CENTRO ALTI STUDI
PER LA DIFESA
CENTER FOR HIGH
DEFENCE STUDIES

CENTRO MILITARE
DI STUDI STRATEGICI
MILITARY CENTER FOR
STRATEGIC STUDIES

Analisi Strategica del 2021

Sfide e minacce non convenzionali

Year 2021, Strategic Analysis

Challenges and unconventional threats

CENTRO ALTI STUDI
PER LA DIFESA

CENTER FOR HIGH
DEFENCE STUDIES

CENTRO MILITARE
DI STUDI STRATEGICI

MILITARY CENTER FOR
STRATEGIC STUDIES

Analisi Strategica del 2021

Sfide e minacce non convenzionali

Year 2021, Strategic Analysis

Challenges and unconventional threats

Indice / Index

Analisi Strategica del 2021

Sfide e minacce non convenzionali

Analisi Strategica del 2021
Sfide e minacce non convenzionali

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dei singoli autori, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali gli autori stessi appartengono.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

L'Osservatorio Strategico è disponibile anche in formato elettronico (file .PDF) e nel formato E-Book (file .epub) al seguente link:
http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OsservatorioStrategico/Pagine/default.aspx

Osservatorio Strategico 2021

Questo volume è stato curato
dall'**Istituto di Ricerca e Analisi della Difesa**

Direttore
Col. c. (li) s. SM Gualtiero Iacono

Vice Direttore
Capo Ufficio Studi, Analisi e Innovazioni
Col. A.A.r.n.n. Pil. (AM) Loris Tabacchi

Redazione
Capo Sezione Studi Strategici per l'Innovazione
Magg. A.A.r.a.s. Luigi Bruschi
Addetti
1º Mar. Massimo Lanfranco – Cº 2ª cl. Gianluca Bisanti – 1° Aviere Capo Alessandro Del Pinto

Progetto grafico
Funz. Amm. Massimo Bilotta – 1º Mar. Massimo Lanfranco – Cº 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello

Autore
Claudio Bertolotti

Stampato dalla Tipografia del Centro Alti Studi per la Difesa

Centro Militare di Studi Strategici
Dipartimento Monitoraggio Strategico
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3204 - fax 06 6879779
e-mail dipms.cemiss@casd.difesa.it

Chiuso a maggio 2022 - Pubblicato a agosto 2022

ISBN 979-12-5515-015-2

Indice

Introduzione

Il presente volume è stato strutturato su tre temi cardine di estrema attualità e che rappresenteranno quelle che vengono indicate come le sfide del futuro per la sicurezza degli stati e delle società.

Il primo tema è l’evoluzione tecnologica, militare e civile, e la spinta verso una nuova rivoluzione militare basata sull’intelligenza artificiale e un campo di battaglia (o terreno di scontro) che si colloca in posizione ibrida tra reale e virtuale generando nuove potenzialità e vulnerabilità.

Il secondo tema si concentra sulla caduta di Kabul e il collasso dello stato afghano sostenuto dalla Comunità internazionale per vent’anni, la vittoria dei talebani e le dirette conseguenze di questo successo all’interno della galassia jihadista globale.

Infine, il terzo tema, anch’esso di estrema attualità, analizza le conseguenze dei disastri naturali, delle epidemie e delle pandemie sulla sicurezza dei Paesi dell’area “5+5” (Mediterraneo occidentale): strategie di cooperazione e mutuo sostegno, in particolare sulle ripercussioni di mutuo interesse della pandemia da COVID-19.

Vent'anni fa, oggi, gli Stati Uniti furono colpiti dagli attentati dell'11/9. Questi attacchi hanno avuto un profondo effetto su molti livelli diversi e hanno segnato l'inizio della Guerra al Terrore inaugurando un intervento militare guidato dagli Stati Uniti in Afghanistan nel 2001 e in Iraq nel 2003. Due decenni dopo, il ritiro delle truppe statunitensi dall'Afghanistan è giunto al termine, consentendo al presidente degli Stati Uniti Joe Biden di annunciare la fine della "guerra più lunga" d'America mentre i talebani riprendevano il controllo dell'Afghanistan. Vent'anni dopo l'11 settembre, chi sono i “nuovi” talebani e gli altri gruppi terroristi?

Dopo la caduta di Kabul cosa dobbiamo aspettarci? La minaccia si evolve in "Nuovo terrorismo insurrezionale" (NIT). La minaccia che stiamo affrontando oggi è già stata soprannominata "Nuovo terrorismo insurrezionale" (NIT), un concetto che include essenzialmente tutti i tentativi di sconvolgere l'ordine politico nazionale e/o internazionale attraverso la violenza. Il NIT è rivoluzionario, utopico e si evolve continuamente.

Numeri e profili del terrorismo jihadista in Europa: l'analisi dell'Osservatorio sul Radicalismo e il Contrasto al Terrorismo (ReaCT). L'onda lunga del terrorismo jihadista in Europa, riemerso con il fenomeno "Stato islamico" nel 2014 e amplificato dagli effetti emotivi e propagandistici della vittoria jihadista talebana in Afghanistan, ha portato a 158 azioni nel 2014-21: 201 i terroristi (60 morti nella condotta degli attacchi), 421 i morti e 2.439 i feriti (database START InSight, si veda www.startinsight.eu).

Aumenta la minaccia nel cyberspazio: tra capacità e vulnerabilità Le minacce nel cyberspazio possono essere generate da almeno tre tipologie distinte di attori: l'"hacker solitario", gli "hacktivisti", gli attori statali. I più recenti casi di attacchi informatici, da "WannaCry" al caso "Pegasus", dimostrano una crescente attività malevola attraverso gli strumenti informatici che via via stanno sempre più caratterizzando la nostra quotidianità, così come i sistemi di commando, controllo e sicurezza degli apparati statali, in particolare il settore della Difesa e dei servizi collettivi. Un Quadro evolutivo all'interno del quale si colloca il paradosso capacità/vulnerabilità.

La dipendenza statunitense dalla rete: vulnerabilità, criticità e punti deboli della Network Centric Warfare (NCW)1 La Network Centric Warfare traduce la superiorità dell'informazione in potenza di combattimento, collegando efficacemente le diverse capacità nello "spazio di battaglia". Ma la capacità militare degli Stati Uniti è di fatto dipendente dalla tecnologia di rete al punto che la dottrina stessa su cui si basa l'impiego dello strumento militare impone l'integrazione della tecnologia di rete in quasi tutti gli ambiti, in particolare proprio la Network Centric Warfare.

Le applicazioni militari dell'Intelligenza Artificiale e l'evoluzione della guerra: swarming e machine teaming nella rivoluzione degli affari militari. Esiste un legame sempre più stretto tra intelligence e intelligenza artificiale (AI). Contrastare le minacce asimmetriche contemporanee richiederà progressivamente un uso sistemico dell'AI che, sul piano militare, potrà dare supporto nel determinare l'entità, la natura e la posizione delle truppe e degli equipaggiamenti utilizzati, sia dagli alleati sia dai nemici; così come potrà aiutare nella valutazione di azioni militari, nella revisione della condotta delle operazioni a seconda dell'evoluzione del campo di battaglia. La valutazione è che l'AI imponga potenzialmente un cambiamento radicale alla Rivoluzione negli affari militari (RMA), sebbene il grado di sviluppo e dispiegamento dell'AI dipenda molto dai vincoli etici che ogni singolo attore saprà e vorrà imporsi e rispettare, pur nella consapevolezza che solo coloro che opteranno per trascurare l'aspetto etico e abbattendo i "confini" d'impiego dell'intelligenza artificiale, prevarranno sul campo di battaglia.

Le conseguenze di disastri naturali, epidemie e pandemie sulla sicurezza dei Paesi "5+5" (area del Mediterraneo occidentale): strategie di cooperazione e mutuo sostegno. I risultati del gruppo di ricerca internazionale presentati ai dieci ministri della Difesa e le ripercussioni della pandemia da COVID-19 sulla sicurezza dei paesi "5+5". Come riportato nel recente documento di ricerca pubblicato dal CEMRES nell'ambito della "5+5 Defense Initiative" e presentato il 15 dicembre 2021 ai dieci ministri della Difesa dei paesi aderenti al forum per la sicurezza del Mediterraneo occidentale, di cui l'autore di questo contributo è il rappresentante italiano,[2] le pandemie rappresentano un grave problema a livello mondiale e una seria minaccia alla sostenibilità e allo sviluppo. L'epidemia di Covid-19 rappresenta la peggiore pandemia sperimentata dalla generazione vivente a livello globale e con i più gravi riflessi in termini sanitari, sociali ed economici. La sponda sud del Mediterraneo occidentale sta affrontando sfide di governance, socio-economiche, climatiche, ambientali e di sicurezza; molte di queste sfide derivano da tendenze globali derivanti dale vulnerabilità create dalla diffusione del Covid-19 e richiedono un'azione comune da parte dei paesi componenti la "5+5 Defense Initiative", di cui l'Italia è parte.

