionali da Egitto/Unione Europea (East Africa) e Algeria/Germania (West Africa).
Il GCTF sino ad oggi ha adottato i seguenti memoranda:
- memorandum di Rabat sulla cooperazione giudiziaria CT;
- memorandum di Roma su de-radicalizzazione e riabilitazione nelle carceri;
- memorandum di Algeri sul kidnapping for ransom;
- memorandum di Madrid sulle vittime del terrorismo;
- memorandum di Ankara sulle buone pratiche per un approccio multisettoriale per il contrasto del terrorismo violento.

Nel merito delle iniziative del GCTF svolte nel corso del 2020, si segnala la partecipazione del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno a diverse iniziative: il 22 gennaio 2020 si è svolto a New York l'incontro: "Initiative Launch Event", per elaborare un Watchlisting Guidance Manual che definisca criteri uniformi per la composizione delle liste di soggetti sospettati di far parte di organizzazioni terroristiche (watchlist), allo scopo di rafforzare i controlli alle frontiere, soprattutto nei confronti dei foreign terrorist fighters, nel rispetto dei diritti umani e dello stato di diritto nell'ambito dei Paesi membri delle Nazioni Unite.
Dal 6 al 9 aprile 2020 si sarebbe dovuto tenere a Roma il primo seminario regionale sul ruolo della sicurezza marittima nell'interdizione degli spostamenti dei terroristi, con focus sul Mediterraneo, ma a causa dell'emergenza pandemica da COVID 19 è stata annullata e rimandata a data da destinarsi.
Nei giorni 21 e 28 luglio 2020, si sono svolti due seminari virtuali, organizzati dal GCTF, preannunciati alla 16ª riunione del Comitato di Coordinamento del GCTF, del 23 settembre 2019, cui hanno preso parte numerosi esperti a livello globale dei Paesi partner, sui temi "Il ruolo delle legislazioni nazionali, internazionali e delle politiche di prevenzione, contrasto e di risposta al fenomeno degli spostamenti marittimi dei terroristi" e "Strumenti e risposte per il contrasto agli spostamenti marittimi dei terroristi – enti rilevanti pubblici e privati".
L'iniziativa è stata finalizzata alla condivisione di conoscenze sull'attuale, potenziale possibilità di sfruttamento del settore marittimo da parte dei terroristi per gli spostamenti, nonché sugli approcci nazionali di contrasto, con il particolare obiettivo di sviluppare un addendum al New York Memorandum on Good Practices for Interdicting Terrorist Travel. Tale documento conterrà ulteriori raccomandazioni di buone prassi per i partner governativi e del settore privato impegnati nella prevenzione del fenomeno. Esso rappresenterà un complemento per altri esercizi internazionali in materia e, in particolare, per quello dell'Interpol nel bacino mediterraneo e nell'Asia sud-est. L'addendum sarà presentato per l'approvazione alla prossima riunione ministeriale del GCTF che si terrà nel 2021.
Il 29 settembre 2020 si è tenuta, in formato virtuale, la 17ª Riunione del Comitato di coordinamento del Global Counter Terrorism Forum (GCTF); i lavori sono stati co-presieduti dal Direttore delle Questioni Globali del Ministero degli Affari Esteri del Marocco e dallo Special Advisor anti-terrorismo della Direzione Generale Affari Globali del Ministero degli Affari Esteri del Canada.

È stato sottolineato un punto di situazione sulle attività condotte dai 5 gruppi di lavoro del foro, di cui 3 tematici (Contrasto all'estremismo violento, Terroristi stranieri combattenti, Cooperazione giudiziaria penale e rule of law) e 2 geografici (Rafforzamento delle capacità in Africa Orientale e Occidentale).
Sono successivamente state illustrate alcune iniziative del foro, tra le quali le risposte di giustizia penale ai collegamenti tra terrorismo e crimine organizzato, il contrasto al finanziamento del terrorismo, questioni di genere nella prevenzione e contrasto al terrorismo e sicurezza marittima.
A fine sessione, sono stati approvati alcuni documenti, tra i quali una Dichiarazione ministeriale, la Visione strategica del GCTF per la prossima decade, una Raccolta di buone prassi sul rafforzamento della cooperazione nella prevenzione e contrasto dell'estremismo violento ed altra Raccolta di buone prassi sul nesso tra crimine organizzato e terrorismo, con focus sulla giustizia penale.
In merito al supporto fornito dall'Italia al CGTF, si segnala la partecipazione del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno a diverse iniziative tenutesi nel 2020; in particolare si richiama la partecipazione alla "17^ Riunione del Comitato di Coordinamento del GCTF", che si è tenuta in VTC il 29 settembre 2020, e al "Second Technical Workshop on the Application of Watchlists of Known and Suspected Terrorists, including FTFs", che si è tenuto sempre in modalità VTC l'8 dicembre 2020.

La **Coalizione Globale Anti Isil-Daesh**. All'indomani della caduta di Mosul, nel giugno 2014, gli Stati Uniti hanno promosso la creazione di una coalizione di contrasto all'autoproclamato Stato islamico (Daesh). Fin dal principio la Coalizione, pur concentrandosi sull'emergenza militare, ha adottato un approccio multidimensionale strutturato lungo cinque linee d'azione: l'operazione militare; il contrasto al flusso di combattenti stranieri; il contrasto alle fonti di finanziamento di Daesh; la lotta alla sua propaganda; la stabilizzazione delle aree liberate. Attualmente la Coalizione si compone di 83 partner, di cui quattro organizzazioni internazionali (Unione Europea, NATO, Lega Araba e INTERPOL). L'Italia è stata in questi anni attivamente impegnata in tutti gli ambiti di intervento della Coalizione. In particolare, il nostro Paese ha schierato in Iraq il secondo principale contingente militare dopo quello degli Stati Uniti, con l'obiettivo di formare unità militari (inclusi i Peshmerga curdi) e della polizia irachena. Queste ultime sono state addestrate da una Task Force multinazionale guidata dai Carabinieri. Militari italiani sono impegnati nella protezione del cantiere della diga di Mosul. Assetti aerei schierati in Kuwait hanno svolto attività di intelligence, sorveglianza e di ricerca e soccorso. L'Italia inoltre co-presiede, insieme a Stati Uniti e Arabia Saudita, il Gruppo di lavoro sul contrasto al finanziamento di Daesh (Counter-ISIS Finance Group – CIFG), che promuove una fattiva collaborazione e concrete misure degli Stati membri volte a eliminare le fonti di reddito di Daesh e dei suoi affiliati e a impedirne l'accesso al sistema finanziario internazionale.

L'Alleanza per la Sicurezza Internazionale (ISA) tra Ministeri dell'Interno di Paesi europei, asiatici e africani, è un meccanismo informale di consultazione, di cui fa parte l'Italia unitamente a Bahrein, Francia, Israele, Italia, Marocco, Senegal, Singapore, Slovacchia, Spagna e gli Emirati Arabi Uniti (che svolgono anche le funzioni di Segretariato), volto alla prevenzione e al contrasto del terrorismo e del crimine organizzato transnazionale, mediante lo scambio di esperienze e conoscenze e la diffusione di buone prassi.
Nell'ambito dei lavori del foro, sin dall'inizio, l'ISA si è concentrata su progetti per lo sviluppo di una matrice per la valutazione e la riduzione del rischio terrorismo di matrice jihadista, mediante l'individuazione delle piattaforme digitali per la navigazione in internet più utilizzate a livello globale per il reclutamento di nuovi combattenti, la diffusione di ideologie fondamentaliste e il conseguimento di finanziamenti, nonché l'individuazione di forme di collaborazione con il settore privato. A seguire, lo sviluppo di una matrice di valutazione rischi mirata al contrasto della diffusione della propaganda sulle piattaforme digitali anche in video, mediante la creazione di un database di parole chiave che determinino il blocco dei risultati delle ricerche. L'ISA, nell'ottica di una riduzione della minaccia terroristica, ha mostrato particolare interesse nei processi per la riabilitazione dei detenuti radicalizzati, enfatizzando al riguardo l'importanza dei leader religiosi, l'individuazione di figure idonee a fornire assistenza spirituale ai detenuti di credo musulmano nonché lo sviluppo di un dialogo inter-religioso.

Nel 2020, a causa della pandemia da Covid-19, la riunione ministeriale prevista in Slovacchia (in presenza) è stata rinviata a data da definirsi. In compenso, è stata avviata una serie di videoteleconferenze, su base quindicinale, incentrate su tematiche prescelte tra quelle che hanno registrato maggior interesse nel periodo pandemico, quali: abuso sessuale online su minori, a cui ha fatto seguito la Joint Operation "Online child sexual abuse and exploitation" consistita nella raccolta dei dati statistici di ogni Paese membro (numero, arresti, numero vittime identificate, numero siti web oscurati) nel periodo concordato (1 giugno – 1 settembre 2020); rilevamento del Covid-19 a mezzo di capacità olfattive di unità cinofile (28 maggio 2020); reati concernenti le sostanze stupefacenti durante il Covid 19 (28 luglio 2020). In più sono state effettuate la riunione dei Direttori dei Servizi della Cooperazione Internazionale (10 settembre 2020) e la 3^ riunione ministeriale (9 dicembre 2020).

Il **Financial Action Task Force - Group d'Action Financière (FATF- GAFI)** è un organismo intergovernativo che ha l'obiettivo di fissare standard comuni e promuovere l'adozione di regole e prassi per una efficace lotta al riciclaggio di denaro, al finanziamento del terrorismo e ad altre minacce correlate all'integrità del sistema finanziario interazionale.
Ne fanno parte 39 membri, tra cui l'Italia, e diverse organizzazioni che partecipano in qualità di membri associati (quali i Gruppi regionali costituiti sul modello del GAFI) o osservatori (ad es. IMF, WB, UNODC, Europol, ecc).
Le Raccomandazioni del FATF sono lo standard interazionale di riferimento in materia di contrasto del finanziamento del terrorismo e le Risoluzioni del Consiglio di Sicurezza delle Nazioni Unite rilevanti in materia chiedono ai Paesi di darvi attuazione.
Il GAFI ha condotto analisi specifiche sul sistema di finanziamento dei gruppi terroristici, in particolare dell'ISIL.
Il modello di cooperazione del GAFI si è andato estendendo, negli ultimi anni, ad organismi regionali similari, anche con l'obiettivo di rendere di applicazione universale gli standard elaborati dal GAFI stesso ed armonizzare le legislazioni nazionali in questo senso.
Il nuovo programma operativo del GAFI in materia di contrasto al finanziamento al terrorismo, adottato nel febbraio del 2018, si focalizza sugli attuali rischi di finanziamento del terrorismo, caratterizzati da una continua evoluzione, al fine di assicurare che l'effettiva attuazione degli standard globali del Gruppo contribuisca a preservare l'integrità del sistema finanziario.

L'**Unione Europea** si fonda su valori universali di dignità umana, libertà, uguaglianza e solidarietà, e rispetto dei diritti umani e delle libertà fondamentali. Gli atti terroristici costituiscono una delle più gravi violazioni dei valori universali di dignità umana, libertà, uguaglianza e solidarietà, e godimento dei diritti umani e delle libertà fondamentali su cui si fonda l'Unione. Essi rappresentano inoltre uno dei più seri attentati alla democrazia e allo Stato di diritto, principi che sono comuni agli Stati membri e sui quali si fonda l'Unione.
Per fornire una risposta all'evoluzione della minaccia terroristica, l'UE sta continuamente implementando ed ampliando gli strumenti a sua disposizione.
L'attuale strategia antiterrorismo dell'UE[1] mira a combattere il terrorismo su scala mondiale nel rispetto dei diritti umani e a rendere l'Europa più sicura, consentendo ai suoi cittadini di vivere in uno spazio di libertà, sicurezza e giustizia ed è **incentrata su quattro pilastri principali: 1.** la prevenzione del fenomeno terroristico; **2.** la protezione dei cittadini, delle infrastrutture, dei trasporti, con il necessario rafforzamento delle strutture di sicurezza; **3.** il perseguimento, inteso come il tentativo di impedire ai gruppi o singoli terroristi di comunicare, muoversi liberamente e pianificare attacchi, attraverso lo smantellamento delle loro reti di supporto e di finanziamenti; **4.** la risposta, intesa come la capacità di gestire e minimizzare le conseguenze di possibili attacchi terroristici in un'ottica di cooperazione e solidarietà. In tutti i pilastri, si riconosce l'importanza della cooperazione con i Paesi terzi e le istituzioni internazionali.
L'Unione Europea annovera tra le sue istituzioni deputate al contrasto del terrorismo anche quella del **"Coordinatore UE per la lotta al terrorismo"**[2]. Il suo incaricato è quello di: coordinare i lavori del Consiglio nella lotta al terrorismo; presentare raccomandazioni politiche e proporre al Consiglio settori prioritari d'azione; monitorare l'attuazione della strategia antiterrorismo dell'UE;

---

1 DOC.14469/4/05 REV 4 del 30 novembre 2005

2 Carica tuttora ricoperta dal belga Gilles de Kerchove

mantenere una visione d'insieme di tutti gli strumenti dell'UE, riferire al Consiglio e assicurare il follow-up delle decisioni del Consiglio; coordinarsi con i competenti organi preparatori del Consiglio, la Commissione e il SEAE, assicurare che l'UE svolga un ruolo attivo nella lotta al terrorismo; migliorare la comunicazione tra l'UE e i Paesi terzi.

Il terrorismo viene seguito in seno al Consiglio dell'UE, per gli aspetti interni nel settore GAI, **dal Gruppo di lavoro "TWP" (Terrorism Working Party).** Tale Gruppo dirige e gestisce il programma generale delle attività del Consiglio in materia di antiterrorismo. Il Gruppo è principalmente responsabile: dello scambio di informazioni e della valutazione delle minacce terroristiche; della lotta alla radicalizzazione e al reclutamento di potenziali terroristi; dello svolgimento di valutazioni reciproche delle migliori prassi degli Stati membri in materia di lotta al terrorismo.

Nell'ambito del TWP, si segnala l'impegno profuso dalla delegazione italiana per superare la situazione di stallo derivante dalla difficoltà di giungere a un approccio condiviso tra i Paesi UE per l'inserimento nel Sistema Informativo Schengen (SIS) di alerts, con dati identificativi e biometrici, per i foreign terrorist fighters forniti da Paesi terzi "affidabili", assicurando una maggiore protezione delle frontiere esterne dal rischio di ingressi di individui che rappresentano una minaccia per la sicurezza comune. Nel contesto delle iniziative dell'UE sulla prevenzione e contrasto della radicalizzazione che conduce all'estremismo violento e al terrorismo e stata assicurata l'attiva partecipazione al "Meccanismo Europeo di Cooperazione per la Prevenzione della Radicalizzazione". A tal proposito si segnala che nel corso del 2020, su iniziativa della Direzione Centrale della Polizia di Prevenzione del Dipartimento della PS, è stato dato avvio a un Progetto di collaborazione (Project Based Collaboration - PBC), per supportare i Paesi dei Balcani Occidentali nella gestione dei foreign fighters di rientro dalle zone di conflitto.

Il Gruppo collabora strettamente con il coordinatore antiterrorismo dell'UE ed Europol ed inoltre in diversi settori strategici con **il "Gruppo Terrorismo COTER" (aspetti internazionali).** Nel 2020 le tematiche che più hanno impegnato i lavori del Gruppo sono state: i cd. returnees (foreign terrorist fighters europei reduci dal conflitto siro-iracheno); utilizzo di internet con finalità terroristiche e l'approvazione del Regolamento sulla prevenzione della diffusione di contenuti terroristici online; attività di prevenzione della radicalizzazione; massimizzare lo sfruttamento delle potenzialità offerte dal Sistema Informativo Schengen (SIS), attraverso la costante implementazione degli alerts con i dati a disposizione e con quelli derivanti dalla cooperazione internazionale di polizia anche con Paesi ed Agenzie extra europee (in particolare Interpol); valutazione della minaccia; estremismo di destra.

Inoltre, l'Unione Europea dispone della **Commissione speciale sul terrorismo**[3], la quale ha il compito di esaminare, valutare ed analizzare la portata della minaccia terroristica sul territorio europeo, sulla base di quanto fornito dalle singole autorità nazionali degli Stati membri e dalle agenzie europee competenti in materia. L'obiettivo è quello di rafforzare la capacità europea di prevenire, indagare e perseguire i reati terroristici.

In tema, giova evidenziare anche **il ruolo del Comitato Permanente per la Cooperazione Operativa in materia di Sicurezza Interna (Co.S.I.)** quale referente strategico dell'UE nell'assicurare la promozione e il rafforzamento della cooperazione operativa sulla sicurezza interna dell'Unione europea e quale organismo in collegamento con i competenti gruppi del Consiglio, nonché con la Commissione e con le Agenzie dell'UE, per assicurare l'effettiva attuazione delle misure operative concordate. In tale contesto, il COSI esamina di volta in volta la possibilità di sviluppare una metodologia per un approccio strutturato e multilaterale alla cooperazione operativa nella lotta alle minacce terroristiche. Le principali tematiche discusse dal Co.S.I., nel corso del 2020, nella lotta al terrorismo sono state: estremismo violento di destra e terrorismo; foreing fighters in relazione alla situazione siriana e turca; valutazione della minaccia terroristica. Mentre quelle discusse dal Co.S.I. nelle riunioni congiunte con il Co.P.S. sono state: la raccolta e scambio di informazioni provenienti dai territori di conflitto nel contrasto al terrorismo; il Patto sulle missioni civili PSDC (Civilian CSDP Compact): nesso fra le dimensioni interna ed esterna della sicurezza dell'Unione Europea; i progetti di partenariato per la formazione all'antiterrorismo attuati nella regione MENA; la minaccia ibrida in relazione alla connessione fra dimensione interna ed esterna della sicurezza dell'Unione europea.

---

[3] TERR - Istituita dal Parlamento europeo nel luglio 2017, *"per affrontare le carenze pratiche e legislative nella lotta contro il terrorismo in tutta l'Unione europea e con partner e attori internazionali, con particolare riguardo alla cooperazione e sullo scambio di informazioni "*

La sicurezza è una delle principali preoccupazioni dei cittadini e i continui attentati terroristici sul territorio europeo hanno ulteriormente sottolineato la necessità di un intervento dell'UE in questo campo. Il 24 luglio 2020 la Commissione ha adottato una **strategia dell'UE per l'Unione della sicurezza 2020-2025**[4] proprio per concentrare l'azione sui settori prioritari in cui l'UE può apportare un valore aggiunto agli interventi nazionali e si incentra sulla creazione di competenze e capacità per garantire un ambiente di sicurezza adeguato alle esigenze future. L'obiettivo è offrire un vero valore aggiunto in termini di sicurezza per proteggere tutti i cittadini dell'UE e il pieno rispetto dei diritti fondamentali è al centro di questo lavoro, poiché la sicurezza dell'Unione può essere garantita solo se tutti sono convinti che i propri diritti fondamentali siano pienamente rispettati.

La minaccia rappresentata dalle reti terroristiche transnazionali dimostra chiaramente che un'azione coordinata dell'UE è indispensabile. L'attuale situazione indica la comparsa di minacce alla sicurezza transfrontaliere e intersettoriali sempre più complesse, che rendono ancora più essenziale una maggiore cooperazione in materia di sicurezza a tutti i livelli. La crisi causata dalla COVID-19 ha inoltre posto la sicurezza europea al centro dell'attenzione e rappresenta un banco di prova per la resilienza delle infrastrutture critiche, la preparazione alle crisi, le catene del valore strategiche e i sistemi di gestione delle crisi in Europa, oltre che per la resilienza delle nostre società nei confronti di interferenze manipolative e disinformazione.