---

1 Bertolotti C. (2022), *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).

2 AA.VV. (a cura di) Salem Shanbr (2021), *The repercussions of natural disaster, epidemics and pandemics on the security of 5 + 5 countries: "means of cooperation and mutual support*, CEMRES, Tunis.

1. Il Nuovo Terrorismo Insurrezionale (NIT)

Vent'anni dopo l'11 settembre: i "nuovi" talebani e gli altri gruppi in Afghanistan

Lo scontro: lotta nazionale e jihadismo globale

La guerra ventennale in Afghanistan (2001 al 2021) è giunta al termine. Quest'ultimo conflitto è stato caratterizzato da due fronti: uno più esplicito, che ha opposto una lunga insurrezione talebana agli eserciti stranieri e a un governo nazionale ritenuto illegittimo dal movimento fondamentalista; e un altro, meno manifesto, incarnato nella lotta al terrorismo jihadista che ha attecchito nel Paese e che è perseguito da diversi gruppi e sigle.

Oggi il mondo deve trovare un modo per affrontare un movimento talebano vittorioso che non solo ha preso il sopravvento sul campo di battaglia, ma ha anche imparato a sfruttare in modo efficiente l'ecosistema digitale al fine di influenzare l'opinione pubblica all'interno e all'esterno dell'Afghanistan. Tuttavia, il gruppo ora deve affrontare l'ostacolo della gestione di un paese e l'esito di quest'ultima impresa è ancora incerto. Una delle maggiori difficoltà risiede nella composizione eterogenea del movimento. Con Kabul sotto il controllo nominale dei talebani, le divisioni interne stanno diventando più evidenti, con le fazioni in competizione per un accordo di condivisione del potere che dovrebbe soddisfare le ambizioni personali e di gruppo. Un ulteriore punto interrogativo aleggia sulla capacità dei talebani di riconoscere una società civile afghana profondamente cambiata e sulla misura in cui il braccio politico talebano sarà in grado di tenere a freno una generazione più giovane di combattenti che sono stati esposti a ideologie, obiettivi e tattiche. I loro ranghi potrebbero ingrossarsi con una diaspora talebana, a seconda delle scelte della leadership in materia di politica e sicurezza, ad esempio per quanto riguarda la conservazione dei diritti e dei ruoli delle donne, l'inclusione etnica e religiosa, le alleanze aperte o segrete con gli ex nemici nella guerra e contro il cosiddetto *Stato Islamico*.

Tuttavia i talebani – che non hanno evitato di reprimere il dissenso all'interno delle loro stesse file – sebbene non siano una realtà monolitica, conservano essenzialmente le caratteristiche di un movimento internamente coerente e collaborativo. Una caratteristica che è in netto contrasto con una galassia di altri gruppi jihadisti che arruolano un numero crescente di combattenti stranieri veterani provenienti da Siria e Iraq.

In termini pratici, si stima che il fronte insurrezionale comprenda una quarantina di diversi gruppi militanti, alcuni organizzati in fazioni politiche, altri basati su affiliazioni tribali o etniche. Da qui la difficoltà di poter valutare quanti mujaheddin operano effettivamente sul campo di battaglia. Nel 2007, fonti dell'intelligence militare hanno fornito una cifra che va dai 5.000 ai 7.000 elementi – che salgono a 15.000 secondo fonti pachistane, che includevano nei loro calcoli anche le milizie tribali pashtun[3]. Nel febbraio 2009, il ministero degli Interni afghano stimava a 10-15.000 la forza combattente dei combattenti dei gruppi antigovernativi e jihadisti fossero[4].

Secondo l'intelligence statunitense, prima dell'offensiva finale che ha portato alla caduta di Kabul il 15 agosto 2021, la cifra era di circa 60.000 militanti attivi su circa 200.000 elementi totali[5]. Un numero che si pensa sia aumentato di alcune decine di migliaia nei mesi precedenti la conquista talebana, attraverso il reclutamento di nuovi *mujaheddin* tra le comunità sia pashtun che non pashtun e grazie a un'organizzazione efficiente e decentralizzata basata su un'organizzazione autonoma, "compartimentata" e tatticamente flessibile.

---

3 The Human Cost, *The consequences of insurgent attacks in Afghanistan*, Human Rights Watch, Vo. 19, N. 6(C), aprile 2007, p. 14.

4 Xinhua, *Number of Afghan Insurgent Grow Rapidly Since 2006*, in Daily outlook Afghanistan, 11 ottobre 2009.

5 Giustozzi A., *Afghanistan: Taliban's organization*…, cit.

Il DNA dei talebani: ideologia e tradizione sovra-tribale

I talebani sono un movimento prevalentemente pashtun ma, grazie a legami e accordi a livello locale, sono riusciti a coinvolgere anche altri gruppi etnici. Basato su una fitta rete di appartenenze, radicato in una forma di islamismo intriso di tradizione tribale e con un generico riferimento all'esperienza del jihad islamico contro i sovietici, il movimento talebano si è battuto con l'obiettivo di tornare al potere in Afghanistan.

Secondo gli esperti Thomas Ruttig[6] e Antonio Giustozzi[7], il movimento talebano poggia su una natura dualistica: cioè strutturale e ideologica. Può essere descritto come un'organizzazione caratterizzata da una struttura verticale, che nel corso degli anni si è trasformata in uno stato centrale "ombra", poggiante su un'ideologia sovra-tribale e sovra-etnica che può accogliere aspirazioni "nazionalistiche". Ma il movimento è anche definito da una struttura di rete orizzontale profondamente radicata nella segmentata società tribale pashtun.

Il movimento può essere visto come una rete di reti[8]; fattori religiosi, tribali e regionali si fondono con i principi organizzativi dei talebani che, politicamente, mirano alla costruzione di uno Stato che superi i limiti tribali a favore di una diffusione "nazionale" e del ristabilimento dell'*Emirato Islamico* (il nome ufficiale che ha unito nell'obiettivo finale le diverse fazioni del movimento). Ma se è vero che i talebani condividono una spinta nazionalista, non sono, tuttavia, pashtun irredentisti che cercano la riunificazione delle aree pashtun: la loro ideologia sovra-tribale lascia spazio all'inclusione delle comunità non pashtun, un approccio che li ha aiutati a conquistare "cuori e menti "di popoli non pashtun, come quelli che vivono nelle province settentrionali e occidentali.

Per i talebani, a differenza di altri gruppi jihadisti la cui progressiva crescita rappresenta una prossima sfida per l'Afghanistan, l'Islam è un ombrello che accoglie diverse comunità; la combinazione di strutture verticali (religiose/ideologiche) e orizzontali (tribali) avrebbe in questo modo conferito ai talebani un alto livello di coesione e una forte efficacia organizzativa[9].

I gruppi terroristi: Al-Qa'ida, lo *Stato islamico-Khorasan* e i gruppi minoritari in Afghanistan[10]

L'Afghanistan rischia di diventare un rifugio per gruppi estremisti, tra cui i pakistani Jaish-e-Mohammad e Lashkar-e-Taiba che hanno compiuto i devastanti attacchi terroristici di Mumbai del 2008 in India e continuano la loro offensiva contro obiettivi indiani in Afghanistan. Ma più gruppi terroristici stanno in realtà operando in Afghanistan e forse potranno operare dal Paese, *in primis* la cosiddetta Provincia dello Stato Islamico Khorasan (*Islamic State Khorasan Province*, IS-KP) e gruppi di *al-Qa'ida* nella doppia identità del nucleo originario di Al-Qaeda e del modello in franchise di al-Qa'ida nel subcontinente indiano (*Al-Qaeda in the Indian Subcontinent*, AQIS).