La strategia per l'Unione della sicurezza **si compone di quattro priorità strategiche** di azione a livello dell'UE: **1.** creare un ambiente della sicurezza adeguato alle esigenze del futuro; **2.** affrontare le minacce in evoluzione; **3.** proteggere l'Europa dal terrorismo e dalla criminalità organizzata; **4.** garantire un ecosistema europeo forte in materia di sicurezza. Il fulcro della strategia è un'attuazione che richiede la piena partecipazione delle autorità nazionali in prima linea in materia di sicurezza nell'UE.

Anche se la responsabilità primaria della sicurezza incombe ai singoli Stati membri, negli ultimi anni è emerso chiaramente che la sicurezza di uno Stato membro è la sicurezza di tutti. L'UE può apportare una risposta multidisciplinare e integrata, fornendo agli operatori della sicurezza negli Stati membri gli strumenti e le informazioni di cui hanno bisogno[5]. A tal fine esistono già importanti strumenti giuridici, pratici e di sostegno, che però devono essere rafforzati e attuati più adeguatamente. Sono stati compiuti molti progressi per migliorare lo scambio di informazioni e la cooperazione in materia di intelligence con gli Stati membri e per restringere lo spazio in cui i terroristi e i criminali operano. Permane tuttavia il problema della frammentazione.

Proteggere l'Unione e i suoi cittadini non significa più garantire solo la sicurezza all'interno delle frontiere dell'UE, ma anche affrontare la dimensione esterna della sicurezza. L'approccio dell'UE alla sicurezza esterna nel quadro della politica estera e di sicurezza comune (PESC) e della politica di sicurezza e di difesa comune (PSDC) rimarrà un elemento essenziale dell'attività dell'UE volta a rafforzare la sicurezza all'interno dell'UE.

La nostra vita quotidiana dipende da un'ampia gamma di servizi che si fondono su infrastrutture, sia fisiche che digitali, e questo aspetto ne aumenta la vulnerabilità e la possibilità che possano subire perturbazioni. Durante la pandemia della COVID-19, le nuove tecnologie hanno consentito a molte imprese e servizi pubblici di continuare a operare. Tuttavia, ciò ha anche dato il via a un aumento impressionante di attacchi dolosi, ad opera di coloro che hanno tentato di sfruttare per finalità criminali le perturbazioni dovute alla pandemia e il passaggio al telelavoro grazie alle tecnologie informatiche[6]. Le conseguenze avrebbero potuto essere disastrose, mettendo a repentaglio i servizi sanitari essenziali nel periodo in cui sono stati sottoposti alle pressioni più intense. La crisi dovuta alla COVID-19 ha altresì posto in evidenza in che modo le divisioni e le incertezze sociali creino vulnerabilità sul piano della sicurezza. Ciò aumenta la possibilità che si verifichino attacchi più sofisticati e ibridi da parte di soggetti statali e non statali, che sfruttano i punti deboli ricorrendo a una combinazione di attacchi informatici, danni alle infrastrutture critiche[7], campagne di disinformazione e radicalizzazione del discorso politico[8].

---

4 COM(2020) 605.

5 Ad esempio mediante i servizi forniti dai programmi spaziali dell'UE, come Copernicus, che forniscono dati di osservazione della Terra e applicazioni per la sorveglianza delle frontiere, la sicurezza marittima, le attività di contrasto, la lotta alla pirateria, la dissuasione del traffico di stupefacenti e la gestione delle emergenze.

6 Europol: *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (Al di là della pandemia - In che modo la COVID-19 modificherà il panorama della criminalità organizzata e delle forme gravi di criminalità) (aprile 2020).

7 Le infrastrutture critiche sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini e il loro danneggiamento o distruzione avrebbe un impatto significativo (Direttiva 2008/114/CE del Consiglio).

8 Il 97 % dei cittadini dell'UE si è imbattuto in notizie false, il 38 % su base giornaliera. Cfr. JOIN(2020) 8 final.

L'UE ha già dimostrato in che modo può apportare un reale valore aggiunto. La strategia sull'Unione della sicurezza stabilisce assi di intervento concreti e si articola intorno a questi obiettivi comuni: s**viluppare competenze e capacità in materia di individuazione tempestiva, prevenzione e reazione rapida alle crisi:** l'Europa deve essere più resiliente per prevenire, proteggere e resistere agli shock futuri; **priorità ai risultati**: una strategia orientata ai risultati deve basarsi su un un'attenta valutazione delle minacce e dei rischi in modo che il nostro impegno sia più efficace possibile. Deve definire e applicare le norme e gli strumenti adeguati e richiede una intelligence strategica alla base delle politiche di sicurezza dell'UE; **associare tutti gli operatori del settore pubblico e del settore privato in uno sforzo comune:** i principali operatori sia del settore pubblico che di quello privato sono stati finora poco propensi a condividere informazioni in materia di sicurezza per timore di compromettere la sicurezza nazionale o la competitività[9].

L'analisi della minaccia menzionata evidenzia quattro priorità strategiche interdipendenti su cui occorre lavorare a livello unionale, nel pieno rispetto dei diritti fondamentali: **a)** un ambiente della sicurezza adeguato alle esigenze future; **b)** affrontare le minacce in evoluzione; **c)** proteggere i cittadini europei dal terrorismo e dalla criminalità organizzata; **d)** un ecosistema europeo forte in materia di sicurezza.

Protezione e resilienza delle infrastrutture critiche

Nella vita quotidiana gli individui dipendono da infrastrutture chiave. L'attuale quadro dell'UE in materia di protezione e resilienza delle infrastrutture critiche[10] non è al passo con l'evoluzione dei rischi. Con l'aumento della dipendenza della nostra economia e della nostra società dalle tecnologie online, i rischi di un possibile attavvo terroristico non fanno che aumentare. Il quadro legislativo deve far fronte all'aumento dell'interconnessione e dell'interdipendenza, con misure rigorose in materia di protezione e resilienza delle infrastrutture critiche, sia informatiche che fisiche. Ciò richiederà una serie di atti legislativi che, rivedendo le norme esistenti, garantiscano un livello comune elevato di sicurezza. Un elemento fondamentale per proteggere le principali risorse digitali dell'UE e nazionali consiste anche nel dotare le infrastrutture critiche di un canale sicuro per le comunicazioni. La Commissione sta collaborando con gli Stati membri per istituire un'infrastruttura quantistica da punto a punto sicura, terrestre e spaziale, associata al sistema di comunicazioni satellitari governative sicure previsto dal regolamento relativo al programma spaziale[11].

Cybersicurezza

I benefici sempre più numerosi che le tecnologie digitali hanno apportato alla nostra vita hanno fatto della **cybersicurezza** delle tecnologie una questione di importanza strategica[12]. Il numero di attacchi informatici continua ad aumentare[13]. Nel 2017 l'UE ha presentato un approccio alla cybersicurezza fondata sullo sviluppo della resilienza, su una risposta rapida e un'azione efficace di dissuasione[14]. L'UE adesso deve garantire che le sue capacità in materia di cybersicurezza siano al passo con la realtà, al fine di garantire resilienza e risposte adeguate. La prossima fase del lavoro dell'UE dovrebbe esserela presentazione di una nuova strategia europea per la cybersicurezza.

Dato il dispiegamento in corso dell'**infrastruttura 5G** nell'UE e la potenziale dipendenza di molti servizi critici dalle reti 5G, le conseguenze di una perturbazione sistemica e generalizzata sarebbero particolarmente gravi. Il processo avviato dalla raccomandazione della Commissione del 2019 sulla cybersicurezza delle reti 5G[15] ha portato adesso a interventi specifici degli Stati membri in relazione alle misure chiave stabilite nel pacchetto di strumenti per il 5G[16]. Per garantire una cooperazione operativa strutturata e coordinata la Commissione ha già individuato la necessità di un'**unità congiunta per il ciberspazio**, che potrebbe includere un meccanismo di assistenza reciproca a livello dell'UE nei periodi di crisi.

Altrettanto importanti sono le norme comuni in **materia di sicurezza delle informazioni e sicurezza informatica** per l'insieme delle istituzioni, organi e agenzie dell'UE. L'obiettivo

---

[9] Comunicazione congiunta "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE", JOIN(2017) 450 final.

[10] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016). Direttiva 2008/114/CE del Consiglio, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

[11] Proposta di regolamento che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale, COM(2018) 447 final.

[12] Raccomandazione della Commissione sulla cibersicurezza delle reti 5G, C(2019) 2335; Comunicazione "Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE", COM(2020) 50 final.

[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[14] Comunicazione congiunta "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE", JOIN(2017) 450 final.

[15] Raccomandazione della Commissione sulla cibersicurezza delle reti 5G, C(2019) 2335 final, di cui è prevista, nel documento stesso, una revisione nell'ultimo trimestre del 2020.

[16] Cfr. la relazione del gruppo di cooperazione NIS sull'attuazione del pacchetto di strumenti del 24 luglio 2020.

dovrebbe essere quello di elaborare norme comuni obbligatorie e rigorose per lo scambio sicuro di informazioni e la sicurezza delle infrastrutture e dei sistemi digitali in tutte le istituzioni, gli organismi e le agenzie dell'UE. Questo nuovo quadro dovrebbe fungere da base per una cooperazione operativa forte ed efficiente sulla cybersicurezza, incentrata sul ruolo della squadra di pronto intervento informatico (CERT-UE).

Protezione degli spazi pubblici

I recenti attentati terroristici si sono concentrati negli **spazi pubblici**, tra cui luoghi di culto e nodi di trasporto, sfruttando la loro natura aperta e accessibile. L'aumento degli atti di terrorismo scatenati dall'estremismo politico o ideologico ha reso questa minaccia ancora più grave. Ciò richiede il rafforzamento della protezione fisica di tali luoghi e sistemi di rilevamento adeguati, senza compromettere le libertà dei cittadini[17]. La Commissione rafforzerà la cooperazione tra settore pubblico e privato per la protezione degli spazi pubblici, con finanziamenti, scambi di esperienze e buone pratiche, orientamenti specifici e raccomandazioni[18].

Il mercato dei **droni** continua ad ampliarsi, con molti utilizzi validi e legittimi. Tuttavia i droni possono anche essere impropriamente utilizzati da criminali e terroristi, e in tal caso gli spazi pubblici sono particolarmente minacciati. Le conoscenze sull'uso dei droni nei conflitti potrebbero essere sfruttate in Europa sia direttamente (da parte dei combattenti terroristi stranieri di ritorno) che online. Le norme già elaborate dall'Agenzia europea per la sicurezza aerea costituiscono un primo passo importante anche per quanto riguarda la registrazione degli operatori di droni e l'identificazione remota obbligatoria dei droni. Adesso che i droni sono sempre più disponibili, economicamente accessibili e perfezionati, sono tuttavia necessari ulteriori interventi che potrebbero includere la condivisione di informazioni, orientamenti e buone pratiche ad uso di tutti, autorità di contrasto comprese, o la sperimentazione su più ampia scala di contromisure per i droni[19]. Inoltre, occorre analizzare e affrontare ulteriormente le implicazioni dell'uso dei droni negli spazi pubblici per la protezione della riservatezza dei dati.

Cibercriminalità

La tecnologia offre nuove opportunità per la società, e anche nuovi strumenti per il sistema giudiziario e le autorità di contrasto. La dipendenza da sistemi online ha dato anche il via a un'ondata di attacchi da parte della **cibercriminalità**[20]. Il cosiddetto "cybercrime as-a-service" (ossia l'offerta di servizi illegali) e l'economia "cibercriminale" sotterranea offrono un agevole accesso a prodotti e servizi informatici online offerti dalla criminalità informatica. Ad esempio, nella filiera farmaceutica legale sono stati inseriti medicinali contraffatti e falsificati[21]. L'aumento esponenziale di materiale pedopornografico online[22] ha messo in luce le conseguenze sociali dell'evoluzione dei modelli di criminalità. Il primo strumento di difesa è la **creazione di un ambiente resiliente grazie ad una solida cybersicurezza**. Le autorità di contrasto devono poter di lavorare nel settore delle indagini digitali disponendo di norme chiare per indagare e perseguire i reati e offrire alle vittime la protezione necessaria. Queste attività dovrebbero fondarsi sulla task force di azione congiunta contro la criminalità informatica di Europol e il protocollo di risposta alle emergenze delle autorità di contrasto istituiti per coordinare la risposta ai ciberattacchi su vasta scala. Occorrono inoltre meccanismi efficaci che consentano di istituire dei partenariati e una cooperazione tra il settore pubblico e quello privato. L'UE sostiene **la convenzione di Budapest del Consiglio d'Europa** sulla criminalità informatica; quale modello efficace e consolidato che consente a tutti i paesi di individuare i sistemi e i canali di comunicazione di cui hanno bisogno per collaborare efficacemente.

Moderni organismi di contrasto

Gli operatori della giustizia e delle attività di contrasto devono adeguarsi alle nuove tecnologie. Per stare al passo con l'evoluzione tecnologica e le minacce emergenti, le autorità di contrasto devono avvalersi di nuovi strumenti, acquisire nuove competenze e sviluppare tecniche investigative alternative. Ad integrazione delle azioni legislative volte a migliorare l'accesso transfrontaliero alle

---

[17] I sistemi di identificazione biometrica remota meritano una particolare attenzione. Le osservazioni iniziali della Commissione figurano nel Libro bianco della Commissione del 19 febbraio 2020 sull'intelligenza artificiale, COM(2020) 65.

[18] Orientamenti in materia di buone pratiche sono contenuti nel documento SWD(2019) 140 che contiene una sezione sulla cooperazione pubblico-privato. I finanziamenti nell'ambito dell'ISF-Polizia sono incentrati in modo particolare sul rafforzamento della cooperazione pubblico-privato.

[19] Di recente è stato istituito un programma pluriennale di test per aiutare gli Stati membri a mettere a punto una metodologia comune e una piattaforma di prova in questo ambito.

[20] Secondo alcune proiezioni, i costi delle violazioni di dati raggiungeranno 5 000 miliardi di USD l'anno entro il 2024, con un aumento di 3 000 miliardi di USD nel 2015 (*Juniper Research, The Future of Cybercrime & Security*).

[21] Uno studio del 2016 (Legiscript) ha stimato che, a livello globale, solo il 4 % delle farmacie online opera in modo legale, e le 30000/35000 farmacie illegali online mirano in particolare alla clientela dell'UE.

[22] Strategia dell'UE per una lotta più efficace contro l'abuso sessuale dei minori, COM (2020) 607.

prove elettroniche nelle indagini penali, l'UE può aiutare le autorità di contrasto a sviluppare le capacità di cui hanno bisogno per individuare, proteggere e leggere i dati necessari alle indagini sui reati e per utilizzare tali dati come prove nei procedimenti giudiziari. La Commissione esaminerà misure volte a **rafforzare la capacità di contrasto nelle indagini digitali**, definendo le modalità per utilizzare al meglio la ricerca e lo sviluppo al fine di creare nuovi strumenti di contrasto e per fornire un adeguato insieme di competenze alle attività di contrasto e al sistema giudiziario attraverso azioni di formazione.

Approcci comuni possono anche garantire che **l'intelligenza artificiale, le capacità spaziali, i Big Data** e **il calcolo ad alte prestazioni** siano integrati nella politica di sicurezza in modo efficace, sia per quanto riguarda la lotta al terrorismo che per garantire i diritti fondamentali. L'intelligenza artificiale potrebbe agire come potente strumento per combattere la criminalità, aprendo enormi capacità investigative grazie all'analisi di grandi quantità di informazioni e all'individuazione di modelli e anomalie[23]. Può inoltre fornire strumenti concreti, ad esempio per contribuire a individuare i contenuti terroristici online, scoprire transazioni sospette nelle vendite di prodotti pericolosi o offrire assistenza ai cittadini in situazioni di emergenza. Realizzare questo potenziale significa creare ponti tra la ricerca, l'innovazione e gli utenti dell'intelligenza artificiale grazie a una governance e a infrastrutture tecniche adeguate, coinvolgendo attivamente il settore privato e il mondo accademico. Significa anche applicare i più elevati standard di conformità ai diritti fondamentali, garantendo nel contempo un'efficace protezione dei cittadini.

Le informazioni e le prove elettroniche sono necessarie per circa l'85 % delle indagini relative a reati gravi e di terrorismo, e il 65 % delle richieste totali è rivolto a prestatori con sede in un'altra giurisdizione[24]. È essenziale stabilire norme chiare per l'accesso transfrontaliero alle prove elettroniche nelle indagini penali. La rapida adozione da parte del Parlamento europeo e del Consiglio delle proposte relative alle prove elettroniche è pertanto fondamentale per fornire agli operatori uno strumento efficace.

L'accesso alle prove digitali dipende anche dalla disponibilità di informazioni. Se i dati vengono cancellati troppo rapidamente, prove importanti possono scomparire impedendo di identificare e localizzare le persone sospettate e le reti criminali (oltre alle vittime). D'altro canto, i meccanismi di conservazione dei dati sollevano questioni relative alla tutela della vita privata. In funzione dell'esito delle cause pendenti dinanzi alla Corte di giustizia dell'Unione europea, la Commissione valuterà la via da seguire in materia di conservazione dei dati.

Attualmente una parte sostanziale delle indagini contro tutte le forme di criminalità e terrorismo implica **informazioni cifrate**. La cifratura è essenziale nel mondo digitale, in quanto rende sicuri i sistemi digitali e le transazioni e tutela una serie di diritti fondamentali, tra cui la libertà di espressione, la privacy e la protezione dei dati. Tuttavia, se utilizzata a fini criminali e terroristici, può mascherare anche l'identità dei criminali e nascondere il contenuto delle loro comunicazioni. La Commissione esplorerà e sosterrà soluzioni tecniche, operative e giuridiche equilibrate rispetto alle sfide e promuoverà un approccio che mantenga l'efficacia della cifratura nel proteggere la privacy e la sicurezza delle comunicazioni, fornendo nel contempo una risposta efficace alla criminalità e al terrorismo.

Lotta ai contenuti illegali online

Allineare la sicurezza degli ambienti fisici e di quelli online significa continuare a mettere in atto azioni per **contrastare i contenuti illegali online**. Sempre più spesso, le minacce principali per i cittadini, quali il terrorismo, l'estremismo o gli abusi sessuali sui minori, fanno affidamento sull'ambiente digitale: ciò richiede un'azione concreta e un quadro per garantire il rispetto dei diritti fondamentali. Un primo passo essenziale in questa direzione è stata la conclusione dei negoziati sulla proposta di legislazione[25] sui contenuti terroristici online, di cui va garantita l'attuazione. Il rafforzamento della cooperazione volontaria tra le autorità di contrasto e il settore privato nel **Forum dell'UE su Internet** è fondamentale anche per contrastare l'abuso di Internet da parte di terroristi, estremisti violenti e criminali. L'unità UE addetta alle segnalazioni su Internet di Europol continuerà a svolgere un ruolo cruciale nel monitorare l'attività dei gruppi terroristici online e le azioni intraprese dalle piattaforme[26] nonché nell'ulteriore sviluppo del **protocollo di crisi**

---

[23] Ad esempio, nel caso dei reati finanziari.

[24] Commissione europea, SWD (2018) 118 final.

[25] Proposta sulla prevenzione della diffusione di contenuti terroristici online, COM (2018) 640, 12 settembre 2018.

[26] Europol, novembre 2019.

dell'UE[27]. Inoltre, la Commissione continuerà a collaborare con i partner internazionali, anche partecipando al **Forum Internet mondiale per la lotta contro il terrorismo**, al fine di affrontare queste sfide a livello mondiale. Proseguiranno i lavori volti a sostenere lo sviluppo di narrazioni alternative e contronarrazioni grazie al programma di responsabilizzazione della società civile[28].

Per prevenire e contrastare la diffusione di forme illegali di incitamento all'odio online, nel 2016 la Commissione ha introdotto il codice di condotta contro l'incitamento all'odio online, con l'impegno volontario da parte delle piattaforme online di rimuovere i contenuti dell'incitamento all'odio. Tuttavia, le piattaforme devono migliorare ulteriormente la trasparenza e il feedback agli utenti e garantire una valutazione coerente dei contenuti segnalati[29].

Il Forum dell'UE su Internet agevolerà inoltre gli scambi sulle tecnologie, esistenti e in via di sviluppo, per affrontare le sfide legate agli abusi sessuali online sui minori. La lotta contro gli abusi sessuali online sui minori è al centro di una nuova strategia per potenziare la **lotta contro gli abusi sessuali su minori**[30], che intende sfruttare al massimo gli strumenti disponibili a livello dell'UE per contrastare tali reati. Inoltre, la Commissione continuerà a dialogare con i partner internazionali e con il **Forum Internet mondiale per la lotta contro il terrorismo**, anche attraverso il comitato consultivo indipendente, al fine di affrontare tali sfide a livello mondiale, preservando nel contempo i valori e i diritti fondamentali dell'UE. Dovrebbero essere affrontati anche nuovi temi come gli algoritmi o il gioco on line[31].

Minacce ibride

La portata e la diversificazione attuali delle minacce ibride non hanno precedenti. La crisi causata dalla COVID-19 ne offre numerosi esempi, con diversi soggetti statali e non statali che cercano di strumentalizzare la pandemia, in particolare attraverso la manipolazione dell'ambiente di informazione e ponendo sfide alle infrastrutture fondamentali. Ciò rischia di indebolire la coesione sociale e di minare la fiducia nelle istituzioni dell'UE e nei governi degli Stati membri.

L'approccio dell'UE alle minacce ibride è definito nel quadro congiunto del 2016 e nella comunicazione congiunta del 2018 sul rafforzamento della resilienza ibrida. L'azione a livello dell'UE è sostenuta da un insieme consistente di strumenti che interessano anche il nesso tra sicurezza interna ed esterna e sono basati su un approccio esteso a tutta la società e sulla stretta cooperazione con i partner strategici, in particolare la NATO e il G7.

Con la pubblicazione di una relazione sull'attuazione dell'approccio dell'UE alle minacce ibride[32] e in base alla relativa mappatura[33], i servizi della Commissione e il Servizio europeo per l'azione esterna istituiranno una **piattaforma online ristretta** che servirà da riferimento agli Stati membri per quanto riguarda gli strumenti e le misure per la lotta alle minacce ibride a livello dell'UE.

La cellula dell'UE per l'analisi delle minacce ibride rimarrà il punto di contatto dell'UE per le valutazioni delle minacce ibride. L'obiettivo è massimizzare l'effetto dell'azione dell'UE riunendo in tempi rapidi le risposte settoriali e garantendo una cooperazione senza soluzione di continuità con i nostri partner, la NATO in primo luogo.

Terrorismo e radicalizzazione

La minaccia terroristica nell'UE rimane elevata. Nonostante la diminuzione generale del loro numero, il rischio per i cittadini UE di un attacco jihadista effettuato o ispirato da Da'esh e al-Qaeda e i loro affiliati rimane elevato[34]. D'altro canto sta aumentando anche la minaccia dell'estremismo di destra violento[35]. La grande maggioranza degli attentati terroristici recenti è costituita da attacchi a "tecnologia bassa", eseguiti da soggetti che agiscono da soli in spazi pubblici, mentre la propaganda terroristica online ha assunto un nuovo significato con la diretta streaming degli attacchi di Christchurch[36]. La minaccia rappresentata dalle persone radicalizzate resta elevata ed è potenzialmente rafforzata dai combattenti terroristi stranieri di ritorno e dagli estremisti che escono

---

27 A Europe that protects - EU Crisis Protocol: responding to terrorist content online(Un'Europa che protegge - Protocollo di crisi dell'UE: reagire ai contenuti terroristici online), (ottobre 2019).

28 In collegamento con le iniziative del programma di sensibilizzazione al problema della radicalizzazione, cfr. la sezione IV.3.

29 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

30 Una strategia per una lotta più efficace contro gli abusi sessuali sui minori, COM(2020) 607.

31 I terroristi ricorrono sempre più spesso al sistema di messaggistica delle piattaforme di gioco per gli scambi e i giovani terroristi hanno nuovamente sferrato attacchi violenti nei videogiochi.

32 Relazione sull'attuazione del quadro congiunto per contrastare le minacce ibride del 2016 e comunicazione congiunta del 2018 "Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride", SWD (2020) 153.

33 Mappatura delle misure relative al rafforzamento della resilienza e al contrasto delle minacce ibride, SWD (2020) 152.

34 In totale 13 Stati membri dell'UE hanno segnalato 119 attentati terroristici completati, falliti e sventati, con dieci morti e 27 feriti (Europol, Relazione sulla situazione e sulle tendenze del terrorismo nell'Unione europea, 2020).

35 Nel 2019 ci sono stati sei attacchi terroristici ad opera di gruppi di destra (uno è stato portato a termine, uno è fallito, quattro sono stati sventati: in tre Stati membri), rispetto ad uno solo nel 2018, e vi sono stati altri morti in casi non classificati come terrorismo (Europol, 2020).

36 Nel periodo che va da luglio 2015 alla fine del 2019 Europol ha reperito contenuti terroristici in 361 piattaforme (Europol, 2020).

di prigione. Gli Stati membri detengono la responsabilità primaria nella lotta al terrorismo e alla radicalizzazione. Tuttavia, la crescente dimensione transfrontaliera/intersettoriale della minaccia richiede ulteriori passi per quanto riguarda la cooperazione e il coordinamento a livello dell'UE. L'efficace attuazione della legislazione antiterrorismo dell'UE, comprese le misure restrittive[37], è una priorità.

Per sostenere ulteriormente gli Stati membri nella lotta contro il terrorismo e la radicalizzazione, la Commissione ha adottato un **programma di lotta al terrorismo dell'UE**[38]. Il programma si basa sulle politiche e sugli strumenti esistenti e rafforzerà il quadro dell'UE per migliorare ulteriormente l'anticipazione delle minacce e dei rischi, la prevenzione della radicalizzazione e dell'estremismo violento, la protezione delle persone e delle infrastrutture, anche attraverso la sicurezza delle frontiere esterne e un seguito efficace dopo gli attacchi.

La prevenzione è fondamentale per combattere il terrorismo. Gli sforzi dell'UE nel settore della **prevenzione della radicalizzazione** si basano sulla solida esperienza acquisita finora nel sostegno agli operatori di prima linea e ai responsabili politici. Il 24 novembre 2020 la Commissione ha adottato **un nuovo piano d'azione sull'integrazione e l'inclusione**[39]. Gli strumenti esistenti sono integrati da azioni nell'ambito del programma di lotta al terrorismo per contrastare le ideologie estremiste online, intensificare gli sforzi nelle carceri e in materia di riabilitazione e reinserimento, anche per i combattenti terroristi stranieri, rafforzare il sostegno agli attori locali e creare comunità più resilienti.

I terroristi cercano di acquistare e di utilizzare come armi **materiali chimici, biologici, radiologici e nucleari** (CBRN)[40] e di sviluppare le conoscenze e le capacità per utilizzarli[41]. Il potenziale degli attacchi CBRN è posto in primo piano dalla propaganda terroristica. Data l'entità del danno potenziale, si tratta di una questione che merita grande attenzione. Sulla base dell'approccio utilizzato per regolamentare l'accesso ai precursori degli esplosivi, la Commissione cercherà di limitare l'accesso ad alcune sostanze chimiche pericolose che potrebbero essere utilizzate per compiere attentati. Sarà inoltre fondamentale sviluppare le capacità di risposta dell'UE per quanto riguarda la protezione civile (rescEU) sul campo nel settore CBRN.

L'UE ha sviluppato la legislazione più avanzata al mondo per limitare l'accesso ai **precursori di esplosivi**[42] e individuare operazioni sospette volte alla costruzione di ordigni esplosivi improvvisati. Ma la minaccia rappresentata dagli esplosivi artigianali, usati in molteplici attentati in tutta l'UE, rimane elevata[43]. Il primo passo deve essere l'attuazione delle norme, oltre a garantire che l'ambiente online non consenta di sfuggire ai controlli.

Anche l'efficace perseguimento di coloro che hanno commesso reati di terrorismo, inclusi i **combattenti terroristi stranieri** attualmente in Siria e in Iraq, costituisce un elemento importante della politica antiterrorismo. Sebbene tali questioni siano affrontate in primo luogo dagli Stati membri, il coordinamento e il sostegno dell'UE possono dare un contributo per affrontare le sfide comuni. Le misure in corso per attuare pienamente la legislazione sulla sicurezza delle frontiere[44] e utilizzare al meglio tutte le pertinenti banche dati dell'UE per condividere informazioni su sospetti noti costituiranno un passo importante. Oltre ad individuare le persone ad alto rischio, occorre una politica di reinserimento e di riabilitazione.

La sfida costituita dai combattenti terroristi stranieri è emblematica del legame tra **sicurezza esterna** ed interna. La cooperazione in materia di lotta al terrorismo nonché prevenzione e contrasto della radicalizzazione e dell'estremismo violento è fondamentale per la sicurezza all'interno dell'UE[45]. Occorrono ulteriori misure per sviluppare partenariati e cooperazione in materia di lotta al terrorismo con i paesi del vicinato e oltre, attingendo alle competenze della rete per la lotta al

---

37 Nell'intento di combattere il terrorismo, il Consiglio ha adottato misure restrittive riguardanti l'ISIL (Daesh) e Al-Qaeda e misure restrittive specifiche contro determinate persone ed entità. Per una panoramica di tutte le misure restrittive, cfr. la mappa delle sanzioni dell'UE (https://www.sanctionsmap.eu/#/main).

38 COM(2020) 795.

39 COM(2020) 758.

40 Negli ultimi due anni, ad esempio, si sono verificati diversi casi in Europa (Francia, Germania, Italia) e altrove (Tunisia, Indonesia) che implicavano agenti biologici (in genere tossine di origine vegetale).

41 Il Consiglio ha adottato misure restrittive contro la proliferazione e l'uso delle armi chimiche.

42 Le sostanze chimiche che potrebbero essere utilizzate impropriamente per fabbricare esplosivi artigianali. Esse sono disciplinate dal regolamento (UE) 2019/1148 relativo all'immissione sul mercato e all'uso di precursori di esplosivi.

43 Gli attentati di Oslo (2011), Parigi (2015), Bruxelles (2016) e Manchester (2017) sono alcuni esempi di queste azioni devastanti. Un attentato compiuto a Lione (2019) con esplosivo artigianale ha provocato il ferimento di 13 persone.

44 Compreso il nuovo mandato dell'Agenzia europea della guardia di frontiera e costiera (Frontex).

45 Le conclusioni del Consiglio del 16 giugno 2020 hanno sottolineato la necessità di proteggere i cittadini dell'UE dal terrorismo e dall'estremismo violento, in tutte le loro forme e indipendentemente dalla loro origine, e di rafforzare ulteriormente l'impegno e l'azione esterna dell'UE in materia di antiterrorismo in determinate aree geografiche e tematiche prioritarie.

terrorismo e agli esperti di sicurezza dell'UE. Il piano d'azione comune sulla lotta al terrorismo per i **Balcani occidentali** è un buon punto di riferimento per tale cooperazione mirata. In particolare, dovrebbero essere compiuti sforzi per sostenere la capacità dei paesi partner di individuare e localizzare i combattenti terroristi stranieri.

L'UE continuerà inoltre a promuovere la cooperazione multilaterale, in collaborazione con i principali organismi globali in questo settore, quali **le Nazioni Unite, la NATO, il Consiglio d'Europa, l'Interpol e l'OSCE**. Si impegnerà inoltre con il Forum globale contro il terrorismo e la coalizione internazionale per combattere il Daesh, nonché con i relativi attori della società civile. Gli strumenti di politica esterna dell'Unione, compresi lo sviluppo e la cooperazione, svolgono anche un ruolo importante a livello di cooperazione con i paesi terzi per prevenire il terrorismo e la pirateria. La cooperazione internazionale è essenziale anche per prosciugare tutte le fonti di **finanziamento del terrorismo**, ad esempio attraverso il Gruppo di azione finanziaria internazionale.

Cooperazione e scambio d'informazioni

Uno dei contributi più cruciali che l'UE può fornire alla protezione dei cittadini consiste nell'aiutare i responsabili della sicurezza a lavorare bene insieme. La cooperazione e lo scambio di informazioni sono gli strumenti più efficaci per combattere la criminalità e il terrorismo e far applicare la legge. Per essere efficienti, gli interventi devono essere mirati e tempestivi. Per essere affidabili, deve essere oggetto di salvaguardie e controlli comuni.

Sono stati messi a punto diversi strumenti e strategie settoriali dell'UE per sviluppare ulteriormente la **cooperazione operativa nell'attività di contrasto** tra gli Stati membri. Tuttavia, il livello di collaborazione potrebbe essere migliorato attraverso l'integrazione e l'aggiornamento degli strumenti disponibili. La Commissione esaminerà in che modo un nuovo codice di cooperazione di polizia possa sostenere una cooperazione specifica in materia di attività di contrasto. Le autorità di contrasto degli Stati membri si avvalgono sempre più spesso di sostegno e competenze a livello dell'UE, mentre l'EU INTCEN ha svolto un ruolo chiave nel promuovere lo scambio di intelligence strategica tra i servizi di intelligence e di sicurezza degli Stati membri, fornendo alle istituzioni dell'UE conoscenza situazionale basata sull'intelligence[46]. **Europol** può inoltre svolgere un ruolo chiave nell'ampliare la cooperazione con i paesi terzi per contrastare la criminalità e il terrorismo. Tuttavia, Europol si trova oggi ad affrontare una serie di gravi limitazioni - in particolare per quanto riguarda lo scambio diretto di dati personali con parti private - il che le impedisce di sostenere efficacemente gli Stati membri nella lotta al terrorismo e alla criminalità. Un altro elemento fondamentale per creare connessioni è l'ulteriore sviluppo di **Eurojust** per massimizzare la sinergia tra la cooperazione nell'attività di contrasto e la cooperazione giudiziaria.

Le **informazioni sui viaggiatori** hanno contribuito a migliorare i controlli alle frontiere, ridurre la migrazione irregolare e individuare le persone che presentano rischi per la sicurezza. Le informazioni anticipate sui passeggeri sono costituite dai dati biografici di ogni passeggero raccolti dai vettori aerei durante il check-in e trasmessi in anticipo alle autorità di controllo delle frontiere del paese di destinazione. La revisione del quadro giuridico[47] potrebbe consentire un uso più efficace delle informazioni, garantendo al contempo il rispetto della legislazione in materia di protezione dei dati e agevolando il flusso di passeggeri. I dati del codice di prenotazione (Passenger Name Records — PNR) corrispondono ai dati forniti dai passeggeri al momento della prenotazione dei voli. L'attuazione della direttiva sul codice di prenotazione[48] è fondamentale al riguardo e la Commissione continuerà a sostenerne l'applicazione. Inoltre, come azione a medio termine, la Commissione avvierà una revisione dell'attuale approccio relativo al **trasferimento dei dati del codice di prenotazione (PNR) verso i paesi terzi**.

Le autorità di contrasto dell'UE si affidano anche ai principali paesi partner per individuare criminali e terroristi e svolgere le relative indagini. **Partenariati per la sicurezza tra l'UE e i paesi terzi** potrebbero venire potenziati al fine di intensificare la cooperazione per contrastare minacce condivise quali il terrorismo, la criminalità organizzata, la criminalità informatica, gli abusi sessuali sui minori e la tratta di esseri umani. Tale approccio si baserebbe su interessi comuni in materia di sicurezza e sui dialoghi consolidati in materia di cooperazione e sicurezza.

---

[46] Il Centro UE di situazione e di intelligence (INTCEN) funge da unico punto di accesso per i servizi di intelligence e di sicurezza degli Stati membri per fornire all'UE una conoscenza situazionale basata sull'intelligence.

[47] Direttiva 2004/82/CE del Consiglio concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

[48] Direttiva 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

Oltre alle informazioni, lo scambio di conoscenze può essere particolarmente utile per aumentare la preparazione delle attività di contrasto nel caso di **minacce non tradizionali**. Oltre a incoraggiare lo scambio di buone pratiche, la Commissione esaminerà un eventuale **meccanismo di coordinamento a livello dell'UE per le forze di polizia** in caso di eventi di forza maggiore, quali le pandemie. L'attuale pandemia ha inoltre dimostrato che il controllo digitale del territorio da parte della polizia di prossimità, accompagnata da quadri giuridici per facilitare l'attività di polizia online, sarà fondamentale nella lotta alla criminalità e al terrorismo. Le forme di cooperazione tra polizia e comunità, offline e online, possono prevenire la criminalità e mitigare l'impatto della criminalità organizzata, della radicalizzazione e delle attività terroristiche. Il collegamento tra interventi di polizia a livello locale, regionale, nazionale e dell'UE è un fattore chiave per il successo dell'Unione della sicurezza nel suo complesso.

Frontiere esterne solide

La gestione moderna ed efficiente delle frontiere esterne ha il duplice vantaggio di mantenere l'integrità di Schengen e di garantire la sicurezza ai nostri cittadini. Il coinvolgimento di tutti i soggetti interessati al fine di sfruttare al meglio la sicurezza alle frontiere può avere un impatto reale sulla prevenzione della criminalità transfrontaliera e del terrorismo. Le attività operative congiunte della guardia di frontiera e costiera europea[49], rafforzate di recente, contribuiscono alla prevenzione e all'individuazione della criminalità transfrontaliera alle **frontiere esterne** e al di fuori dell'UE. Le attività doganali volte a individuare i rischi per la sicurezza di tutte le merci prima che entrino nell'UE e a controllarle al loro arrivo sono fondamentali nella lotta contro la criminalità transfrontaliera e il terrorismo. Il prossimo piano d'azione sull'Unione doganale annuncerà azioni volte a rafforzare la gestione dei rischi e a migliorare la sicurezza interna, in particolare valutando la fattibilità di un collegamento tra i sistemi di informazione responsabili dell'analisi dei rischi in materia di sicurezza.

Il quadro per l'**interoperabilità tra i sistemi di informazione dell'UE** nel settore della giustizia e degli affari interni è stato adottato nel maggio 2019. La nuova architettura mira a migliorare l'efficienza e l'efficacia di sistemi d'informazione nuovi o aggiornati[50]. Ciò comporterà informazioni più rapide e più sistematiche per gli operatori delle autorità di contrasto, le guardie di frontiera e i responsabili della migrazione e contribuirà alla corretta identificazione e alla lotta contro la frode d'identità. Per realizzare questo obiettivo, occorre che l'attuazione dell'interoperabilità costituisca una priorità a livello sia politico che tecnico. Una stretta cooperazione tra le agenzie dell'UE e tutti gli Stati membri sarà fondamentale per raggiungere l'obiettivo della piena interoperabilità entro il 2023.