Al-Qa'ida (AQ)

Al-Qa'ida è stato un obiettivo primario degli Stati Uniti in Afghanistan dal 2001, in particolare la sua leadership: il leader Ayman al Zawahiri e i suoi vice. Nel settembre 2019, Washington annunciavano l'uccisione, "nella regione Afghanistan/Pakistan", di Hamza bin Laden, figlio del fondatore di AQ Osama bin Laden e leader in ascesa del gruppo. I raid e gli attacchi aerei statunitensi su obiettivi di AQ, inclusa la distruzione nel 2015 di un grande campo di addestramento nella provincia di Kandahar, avrebbero ridotto la presenza di AQ in Afghanistan, sebbene non l'abbiano sradicata. Un rapporto dell'aprile 2021 del Dipartimento della Difesa (DOD) stimava che i leader

6 Ruttig T., *How tribal are the Taleban*, AAN, Kabul 2012.
7 Giustozzi A., *Decoding the New Taleban*, C. Hurst & Co. Publishers Ltd, London 2009.
8 Ruttig T., *How tribal are the Taleban*, in Bashir S. and Crews R.D., "Under the Drones. Modern Lives in the Afghanistan-Pakistan Borderlands", Harvard 2012.
9 Ruttig T., *How tribal are the Taleban?...*, cit.
10 *Al Qaeda and Islamic State Affiliates in Afghanistan*, Congressional Research service, In Focus 7-5700, 23 agosto 2018; and *Terrorist Groups in Afghanistan*, Congressional Research service, In Focus IF10604, 17 agosto 2021

principali di AQ in Afghanistan fossero "una minaccia limitata" perché concentrati "principalmente sulla sopravvivenza" e non sulla pianificazione e condotta di operazioni.

L'accordo tra Stati Uniti e talebani, siglato a Doha nel febbraio 2020, impegna i talebani a impedire a qualsiasi gruppo terroristico, inclusa *al-Qa'ida*, di utilizzare il suolo afghano per minacciare la sicurezza degli Stati Uniti o dei suoi alleati. Ma i legami tra talebani e AQ sono stati invece rafforzati dall'impegno condiviso contro le forze internazionali in Afghanistan, nonché da matrimoni misti e altri legami personali tra i membri dei due gruppi. Come riportato da un rapporto delle Nazioni Unite (ONU) nell'aprile 2021, AQ e i talebani "rimangono strettamente allineati e non mostrano segni di rottura dei legami". Sul piano formale, nel febbraio 2021 i talebani hanno emesso ordini che vietano ai loro membri di dare rifugio ai combattenti stranieri, ma per il resto non sembrano aver adottato misure tangibili che possano confermare una rottura dei legami con AQ; al contrario, la conquista talebana dell'Afghanistan ha portato i talebani a liberare tutti i prigionieri di AQ precedentemente detenuti presso le carceri talebane.

AQ, inoltre, ha reagito positivamente all'accordo con gli Stati Uniti, con dichiarazioni dei suoi accoliti che celebravano tale fatto come una vittoria della causa talebana e quindi della militanza jihadista globale. A conferma di ciò, dopo la caduta di Kabul, la leadership di Al-Qa'ida ha rilasciato una densa dichiarazione di due pagine sull'Afghanistan, congratulandosi con la leadership dell'Emirato islamico, definendola una vittoria per gli afgani e la *Umma* (comunità musulmana globale): una vittoria che "dimostra" come la jihad sia la strategia giusta e "predicendo" altre vittorie a venire. Ciò che emerge dalle dichiarazioni degli affiliati di AQ in tutto il mondo è che, secondo la loro propaganda, l'istituzione dell'Emirato islamico in Afghanistan preannuncia più ampi trionfi e una nuova era di dominio islamico, con ciò dimostrando che il jihad è il metodo per raggiungere gli obiettivi dei movimenti combattenti islamisti contro "il modello fallimentare della democrazia occidentale".

Nel complesso, con il ritorno dei talebani conseguente al ritiro degli Stati Uniti, si valuta che al-Qaeda possa sfruttare la situazione per riorganizzarsi, aumentando il rischio che l'Afghanistan torni ad essere un hub per il reclutamento e l'addestramento del terrorismo jihadista. Un timore avvalorato dal ritorno nella natia provincia di Nangarhar in Afghanistan di Amin-ul-Haq, uno dei maggiori leader di al-Qaeda in Afghanistan ed ex aiutante di Osama bin Laden.

Infine, le relazioni tra i talebani, in particolare la rete Haqqani (HQN, vedi sotto), e AQ rimangono strette, basate sull'amicizia, una storia di lotte condivise, simpatia ideologica e unioni matrimoniali.

Al Qaeda in the Indian Subcontinent (AQIS)

Al-Qa'ida nel subcontinente indiano ha consolidato la sua presenza in Afghanistan incorporando combattenti nei talebani; nel settembre 2014, il leader di AQ, al-Zawahiri, ha annunciato la creazione di questa formale, separata e affiliata di AQ in Asia meridionale.

La distinzione tra AQ e AQIS è difficile, ma esistono alcuni elementi distintivi specifici. In sostanza, AQIS, nel rispetto del modello di *franchising*, si impone come tentativo di AQ di stabilire una presenza più duratura nella regione rafforzando i legami con gli attori locali, in parte spinti dal trasferimento di alcuni leader di AQ in Siria. L'ex leader dell'AQIS, Asim Umar, che era "protetto" dalle forze talebane quando fu ucciso in un'operazione congiunta USA-Afghanistan (settembre 2019), era un cittadino indiano profondamente radicato in Pakistan; al contrario, i leader principali di AQ sono prevalentemente arabi.

Secondo il rapporto del Dipartimento della Difesa statunitense dell'aprile 2021, AQIS ha minacciato le forze statunitensi in Afghanistan, un riflesso della cooperazione del gruppo con i talebani, sebbene sia valutato che il gruppo non possegga mezzi materiali per condurre attacchi al di fuori della regione.

Islamic state-Khorasan Province (IS-K, IS-KP)

Lo *Stato Islamico* ha annunciato la formazione della sua affiliata afghana (*Islamic State Khorasan Province*, IS-KP) nel gennaio 2015, ma i primi passi sono stati compiuti alla fine del 2014. L'IS-KP un tempo era concentrato nella provincia orientale di Nangarhar in Afghanistan, che confina con la provincia pakistana di Khyber Pakhtunkhwa. Inizialmente l'IS-KP era composto in prevalenza da ex militanti di Tehrik-e-Taliban Pakistan (TTP, vedi sotto) fuggiti dalle operazioni dell'esercito pakistano nel Khyber Pakhtunkhwa dopo la metà del 2014. Probabilmente uno degli affiliati di maggior successo dello Stato Islamico, l'IS-K è stato "quasi sradicato" dalla sua base principale nell'Afghanistan orientale alla fine del 2019 dalle offensive militari statunitensi e afghane e, separatamente, dai talebani. Un contingente IS-K nel nord dell'Afghanistan è stato contrastato in modo simile nel 2018. Queste perdite territoriali hanno costretto il gruppo a "decentrarsi", pur mantenendo una forza stimata di circa 2.000 combattenti, dislocati principalmente nell'est ma anche nel nord dell'Afghanistan. Alcuni leader di medio-alto livello dell'IS-K sono stati eliminati in attacchi statunitensi o catturati dalle forze afghane a partire dal 2016; ciò nonostante, l'IS-K rimane una minaccia e i recenti attacchi attribuiti al gruppo, in particolare gli attacchi all'aeroporto di Kabul alla fine di agosto 2021, indicano un alto livello di resilienza operativa e di capacità organizzativa. Oltre agli attacchi contro i civili, gli Stati Uniti e i talebani durante il ritiro da Kabul, l'IS-K ha rivendicato precedenti attentati su larga scala contro i civili, principalmente contro la minoranza sciita afghana e il più recente attacco con ordigni esplosivi improvvisati (*Improvised, explosive device*, IED) nella provincia di Nangarhar il 18 settembre 2021.

L'IS-KP e le forze talebane si sono a volte combattute per il controllo del territorio, delle risorse economiche e commerciali, o a causa di differenze politiche o di altro tipo; ora i due gruppi sono allo stesso tempo contrapposti sul piano ideologico e sul campo di battaglia. Dopo aver preso il potere, i talebani hanno giustiziato un ex leader dell'IS-K imprigionato nell'agosto 2021. Si stima che i talebani appartenenti all'ala dura del movimento, e dunque non propensi ad una politica moderata – in particolare elementi della rete terroristica Haqqani (vedi sotto) e giovani radicali – potrebbero disertare a favore dell'IS-KP se i leader talebani scendessero a compromessi di governo necessari a un'apertura da parte della comunità internazionale.