Il fenomeno della **falsificazione dei documenti di viaggio** è considerato uno dei reati commessi con maggiore frequenza. Facilita il movimento clandestino di criminali e terroristi e svolge un ruolo fondamentale nella tratta di esseri umani e nel commercio di stupefacenti. La Commissione esaminerà come estendere i lavori in corso sulle norme di sicurezza dei documenti di soggiorno e di viaggio dell'UE, anche attraverso la digitalizzazione. A partire dall'agosto 2021, gli Stati membri inizieranno a rilasciare carte d'identità e titoli di soggiorno conformemente a norme di sicurezza armonizzate, compreso un chip contenente identificatori biometrici che può essere verificato da tutte le autorità di frontiera dell'UE.

I lavori volti a garantire la cybersicurezza e a combattere la criminalità organizzata, la criminalità informatica e il terrorismo dipendono in larga misura dallo sviluppo futuro di strumenti volti a: contribuire a creare nuove tecnologie più protette e sicure, affrontare le sfide poste dalle tecnologie e sostenere il lavoro delle autorità di contrasto. Ciò, a sua volta, dipende da partner privati e dalle industrie.

L'innovazione dovrebbe essere considerata uno strumento strategico per contrastare le attuali minacce e anticipare i rischi e le opportunità per il futuro. Le tecnologie innovative possono apportare nuovi strumenti a sostegno delle attività di contrasto e di altri attori della sicurezza. **L'intelligenza artificiale e l'analisi dei Big Data** potrebbero sfruttare il calcolo ad alte prestazioni per offrire un'analisi migliore, rapida e completa[51]. Un prerequisito fondamentale per lo sviluppo di tecnologie affidabili è costituito da insiemi di dati di elevata qualità a disposizione delle autorità

---

[49] Composta dall'Agenzia europea della guardia di frontiera e costiera (Frontex), dalle guardie di frontiera degli Stati membri e dalle autorità di guardia costiera.

[50] Il sistema di ingressi/uscite (EES), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), il sistema europeo di informazione sui casellari giudiziali (ECRIS-TCN) allargato, il sistema d'informazione Schengen, il sistema d'informazione visti e il futuro Eurodac aggiornato.

[51] Ciò dovrebbe basarsi sulla strategia della Commissione in materia di intelligenza artificiale.

competenti per la formazione, la prova e la convalida degli algoritmi[52]. Più in generale, si registra oggi un forte rischio di dipendenza tecnologica: l'UE, ad esempio, è un importatore netto di prodotti e servizi in materia di cybersicurezza, con tutte le conseguenze che ciò comporta per l'economia e le infrastrutture critiche. Al fine di padroneggiare la tecnologia e garantire la continuità dell'approvvigionamento anche in caso di eventi avversi e crisi, l'Europa ha bisogno di una presenza e di una capacità nelle parti critiche delle pertinenti catene di valore.

La ricerca, l'innovazione e lo sviluppo tecnologico dell'UE offrono l'opportunità di tener conto della dimensione della sicurezza nella fase di sviluppo e applicazione di queste tecnologie. La prossima generazione di proposte di finanziamento dell'UE può agire come importante stimolo in tal senso. Le iniziative riguardanti i dati europei e le infrastrutture cloud hanno tenuto conto della sicurezza fin dall'inizio.

Nell'ambito del riesame del mandato di Europol, la Commissione esaminerà la creazione di un **polo europeo dell'innovazione per la sicurezza interna**[53], che mirerebbe a fornire soluzioni comuni alle sfide e alle opportunità comuni in materia di sicurezza, che gli Stati membri potrebbero non essere in grado di sfruttare da soli. La cooperazione è fondamentale per concentrare gli investimenti in modo da ottenere i risultati migliori e per sviluppare tecnologie innovative con un vantaggio in termini sia di sicurezza che economici.

1.2 Che tipo di legislazione nazionale è stata adottata nel vostro Stato per dare attuazione alle intese e agli accordi sopra indicati?

Le seguenti Convenzioni interazionali sono state recepite nell'ordinamento giuridico nazionale nelle date indicate a fianco di ciascuna di esse:

1. Convenzione per i Servizi Aerei, Tokyo, 14.9.1963 (firmata il 14.9. 1963 e ratificata con Legge n. 468 dell'11.6.1967);
2. Convenzione per la repressione della cattura illecita di aeromobili, L'Aja, 16.12,1970 (firmata il 16.12.1970, ratificata con Legge n.906 del 22.10.1973);
3. Convenzione per la repressione degli atti illeciti contro la sicurezza dell'aviazione civile, Montreal, 23.9.1971 (firmata il 23.9.1971, ratificata con Legge n. 906 del 22.10.1973);
4. Convenzione sulla prevenzione e la repressione dei reati contro le persone internazionalmente protette, compresi gli agenti diplomatici, New York, 14.12.1973 (firmata il 30.12.1971, ratificata con Legge n. 485 del 8.7.1977);
5. Convenzione Europea per la soppressione del terrorismo, Strasburgo, 27. 1.1977 (firmata il 27.1.1977, ratificata con Legge n. 719 del 26.11.1985);
6. Convenzione contro la cattura degli ostaggi, New York, 18.12.1979 (firmata il 18.4.1980, ratificata con Legge n. 719 del 26.11.1985);
7. Convenzione sulla protezione fisica dei materiali nucleari, Vienna, 3.3.1980 (firmata il 13.6.1980, ratificata con Legge n.704 del 7.8.1982);
8. Protocollo per la repressione degli atti illeciti di violenza negli aeroporti adibiti all'aviazione civile internazionale, Montreal, 24.2.1988 - complementare alla Convenzione per la repressione dei reati diretti contro la sicurezza dell'aviazione civile, Montreal, 23.9.1971 - (firmato il 24.2.1988, ratificato con Legge n.394 del 30.11.1989);
9. Convenzione per la repressione dei reati diretti contro la sicurezza della navigazione marittima, Roma, 10.3.1988 (firmata il 10.3.1988, ratificata con Legge n.422 del 28.12.1989);
10. Protocollo per la repressione di atti illeciti contro la sicurezza delle piattaforme fisse situate sulla piattaforma continentale, Roma, 10.03.1988 (firmata il 10.3.1988, ratificata con Legge n.422 del 28.12.1989);
11. Convenzione sulla marcatura di esplosivi plastici e in foglie ai fini di identificazione, Montreal, 1.03.1991 (ratificata con Legge n.420 del 20.12.2000);
12. Convenzione sulla criminalità informatica (firmata il 23.11.2001, ratificata con legge n. 48 del 18.03.2008);
13. Convenzione ONU per la repressione degli attentati terroristici mediante utilizzo di esplosivo, New York, 15.12.1997 (firmata il 12.1.1998, ratificata con Legge n.34 del 14.2.2003);

---

[52] Una strategia europea per i dati (COM (2020) 66 final).

[53] Il polo coopererebbe anche con EBCGA/Frontex, CEPOL, eu-LISA e il Centro comune di ricerca.

14. Convenzione ONU per la soppressione del finanziamento del terrorismo, New York, 9.12.1999 (firmata il 14.1.2000, ratificata con Legge n.7 del 14.1.2003).
15. Convenzione sulla messa al bando delle munizioni a grappolo (firmata a Oslo il 3.12.2008, ratificata con Legge n. 95 del 14.6.2011).
16. Convenzione e Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001 (ratifica ed esecuzione con legge 16 marzo 2006, n. 146). La Risoluzione n.1373/2001, in seguito, ha ampliato la portata del sistema delle liste di congelamento, estendendola ad ulteriori liste di persone sospettate di appartenere o sostenere organizzazioni terroristiche gestite direttamente dagli Stati membri.
    Sono poi state rafforzate le garanzie procedurali a tutela dei soggetti listati, aumentando la trasparenza dei procedimenti di listing e de-listing, ed è stata rafforzata la figura dell'Ombudsperson, competente a valutare le istanze di de-listing.
17. Decreto legge n.7 del 18 febbraio 2015 su "Misure urgenti per il contrasto del terrorismo anche di matrice interazionale", adottato in conformità con la Risoluzione 2178 del Consiglio di Sicurezza delle Nazioni Unite. Per dare attuazione agli accordi interazionali relativi alla prevenzione ed al contrasto del terrorismo, in Italia, oltre alle disposizioni introdotte con il decreto-legge n. 7/2015, convertito con modificazioni dalla legge n. 43/2015, è stata approvata la Legge 28 luglio 2016 n.153 recante Norme per il contrasto al terrorismo, nonché ratifica e esecuzione a) della Convenzione del Consiglio d'Europa per la Prevenzione del terrorismo, fatta a Varsavia, 16 maggio 2005; b) della Convenzione interazionale per la soppressione di atti di terrorismo nucleare, fatta a New York, 14 settembre 2005; c) della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, fatta a Varsavia, 16 maggio 2005; d) del Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatto a Riga, 22 ottobre 2015. La Legge n. 153 del 2016, inoltre, al fine di adeguare la legislazione nazionale alle Convenzioni ratificate, introduce le seguenti modifiche al codice penale: finanziamento di condotte con finalità di terrorismo (art. 270 quinquies.2. c.p.); Confisca (art.270 septies c.p.); Atti di terrorismo nucleare (art. 280 ter c.p.).
18. Decreto Legge 4 ottobre 2018 n. 113, convertito in legge 1° dicembre 2018, n. 132 recante "Disposizioni urgenti in materia di protezione internazionale e immigrazione, sicurezza pubblica, nonché misure per la funzionalità del Ministero dell'interno e l'organizzazione e il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata".

Altri sviluppi legislativi o politici ed elaborazione di nuovi piani d'azione o strategie nazionali ed internazionali in materia di terrorismo

L'Italia è dotata di una legislazione in linea con i più elevati standard internazionali in materia di contrasto al terrorismo e all'estremismo violento. Il nostro ordinamento ha gradualmente abbandonato il quadro normativo approvato per fronteggiare la minaccia terroristica degli anni '70 del secolo scorso per adeguarsi alle mutate sfide poste dalla minaccia terroristica dei decenni successivi, coniugando misure repressive con intenti di prevenzione del fenomeno. sempre entro i confini tracciati dal dettato costituzionale. Per quanto concerne le fattispecie penali, si è reso necessario implementare le forme di tutela anticipate attraverso l'estensione della portata applicativa di nonne già esistenti. In particolare. alla fattispecie dettata dall'art. 270 bis c.p. "Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico" si è aggiunta quella dell'art. 270 ter c.p. "Assistenza agli associati" (che punisce chiunque dia rifugio o fornisca vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano ad associazioni terroristiche). Negli anni successivi, rispettivamente nel 2005 e nel 2015, sono stati introdotti il reato di "Addestramento e arruolamento con finalità di terrorismo" (art. 270 quater c.p.), "Organizzazione, supporto e finanziamento dei trasferimenti per finalità di terrorismo" (art. 270 quater 1 c.p.). Nel 2016, in attuazione alla Convenzione del Consiglio d'Europa, sono stati inseriti i reati di "Finanziamento di condotte con finalità di terrorismo" (art. 270 quinqueis c.p.). "Sottrazione di beni o denaro sottoposti a sequestro per prevenire il finanziamento del terrorismo" (art. 270 quinquies 2 c.p.) e la previsione della "confisca" in caso di condanna per taluno dei reati previsti all'art. 270 sexies (art. 270 septies c.p.).

Tra le misure preventive, fondamentale importanza è rivestita dall'"espulsione amministrativa dello straniero per motivi di ordine e sicurezza pubblica". prevista dal D. Lgs. 286/1998. adottata dal Ministro dell'Interno (o dal Prefetto con delega del Ministro) con provvedimento che motivi la pericolosità dell'espulso in relazione alla "sicurezza dello Stato", nel caso di soggetti implicati in attività di terrorismo. Si tratta di uno strumento flessibile. che permette di contrastare sul piano preventivo il rischio terroristico nei confronti di quei cittadini. regolarmente presenti sul territorio nazionale. che pur non avendo compiuto reati riconducibili alle categorie sopra menzionate. rappresentano comunque un pericolo per lo Stato. In tale quadro normativo si colloca, inoltre. il D. Lgs. 109/2007, che ha istituito, tra l'altro. l'Unità di Informazione Finanziaria (UIF) della Banca d'Italia, deputata alla prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo. Gli adempimenti in capo ai soggetti destinatari della normativa antiriciclaggio prevedono l'adozione di misure di congelamento e di segnalazione di operazioni sospette.

Il Ministero dell'Interno, tramite il Dipartimento della Pubblica Sicurezza, ha assunto le seguenti iniziative, a livello nazionale e internazionale, in linea con le indicazioni di carattere strategico individuate nei "pilastri" della Risoluzione 70/291 dell'Assemblea Generale delle Nazioni Unite.

Misure per affrontare le condizioni che favoriscono la diffusione del terrorismo.

Per quanto attiene alla prevenzione della radicalizzazione e dell'estremismo violento, negli ultimi anni, il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno ha seguito le iniziative svolte a livello internazionale in materia, nella consapevolezza della forte interconnessione tra lotta al terrorismo e contrasto alla radicalizzazione religiosa.

È ormai generalmente condivisa l'esigenza di sviluppare un "approccio di comunità" (community approach), con il contributo necessario delle autorità governative, sia centrali che locali e della "società civile" che possano incidere positivamente nell'attività di prevenzione.

Sulla base di tale indirizzo sono state orientate le strategie di molti Paesi e anche in Italia è in corso di definizione un quadro giuridico che prevede, tra l'altro, l'istituzione di tavoli multidisciplinari e inter-agenzia, sia a livello centrale che locale.

Proprio in ragione della necessità di coinvolgere in una complessiva azione di sistema tutte le componenti sociali interessate alla problematica, il Ministero dell'Interno ha inteso sviluppare una costruttiva interlocuzione con le comunità islamiche, nell'ottica di dare concretezza a un partenariato specificamente indirizzato alla prevenzione della radicalizzazione.

L'intenso dialogo avviato con le associazioni islamiche ha quindi prodotto la firma di un "patto per un islam italiano" che prevede espressamente la collaborazione proattiva delle comunità nel contrasto dei fenomeni di radicalizzazione religiosa.

Misure per prevenire e combattere il terrorismo.

Nel contesto della lotta al fenomeno, gli assetti dell'antiterrorismo italiano hanno sempre rivolto la massima attenzione all'ottimizzazione dello scambio di informazioni tra tutte le Autorità di sicurezza e al miglioramento della cooperazione operativa con i Paesi partner.

In tale ottica è stato assicurato anche il pieno utilizzo degli strumenti e dei database europei e internazionali (ECTC di Europol, SIS II, database di Interpol).

In particolare, per quanto attiene allo scambio di informazioni e alla cooperazione operativa in relazione alla minaccia posta dai combattenti stranieri, si evidenzia che il Dipartimento della Pubblica Sicurezza nel 2014, nel corso del semestre di Presidenza del Consiglio UE, ha promosso l'istituzione di una rete dei punti di contatto antiterrorismo esclusivamente dedicata al fenomeno dei Foreign Terrorist Fighters (FTFs), esperienza positivamente valutata anche dal Consiglio d'Europa (CoE) che ne ha promosso l'attivazione tra i Paesi aderenti nel Protocollo Aggiuntivo di Riga alla Convenzione del CoE per la prevenzione del terrorismo.

Anche in chiave di protezione delle frontiere al fine di prevenire il rischio di infiltrazioni terroristiche nei flussi migratori, il Dipartimento della Pubblica Sicurezza collabora attivamente con le altre strutture nazionali competenti, coordinando le attività svolte dalle articolazioni territoriali impegnate nell'attuazione dei controlli di sicurezza, operati nelle sedi italiane di Hotspot anche con il contributo dei Guest Officers di Europol, che intervengono nello "screening" di secondo livello.

L'esercizio ha garantito un sistematico innalzamento del livello di controllo dei migranti e, oltre a generare numerosi riscontri positivi (hit) nei database di Europol, ha consentito l'acquisizione di informazioni utili per lo sviluppo di attività investigative.

Per contrastare il fenomeno terroristico viene messa in campo una complessa attività informativa di prevenzione, volta a prevenire le minacce alle istituzioni democratiche.

Le politiche in materia prevedono oltre al contrasto interno, di cui in Italia si occupa il Ministero dell'Interno in collaborazione con l'intelligence, anche strategie comuni a livello dell'Unione europea e internazionale.
Con la Legge 438/2001 sono state adottate misure urgenti per la prevenzione ed il contrasto dei reati commessi per finalità di terrorismo internazionale ed è stata introdotta la nuova fattispecie penale di associazione con finalità di terrorismo internazionale (art. 270 bis del Codice Penale).
Le norme prescrivono una collaborazione in base alla quale i servizi di intelligence sono tenuti a "fornire ai competenti organi di polizia giudiziaria le informazioni e gli elementi di prova relativi a fatti configurabili come reati". Agenti e ufficiali di polizia giudiziaria hanno anche l'obbligo di "fornire ogni possibile cooperazione agli agenti dei servizi".
La strategia di prevenzione e contrasto a livello europeo prevede il Piano d'Azione contro il terrorismo che contiene un'ampia serie di misure da adottare nei vari settori cruciali della lotta al terrorismo (cooperazione giudiziaria e di polizia, sicurezza dei trasporti, controllo delle frontiere e sicurezza dei documenti, lotta al finanziamento, dialogo politico e relazioni esterne, difesa contro attacchi biologico-chimico-radiologico-nucleari ecc.).

1.3 Quali sono i ruoli e le missioni delle forze militari, paramilitari e di sicurezza, nonché delle forze di polizia nella prevenzione e nel contrasto del terrorismo nel vostro Stato?

In Italia l'attività di contrasto al terrorismo viene posta in essere su due contigui ma distinti livelli d'impegno. Un livello, definito "tecnico-operativo" vede essenzialmente coinvolte, in uno sforzo coordinato e sinergico, le Forze di Polizia: Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza e Polizia Penitenziaria. A tali Forze si affiancano, per gli aspetti connessi esclusivamente alla sicurezza nazionale, gli Organismi di informazione e sicurezza che fanno capo alla Presidenza del Consiglio dei Ministri. Vi è poi un livello "strategico" che prevede il coinvolgimento di tutte le componenti operative nonché di tutte quelle strutture di altri Dicasteri (Esteri, Difesa, Economia e Finanze, Infrastrutture, Salute) che possono comunque, nell'ambito delle loro specifiche competenze, fornire un prezioso contributo informativo.
Il Comitato di Analisi Strategica Antiterrorismo (C.A.S.A.).
Il Ministero dell'Interno, al fine di assicurare la compiutezza del circuito informativo e la valutazione della minaccia terroristica, nonché di gestire l'emergenza per gli aspetti di tutela dell'ordine e della sicurezza pubblica, si avvale dell'Unità di Crisi e del Comitato di Analisi Strategica Antiterrorismo (C.A.S.A).
Si tratta di un tavolo permanente, tra polizia giudiziaria e servizi di intelligence, volto ad assicurare, a livello nazionale, la tempestiva condivisione e la conseguente valutazione delle informazioni relative alla minaccia terroristica interna ed internazionale.
Il citato consesso è stato formalmente costituito, il 6 maggio 2004, con decreto del Ministro dell'Interno, avente ad oggetto il Piano Nazionale per la gestione di eventi di natura terroristica, nonché le modalità di funzionamento dell'Unità di Crisi, prevista all'art. 6 del D. Lgs. 6 maggio 2002 n. 8, conv. nella Legge n. 133/2002.
Nello specifico, l'analisi del C.A.S.A. riguarda notizie su situazioni, spesso in fieri, potenzialmente suscettibili di produrre rischi nel panorama generale della sicurezza. La valutazione riguarda le informazioni provenienti da un circuito alimentato principalmente:
- da organi di Polizia ed Agenzie di informazioni per la Sicurezza, in relazione alle attività investigative ed informative svolte sul territorio;
- dall'Autorità Giudiziaria, in ottemperanza alle disposizioni del codice di procedura penale;
- da Organi di Polizia di altri Paesi, in contesti di collaborazione internazionale di polizia e di intelligence;
- dall'attività degli Ufficiali di collegamento (Europol, Interpol ecc.);
- da relazioni e reports di Pubbliche Amministrazioni;
- da fonti aperte ed acquisizioni sul web, avvalendosi di elaborazioni OSINT.