Haqqani Network (HQN)

La rete Haqqani (Haqqani network, HQN) è un ramo ufficiale e semi-autonomo dei talebani afghani con solidi legami con al-qa'ida (AQ). È stata fondata da Jalaluddin Haqqani (morto nel 2018), un importante comandante islamista antisovietico che è diventato un capo talebano e un leader chiave nell'insurrezione post-2001.

L'attuale leader del gruppo è Sirajuddin Haqqani (figlio di Jalaluddin) che è anche vice leader dei talebani dal 2015. La nomina di Sirajuddin a guidare la rete ha probabilmente rafforzato la cooperazione tra i talebani e AQ; si valuta che HQN sia il "collegamento primario" tra talebani e AQ e si segnala una sorta di recente legame, o forma di cooperazione tra HQN ed elementi di IS-K nella conduzione di attacchi complessi e attentati suicidi a Kabul. Nota bene: l'HQN è principalmente responsabile degli attacchi più mortali della guerra in Afghanistan.

Tehrik-e Taliban Pakistan (TTP)

Tehrik-e-Taliban Pakistan (TTP), noto anche come gruppo dei Talebani pakistani, ha come obiettivo il governo pakistano e il suo abbattimento. Il TTP operara in e dall'Afghanistan, con migliaia di combattenti, a fianco dei talebani afghani. Nel 2014, alcuni membri del TTP hanno giurato fedeltà al gruppo *Stato Islamico* e successivamente si sono trasferiti nell'Afghanistan orientale in risposta alle operazioni dell'esercito pakistano che per lo più hanno allontanato il gruppo dai suoi rifugi sicuri nella provincia pakistana di Khyber Pakhtunkhwa. La riunificazione tra il nucleo TTP e alcuni ex gruppi scissionisti (facilitata da AQ) dal 2020 ha ingrossato i ranghi del gruppo; alcuni membri del

TTP che hanno operato in Siria sotto l'ombrello dell'IS sono tornati in Afghanistan insieme ad elementi jihadisti arabi: questo trasferimento di ex combattenti dell'IS è una possibile conferma del rischio di trasformazione del suolo afghano in un paradiso sicuro per i gruppi jihadisti globali. Si valuta che il TTP possa trarre ulteriore vantaggio dall'acquisizione e dal rilascio dei prigionieri del TTP in Afghanistan da parte dei talebani.

Altri gruppi minoritari

***Islamic Movement of Uzbekistan* (IMU)**

Il Movimento islamico dell'Uzbekistan (IMU) era un tempo un importante alleato di AQ. Formato da uzbeki che hanno combattuto con le forze islamiste nella guerra civile del Tagikistan 1992-1997, l'IMU si è alleata con i talebani e ha lanciato attacchi in altri stati dell'Asia centrale. Dopo l'inizio delle operazioni degli Stati Uniti nel 2001, il gruppo si è concentrato in Afghanistan e Pakistan. Le forze dell'IMU operano nel nord dell'Afghanistan sotto il controllo dei talebani. Nel 2014 alcuni membri dell'Imu hanno giurato fedeltà allo Stato Islamico e, analogamente agli ex membri del TTP, ha poi operato in Afghanistan sotto l'IS-K e in Siria: alcuni veterani sono tornati in Afghanistan insieme ad elementi jihadisti arabi.

***East Turkestan Islamic Movement* (ETIM)**

Il Movimento islamico del Turkestan orientale (ETIM) mira a stabilire uno stato islamico indipendente per la minoranza musulmana degli uiguri, il popolo di lingua turca della Cina occidentale. Il gruppo ha legami con AQ. Come riportato di recente sui colloqui e sugli accordi Cina-talebani, i talebani provvederanno all'eliminazione della presenza dell'ETIM dall'Afghanistan. Al momento il gruppo è ancora operativo con centinaia di combattenti nel nord-est dell'Afghanistan e una presenza più ampia a Idlib, in Siria, e sarebbe in grado di muovere i combattenti tra le due aree. L'ETIM in Afghanistan si concentra sulla Cina; il contingente siriano ha "una prospettiva più globale", in linea con la visione globale di IS-K della jihad. Si valuta che, se i talebani interrompessero i rapporti con l'ETIM (in accordo con l'accordo con la Cina), è probabile che i combattenti dell'ETIM potrebbero passare nei ranghi dell'IS-K.

Dopo la caduta di Kabul cosa dobbiamo aspettarci? La minaccia si evolve in "Nuovo terrorismo insurrezionale" (NIT)

La diffusione ideologica e territoriale del Gruppo terroristico *Stato Islamico in Iraq e Siria*, poi *Stato islamico* (IS) ha innescato quelle che sino a poco tempo prima era una latente violenza jihadista globale. Il trionfo dei talebani in Afghanistan ha dato nuovo impulso vitale al jihadismo internazionale ed è ora presentato dalla propaganda jihadista come la vittoria dell'Islam sull'Occidente e sui suoi "valori corrotti". Pur tuttavia, ciò accade in contrasto con l'approccio talebano al jihad, che si limita a benedire quello che per i talebani è un successo nazionale, frutto di una guerra (anche comunicativa) che ha sempre avuto un carattere nazionalistico, mai transnazionale o globale: una guerra di liberazione nazionale, in opposizione all'IS-K (*Islamic State Khorasan Province*, il *franchise* afghano dello *Stato islamico*) e ad altri gruppi che cercano un trionfo globale.

Ma a prescindere da ciò, la vittoria dei talebani e dei gruppi di opposizione armata che compongono la galassia terroristica che affonda le radici nel post-stato islamico sta già avendo effetti diretti sulla volontà e sulla capacità operativa di gruppi e individui terroristi jihadisti a livello globale: dalla propaganda-comunicativa all'attivismo tattico e operativo.

Negli ultimi 20 anni gruppi terroristici, cellule e singoli combattenti jihadisti hanno iniziato ad adottare sempre più nuove tattiche, tecniche e procedure, che hanno esportato dai campi di battaglia del Medioriente, del Nord Africa e dell'Afghanistan e che hanno saputo adattare alla guerra jihadista

contemporanea e futura. Un primo, amaro assaggio di ciò che ci aspetta per il futuro sono stati gli attentati di Mumbai del 2008, quando un gruppo di dieci terroristi divisi in gruppi più piccoli lanciò un assedio durato quasi tre giorni. Da allora le città occidentali sono diventate occasionalmente il set di complessi attacchi suicidi e raid di nuclei d'assalto e, ancora più spesso, di assalti individuali in cui gli autori sfruttano efficacemente proprio quelle tecniche apprese nei vari teatri di guerra. I militanti e simpatizzanti dello *Stato Islamico* o di *al-Qa'ida* si sono ampiamente dimostrati in grado di compiere attacchi mortali e di costituire una minaccia diretta alla sicurezza dei cittadini e delle istituzioni nazionali. Come tale, il terrorismo contemporaneo può essere descritto e deve essere riconosciuto come un fenomeno con caratteristiche o ispirazioni militari, così come dimostrato proprio dall'IS attraverso le sue azioni e operazioni esterne.

"Nuovo Terrorismo Insurrezionale" (NIT): è rivoluzionario, sovversivo e utopistico[11]

Oggi, dopo la caduta di Kabul e il successo ottenuto dai talebani in Afghanistan, lo spettro del terrorismo supera i confini dei campi di battaglia afghani, o siriani, libici o dell'intero Sahel. In tale prospettiva, possiamo affermare che il significativo aumento della violenza legata al terrorismo jihadista registrato nel mondo e in Europa negli ultimi 20 anni sia coerente con il concetto classico di terrorismo?