Inoltre, il Comitato analizza la documentazione e la messaggistica proveniente da gruppi eversivi interni ed internazionali, valuta l'impatto, in termini di sicurezza, delle più significative manifestazioni di piazza, nonché considera i rischi connessi allo svolgimento di grandi eventi sul territorio nazionale.
In conseguenza della recrudescenza del fenomeno terroristico di matrice jihadista sul territorio europeo e della conseguente necessità di elevare – anche in ambito nazionale – il complessivo

livello di attenzione, con particolare riguardo ai soggetti a vario titolo presenti sul territorio italiano che si presume possano essere "prossimi" ad una eventuale strategia di tensione, il C.A.S.A. ha costituito – già nel giugno 2014 – apposito "tavolo tecnico", finalizzato al monitoraggio del fenomeno dei combattenti stranieri nelle milizie jihadiste ed alla conseguente predisposizione ed aggiornamento di una "lista di foreign fighters", collegati a vario titolo con l'Italia.
Il citato tavolo tecnico si riunisce, altresì, per l'analisi delle informazioni inerenti i detenuti stranieri a rischio di radicalizzazione, oggetto di specifico monitoraggio in ambito carcerario e, a partire dal 1° gennaio 2015, predispone – con cadenza settimanale – mirati controlli straordinari di sicurezza, a carattere preventivo, per il contrasto al fenomeno del terrorismo, verso i luoghi noti come centro di aggregazione di soggetti prevenienti da Paesi a rischio.
Il Decreto Legge nr. 13/2017, convertito in L.46/2017, recante "Disposizioni urgenti per l'accelerazione dei procedimenti in materia di protezione internazionale, nonché per il contrasto dell'immigrazione illegale", tra l'altro, attribuisce al Direttore della Direzione Centrale della Polizia di Prevenzione del Ministero dell'Interno il potere di disporre, su conforme parere del C.A.S.A., l'iscrizione nel Sistema di Informazione Schengen di seconda generazione (Banca Dati SIS II) di un provvedimento di "inammissibilità in area Schengen" nei confronti di un cittadino di un Paese terzo, per il quale esistano fondati motivi di ritenere che abbia commesso un reato grave ovvero indizi concreti circa l'intenzione di commetterlo nel territorio di uno Stato membro.
Tale novella, che conferma la centralità del "Comitato di Analisi Strategica Antiterrorismo" nel circuito delle informazioni in materia di sicurezza dello Stato, integra l'impianto normativo nazionale già delineato dal d.l. 7 del 2015 che:

- dal punto di vista repressivo, aggiornando il d.l. 144 del 2005, ha introdotto, a fronte del rilevato fenomeno dei foreign fighters, il reato di "Organizzazione di trasferimenti per finalità di terrorismo", nonché le aggravanti per "uso di strumenti informatici";
- sul piano preventivo, l'applicabilità delle misure di prevenzione ai soggetti connessi con il terrorismo (art. 4 d.l. 159/2011) che si affiancano alle espulsioni di cittadini stranieri per motivi di sicurezza dello Stato (art. 13 c. 2 del d.lgs. 286/98).

Relativamente alla specifica attività del Corpo delle Guardia di Finanza, per effetto dell'art. 2 del decreto legislativo 19 agosto 2016, n. 177, e del decreto del Ministro dell'Interno del 15 agosto 2017, è stato riservato alla Guardia di Finanza, tra gli altri, il compito della sicurezza in materia di circolazione dell'euro e degli altri mezzi di pagamento, rafforzando la missione del Corpo come Forza di Polizia a competenza generale su tutta la materia economico finanziaria già sancita dall'art. 2, comma 2, lettera h), del decreto legislativo 19 marzo 2001, n. 68, per la prevenzione, ricerca e repressione delle violazioni in tema di valute, titoli, valori, mezzi di pagamento nazionali, europei ed esteri, movimentazioni finanziarie e di capitali, nonché dal decreto legge 25 settembre 2001, n. 350, convertito in legge 23 novembre 2001, n. 409, e dal decreto legislativo n. 231 del 2007.
Con riferimento al concorso delle Forze Armate nei servizi di sicurezza a supporto delle Forze di Polizia, detto concorso straordinario, denominato Operazione Strade Sicure, ha preso avvio il 4 agosto 2008 a seguito dell'emanazione del decreto legge n. 92 del 23 maggio 2008, convertito in legge n. 125 del 24 luglio 2008, successivamente prorogato fino al corrente anno con specifici provvedimenti normativi che ne definiscono il contingente massimo impiegabile, il periodo nonché il finanziamento. In particolare, la finalità dell'Operazione è quella di assicurare la vigilanza di siti e obiettivi sensibili, anche in funzione preventiva. antiterrorismo, consentendo il recupero delle Forze di Polizia impiegate nella vigilanza da destinare al potenziamento delle attività di controllo del territorio, prevenzione e contrasto della criminalità. Il personale delle Forze Armate assegnato nei diversi ambiti territoriali è posto formalmente a disposizione dei Prefetti mentre, l'attività operativa dei militari, secondo modelli predefiniti, è disciplinata con apposita Ordinanza di servizio del Questore, ex art. 37 DPR 782/85. I predetti militari svolgono l'attività di vigilanza agli obiettivi sensibili, individuati in sede di Comitato provinciale per l'ordine e la sicurezza pubblica, sempre in collegamento radio con le Forze di Polizia, in quanto il legislatore riconosce loro unicamente la qualifica di agente di PS., con esclusione delle funzioni di polizia giudiziaria.
Per quanto concerne la pianificazione dell'Operazione Strade Sicure, il Piano di Impiego del personale delle Forze armate, ai sensi dell'art. 7 bis, comma 2, del citato DL. 92/2008, è adottato con decreto del Ministro dell'Interno, di concerto con il Ministro della Difesa, sentito il Comitato nazionale dell'ordine e della sicurezza pubblica integrato dal Capo di stato maggiore della difesa e previa informazione al Presidente del Consiglio dei Ministri. In caso di necessità e urgenza, anche su richiesta dei Prefetti delle province interessate, il Capo della Polizia - Direttore Generale della

Pubblica Sicurezza, d'intesa con il Capo di Stato Maggiore della Difesa, previa comunicazione al Ministro dell'Interno e al Ministro della Difesa, può con proprio Decreto modificare il numero delle unità di personale delle Forze armate indicate nel Piano di Impiego, nonché le province di destinazione, ferme restando le entità massime e le specifiche finalità dei contingenti di volta in volta autorizzati. Detto provvedimento deve comunque essere successivamente ratificato con Decreto dei Ministri competenti.

1.4 Fornite ulteriori pertinenti informazioni sulle iniziative a livello nazionale per prevenire e combattere il terrorismo in relazione, tra l'altro, ai seguenti settori: finanziamento del terrorismo; controlli delle frontiere e sicurezza dei documenti di viaggio; sicurezza dei container e della catena di approvvigionamento; sicurezza delle fonti radioattive; uso di Internet e di altri reti informative a scopi terroristici; cooperazione giudiziaria (anche con riguardo all'estradizione); rifugi e ripari sicuri per terroristi ed organizzazioni terroristiche.

- **Finanziamento del Terrorismo**

  Nel settore del contrasto al terrorismo internazionale, il Dipartimento della Pubblica Sicurezza, le Forze di Polizia a competenza generale - Polizia di Stato e Arma dei Carabinieri - e il Corpo della Guardia di Finanza, altamente specializzato in materia, svolgono la propria attività con specifico riguardo agli aspetti connessi al finanziamento di tale fenomeno illecito.

  In particolare, il citato Corpo va ad integrare lo sforzo e l'apparato investigativo antiterrorismo, che gravita principalmente sulle due altre Forze di Polizia a competenza generale, affiancando all'azione repressiva tradizionale lo sviluppo di indagini preventive e collaterali, mirate sui flussi finanziari che alimentano gli investimenti a sostegno dei gruppi criminali nazionali ed internazionali.

  Sul punto, il Ministro dell'Interno ha emanato precise direttive di coordinamento in materia di compiti ed attività delle Forze di Polizia, ribadendo, da ultimo, con il citato Decreto del 15 agosto 2017 che la Guardia di Finanza ha assunto, per effetto del D. Lgs. n. 68/2001, un ruolo centrale nel settore della tutela dei mezzi di pagamento, vedendo così valorizzata la sua funzione di contrasto, tra l'altro, al fenomeno del finanziamento del terrorismo internazionale, coordinandosi, per tali finalità, con le strutture centrali e periferiche dell'Amministrazione della Pubblica Sicurezza.

  Ulteriore apporto della Guardia di Finanza viene fornito in seno al Comitato di Sicurezza Finanziaria (C.S.F.), Organismo di coordinamento interministeriale di cui si avvale il Ministro dell'Economia e delle Finanze nella definizione delle politiche di prevenzione in materia di riciclaggio e finanziamento del terrorismo, con i seguenti obbiettivi: individuare i flussi finanziari potenzialmente destinati a finanziare le attività di gruppi/cellule terroristiche; ricostruire il profilo patrimoniale e finanziario dei soggetti/entità indiziati o sospettati di far parte a vario titolo o di fornire supporto ad organizzazioni di stampo terroristico.

  Comitato di Sicurezza Finanziaria.

  Il Comitato di sicurezza finanziaria (CSF) presieduto dal Direttore generale del Tesoro, è istituito presso il Ministero dell'Economia e delle Finanze in ottemperanza agli obblighi assunti dall'Italia nel 2001 nell'ambito della strategia internazionale di contrasto al finanziamento del terrorismo. Tra le altre competenze, assicura l'attuazione delle misure di congelamento dei fondi e delle risorse economiche di persone fisiche, giuridiche, gruppi o entità disposte dalle Nazioni unite e dall'Unione europea (art. 4 del decreto legislativo 22 giugno 2007, n. 109), popone al Ministro dell'economia e delle finanze misure di congelamento nazionale (art. 4 bis del decreto legislativo 22 giugno 2007, n. 109) e coordina le attività delle diverse autorità ed enti competenti in materia.

  Il Comitato rappresenta la "cabina di regia" in materia di prevenzione dell'utilizzo del sistema finanziario ed economico per fini di riciclaggio dei proventi di attività criminose, di contrasto e repressione del finanziamento al terrorismo, del finanziamento della proliferazione delle armi di distruzione di massa, e delle attività dei Paesi che minacciano la pace e la sicurezza internazionale (art. 3 del decreto legislativo 22 giugno 2007, n. 109).

  L'organizzazione dei lavori è disciplinata dal D.M. 20 ottobre 2010, n. 203.

  Nel Comitato sono rappresentati il Ministero dell'Interno, il Ministero della Giustizia, il Ministero degli Affari Esteri, il Ministero dello Sviluppo Economico, il Ministero

dell'Economia e delle Finanze, la Banca d'Italia, la Commissione nazionale per le società e la Borsa, l'Istituto per la Vigilanza sulle Assicurazioni, l'Ufficio di Informazione Finanziaria, la Polizia di Stato, l'Arma dei Carabinieri, la Guardia di Finanza, la Direzione Investigativa Antimafia, la Direzione nazionale antimafia e antiterrorismo, l'Agenzia delle dogane e dei monopoli. Il Comitato è integrato da un rappresentante dell'Agenzia del Demanio ai fini dello svolgimento dei compiti riguardanti il congelamento delle risorse economiche.
L'attività del Comitato è coadiuvata e supportata nelle materie di sua competenza dalla Rete degli esperti, composta da rappresentanti designati dalle diverse amministrazioni che compongono il Comitato.
Le competenze del CSF sono definite dall'articolo 3 del decreto legislativo 22 giugno 2007, n. 109), e dall'art.5 del decreto legislativo 21 novembre 2007, n. 231.
Più in particolare, in materia di prevenzione dell'utilizzo del sistema finanziario ed economico per fini di riciclaggio dei proventi di attività criminose o di finanziamento del terrorismo nonché di contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale:

- elabora l'analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo;
- propone al Ministero dell'economia e delle finanze le misure di designazione e congelamenti dei fondi e delle risorse economiche detenuti, anche per interposta persona, da persone fisiche, persone giuridiche, gruppi o entità che commettono o tentano di commettere atti di terrorismo;
- presenta al Ministero dell'economia e delle finanze, entro il 30 maggio di ogni anno, una relazione contenente la valutazione dell'attività di prevenzione del riciclaggio o del finanziamento del terrorismo e proposte dirette a renderla più efficace;
- formula i pareri e le proposte previste dal decreto legislativo n.231/2007 e fornisce consulenza al Ministero dell'economia e delle finanze in materia di prevenzione del riciclaggio o del finanziamento del terrorismo;
- quale autorità italiana responsabile per l'attuazione delle misure di congelamento dei fondi e delle risorse economiche di persone fisiche, giuridiche, gruppi o entità disposte dalle Nazioni unite e dall'Unione europea per contrastare e reprimere il finanziamento del terrorismo nonché per il contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale, il CSF può formulare ai competenti organi delle Nazioni Unite e dell'Unione Europea proposte di designazione di individui ed entità in base agli elementi informativi a sua disposizione, nonché di cancellazione dalle medesime liste, sulla base delle istanze presentate dai soggetti interessati.

Unità di Informazione Finanziaria.
L'U.I.F. svolge un ruolo attivo sostanziale nell'attuazione dei congelamenti e dei dispositivi di prevenzione e contrasto al terrorismo. Il D. Lgs. 109/2007 infatti assegna all'Unità il controllo dell'attuazione delle misure finanziarie adottate dall'Unione Europea; correlati a tale compito vi sono quelli relativi alla raccolta delle informazioni e dei dati di natura finanziaria relativi ai soggetti designati, ai fondi ed alle risorse economiche sottoposti a congelamento (che i soggetti obbligati sono tenuti a comunicare entro i trenta giorni dall'avvenuta adozione del congelamento) e quello di agevolare la diffusione delle liste dei soggetti designati e delle successive modifiche.
Inoltre la UIF riceve da parte di intermediari finanziari, operatori non finanziari e professionisti o (cd. Soggetti obbligati) le segnalazioni di operazioni sospette relative ad operazioni (tentate od effettuate) di finanziamento del terrorismo, e le trasmette, arricchite dell'analisi finanziaria, al Nucleo speciale di polizia valutaria della Guardia di Finanza (NSPV) e alla Direzione Investigativa Antimafia (DIA) composta da tutte le Forze di Polizia.
In tale ambito, la Banca d'Italia ha emanato degli "indicatori di anomalia" al fine di agevolare la valutazione da parte degli intermediari sugli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo, al quale è dedicata una specifica sezione del provvedimento.
Infine la UIF cura i rapporti con le altre Financial Intelligence Unit, scambiando informazioni per finalità di contrasto al riciclaggio e finanziamento del terrorismo.

- **Controlli delle frontiere e sicurezza dei documenti di viaggio**

Una tappa fondamentale nel sistema di riorganizzazione e potenziamento dei controlli alle frontiere, secondo le più recenti direttive europee, è rappresentato dall'adozione per tutti i Paesi dell'U.E. del passaporto elettronico aderente agli standard ICAO.

In base a quanto previsto, l'Istituto Poligrafico e Zecca dello Stato ha predisposto un modello di passaporto con elementi di sicurezza basati sulla stampa di un codice MRZ (Machine Readable Zone) leggibile in automatico, oltre una serie di elementi di sicurezza tra i quali inchiostri speciali, ologrammi di sicurezza, ghost image ed un microprocessore e sistema di antenna integrato nell'ultima pagina di copertina.
Oltre alla tradizionale verifica a vista da parte dell'operatore preposto ai controlli di frontiera, viene svolta anche la lettura del codice MRZ tramite uno scanner ad hoc utilizzato in frontiera (che analizza anche con fonti di luce alternativa a raggi ultravioletti, altri elementi di sicurezza quali gli ologrammi dei singoli Stati emettitori).
Con questa tecnologia l'operatore raggiunge due obiettivi: 1) può verificare il riscontro tra il codice MRZ ed i dati demografici scritti in chiaro sulla prima pagina; 2) è in grado di effettuare una ricerca automatica nel sistema delle frontiere per eventuali incroci con le banche dati. A tali operazioni, si aggiunge anche la possibilità di verificare il fattore biometrico facciale, da cui deriva la possibilità di sviluppare una serie di controlli automatici sul volto.
Il Dipartimento della Pubblica Sicurezza, tramite le sue competenti articolazioni, coordina le attività degli uffici periferici (DIGOS) che, nell'ambito dei controlli delle frontiere, sono investiti in via esclusiva dell'attività di prevenzione e contrasto del terrorismo. In particolare le DIGOS, in collaborazione con i guest officers inviati da Europei, svolgono controlli di sicurezza secondari, negli hotspot o nei luoghi di sbarco, per prevenire il pericolo di infiltrazione nell'ambito dei flussi migratori di individui estremisti o contigui a organizzazioni terroristiche.
Nell'ambito dei controlli delle frontiere, il Dipartimento della Pubblica Sicurezza collabora attivamente con le altre strutture nazionali competenti, coordinando le attività svolte dalle articolazioni territoriali impegnate nell'attuazione dei controlli di sicurezza, operati nelle sedi italiane di Hotspot anche con il contributo dei Guest Officers di Europol, che intervengono nello "screening" di secondo livello.
Sempre al fine dell'ottimizzazione dei controlli alle frontiere, è stato creato uno specifico software noto con il nome di S.I.F. (Sistema Informativo delle Frontiere), che ha lo scopo di supportare l'operatore preposto ai controlli di frontiera nello svolgimento dell'attività di controllo ai varchi di accesso tramite sistemi che prevedono l'utilizzo di tecniche biometriche per l'autenticazione e la validazione dei documenti (passaporti, carte d'identità elettroniche, visti) nell'espletamento di accertamenti di prima e seconda linea.
Attualmente, tutti gli Uffici di Polizia di Frontiera sono dotati di postazioni SIF e sono in corso di consegna, alle articolazioni che espletano controlli alle frontiere esterne, kit "SIF App Mobile", consistenti in smartphone che consentiranno di effettuare verifiche al di fuori delle cabine di 1° linea. Detti apparati saranno operativi già nel mese di maggio 2021, al termine di apposite sessioni di addestramento del personale di frontiera.
Il Sistema di informazione Visti (VIS) è uno strumento finalizzato alla gestione/scambio di dati e informazioni concernenti i visti d'ingresso nello Spazio Schengen tra gli Stati che ne fanno parte.
Il VIS è basato su un'architettura centralizzata ed è costituito da un sistema d'informazione centrale (C-VIS) con un'interfaccia nazionale in ciascuno Stato membro (N-VIS), che assicura il collegamento con la competente Autorità centrale nazionale del rispettivo Stato membro, e dall'infrastruttura di comunicazione tra il sistema centrale d'informazione visti e le interfacce nazionali. Per consentire il funzionamento del VIS, gli uffici consolari e i valichi di frontiera sono connessi alla banca dati centrale del sistema.
Principali scopi del VIS sono: agevolare le procedure relative alle domande di visto; facilitare i controlli ai valichi di frontiera esterni e rafforzare la sicurezza. Lo stesso previene altresì il cd. "visa shopping" e assiste gli Stati membri nella lotta contro le frodi.

- **Sicurezza delle fonti radioattive**

Per quel che concerne la minaccia di attacchi terroristici perpetrati a mezzo di agenti biologici, chimici, tossicologici e fisici, il Comando Carabinieri per la Tutela della Salute è il Punto di Contatto a livello nazionale del Sistema di Allerta Rapido istituito nel 2001. Oggi, in virtù della capillare distribuzione del proprio dispositivo territoriale, l'Arma dei Carabinieri è presente nella "Rete Nazionale della Protezione Civile per il Rilevamento Automatico della Ricaduta Radioattiva". Inoltre, un Ufficiale dell'Arma partecipa al Gruppo di Lavoro interforze per l'elaborazione del "Piano di Settore N.B.C.R." del Ministero della Difesa, il quale definisce le

misure da adottare per fronteggiare un attacco terroristico di tipo "nucleare, biologico, chimico e radiologico", mediante l'integrazione di tutte le risorse dell'Amministrazione della Difesa deputate alla prevenzione, protezione e soccorso.
Il Comando Carabinieri per la Tutela dell'Ambiente sviluppa, inoltre, attraverso la "Sezione inquinamento da sostanze radioattive", un'azione di contrasto alle forme di illegalità derivanti dal trattamento delle varie tipologie di rifiuti pericolosi e dal traffico di materiali nucleari e di sostanze radioattive.

- **Uso di Internet e di altre reti informative a scopi terroristici**

Nell'ambito della prevenzione e del contrasto al terrorismo internazionale, con particolare riferimento ai fenomeni di radicalizzazione sul web, il law enforcement italiano effettua un costante monitoraggio della rete, al fine di individuare i contenuti illeciti presenti all'interno degli spazi e servizi di comunicazione online di ogni genere.
Tale attività ha permesso di contrastare i fenomeni di radicalizzazione e terrorismo di matrice jihadista e di riscontrare come l'attuale struttura centrale dell'apparato di propaganda del Daesh, con produzione mediatica in costante diminuzione nel corso degli ultimi mesi, risulti essere costituita da vari Media Center, che si appoggiano ai cd. Supporter Generated Content per la diffusione del materiale di propaganda.
Nel dettaglio, anche nel corso del 2020 è stato possibile constatare come tale struttura mediatica abbia continuato a basarsi su moltissimi account, seppur in numero inferiore rispetto all'anno precedente, attivati quotidianamente (anche in forma automatizzata tramite apposite strutture dipendenti dal Daesh deputate al mantenimento dell'operatività mediatica) con l'obiettivo di divulgare magazine online, aggiornamenti sulle attività dei combattenti, video, documenti, manuali, pubblicazioni di esponenti di spicco della corrente radicale islamista, e minacce di ogni genere.
L'adozione di tale modalità operativa per la diffusione della propaganda jihadista è stata determinata sia dall'incremento dell'azione di rimozione dei contenuti illeciti presenti sulle proprie piattaforme da parte dei maggiori fornitori di servizi internet (tra i quali Telegram, Facebook, Google, Twitter, etc), che per le particolari attività di contrasto attuate dal law enforcement internazionale.
Nello specifico, nel corso del 2020 sono proseguite le attività svolte all'interno dei tavoli di lavoro internazionali deputati al contrasto del cyberterrorismo, con il coordinamento di Europol e con il coinvolgimento di tutte le Forze dell'Ordine degli Stati Membri, nonché dei rappresentanti dei maggiori Internet Service Provider, tra i quali soprattutto Telegram (è stato il fornitore di servizi online che ha ricevuto il maggior numero di richieste di rimozione ed ha allontanato dalla propria piattaforma una parte significativa degli attori chiave all'interno della rete di diffusione della propaganda IS).
Appare evidente, dunque, come il carattere transnazionale delle operazioni di contrasto appena descritte, sia per la natura del fenomeno, che per la stessa struttura della rete, abbia comportato l'imprescindibile attivazione di strumenti di cooperazione sovranazionale che hanno determinato un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse Forze di Polizia nazionali.
Invero, l'analisi relativa alla diminuzione, nel corso del 2020, del numero degli spazi web riconducibili alla propaganda jihadista ha permesso di evidenziare l'importanza del lavoro svolto dal Servizio Polizia Postale e delle Comunicazioni, quale punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, nell'ambito degli "action day", ovvero di eventi dedicati che hanno determinato un massiccio "take down" di migliaia di gruppi, canali ed account, oggetto di preventiva segnalazione da parte del law enforcement, perchè considerati responsabili della pubblicazione del settimanale di propaganda jihadista al-Naba.
In tale contesto operativo transnazionale, tra le principali attività svolte nel corso del 2020 dal personale della Specialità, si evidenzia la partecipazione all'azione denominata "RAD - Referral Action Day on instructional material online", svoltasi il 2 luglio 2020 e promossa da Europol, al fine di procedere, tramite la segnalazione ai rispettivi provider interessati, alla rimozione di ogni tipo di contenuto didattico in formato digitale utilizzato per la pianificazione e realizzazione di attacchi terroristici. L'Action Day ha coinvolto unità specializzate del Centro Europeo Antiterrorismo (ECTC) e rappresentanti di 18 Paesi, tra cui 13 Stati membri dell'UE e 5 Paesi extra UE.

Durante l'azione, gli esperti in cyberterrorismo hanno rilevato, valutato e segnalato i contenuti online, inclusi manuali e tutorials su come preparare ed attuare attacchi terroristici, come selezionare gli obiettivi, come utilizzare le armi e costruire bombe. Alcuni dei documenti individuati contenevano anche le istruzioni su come rimanere anonimi online e le modalità per evitare di essere individuati durante la pianificazione di un attacco terroristico (al riguardo, si segnala che i manuali "fatti in casa" e le guide individuate nel corso dell'operazione costituiscono il principale strumento per la realizzazione delle armi utilizzate per gli attacchi condotti dai gruppi terroristici e dai loro sostenitori, molto spesso innescati come attori solitari).
Le descritte attività hanno permesso di registrare, nel corso degli ultimi anni anche un notevole incremento nell'ambito del settore della propaganda online legata all'estremismo razzista e xenofobo e di riscontrare un trend in costante aumento di forum e discussioni dedicate all'argomento.
Anche in tale ambito, infatti, il web rappresenta uno strumento strategico che agevola la diffusione della propaganda delle ideologie estremiste e violente, nonché il reclutamento di nuovi combattenti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.
L'indottrinamento e il reclutamento, come nel caso del radicalismo jihadista, avvengono sempre sulla rete, attraverso una graduale autoformazione (che inizia con la visualizzazione di contenuti diffusi soprattutto in spazi virtuali riservati, diversi dai principali social network) agevolata dalla digitalizzazione delle tecnologie dell'informazione e della comunicazione.
L'analisi effettuata sulle modalità utilizzate nel corso degli ultimi attacchi terroristici, in cui si è assistito alla diffusione in diretta streaming delle immagini all'interno di varie piattaforme online, ha determinato un evidente innalzamento del rischio ed un conseguente incremento del livello di attenzione proprio nei tavoli di lavoro internazionali.
In particolare, in seno all'EU Internet Forum, rappresentanti italiani, degli altri Stati Membri e di Europol, nonché di alcuni delegati delle maggiori compagnie fornitrici di servizi internet (tra le quali Facebook, Google, Microsoft, Telegram, Twitter, Snap, JustPaste.it e Dropbox) hanno contribuito all'elaborazione di un protocollo dell'Unione Europea finalizzato al contrasto ed al contenimento della rapida diffusione online di contenuti terroristici e di estremismo violento.
L'adozione del protocollo in argomento che vede il Servizio di Polizia Postale quale punto di contatto nazionale, ha determinato la predisposizione di un meccanismo, attivo h.24, sette giorni su sette, volto a garantire una risposta coordinata e tempestiva ad una crisi terroristica online transfrontaliera (intesa come evento che descrive un danno alla vita o all'integrità fisica).
La grave emergenza socio-sanitaria, tuttora in corso, accompagnata dalle restrizioni introdotte dai decreti governativi per contrastare la diffusione del virus Covid-19 ha, inoltre, determinato un'intensa attività, sia di controinformazione che di incitamento ad azioni di protesta, che trova un efficace strumento di veicolazione nell'oggettivo, considerevole, aumento di canali e gruppi all'interno delle varie piattaforme di comunicazione online, appunto utilizzate per diffondere commenti e propositi di reazione alle decisioni governative attraverso azioni di piazza.
Conseguentemente, viene effettuato il costante monitoraggio dei social nonché dei canali e dei gruppi presenti sulle piattaforme di comunicazione online, intensificando, soprattutto nell'ambito delle diverse forme di espressione del dissenso contro le politiche adottate per il contenimento dell'emergenza sanitaria, la raccolta informativa e l'attività investigativa sul web, al fine di individuare e prevenire iniziative che possano turbare l'ordine e la sicurezza pubblica.
In ambito europeo, il sistema di law enforcement nazionale ha individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno quale il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda jihadista diffusi in rete e di orientarne l'attività. Lo scambio delle informazioni tra Paesi Membri viene effettuato attraverso l'utilizzo di specifiche piattaforme tecnologiche, tra cui Check-the-Web (CTW) e SIRIUS, appositamente create in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet.
La Legge n. 155/2005, recante "Misure urgenti per il contrasto del terrorismo interazionale", ha individuato nel citato Servizio Polizia Postale e delle Comunicazioni, l'unità specializzata dedicata alla prevenzione e alla repressione dei crimini informatici ai danni delle infrastrutture critiche nazionali, ed ha istituito, per la gestione delle peculiari emergenze legate alle

infrastrutture informatiche, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC).
Composto da risorse di elevato livello tecnologico e personale altamente qualificato, il Centro è incaricato, in via esclusiva, della prevenzione e repressione dei crimini informatici (di matrice comune, organizzata o terroristica) che hanno per obiettivo le infrastrutture informatiche di natura critica e di rilevanza nazionale che assolvono a funzioni istituzionali ovvero erogano, gestiscono e controllano servizi strategici per la sicurezza e la prosperità del Paese.

- **Cooperazione giudiziaria, anche con riguardo all'estradizione**
  Il Dipartimento della Pubblica Sicurezza, tramite il Servizio per la Cooperazione Internazionale di Polizia incardinato all'interno della Direzione Centrale della Polizia Criminale, cura l'attività di raccordo informativo sui canali della cooperazione internazionale di polizia anche al fine di localizzare persone destinatarie di provvedimenti restrittivi della libertà emessi dalle Autorità Giudiziarie competenti per reati di terrorismo, assicurandone l'estradizione.

2. Stazionamento di forze armate su territori stranieri

2.1 Fornite informazioni sullo stazionamento di forze armate del vostro Stato sul territorio di altri Stati partecipanti conformemente ad accordi liberamente negoziati nonché in base al diritto internazionale.

L'art. 11 della Costituzione sancisce che "l'Italia ripudia la guerra come strumento di offesa alla libertà di altri popoli e come mezzo di risoluzione delle controversie internazionali". E' il sistema di controllo democratico delle F.A. proprio dell'ordinamento italiano a garantire che l'invio di contingenti nazionali all'estero sia deliberato sulla base di accordi liberamente sottoscritti dai Paesi ospitanti e, in conformità al diritto internazionale, in stretta aderenza agli impegni assunti con l'adesione all'ONU, all'UE, alla NATO, all'OSCE e al Consiglio d'Europa. Anche i più recenti interventi fuori area sono stati disposti secondo i principi del diritto internazionale sulla base di risoluzioni ONU e di decisioni assunte in ambito UE, NATO, OSCE o sulla base di accordi liberamente sottoscritti con i Paesi ospitanti. In tale quadro, particolare rilievo assumono la Convenzione di Londra (NATO SOFA) del 19 giugno 1951 (ratificata con legge 30 novembre 1955, n. 1335) e la Convenzione NATO/PfP del 19 giugno 1995 (ratificata con legge 30 giugno 1998, n. 228) che delineano un quadro giuridico dei rapporti tra Paesi ospiti e Paesi ospitanti essenzialmente improntati ad una collaborazione paritetica in cui sono definiti, con criteri di reciprocità, le regole per l'esercizio della giurisdizione e per un sostanziale rispetto degli ordinamenti di ciascuna Nazione.

3. Attuazione di altri impegni internazionali connessi al Codice di Condotta

3.1 Fornite informazioni su come il vostro Stato assicura che siano attuati in buona fede gli impegni nel campo del controllo degli armamenti, del disarmo, del rafforzamento della fiducia e della sicurezza quale elemento di sicurezza indivisibile.

L'impegno per il disarmo, il controllo degli armamenti e la non proliferazione rappresenta un elemento qualificante della politica estera italiana. L'Italia è tradizionalmente attiva su più fronti: in seno alle Nazioni Unite, all'OSCE, all'Unione Europea, al G7 nonché nell'ambito dei processi di riesame delle maggiori convenzioni internazionali in materia. In particolare:

- E' parte della Convenzione di Ottawa sulle Mine Antipersona. Partecipa agli scambi di informazione e destina risorse allo sminamento umanitario per mezzo di un Fondo appositamente istituito per legge (nel 2020 con tale Fondo sono stati finanziati interventi per un ammontare di circa 4 milioni di euro);

- è parte della Convenzione di Oslo sulla messa al bando delle munizioni a grappolo nei confronti della quale ha esaurito i propri obblighi di distruzione – con ben quattro anni di anticipo rispetto ai limiti temporali previsti dalla stessa – del munizionamento vietato;
- è parte della Convenzione sui Certe Armi Convenzionali (CCW) e di tutti i suoi Protocolli (I – V) e sostiene le iniziative in tale ambito, svolgendo un ruolo attivo e propositivo per l'adozione di strumenti giuridicamente vincolanti volti a minimizzare l'impatto umanitario dei conflitti. Le Forze Armate hanno già radiato tutte quelle armi considerate inumane e oggetto di specifici Protocolli limitativi annessi alla Convenzione CCW;
- è parte del Trattato sul commercio delle Armi (ATT);
- è parte delle Convenzioni dell'Aja sulle Leggi di Guerra e del Protocollo di Ginevra sul divieto di impiego di Gas Asfissianti e di Armi Batteriologiche;
- è parte della Convenzione sulle Armi Batteriologiche e Tossiche;
- è parte delle Convenzione sulle Armi Chimiche.

3.2 Fornite informazioni su come il vostro Stato persegue misure di controllo degli armamenti, di disarmo e di rafforzamento della fiducia al fine di rafforzare la sicurezza e la stabilità nell'area dell'OSCE.

L'Italia è parte del Trattato sulla limitazione delle Forze Convenzionali in Europa (CFE). L'Italia ottempera costantemente agli obblighi previsti dal Trattato mantenendo le proprie consistenze di equipaggiamenti ben al disotto dei limiti previsti, procedendo alla distruzione di quelli via via ritenuti obsoleti in aderenza alle specifiche metodologie e scambiando annualmente con gli altri Stati Parte [1] tutte le informazioni richieste e relative a strutture ordinative, consistenze di uomini e mezzi delle Unità soggette a limitazione.

L'Italia è anche parte del Trattato Cieli Aperti (Open Skies) e in tale ambito effettua e permette voli di osservazione aerea finalizzati ad accrescere la trasparenza, la fiducia e la sicurezza collettiva.

Nell'area OSCE l'Italia aderisce al Documento di Vienna 2011 adottando tutte le misure contenute con lo spirito di massima trasparenza, scambiando le informazioni militari sulle proprie Unità, organizzando periodicamente ed invitando tutti gli Stati Parte ai previsti eventi improntati alla mutua conoscenza (visita istallazioni militari e Basi aeree), alla presentazione, all'occorrenza, di eventuali nuovi sistemi d'arma introdotti in servizio, alla diffusione di tutte le notizie riguardanti il processo di pianificazione della difesa, l'organizzazione, il reclutamento e stato giuridico del personale, l'approvvigionamento di nuovi materiali. Nella ricezione delle visite valutative e ispezioni VD2011 il personale militare e le unità coinvolte operano nel pieno rispetto delle misure e dello spirito su cui si impronta il Documento. Attualmente l'Italia persegue l'obiettivo dell'aggiornamento dello stesso.

A partire da marzo 2020 le attività di controllo armamenti hanno subito limitazioni a causa dell'emergenza COVID-19.

Per quanto attiene alle Armi di Piccolo Calibro e Leggere (SALW) l'Italia sostiene le iniziative internazionali volte a combatterne la proliferazione, adottando le migliori prassi e, dal punto di vista normativo, imponendo una stringente regolamentazione sull'acquisizione, trasferimento, detenzione, marcatura e tracciamento delle armi.

SEZIONE II. ELEMENTI INTRASTATALI

1. Processi decisionali e di pianificazione a livello nazionale

1.1Quali sono i processi decisionali e di pianificazione a livello nazionale nella determinazione/approvazione dell'assetto militare e delle spese per la difesa del vostro Stato?

a) L'assetto militare

La pianificazione nazionale in materia di Difesa è in stretta aderenza alla linea d'indirizzo della Politica Estera e di Difesa definita dal Governo, in conformità agli impegni assunti in sede internazionale, e sottoposta al vaglio del Parlamento il cui ruolo si esplica:

- nell'approvazione della Legge Finanziaria e dei provvedimenti collegati:
- nella ratifica degli accordi di cooperazione internazionale anche nel settore della Difesa;
- nell'approvazione dei disegni di legge riguardanti le Forze Armate;
- nell'esercizio dei poteri di controllo mediante interrogazioni, interpellanze e visite che consentono ad ogni singolo parlamentare di verificare l'operato delle F.A.

I compiti del Ministro della Difesa, contenuti nel Decreto legislativo 15 marzo 2010 n. 66, consistono:

- nell'attuazione delle deliberazioni in materia di difesa e sicurezza adottate dal Governo e approvate dal Parlamento;
- nell'approvazione della pianificazione generale ed operativa interforze e dei conseguenti programmi tecnico – finanziari nonché della pianificazione relativa all'area industriale, pubblica e privata, di interesse della Difesa;
- nell'illustrazione al Parlamento dell'evoluzione del quadro strategico e degli impegni operativi interforze, della preparazione delle F.A., delle previsioni di spesa e della ripartizione delle risorse finanziarie, dello stato di attuazione dei programmi di investimento.

b) Le spese per la difesa

Il Parlamento approva le leggi di bilancio che definiscono lo stato di previsione, l'assestamento e il rendiconto generale delle spese della Difesa.

Ogni anno il Ministero della Difesa elabora un proprio bilancio che, integrato con quelli degli altri Dicasteri pubblici, è presentato dal Governo al Parlamento per l'approvazione entro la fine dell'anno nel quadro della legge finanziaria.

Negli ultimi due anni la percentuale di spesa della difesa in relazione al PIL è stata pari a circa l'1 per cento. Il controllo sulle spese per la difesa è effettuato a livello politico dal Parlamento, e a livello amministrativo - contabile dalla Corte dei Conti.

1.1 In che modo il vostro Stato assicura che, nel determinare le proprie capacità militari, siano tenute presenti le legittime preoccupazioni di altri Stati nonché l'esigenza di contribuire alla sicurezza e alla stabilità internazionali?

L'adesione ai principali Trattati sulla limitazione e controllo degli armamenti e l'attiva partecipazione a quelli improntati a favorire e rafforzare le misure di fiducia e sicurezza reciproca (CSBM) costituiscono incontrovertibili elementi della volontà politica nazionale di mitigare qualsiasi preoccupazione di altri Stati riguardo le capacità militari difensive del Paese improntate a garantire e promuovere la sicurezza e stabilità internazionale.