Gli attentati terroristici verificatisi tra il 2015 e il 2018 in Europa, negli Stati Uniti, così come nei paesi nordafricani o mediorientali, confermano l'effettiva capacità operativa dei gruppi terroristici, in particolare dello *Stato islamico*, la cui natura è mutata nel tempo: da realtà proto-statale con capacità di controllo territoriale, a ciò che possiamo ritenere un fenomeno denazionalizzato, senza confini. Il "jihad senza leader", che anticipa nella forma e nelle manifestazioni l'IS, è stato perfezionato da quest'ultimo, poiché agli "aspiranti" combattenti è stato impedito di viaggiare e quindi hanno scelto di colpire i loro paesi d'origine. Quello che stiamo affrontando oggi è già stato soprannominato "Nuovo terrorismo insurrezionale" (NIT),[12] un concetto che comprende essenzialmente tutti i tentativi di sconvolgere l'ordine politico nazionale e/o internazionale attraverso la violenza. Il NIT è rivoluzionario e utopico, e mentre il terrorismo è funzionale, il terrorismo insurrezionale si evolve continuamente. Lo scopo di questa nuova "specie" di terroristi non consiste nell'istigare le masse in vista del rovesciamento dei governi, ma nel persuadere un gran numero di musulmani in tutto il mondo ad unirsi alla lotta contro gli "infedeli" insistendo su una narrativa sostenuta dalla vittoria della [loro interpretazione dell'Islam in Afghanistan e allo stesso tempo presentando quella vittoria come una ragione in più per negare qualsiasi compromesso con i paesi occidentali.

Questo emergente "Nuovo Terrorismo Insurrezionale" non ha dunque nulla a che vedere con il terrorismo politico degli anni '70 e '80. È emerso in Medio Oriente dopo l'invasione statunitense dell'Iraq (2003) e si è sviluppato a metà degli anni 2000. Ha attirato l'attenzione del mondo nel 2014, grazie alle sue vittorie sul campo di battaglia in Iraq e Siria (e poi in Afghanistan). Oggi, tuttavia, l'IS – il cui principale gruppo affiliato sta ancora combattendo in (e forse dall') Afghanistan – ha perso gran parte di ciò che ha conquistato negli ultimi dieci anni: territori, risorse energetiche, accesso ai canali commerciali e finanziari. Il suo *appeal* mediatico, però, è ancora forte e utilizzerà il successo afghano e la campagna in corso contro come un "chiaro esempio", diretto anche contro gli stessi talebani descritti come corrotti.

La perdita di "territorio" ha costretto l'IS a concentrarsi, da un lato, sulle attività di *franchising* all'estero, soprattutto nelle aree di crisi, con un nuovo approccio sociale che prevede l'esternalizzazione della violenza basata sul riconoscimento reciproco tra l'organizzazione centrale dell'IS e gruppi terroristici e movimenti di opposizione "locali". Il suo messaggio cerca di trasformare

[11] Bertolotti C., Sulmoni C. (2021), How the Twenty-Year Afghanistan War Paved the Way for New Insurrectional Terrorism, in Carenzi S., Bertolotti C. (2021) "Charting Jihadism Twenty Years After 9/11", Dossier ISPI, 11 September 2021.

[12] Bertolotti C. (2015), NIT: Il 'Nuovo Terrorismo Insurrezionale'. Dalla '5+5 Defense Initiative 2015' il cambio di approccio alla minaccia dello Stato islamico, Analysis ISPI n. 292.

migliaia di individui radicalizzati e decine di giovani e gruppi armati di opposizione in "armi di prossimità" intelligenti e pronte a "uccidere e morire" in nome del Califfato.

In sintesi, il "Nuovo Terrorismo Insurrezionale" consiste nell'uso della violenza, ovvero nell'uso minacciato di violenza intenzionale, calcolata, razionale, autogiustificata al fine di raggiungere obiettivi politici, religiosi e ideologici. Il NIT è caratterizzato da elementi caratterizzanti. La natura del l'attività terroristica consiste nell'usare (o minacciare di usare) la violenza per raggiungere un obiettivo politico, è complessa e soprattutto imprevedibile, è rivoluzionaria, sovversiva e finalizzata alla costituzione di un proto-stato finalizzato all'ottenimento del "monopolio della forza" all'interno di un'area geografica. Inoltre, include aspetti politici, socio-economici e religiosi (giustificati su basi religiose e apocalittiche) e può essere definita "strattica" poiché la sua natura strategica viene veicolata attraverso tattiche che devono essere non necessariamente interconnesse. La sua natura è "glo-cale", transnazionale, senza confini e basata su "flessibilità e adattabilità". I suoi obiettivi sono rappresentati da politici, civili, miltari, religiosi e simbolici. È simbiotico: "esternalizza" la violenza supportata da effetti emulativi, e come risposta alla "chiamata al jihad".

Possiamo ritrovare tutti questi elementi nel fenomeno (ri)emergente dello *Stato islamico* che sta ritrovando nuove energie nella ritirata degli Stati Uniti dall'Afghanistan. Ciò che emerge da questa descrizione è una minaccia alla sicurezza rappresentata da una contemporanea, nuova forma di terrorismo: un fenomeno che si adatta e si evolve senza un obiettivo temporale o geograficamente definito. Il NIT vuole semplicemente imporre un nuovo modello di società (il Califfato) abbattendo le alternative e utilizzerà il simbolismo associato alla guerra in Afghanistan per esaltare la "vittoria dell'Islam" ottenuta grazie al sacrificio dei "martiri" e alla "benedizione divina".

Numeri e profili del terrorismo jihadista in Europa: l'analisi dell'Osservatorio sul Radicalismo e il Contrasto al Terrorismo (ReaCT)

Il nuovo terrorismo in numeri[13]

Come riportato da Europol nel rapporto *Te-Sat 2021*, gli Stati membri dell'Unione europea hanno segnalato un totale di 57 attacchi terroristici completati, falliti e sventati nel 2020. Il Regno Unito ha segnalato 62 incidenti terroristici e la Svizzera ha segnalato due probabili attacchi terroristici jihadisti. Il numero di attacchi terroristici negli Stati membri dell'UE nel 2020 è paragonabile al 2019 (119, 64 dei quali nel Regno Unito) ma è diminuito rispetto al 2018 (129, 60 dei quali nel Regno Unito). Nel 2020 sono state uccise in totale 21 persone in attacchi terroristici nell'Unione europea. Tre persone sono morte nel Regno Unito e una in Svizzera. Ad eccezione dell'omicidio mirato di un insegnante di scuola in Francia, le vittime mortali sembrano essere state scelte a caso come rappresentanti di popolazioni identificate come nemiche per motivi ideologici.[14]

436 gli atti di terrorismo, compresi gli episodi classificati come fallimentari e sventati, che sono stati rilevati dai paesi dell'Unione Europea nel periodo 2017-2019 (895 nel quadriennio 2014-17): il 63 percento sono stati portati a compimento da gruppi di area separatista ed etno-nazionalista, il 16 percento da movimenti radicali di sinistra, il 2,8 percento a gruppi della destra estrema, il 18 percento di matrice jihadista. Sebbene questi ultimi siano marginali rispetto al numero complessivo di azioni, essi sono però all'origine di tutte le morti causate dal terrorismo nel 2019, di 16 uccisioni nel 2020 e 15 nel 2021.

L'onda lunga del terrorismo jihadista in Europa, riemerso con il fenomeno "*Stato islamico*" nel 2014 e amplificato dagli effetti emotivi e propagandistici della vittoria jihadista talebana in

[13] C. Bertolotti, *Numeri e profili dei terroristi jihadisti in Europa*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.

[14] Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.

Afghanistan, ha portato a 158 azioni nel 2014-21: 201 i terroristi (60 morti nella condotta degli attacchi), 421 i morti e 2.439 i feriti (database START InSight, si veda www.startinsight.eu).

Il numero di attacchi jihadisti nell'Unione europea, Svizzera e Regno Unito nel 2020 è più che raddoppiato rispetto al 2019. Nel 2020, a differenza del 2018 e del 2019, il numero di attacchi jihadisti completati gli attacchi hanno superato quello dei complotti sventati (quattro nell'UE, due nel Regno Unito). Se ciò sia legato agli effetti della pandemia di COVID-19 non può essere accertato sulla base delle informazioni disponibili.

Nel 2020 sono stati registrati 25 eventi, contro i 19 del 2019 e con un raddoppio di azioni di tipo "emulativo", ossia ispirate da attacchi portati a termine nei giorni precedenti e che hanno avuto un'eco mediatica che potrebbe aver svolto un ruolo da "innesco" per le successive azioni: sono il 58 percento le azioni emulative nel 2021 (erano il 48 percento l'anno precedente e il 21 percento nel 2019). Il quinquennio 2017-2021 ha inoltre registrato una diminuzione progressiva di azioni strutturate e coordinate che, con il tempo, hanno ceduto il "campo di battaglia" alle ormai quasi esclusive azioni individuali, spontanee e, spesso, dall'esito fallimentare.

Nel 2021 gli attacchi jihadisti sono stati 12 (gennaio-novembre).

Chi sono i terroristi che colpiscono in Europa?

La partecipazione al terrorismo jihadista in Europa è sostanzialmente maschile: il 96 percento degli attentatori sono maschi (194), sebbene nel 2020 siano state riportati tre attacchi perpetrati da donne (il 12 percento delle azioni condotte nel 2020). Un dato interessante, che viene approfondito nella seconda parte di questa analisi, è che il numero di attacchi terroristici di matrice jihadista, registra un incremento all'aumentare dello stock di immigrati maschi, ma non di quello femminile.

I 201 terroristi complessivi di cui si hanno informazioni parziali, uomini e donne, hanno un'età mediana di 26 anni, ma è questo un dato estremamente variabile nel tempo: erano 24 nel 2016, 26 nel 2017, 25,5 nel 2018, 30 nel 2019, 25 nel 2020 e 31,5 nel 2021. L'anagrafica dei 144 terroristi identificati, e dunque con maggiori dati informativi a disposizione, definisce un quadro in cui il 10 percento dei soggetti ha un'età inferiore ai 19 anni, il 36 percento ha tra i 19 e i 26 anni, il 39 percento tra i 27 e i 35 e, infine, il 15 percento ha più di 35 anni.

Aumentano i casi di recidiva

Cresce il numero di recidivi, ossia quegli individui, già condannati per terrorismo a una pena detentiva, che compiono azioni violente al momento dell'uscita dal carcere o dal percorso di reinserimento o, in alcuni casi, direttamente in carcere: dal 3 percento del totale dei terroristi nel 2018 (1 caso), al 7 percento (2) nel 2019, al 27 percento (6) nel 2020. Dati che confermerebbero la pericolosità sociale di individui che, condannati a una pena detentiva e dunque riconosciuti come socialmente pericolosi, non abbandonano l'intento violento, adeguandosi alle limitazioni temporanee, lo posticipano; un'evidenza che potrebbe confermare il rischio di aumento di attacchi terroristici nel breve periodo, a seguito della fine pena detentiva dei molti terroristi ancora detenuti.

Oltre agli individui cosiddetti recidivi, START InSight ha rilevato l'aumento di azioni portate a compimento da jihadisti già noti alle forze di sicurezza europei: oltre il 50 percento del totale nel biennio 2020-21, contro il 10 percento nel 2019 e il 17 percento nel 2018.

Si è rilevato, infine, l'aumento tra i terroristi di individui con precedenti detentivi (compresi i soggetti detenuti per reati non associati al terrorismo): 33 percento nel 2020 – erano il 23 percento nel 2019, 28 percento nel 2018 e 12 percento nel 2017; un'evidenza che rafforza l'ipotesi delle carceri come terreno fertile per la radicalizzazione e l'adesione alla violenza del terrorismo.

Il fenomeno migratorio in Europa e i suoi legami con il terrorismo[15]

Il 90 percento delle azioni terroriste di matrìce jihadiste compiute in Europa di cui abbiamo un'adeguato livello di informazioni, sono state portate a compimento da "immigrati", sia regolari che irregolari, di prima, seconda e terza generazione.

Su un piano meramente statistico è dunque possible affermare che esiste una correlazione tra il fenomeno migratorio verso l'Europa e l'aumento delle azioni terroristiche; ma il numero complessivo di terroristi rispetto alla massa degli immigrati è così marginale da imporre una lettura incontestabile di tale correlazione come non significativa, dato l'ordine di misura dell'unità per milione di immigrati.

Qual è lo *status* dei terroristi: sono "immigrati" o sono europei?

Grazie al database di START InSight, dei 138 profili di terroristi analizzati su 189, 65 (il 47 percento) rientrano nella categoria di "immigrati regolari"; 36 (26 percento) sono figli o nipoti di immigrati (seconda o terza generazione); mentre gli "immigrati irregolari" – o illegali a seconda dell'istituto giuridico applicato dai diversi paesi dell'Unione europea – sono 22 (il 16 percento): un dato, quest'ultimo, in crescita che passa dal 25 percento nel 2020 al 42 percento nel 2021. Significativa anche la presenza di un 7 percento di europei convertiti all'islam.

Complessivamente il 75 percento dei terroristi sono residenti in Europa in maniera regolare, mentre gli immigrati irregolari sono uno ogni sei terroristi.

Possiamo affermare che esista un legame tra immigrazione e terrorismo?

Su un piano statistico, gli immigrati sono indubbiamente veicolo di diffusione del terrorismo da un paese all'altro, in particolare da paesi in cui il fenomeno è rilevante, ma è improbabile che l'immigrazione di per sé sia una causa diretta della manifestazione violenta del terrorismo e che vi sia un legame diretto tra I due fenomeni in termini di causa-effetto.

Nessuna prova empirica ha infatti sinora dimostrato che gli immigrati in quanto tali abbiano una predisposizione ad aderire al terrorismo. È però vero, come in parte accennato, che l'afflusso migratorio di soggetti provenienti da paesi a predominanza musulmana afflitti da terrorismo avrebbe conseguenze significative sul verificarsi di attacchi nel Paese ricevente.

Gli immigrati sono dunque terroristi?

Al di là di semplicistiche quanto inopportune speculazioni, è difficile rilevare la consistenza empirica di un nesso di causalità tra i due fenomeni: l'essere migrante non sarebbe dunque un fattore scatenante per l'adesione terrorismo.

È però vero che vi sono legami accertati e diretti tra immigrazione e terrorismo e tra immigrati e terroristi. Legami che, in particolare, associano la criminalità organizzata ai gruppi terroristi e alla massa dei migranti irregolari che cercano vie alternative a quelle regolari (e legali) per trasferirsi da un paese a un altro. Vi sono poi i cosiddetti "terroristi di andata e ritorno", in particolare i terroristi europei andati a combattere in Siria che sono di fatto "migranti"; in questo caso è addirittura possible guardare all'Europa come area esportatrice di terrorismo, oltre che vittima e obiettivo dello stesso. Inoltre, vi sono i migranti economici aderiscono al terrorismo nel corso del loro viaggio. E, ancora, i migranti che aderiscono al *jihad* o che emigrano per colpire, come confermano gli attacchi terroristici di Nizza (Francia) del 29 ottobre 2020 e di Cannes l'8 novembre 2021, portati a termine da due immigrati irregolari partiti dalla Tunisia e dall'Algeria e transitati dall'Italia.

[15] C. Bertolotti, *Immigrazione e terrorismo: legami e sfide*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.

Nazionalità e gruppi etnici dei terroristi in Europa

Il jihadismo radicale che impone la violenza terroristica in Europa affligge alcuni gruppi nazionali ed etnici specifici. È stato rilevato un significativo rapporto di proporzionalità tra i principali gruppi di immigrati e i terroristi la cui nazionalità di origine (o quella dei loro genitori) è in linea con la dimensione delle comunità straniere all'interno dei paesi appartenenti all'Unione europea. Prevale l'origine maghrebina dei terroristi registrati in Europa: in particolare i gruppi etno-nazionali marocchino (prevalente in Francia, Belgio, Spagna e Italia) e algerino (in Francia).

Aumenta il rischio di terrorismo con l'incremento dei migranti irregolari

Il 18 percento dei terroristi sono immigrati irregolari (2014-2021), il 33 percento nel 2021 (era il 25 percento l'anno precedente).

In particolare è la Francia ad essere il paese ad aver registrato un aumento rilevante di terroristi tra gli immigrati irregolari. Se fino al 2017 non vi erano stati attacchi terroristici condotti da immigrati irregolari, nel 2018 il 16 percento dei terroristi è un irregolare; oltre il 33 percento nel 2020 e il 40 percento nel 2021. Il governo belga ha denunciato nel 2019 alcuni legami tra richiedenti asilo e movimenti jihadisti radicali o gruppi terroristi (Europol).

Possiamo dunque affermare che sia effettivo il rischio statistico, poiché un aumento nel numero di immigrati corrisponde a una maggiore probabilità che tra questi vi siano terroristi o soggetti che potrebbero prendere parte, anche in un secondo momento, ad azioni di terrorismo jihadista. Ma a fronte di un'indubbia correlazione non vi è però un evidente nesso di causalità. In altri termini: non è la condizione di migrante ad alimentare il fenomeno terroristico, ma possono contribuire alla scelta di aderirvi alcuni fattori quali il *backgrounf* individuale, le condizioni di vita al momento dell'arrivo nel paese ospitante, le reti criminali o jihadiste con cui tali soggetti entrano in contatto o dalle quali vengono intercettati.