2. Procedure e Strutture esistenti

2.1 Quali sono le procedure costituzionali vigenti per assicurare il controllo politico democratico delle forze militari, paramilitari e di sicurezza interna, dei servizi di intelligence e della polizia?

a) <u>Forze Armate</u>

La Costituzione italiana prevede la subordinazione dell'organizzazione militare al "Vertice politico – strategico" composto dai massimi organi costituzionali: Presidente della Repubblica, Parlamento e Governo. In particolare:

- il Presidente della Repubblica, in virtù dell'art. 87 della Costituzione, "ha il comando delle Forze Armate" e presiede il Consiglio Supremo di Difesa (cui partecipano il Presidente del Consiglio dei Ministri, i Ministri della Difesa, degli Affari Esteri, dell'Interno, dell'Industria e Commercio, del Tesoro e Bilancio e dal Capo di Stato Maggiore della Difesa) e quando ne ricorrano le condizioni, dichiara lo "stato di guerra" deliberato dalle Camere;
- il Parlamento, ai sensi dell'art. 78, delibera lo "stato di guerra" (in base ai principi della Carta dell'ONU e del Codice di Condotta OSCE) e conferisce al Governo i poteri necessari; esercita la funzione legislativa approvando, tra l'altro, le leggi di bilancio che definiscono lo stato di previsione, l'assestamento e il rendiconto generale delle spese della Difesa; esercita la funzione di controllo sul governo;
- il Governo esercita il potere esecutivo ed è responsabile della politica generale della Nazione. Nel suo ambito, il Ministro della Difesa è responsabile, collegialmente, degli atti del Consiglio dei Ministri e, individualmente, degli atti del Dicastero della Difesa. Nell'esplicazione delle proprie incombenze attua le deliberazioni adottate dal Governo ed emana le direttive in merito alla politica militare, all'attività informativa e di sicurezza ed all'attività tecnico - amministrativa; approva la pianificazione generale ed operativa interforze e quella relativa all'area industriale di interesse della Difesa; illustra al Parlamento l'evoluzione del quadro strategico e degli impegni operativi interforze, le previsioni di spesa per la Difesa e lo stato di attuazione dei programmi di investimento, sottopone all'approvazione del Consiglio dei Ministri i nominativi degli Ufficiali Generali ai quali far assumere le più alte cariche militari.

b) Forze paramilitari

L'Italia non dispone di Forze paramilitari.

c) Forze di sicurezza interna

Nell'ordinamento italiano le forze di sicurezza interna sono le Forze di Polizia.
Le Forze di Polizia (Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza) hanno competenza generale in materia di tutela dell'ordine e sicurezza pubblica ed hanno attribuzioni di Polizia Giudiziaria. Esse operano nell'ambito della vigente normativa e nello svolgimento della loro attività sono soggette al controllo amministrativo (disciplinare) e giurisdizionale della Magistratura, sia civile sia penale.
Il controllo politico delle Forze di Polizia, secondo l'ordinamento costituzionale italiano, spetta esclusivamente al Parlamento e nel caso specifico, essendo la responsabilità politica sull'operato delle Forze di Polizia attribuita al Ministero dell'Interno, membro del Governo e componente del Consiglio dei Ministri, è al Parlamento che questi è chiamato a rispondere. Il controllo di natura politica sull'operato delle Forze di Polizia è quindi assicurato dal Parlamento che, in generale, può avvalersi dell'istituto della "fiducia" ed in casi particolari può istituire Commissioni d'inchiesta su materie di pubblico interesse con gli stessi poteri e le stesse limitazioni dell'Autorità Giudiziaria (art 82 della Costituzione).
Il Decreto Legislativo 5 ottobre 2000, n. 297, pone l'Arma dei Carabinieri, corpo di polizia a statuto militare, alle dipendenze del Capo di Stato Maggiore della Difesa per quanto concerne i compiti militari ed istituisce un collegamento funzionale con il Ministero dell'Interno per quanto riguarda i compiti di tutela dell'ordine e della sicurezza pubblica. Pertanto, per ciò che concerne le sue attività di Polizia Militare l'Arma è soggetta alle stesse norme e procedure indicate per il complesso delle Forze Armate.

d) Servizi di informazione

La Legge n. 124 del 3 agosto 2007 ha riformato la disciplina delle attività dei Servizi di informazione per la sicurezza e del segreto. La legge, successivamente modificata e integrata, di cui sono stati ormai da tempo adottati tutti i regolamenti di attuazione, ha istituito il Sistema di informazione per la sicurezza della Repubblica, ponendone al vertice il Presidente del Consiglio dei ministri.
Al Presidente del Consiglio dei ministri sono affidati la direzione, la responsabilità politica generale ed il coordinamento della politica informativa e di sicurezza, anche in materia di protezione cibernetica e sicurezza informatica nazionali, che esercita anche impartendo le opportune direttive agli Organismi di informazione per la sicurezza (il Dipartimento delle informazioni per la sicurezza - DIS, l'Agenzia informazioni e sicurezza esterna - AISE e l'Agenzia informazioni e sicurezza interna - AISI).
Il Presidente del Consiglio può delegare le attività non attribuitegli dalla legge in via esclusiva ad un Ministro senza portafoglio o ad un Sottosegretario di Stato (Autorità delegata per la sicurezza della Repubblica).
A livello politico, il Sistema di informazione è completato dal Comitato interministeriale per la sicurezza della Repubblica (CISR), presieduto dal Presidente del Consiglio dei ministri e composto dall'Autorità delegata e dai Ministri degli esteri, dell'interno, della difesa, della

giustizia, dell'economia e delle finanze, dello sviluppo economico. Il CISR svolge funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica di informazione per la sicurezza, nonché sulla ripartizione delle risorse finanziarie e sui bilanci degli Organismi di informazione.
Le funzioni del Presidente del Consiglio e dell'Autorità delegata sono assolte tramite il DIS, istituito presso la Presidenza del Consiglio dei ministri, al quale la legge affida il compito di coordinare le attività svolte dall'AISE e dall'AISI e di verificarne i risultati. Al DIS, inoltre, sono affidate diverse competenze, tra le quali la promozione dello scambio informativo tra l'AISE, l'AISI e le Forze di polizia, l'elaborazione di analisi e la formulazione di valutazioni e previsioni, sulla scorta dei contributi analitici settoriali dell'AISE e dell'AISI, la promozione della cultura della sicurezza e la tutela amministrativa del segreto.
A livello operativo, per quanto concerne i Servizi di informazione, l'AISE ha il compito di ricercare ed elaborare tutte le informazioni utili alla difesa della sicurezza nazionale dalle minacce provenienti dall'estero, nonché il compito di individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e quelle volte a danneggiare gli interessi nazionali. Spettano inoltre all'AISE le attività in materia di controproliferazione concernenti i materiali strategici e le attività di informazione per la sicurezza al di fuori del territorio nazionale. All'interno del territorio nazionale, invece, la competenza in materia di ricerca informativa per la sicurezza, di elaborazione di tutte le informazioni utili alla difesa della sicurezza nazionale, di contrasto delle attività di spionaggio e di quelle volte a danneggiare gli interessi nazionali spetta all'AISI.
Il controllo politico sul Sistema di informazione è affidato dalla legge al Comitato parlamentare per la sicurezza della Repubblica (COPASIR).
Il Comitato è composto da cinque deputati e cinque senatori e sono ad esso attribuite funzioni di accertamento, di verifica e di controllo, anche attraverso la richiesta di atti, lo svolgimento di audizioni e di sopralluoghi presso gli uffici degli Organismi di informazione. Il Comitato esprime parere su tutti i provvedimenti di attuazione della legge n. 124 del 2007.

2.2 Come viene assicurata l'osservanza di tali procedure e quali autorità/istituzioni costituzionali sono preposte all'espletamento di tali procedure?

La responsabilità principale in ambito costituzionale per il controllo democratico delle forze armate ricade sul Parlamento, il quale elabora le leggi di bilancio ed esercita le funzioni di controllo sul Governo. Mediante interrogazioni, interpellanze e visite, il Parlamento controlla l'operato delle F.A.
Le menzionate iniziative possono essere adottate anche da ogni singolo parlamentare.
La Costituzione italiana prevede, altresì, la subordinazione dell'organizzazione militare al "Vertice politico – strategico" composto dal Presidente della Repubblica, dal Parlamento e dal Governo in base a quanto sopra illustrato.
Per quanto concerne le Forze di Polizia, si veda la risposta 2.1 lettera c.

2.3 Quali sono i ruoli e le missioni delle forze militari, paramilitari, di sicurezza e come controlla il vostro Stato che tali forze agiscano esclusivamente entro il quadro costituzionale?

Forze Armate

Il Decreto Legislativo 15 marzo 2010 n. 66, art.89, stabilisce che "compito prioritario delle Forza Armate è la difesa dello Stato. Le Forze Armate hanno altresì il compito di operare al fine della realizzazione della pace e della sicurezza, in conformità alle regole del diritto internazionale ed alle determinazioni delle organizzazioni internazionali di cui l'Italia fa parte. Esse, inoltre, concorrono alla salvaguardia delle libere istituzioni e svolgono compiti specifici in circostanze di pubblica calamità ed in altri casi di straordinaria necessità ed urgenza". I ruoli delle Forze Armate sono altresì delineati dagli impegni assunti in sede internazionale con l'adesione al sistema di sicurezza collettivo previsto dalla Carta delle Nazioni Unite e ai principi sanciti dall'adesione all'Unione Europea, alla NATO, all'OSCE e al Consiglio d'Europa. In tale quadro le missioni strategiche definite dal modello di Difesa si identificano nell'assolvimento di quattro funzioni principali:

- Difesa degli interessi vitali del Paese contro ogni possibile aggressione, al fine di salvaguardare l'integrità del territorio nazionale, la sicurezza e la libertà delle vie di comunicazione, delle aree di sovranità nazionale (Ambasciate) e dei connazionali all'estero;
- Salvaguardia degli spazi euro-atlantici, nel quadro degli interessi strategici o vitali del Paese, attraverso il contributo alla difesa collettiva della NATO;
- Gestione delle crisi internazionali, che si realizza tramite la partecipazione ad operazioni di prevenzione e gestione delle crisi, al fine di garantire la pace, la sicurezza, la stabilità e la legalità internazionale, nonché l'affermazione dei diritti fondamentali dell'uomo, nell'ambito di Organizzazioni Internazionali o di accordi multilaterali;
- Concorso alla salvaguardia delle libere istituzioni e svolgimento di compiti specifici in circostanze di pubblica calamità ed in altri casi di straordinaria necessità ed urgenza.

L'invio delle Forze Armate in missione all'estero è definito sul piano internazionale da risoluzioni delle Nazioni Unite e da decisioni assunte in sede UE/NATO/OSCE e perfezionato, sul piano interno, da decisioni prese dal Governo e approvate dal Parlamento in linea con la legge 21 luglio 2016 n. 145. Le procedure delineate garantiscono, pertanto, l'espressione del controllo democratico dell'impiego delle Forze Armate. A ciò si aggiunge l'importante esercizio della funzione Giudiziaria esercitata da Giudici indipendenti dal potere esecutivo e legislativo che vigilano sull'osservanza delle norme.

La Legge n. 125/2008 che ha convertito il D.L. n. 92/2008, recante misure urgenti in materia di pubblica sicurezza, ha autorizzato, per specifiche ed eccezionali esigenze di prevenzione della criminalità, l'impiego di un contingente di personale militare delle Forze Armate. Esso è posto a disposizione dei Prefetti delle Province, per servizi di vigilanza a siti e obiettivi sensibili nonché di perlustrazione e pattuglia in concorso e congiuntamente alle Forze di Polizia. II personate della Forze Armate, non appartenente all'Arma dei Carabinieri, nell'espletamento dei suddetti servizi di controllo del territorio agisce con le funzioni di "agente di pubblica sicurezza". Sulla base di tale iniziale previsione legislativa,

l'impiego delle Forze armate è stato confermato nel tempo anche in relazione ad attività di emergenza ambientale con riferimento a specifici contesti regionali e da ultimo con riguardo ad esigenze sia di prevenzione e contrasto al terrorismo.

Forze di Sicurezza

Le Forze di Polizia (Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza) hanno competenza generale in materia di tutela dell'ordine e sicurezza pubblica ed hanno attribuzioni di Polizia Giudiziaria. Esse operano nell'ambito della vigente normativa e nello svolgimento della loro attività sono soggette al controllo amministrativo (disciplinare) e giurisdizionale della Magistratura, sia civile sia penale.

3. Procedure relative al personale di forze diverse

3.1 Quale tipo di procedure sono previste nel vostro Stato per il reclutamento e il richiamo di personale per prestare servizio nelle vostre forze militari, paramilitari e di sicurezza interna?

Il "Codice dell'ordinamento militare", di cui al decreto legislativo 15 marzo 2010, n. 66 ha riassettato, tra gli altri, la Legge 14 novembre 2000, n. 331 ed il discendente Decreto Legislativo 8 maggio 2001, n. 215 che avevano sancito la sospensione del servizio militare obbligatorio dal 1° gennaio 2007, anticipata al 1° gennaio 2005 dalla legge 23 agosto 2004, n. 226, ed avevano stabilito i volumi organici complessivi di uno strumento militare totalmente professionale. Il personale militare, tanto in servizio permanente quanto in servizio temporaneo, viene ora reclutato esclusivamente su base volontaria mediante procedura concorsuale cui possono partecipare i cittadini italiani di ambo i sessi (il reclutamento femminile nelle Forze Armate italiane è stato introdotto dalla legge 20 ottobre 1999, n. 380).

In particolare, la categoria degli Ufficiali consta per la maggior parte di personale in servizio permanente che viene reclutato, in relazione al ruolo di accesso e al canale di alimentazione, mediante:

- concorsi pubblici cui possono partecipare i cittadini italiani;
- concorsi interni riservati ai Sottufficiali, ai Sergenti, ai Volontari Servizio Permanente ed agli Ufficiali in servizio temporaneo.

Gli Ufficiali in servizio temporaneo vengono invece reclutati con concorso pubblico fra i cittadini italiani in possesso di diploma di istruzione secondaria secondo grado o di diploma di laurea che non abbiano superato i 38 anni.

La categoria dei Sottufficiali è articolata su due ruoli: Marescialli e Sergenti/Brigadieri.
I Marescialli sono reclutati tramite concorso pubblico destinato ai cittadini italiani di età non superiore a 26 anni ed in possesso di diploma di istruzione secondaria di secondo grado ovvero concorso interno riservato al personale appartenente ai ruoli sottostanti. Inoltre, per soddisfare specifiche esigenze delle Forze Armate, è stata recentemente introdotta la possibilità di reclutare con il grado di maresciallo e corrispondenti, giovani in possesso di laurea definita con apposito decreto Ministeriale e con età non superiore a 32 anni.
I Sergenti/Brigadieri vengono reclutati unicamente tramite concorsi interni riservati agli appartenenti ai ruoli iniziali.
Tuttavia, nel modello professionale l'elemento chiave per la completa professionalizzazione delle Forze Armate è rappresentato dal personale di truppa volontario, nella considerazione che le altre categorie di personale erano già reclutate su base volontaria ed erano costituite in gran parte da personale in servizio permanente, oltre al personale di complemento.

Dal 2005 ad oggi, pertanto, i volontari di truppa vengono reclutati con concorsi pubblici destinati ai cittadini italiani in possesso di diploma di istruzione secondaria di primo grado, come Volontari in ferma prefissata di un anno (età non superiore a 25 anni), con possibilità di ottenere due rafferme annuali. I Volontari in ferma prefissata annuale alimentano, tramite concorso pubblico, la categoria dei Volontari in ferma prefissata quadriennale (età non superiore a 30 anni).
I Volontari in ferma prefissata quadriennale, meritevoli e che ne facciano domanda, transitano nel Ruolo dei Volontari in servizio permanente, potendovi accedere anche dopo l'assolvimento di una o massimo due rafferme biennali.
I Volontari in ferma prefissata, in possesso dei requisiti previsti dai rispettivi Ordinamenti, costituiscono poi bacino per alimentare, in parte, le carriere iniziali delle Forze di polizia ad ordinamento civile e militare (con una riserva di posti dal 45% al 70% come riportato all'articolo 703 del Codice dell'Ordinamento Militare).
Il quadro normativo sopra descritto, peraltro, ha sospeso e non abrogato la struttura giuridica che consente il ricorso alla leva, prevedendo la riattivazione del servizio obbligatorio nell'eventualità che il personale in servizio sia insufficiente e non sia possibile colmare le vacanze organiche mediante il richiamo in servizio di personale militare volontario cessato dal servizio da non più di cinque anni, qualora:

- sia deliberato lo stato di guerra ai sensi dell'art. 78 della Costituzione;
- una grave crisi internazionale, nella quale l'Italia sia coinvolta direttamente o in ragione della sua appartenenza ad una organizzazione internazionale, giustifichi un aumento della consistenza numerica delle Forze Armate.

Per quanto concerne il richiamo dal congedo, la normativa attuale, pur prevedendo ancora il richiamo in servizio d'autorità per tutte le categorie di personale per il completamento di unità/comandi/enti in vita, per far fronte ad esigenze inderogabili che non possono essere soddisfatte con personale in servizio e per le chiamate di controllo, di fatto disciplina il richiamo a domanda o previo consenso dei militari in congedo che forniscono la propria disponibilità e possono essere inseriti nel bacino delle Forze di completamento volontarie. Il personale inserito in tale bacino, al verificarsi di specifiche esigenze delle Forze Armate e sulla scorta delle specializzazioni possedute, potrà essere richiamato in servizio per periodi variabili non superiori a un anno.

3.2 Quale tipo di esenzioni o alternative al servizio militare sono previste nel vostro Stato?

Dal 1° gennaio 2005 il servizio militare di leva è stato sospeso.

3.3 Quali sono le procedure giuridiche e amministrative per tutelare i diritti del personale di tutte le forze, nonché dei militari di leva?

Nell'ordinamento giuridico italiano, la posizione del personale militare è definita da un articolato quadro legislativo che configura lo "status giuridico'' dei militari, in termini di «diritti» e «doveri». La tutela dei diritti dei militari è innanzitutto sancita dalla Costituzione e dal Decreto Legislativo 15 marzo 2010, n. 66 "Codice dell'Ordinamento Militare" (in cui

è confluita la legge. n. 382/1978) che, all'art. 1465, comma 1 recita "Ai militari spettano i diritti che la Costituzione della Repubblica riconosce ai cittadini.". E' previsto inoltre un sistema di "controlli" sia interni che esterni all'organizzazione militare.
Sul piano interno, il militare:

- può essere sottoposto a procedimento disciplinare solo per specifiche inosservanze di norme regolamentari ed osservando sempre l'obbligo di garantire l'espressione della propria difesa e di motivare i provvedimenti;
- può presentare al superiore che ha emesso il provvedimento "istanza di riesame" contro eventuali provvedimenti amministrativi (disciplinari e d'impiego) ritenuti lesivi di "diritti" o "interessi" e "ricorso gerarchico" all'organo di comando sovraordinato;
- può altresì conferire con il superiore diretto, e, nelle forme previste, con ogni altro superiore e con il Ministro della Difesa, cui tra l'altro, può essere inoltrato un plico chiuso.