Analisi, valutazioni, previsioni

È opportuna una valutazione obiettiva e approfondita di quello che possiamo considerare il vero successo del terrorismo: il "blocco funzionale", a cui si associa la spinta emulativa a colpire per ispirazione.

Il "blocco funzionale" (o stop operativo) è il più importante dei risultati ottenuti dal terrorismo contemporaneo, indipendentemente dal successo tattico (che corrisponde all'uccisione di almeno un obiettivo): è la capacità di impegnare le forze difesa e di sicurezza distraendole dalle normali attività di *routine*, interrompere o sovraccaricare il servizio sanitario, influire sulla mobilità urbana limitando l'accesso a vie di comunicazione e transito, rallentando o deviando il traffico urbano, aereo e navale, limitare il regolare svolgimento delle attività a danno delle comunità colpite e, più in generale, imporre danni, diretti e indiretti, indipendentemente dalla presenza di vittime.

A fronte di un successo tattico registrato nel 50 percento degli attacchi avvenuti dal 2004 a oggi, il terrorismo ha dimostrato di essere efficace ottenendo il "blocco funzionale" in media nell'82 percento dei casi, ottenendo il risultato maggiore nel 2020 con il 92 percento dei successi (83 percento nel 2021): un risultato eccezionale a fronte delle limitate risorse messe in campo dai terroristi. Questo è un dato che impone una riflessione su quelli che sono i veri obiettivi del terrorismo che, al di la del risultato tattico, ambiscono a colpire la quotidianità delle società colpite, oltre all'amplificazione massmediatica dell'evento, ottenuto grazie ai canali informativi tradizionali e alla propaganda jihadista sul Web. Aspetto che riveste un ruolo via via crescente all'indomani della vittoria jihadista dei talebani in Afghanistan che viene utilizzata e proposta da tutti i gruppi di matrice jihadista a livello globale per giustificare la lotta contro l'Occidente e i valori che lo rappresentano.

2. Il cyber-spazio

Aumenta la minaccia nel cyberspazio: tra capacità e vulnerabilità

La rivoluzione dell'informazione porterà alla guerra?

La storia suggerisce che le rivoluzioni militari sono più destabilizzanti quando sono in grado di creare non solo capacità ma, ancor più, vulnerabilità: è la vulnerabilità delle risorse e non la nuova capacità stessa che incentiva gli attacchi destabilizzanti.

Partendo da tale presupposto, possiamo affermare che la proliferazione della tecnologia digitale ha creato una nuova dimensione del confronto tra stati, anche attraverso il contributo di attori non statali e ha imposto la revisione della dottrina bellica così come la revisione degli strumenti delle relazioni internazionali. Come sottolinea Richard Danzig: le *«tecnologie digitali... sono un paradosso della sicurezza: sebbene concedano poteri senza precedenti, rendono anche gli utenti meno sicuri... la loro concentrazione di dati e potere manipolativo migliora notevolmente l'efficienza e la scala delle operazioni, ma questa concentrazione a sua volta aumenta esponenzialmente la quantità di dati che può essere sottratta o sovvertita da un attacco di successo. La complessità dell'hardware e del software crea grandi capacità che, a loro volta, generano ulteriori complessità*»[16 - 17].

Da "WannaCry" al caso "Pegasus": due esempi di vulnerabilità

Quattro anni fa, nel maggio 2017, più di 200.000 computers in 150 paesi del mondo sono stati colpiti contemporaneamente da un virus *ransomware* chiamato "WannaCry", il quale sfruttando una vulnerabilità del sistema Windows, era in grado di infettare i computers e criptare tutti i file presenti sull'hard drive. Solo pagando un riscatto (in bitcoin) era possibile ottenere la restituzione dei propri dati. Il paradosso è che Windows aveva messo a disposizione degli utenti un aggiornamento software in grado di risolvere la vulnerabilità del sistema un mese prima della diffusione del virus; ma la maggior parte degli utenti, ignorando l'aggiornamento si è esposta ad una contaminazione su larga scala. Ma v'è di più: quattro anni dopo, ancora oltre 1.700.000 di terminali risultano vulnerabili, di cui quasi 7.000 in Italia, e "Wannacry" continua a diffondersi occasionalmente. Il caso "Wannacry" è solo uno degli esempi dai quali emerge in maniera lampante come venga sottostimato il problema della sicurezza dei propri dati e, per estensione, delle reti informatiche[18].

E ancora, il cosiddetto "Progetto Pegasus". Come recentemente riportato dal *The Washington Post*, un programma militare di spyware, concesso in licenza da un'azienda israeliana ai governi per rintracciare terroristi e criminali, sarebbe invece stato utilizzato con successo in tentativi di hacking su smartphone appartenenti a giornalisti, politici, policy macker, influencer e attivisti per i diritti umani. I numeri di telefono sono apparsi su un elenco di oltre 50.000 numeri di utenti appartenenti a paesi noti per la sorveglianza dei propri cittadini; paesi che sarebbero clienti della società israeliana NSO Group, leader mondiale nello spyware privato[19]. Cosa prevede il Progetto Pegasus? Lo spyware israeliano Pegasus può infettare un dispositivo senza l'impegno o la conoscenza del bersaglio. Si tratta di una soluzione di *intelligence* informatica leader a livello mondiale che consente alle forze dell'ordine e alle agenzie di sicurezza di accedere ed estrarre da remoto e in forma anonima i dati da qualsiasi dispositivo mobile. Fino all'inizio del 2018, i clienti della società NSO Group si affidavano principalmente a SMS e messaggi attraverso l'applicazione WhatsApp al fine di indurre gli obiettivi

16 Danzig Richard (2014) '*Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*', Center for a New American Security.

17 Schneider Jacquelyn (2019) *The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war*, Journal of Strategic Studies, 42:6, 841-863, DOI: 10.1080/01402390.2019.1627209. In: https://doi.org/10.1080/01402390.2019.1627209.

18 Basileo Deborah (2020), *Tra Cyberterrorism e guerra dell'informazione. Scarsa consapevolezza e limiti normativi*, in #ReaCT2020, 1° rapporto sul terrorismo e il fondamentalismo in Europa, ed. START InSight.

19 Priest Dana, Timberg Craig, Mekhennet Souad (2021), *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, The Washington Post, July 18.

ad aprire un collegamento (link) malevolo funzionale ad infettare i dispositivi mobili degli utenti interessati dall'attività informativa e di controllo. Una tecnica che sfrutta il principio dell'Enhanced Social Engineering Message (ESEM), in grado di indirizzato il dispositivo mobile a un server in grado di controllare il sistema operativo e di fornire l'appropriato exploit remoto[20].

Quali le fonti della minaccia cibernetica?

Le minacce nel cyberspazio possono essere generate da almeno tre tipologie distinte di attori[21].

Il primo di questi attori è l'"hacker solitario", dove la natura solitaria in genere nasconde la presenza di più individui che operano in coordinamento tra di loro. Oggi, gli hacker solitari sono molto limitati nella loro capacità di infliggere danni di impatto strategico nazionale.

La seconda tipologia è rappresentata da gruppi non statali: "hacktivisti", criminalità organizzata, gruppi terroristici. Gruppi che hanno la capacità di infliggere danni economici sostanziali e disseminare il panico tra il pubblico – ad esempio prendendo di mira le banche o rendendo inaccessibili i siti web del governo – ma a cui manca la capacità di colpire in maniera efficace e distruttiva obiettivi di elevato valore. In genere, il livello di azioni che questi attori possono portare a compimento varia dagli attacchi *Denial of Service* alle frodi informatiche, al furto di identità. I gruppi non statali, di solito, non hanno le capacità per identificare e sfruttare le vulnerabilità dei codici complessi e per questo concentrano i loro sforzi nello sfruttamento degli errori umani, utilizzando tecniche di "*phishing*", in genere inviando *malware* tramite e-mail diffuse. I loro attacchi possono imporre danni significativi, ma non rappresentano una minaccia nazionale strategica.