In base alla legge n. 241/1990 e successive modificazioni ed integrazioni (legge n. 15/2005 "Modifiche ed integrazioni alla legge n. 241/1990, concernenti norme generali sull'azione amministrativa, e legge n. 69/2009 "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile"), il militare può comunque partecipare al procedimento amministrativo che lo riguarda, esercitare il diritto di accesso alla documentazione e ricevere indicazioni sul nome del funzionario responsabile del procedimento. Inoltre si segnala il D.Lgs. 14 marzo 2013, n. 33, come modificato dal D.Lgs. 97/2016, recante il "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni". Può presentare ricorso straordinario al Presidente della Repubblica o ricorso agli organi della Giustizia Amministrativa (in 1° grado ai Tribunali Amministrativi Regionali, in 2° grado al Consiglio di Stato) avverso atti amministrativi ritenuti lesivi di diritti soggettivi o interessi legittimi.
Nel caso di violazione di precetti penali, ciascun militare può rivolgersi all'Autorità Giudiziaria penale militare in caso di reato militare o all'Autorità Giudiziaria ordinaria in caso di altro reato.
Benché nell'ambito dell'ordinamento italiano la cura del benessere del personale rientri nei doveri principali dei Comandanti a tutti i livelli, la tutela degli interessi collettivi del personale militare è altresì assicurata dall'Istituto, di tipo elettivo, della "Rappresentanza Militare" (Decreto legislativo 15 marzo 2010, n. 66, articoli. 1476 e successive articolazioni e Decreto del Presidente della Repubblica 15 marzo 2010, n. 90 "Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare", articoli 870 e seguenti) che, posto all'interno dell'ordinamento militare stesso, formula pareri, proposte e richieste su tutte le materie oggetto di norme legislative o regolamentari circa la condizione, il trattamento, la tutela di natura giuridica, economica, previdenziale, sanitaria, culturale e morale dei militari verso le corrispondenti autorità ai vari livelli.
Nel merito, la Rappresentanza svolge un'attività:

a. propositiva, che si estrinseca tramite riunioni e conseguenti delibere, con cui possono essere presentate istanze di carattere collettivo relative ai seguenti campi di interesse:

- conservazione dei posti di lavoro durante il servizio militare, qualificazione professionale, inserimento nell'attività lavorativa di coloro che cessano dal servizio militare;
- provvidenze per gli infortuni subiti e per le infermità contratte in servizio e per cause di servizio;
- integrazione del personale militare femminile;
- attività assistenziali, culturali, ricreative, di educazione civica e di promozione sociale, anche a favore dei familiari;
- organizzazione delle sale convegno e delle mense;
- condizioni igienico-sanitarie;
- alloggi.

Tali delibere vengono veicolate all'attenzione dei vertici militari fino all'autorità politica (Art. 880 del DPR n. 90 del 15 marzo 2010 "Testo Unico delle disposizioni regolamentari in materia di ordinamento militare");

b. consultiva, che si concretizza con riunioni/audizioni a cui i Consigli ai vari livelli sono chiamate a partecipare dai vertici militari o politici "sulle materie che sono oggetto di attività legislativa o regolamentari", sulle seguenti tematiche (Art. 1478 del D.Lgs. n. 66 del 15 marzo 2010 "Codice dell'ordinamento Militare"):
- la condizione;
- il trattamento;
- la tutela di natura giuridica, economica, previdenziale, sanitaria, culturale e morale, dei militari."

In particolare, per quanto attiene gli Organi Centrali della Rappresentanza Militare l'attività consultiva può essere:

a. facoltativa, quando il legislatore, nel momento della predisposizione di un provvedimento legislativo, sente l'esigenza di ascoltare un parere di merito per meglio definirne i contenuti oppure quando il Comandante militare vuole avvalersi del parere degli organi di rappresentanza per la risoluzione di particolari problematiche;

b. obbligatoria, quando nell'ambito dell'attività legislativa, le nuove disposizioni rientrano tra le materie per cui è prevista la concertazione e nello specifico:
- il trattamento economico fondamentale e accessorio;
- il trattamento di fine rapporto e le forme pensionistiche complementari;
- la durata massima dell'orario di lavoro settimanale;
- le licenze;
- l'aspettativa per motivi privati e per infermità;
- i permessi brevi per esigenze personali;
- il trattamento economico di missione, di trasferimento e di lavoro straordinario;
- i criteri per l'istituzione di organi di verifica della qualità e salubrità dei servizi di mensa e degli spacci, per lo sviluppo delle attività di protezione sociale e di benessere del personale, ivi compresi l'elevazione e l'aggiornamento culturale del medesimo, nonché per la gestione degli enti di assistenza del personale;

- l’istituzione dei fondi integrativi del Servizio sanitario nazionale.

In questo caso, il legislatore è tenuto ad acquisire preventivamente il parere degli organi di rappresentanza in merito al progetto in itinere.

Al livello apicale l’Organismo di Rappresentanza dialoga con il Capo di Stato Maggiore della Difesa, con il Ministro della Difesa e con le Commissioni Parlamentari.

Per quanto riguarda le tre principali Forze di Polizia, occorre operare un’importante distinzione tra quelle ad ordinamento civile (la Polizia di Stato si configura quale “amministrazione civile ad ordinamento speciale”) e quelle ad ordinamento militare (Arma dei Carabinieri e Guardia di Finanza), poiché da essa discende un diverso status giuridico del personale e di conseguenza un diverso quadro legislativo che, a parte i principi generali comuni sanciti dalle leggi primarie, ne configura le specifiche tutele.
Per quanto riguarda il corpus legislativo della Polizia di Stato, la tutela del personale, oltre che dal ricorso alla giustizia amministrativa ordinaria ovvero ai procedimenti di ricorso gerarchico straordinari, viene assicurata dalle norme previste principalmente dalla Legge 121/1981, nonché dai decreti delegati relativi all’Ordinamento del Personale, il Regolamento di Servizio, il Regolamento di Disciplina, l’inquadramento nei ruoli, ed alle norme di comportamento politico-sindacale, ed a seguire dai contratti collettivi ed accordi quadro, che ne stabiliscono in dettaglio tutti i principali aspetti giuridico-ordinamentali, economici, previdenziali, sindacali, etc.

La Corte Costituzionale con la sentenza n. 120 del 2018, dichiarando l’illegittimità costituzionale dell’art. 1475, comma 2, del D.Lgs. 66/2010, ha affermato che i militari possono costituire associazioni professionali a carattere sindacale (APMCS), ma ha contestualmente precisato che:

- tale costituzione dovrà avvenire “…. alle condizioni e con i limiti fissati dalla legge.”;
- “è indispensabile una disciplina legislativa che regolamenti le condizioni e i limiti dell’esercizio del diritto di associazione sindacale”.

Il Ministro della Difesa, nelle more dell’intervento del Legislatore, ha impartito disposizioni con alcune circolari per regolamentare l’istruttoria delle istanze di assenso ministeriale preventivo di tali APMCS che andranno a sostituire la Rappresentanza Militare, tenuto conto che il disegno di legge, attualmente in discussione, ne prevede l’abolizione. Quindi, per il futuro, per conoscere le procedure per la tutela dei diritti del personale militare che attualmente è una prerogativa della Rappresentanza Militare, occorre aspettare l’approvazione della legge ora in discussione.

4. Applicazione di altre norme, decisioni e principi politici e del diritto umanitario internazionale

4.1 Come assicura il vostro Stato che il diritto umanitario internazionale e il diritto di guerra siano resi ampiamente disponibili, ad esempio, attraverso programmi di addestramento e regolamenti militari?

Nozioni di Diritto Internazionale Umanitario (DIU) e Diritto Internazionale dei Conflitti Armati (DICA) sono inseriti nei programmi di formazione di base e avanzata del personale militare di tutte le categorie (Ufficiali, Sottufficiali, Truppa). In particolare, per quanto riguarda la formazione basica, avanzata, superiore e specialistica degli Ufficiali, tali programmi di formazione sono inseriti all'interno di specifici percorsi di studio previsti per il conseguimento di un titolo di studio universitario (laurea, laurea magistrale e Master universitario di II livello). Inoltre, una selezione di Ufficiali, personale civile della Difesa e dei Corpi Ausiliari delle F.A. è ammesso presso il Centro Alti Studi per la Difesa alla frequenza del corso per Consigliere Giuridico nelle Forze Armate a cui è collegato il Master di II livello in "Diritto Internazionale Umanitario e dei Conflitti Armati". Il personale che supera il citato corso ottiene la qualifica di "Consigliere Giuridico nelle F.A." ai sensi dell'art. 82 del I Protocollo Aggiuntivo dell'8 giugno 1977 alle quattro Convenzioni di Ginevra del 1949. In collaborazione con il Corpo Militare della Croce Rossa sono organizzati a livello di Comandi locali corsi sul Diritto Internazionale Umanitario della durata di una o due settimane per conseguire il titolo rispettivamente di "Operatore Internazionale" e "Consigliere qualificato". Infine, i militari di tutte le categorie ricevono "a domicilio" richiami sugli argomenti in parola a premessa dell'immissione in Teatro Operativo tramite "cattedre itineranti" costituite da personale specializzato.

4.2 Che cosa è stato fatto per assicurare che i membri del personale delle Forze Armate siano coscienti di essere individualmente responsabili delle loro azioni ai sensi del diritto nazionale ed internazionale?

Nel quadro della formazione del personale nel settore del Diritto Umanitario, vengono organizzati con cadenza annuale presso il Centro Alti Studi della Difesa (CASD):

- uno specifico seminario in materia di diritti umani dedicato ai frequentatori dell'Istituto Alti Studi per la Difesa (IASD);
- un modulo formativo con esame finale di due settimane "Nozioni e concetti applicativi di Diritto Internazionale Umanitario" erogato a favore dei frequentatori del "Corso Interforze di Stato Maggiore" presso l'Istituto Superiore di Stato Maggiore Interforze (ISSMI);
- il citato corso per Consigliere Giuridico nelle Forze Armate a cui è collegato il Master di II livello in "Diritto Internazionale Umanitario e dei Conflitti Armati".
  In tale ambito, i programmi comprendono, tra l'altro, anche la trattazione del "Codice di Condotta dell'OSCE".

Inoltre, il personale militare destinato ad essere impiegato in missioni fuori del territorio nazionale segue anche specifiche attività formative in materia di Diritto Internazionale e, nello specifico, di quello Umanitario. Tali attività sono integrate da conferenze di carattere storico culturale e da direttive sui comportamenti da tenere nel Paese teatro della missione, nel rispetto degli usi e costumi delle popolazioni locali. Peraltro, le quattro F.A. inviano, ogni anno, propri Ufficiali alla frequenza dei seguenti corsi:

- "Diritto Internazionale Umanitario" presso l'*International Institute of Humaritarian Law* di Sanremo;
- "Corso per Consiglieri qualificati" organizzato dal Comitato Centrale della Croce Rossa Italiana di Sanremo;

Per la preparazione delle Unità da impiegare in operazioni di "mantenimento della pace (*peacekeeping*)", sono state capillarmente diramate specifiche pubblicazioni quali:

- il "Manuale di Diritto Umanitario" in 5 volumi (riportante tutte le principali Convenzioni Internazionali di Diritto Umanitario);
- il "Manuale per le operazioni di mantenimento della pace e per gli interventi umanitari";
- il "Codice di comportamento delle F.A. in operazioni";
- un opuscolo sugli aspetti legali delle operazioni all'estero.

4.3 Come assicura il vostro Stato che le forze armate non siano impiegate per limitare l'esercizio pacifico e legittimo dei diritti dell'uomo e dei diritti civili da parte delle persone, in quanto singoli o in quanto rappresentanti di gruppi, né per privarle della loro identità nazionale, religiosa, culturale, linguistica o etnica?

Si vedano le risposte alle domande 4.1 e 4.2

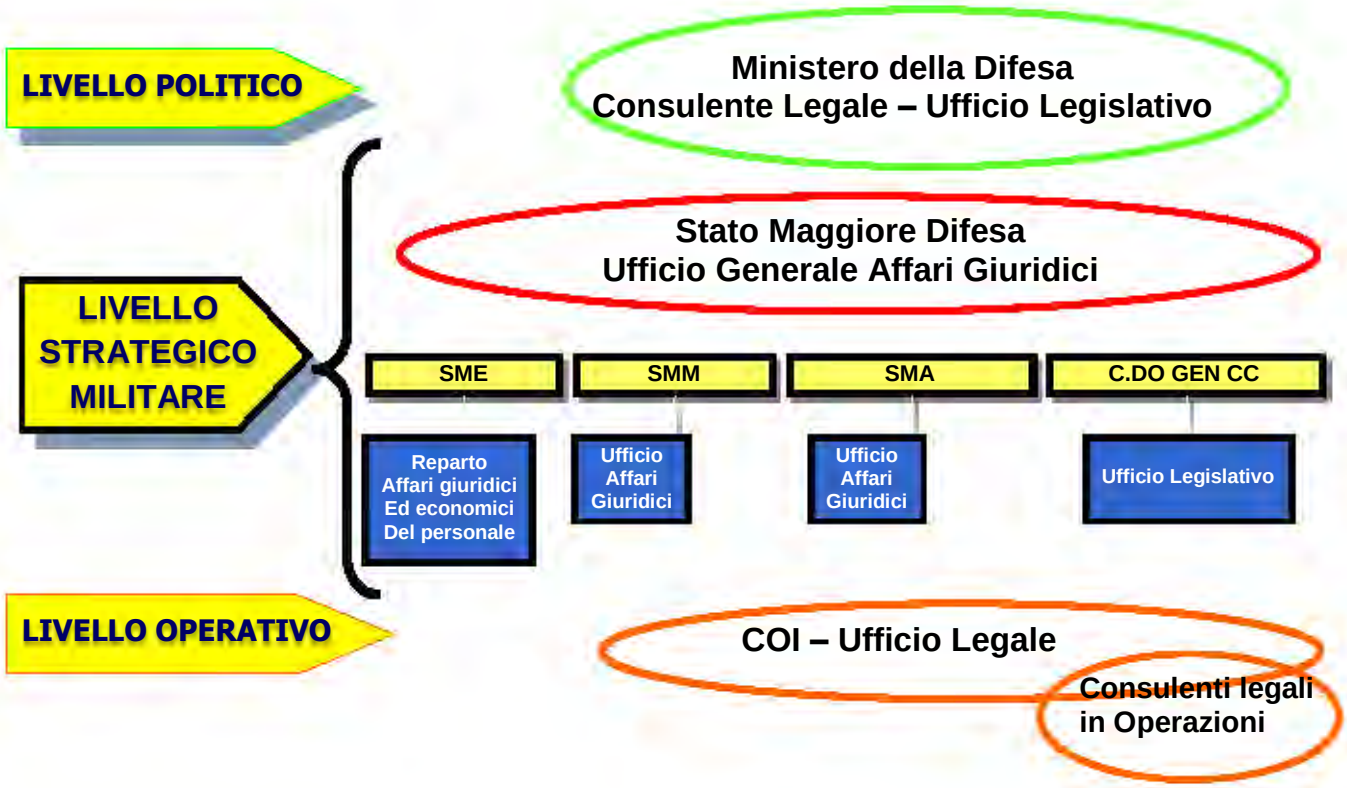
4.4 Che cosa è stato fatto per consentire l'esercizio dei diritti civili da parte dei singoli membri del personale e assicurare che le Forze Armate del Paese siano politicamente neutrali?

Si vedano le risposte alle domande 2.1, 2.2, 2.3 e 3.3 della Sezione II.

4.5 Come assicura il vostro Stato che la sua politica e la sua dottrina di difesa siano conformi al diritto internazionale?

La struttura legale della Difesa si può suddividere in tre differenti livelli politico, strategico militare e operativo come illustrato nello schema di seguito:

Struttura Legale



Lo Stato Maggiore della Difesa, in particolare, si avvale della consulenza giuridica svolta dall'Ufficio Generale Affari Giuridici (UGAG) posto alle dirette dipendenze del Sottocapo di Stato Maggiore della Difesa e i cui compiti specifici sono:

- studiare ed esaminare i provvedimenti legislativi e le evoluzioni giurisprudenziali, assicurando assistenza e consulenza in materia legale;
- fornire supporto in campo giuridico, contribuendo alla definizione degli indirizzi di policy, attraverso l'indicazione del quadro normativo, entro i quali devono essere armonizzati le attività, i piani e i programmi;
- corrispondere direttamente con l'Ufficio Generale del Capo di SMD, con l'Ufficio Legislativo e con i paritetici Uffici del Gabinetto del Ministro, del Segretariato Generale e degli SM di F.A.;
- fornire il supporto giuridico alle attività condotte nel quadro della cooperazione con le F.A, le organizzazioni militari e civili con cui il Paese intrattiene relazioni internazionali e/od alle quale aderisce;
- seguire, analizzare e valutare gli atti normativi che interessano l'impiego delle F.A. fuori dal territorio nazionale, con particolare riguardo alle risoluzioni ONU, alle direttive NATO ed agli altri provvedimenti d'interesse adottati dalle Organizzazioni internazionali, multilaterali e regionali;
- curare l'elaborazione degli accordi di cooperazione di natura politico-militare nel campo della Difesa bi e multilaterali.

Nell'articolazione dell'Ufficio, è anche inclusa, per il settore internazionale, una Sezione UE, OSCE ed organismi bilaterali che fornisce consulenza giuridica nello specifico campo di competenza. Il Capo di UGAG riveste anche l'incarico di consigliere giuridico del Capo di Stato Maggiore della Difesa.

SEZIONE III. ACCESSO DEL PUBBLICO E CONTATTI

1. Accesso del Pubblico

1.1 Come viene informato il pubblico in merito alle disposizioni del Codice di Condotta?

Le informazioni relative al Codice di Condotta verranno pubblicizzate in futuro nei siti WEB istituzionali. Al momento esse sono accessibili tramite il sito WEB OSCE.

1.2 Quali informazioni supplementari relative al Codice di Condotta, come ad esempio le risposte fornite nel Questionario sul Codice di Condotta, sono rese accessibili al pubblico nel vostro Stato?

Non ancora disponibili.

1.3 Come assicura il vostro Stato l'accesso del pubblico a informazioni connesse alle forze armate del vostro Stato?

Le Forze Armate provvedono individualmente alla diffusione di informazioni su modalità di reclutamento, stato giuridico, progressione di carriera e opportunità lavorative post servizio mediante i propri dedicati organi di pubblica informazione.

Propaganda diretta mediante opuscoli informativi o accesso diretto tramite collegamento internet sul WEB consentono di avere un'ampia panoramica sull'organizzazione, sulle attività svolte dalle Forze Armate e sulla condizione del militare.

2. Contatti

2.1 Fornite informazioni relative al punto di contatto nazionale per l'applicazione del Codice di Condotta

Ministero degli Affari Esteri Direzione Generale per gli affari politici e di sicurezza (DGAP) Ufficio VI (OSCE) Piazzale della Farnesina, 1 00135 Roma Tel. +39.06.3691.7380/3745 Email: dgap-06@esteri.it	**Stato Maggiore della Difesa** III Reparto Politica Militare e Pianificazione - Ufficio Controllo e Verifica Armamenti e Controproliferazione Via Mario Mameli snc, Aeroporto Ciampino 00178 Roma Tel. +39 0646915276 Fax +39 0646912930

Ministero dell'Interno Dipartimento della Pubblica Sicurezza Ufficio Coordinamento e Pianificazione per le Forze di Polizia Servizio Relazioni Internazionali – Divisione Affari Multilaterali Via Panisperna, 200 00184 Roma Tel.: +39 06 465354862 Fax: +39 06 4826736	**Ministero dell'Economia e delle Finanze** Dipartimento del Tesoro Direzione V – Prevenzione dell'utilizzo del sistema finanziario per fini illegali Via XX Settembre, 97 00187 Roma Tel. +39 06 4881135 Fax +39 06 47611047 e-Mail: giuseppe.maresca@tesoro.it Web: www.dt.mef.gov.it