La terza tipologia è costituita da attori statali che, disponendo di ampie risorse umane, scientifiche ed economiche, sono in grado di portare a compimento una campagna cibernetica multipla e a lungo termine contro un'ampia gamma di obiettivi e su una vasta area geografica. Gli attori di questo tipo sono spesso indicati come *Advanced Persistent Threats* (APT) e tendono a colpire obiettivi di alto valore attraverso azioni caratterizzate da elevati livelli di segretezza, sofisticate tecniche di raccolta di informazioni ed elevata capacità di sfruttamento delle vulnerabilità delle reti.

Gli attori statali concentrano le loro azioni sui sistemi informatici (IT) e sui database, da un lato, e attacchi ai sistemi di controllo industriale (ICS) dall'altro. Entrambe le tipologie di azioni producono effetti significativi: lo spettro della minaccia sui sistemi IT va dal semplice disturbo o fastidio (ad esempio, la modifica o la non accessibilità di siti Internet), fino a danni funzionali ed economici sufficientemente ampi da essere considerati una minaccia strategica. Tuttavia, negli ultimi anni, gli attacchi informatici hanno iniziato a rappresentare un'altra minaccia, che potrebbe essere persino più distruttiva di quella che rappresentano per l'infrastruttura IT: la minaccia di acquisizione o limitazione del controllo del processo industriale e produttivo con l'intento di provocare un pericoloso impatto cinetico[22].

La dipendenza statunitense dalla rete: vulnerabilità, criticità e punti deboli della Network Centric Warfare (NCW)[23]

La guerra network-centrica (NCW) è definita come un concetto di operazioni basato sulla superiorità dell'informazione che genera una maggiore potenza di combattimento collegando in rete sensori, decisori e combattenti al fine di ottenere una consapevolezza condivisa, una maggiore velocità di comando, un più alto ritmo delle operazioni, una maggiore letalità, una maggiore

[20] Mazoomdaar Jay (2021), *Explained: Here's how NSO Group's spyware Pegasus infects your device*, The Indian express July 22, New Delhi.

[21] Tor Uri (2017) *'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence*, Journal of Strategic Studies, 40:1-2, 92-117, DOI: 10.1080/01402390.2015.1115975. In: https://doi.org/10.1080/01402390.2015.1115975

[22] *Ibidem*.

[23] Bertolotti C. (2022), *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).

sopravvivenza e un elevato livello di auto-sincronizzazione. In sostanza la *Network Centric Warfare* traduce la superiorità dell'informazione in potenza di combattimento, collegando efficacemente le diverse capacità nello "spazio di battaglia"[24].

La capacità militare degli Stati Uniti è di fatto dipendente dalla tecnologia di rete al punto che la dottrina stessa su cui si basa l'impiego dello strumento militare impone l'integrazione della tecnologia di rete in quasi tutti gli ambiti, in particolare proprio la *Network Centric Warfare* (NCW). E sebbene l'orientamento generale sia quello di impiegare personale e sistemi ad alta specializzazione, emerge sempre più la necessità di disporre di capitale umano in grado di operare anche all'interno della "vecchia dimensione analogica" nel caso in cui i sistemi informatici dovessero cessare di essere funzionali, in tutto o in parte. È quello che Matthew Crosston, nel suo sagace articolo *The Millenials' war: dilemmas of network dependency in today's military*, chiama "effetto MacGyver", ossia la capacità di sviluppare e disporre di talenti e soluzioni che consentano di condurre efficacemente operazioni militari anche quando i sistemi principali siano fuori uso (*offline*) e non vi sia la possibilità di accedere o attivare sistemi di rete alternativi.

La crescente minaccia associata alla dipendenza dalla rete è un tema relativamente poco studiato e ancora non tenuto in debita considerazione, sia dal punto di vista politico che militare. Sebbene in ambito accademico, così come in quello operativo, siano già state evidenziate alcune preoccupazioni, queste sono però poste in secondo piano a fronte della vasta gamma di vantaggi legati all'integrazione della tecnologia in ogni aspetto dell'esercito, dai singoli combattenti sul campo di battaglia al sistema di comando e controllo, fino alla *leadership* a livello operativo e strategico. Gli Stati Uniti hanno le forze armate tecnologicamente più avanzate a livello globale e questo è il risultato dei grandi investimenti e della crescente fiducia nello sviluppo delle *Network Centric Operations* (NCO) a cui, di fatto, sono indissolubilmente associate, grazie all'integrazione e alla proliferazione della rete, sia le attività di *routine* quelle straordinarie. Ma il sistema, creato per garantire capacità di difesa, offesa e deterrenza porta con sé – rileva Crosston – alcune vulnerabilità potenzialmente micidiali dal livello più alto (strategico) a quello più basso (tattico).

La prima di queste vulnerabilità è rappresentata dall'approccio concettuale a livello strategico – adottato dalla leadership politica e militare, e avvalorato dalle teorie concettuali e accademiche del *Network Centric Warfare* e della rivoluzione negli affari militari – che di per sé rappresenta la prima vera grande vulnerabilità di sistema poiché si basa su una fiducia incondizionata nei confronti di strumenti informatici che sono ampiamente vulnerabili.

Il secondo grado di vulnerabilità lo si trova a livello tattico, dove gli operatori e gli utilizzatori dei sistemi di rete stanno diventando dipendenti dai sistemi informatici a un livello che possiamo valutare come allarmante dato che, da un lato, la maggior parte degli operatori militari interviene attraverso un computer connesso al sistema e, dall'altro lato, le tecniche, le tattiche e le procedure si sono tutte evolute intorno alla disponibilità e alla capacità di elaborazione in tempo reale di informazioni in rete. L'attuale generazione di militari è nativa digitale, cresciuta immersa nel sistema di rete, con una residua componente "analogica" a livello gerarchico medio-alto e alto che di fatto si è adeguata, a livello dottrinale, all'utilizzo esclusivo del sistema di rete portando a una sostanziale dipendenza da esso. Gli sforzi a livello politico sono stati fatti con l'intento di mitigare le minacce informatiche, ma ponendo in secondo piano l'opzione di una guerra in un ambiente post-attacco informatico caratterizzato dalla disponibilità di reti danneggiate, inaffidabili o addirittura dal completo isolamento della rete. I militari più anziani attualmente in servizio hanno maturato un'esperienza operativa che va dalla fine degli anni '80 ai primi anni '90, un periodo in cui pochissimi ambiti erano gestiti attraverso il collegamento in rete. Questa generazione viene rapidamente sostituita dai *Millenials*, la generazione di Internet che conosce il mondo digitale, che non ha mai vissuto senza una connessione Internet affidabile e prontamente disponibile di cui sono fortemente dipendenti; e

[24] Alberts D.S., Garstka J.J., Stein F.P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised).

nell'arco del prossimo decennio, tutti i rami delle forze armate saranno completamente composti dalla generazione di Internet[25].

Possiamo così considerare sempre più come critico il livello di dipendenza dal sistema di rete poiché, quando una rete si guasta, il lavoro si ferma, e quando il lavoro si ferma nelle forze armate, gli obiettivi operativi non possono essere perseguiti. Oggi, come ben evidenzia Crosston, quando la rete non è operativa e gli operatori sono *offline*, l'unica soluzione è quella di chiedere l'intervento dell'*help desk* e aspettare, mettendosi in coda; nel frattempo, gli operatori non sono in grado di portare a termine il proprio compito. E questo a fronte di scelte organizzative e gestionali che, nel tentativo di ridurre i costi, hanno portato al trasferimento dei servizi di assistenza lontano dagli operatori, di fatto trasformando un collaudato ed efficiente modello decentralizzato per il supporto di rete, in uno centralizzato[26]. Possiamo immaginare cosa potrebbe accadere in caso di interruzione del collegamento alla rete per un'unità impegnata in combattimento e sotto il fuoco avversario mentre tutto intorno piovono bombe da artiglieria, oppure durante un'operazione di *targeting* effettuata con un velivolo a controllo remoto che non può essere gestito? Cosa potrebbe fare l'*help desk*?

Questa crescente e sempre più radicata cultura della dipendenza dalla rete è un effetto collaterale involontario della corsa all'efficienza e alla riduzione dei costi[27]. Gli Stati Uniti possono essere definiti i campioni della gestione della rete e dell'NCW ma, paradossalmente, i paesi in ritardo nel progresso tecnologico, se è vero che sono più deboli e lenti nei loro processi decisionale e operativi, è altresì vero che saranno avvantaggiati da un minore livello di vulnerabilità agli attacchi informatici in rete. E poiché lo strumento militare statunitense procede a tappe forzate alla sostituzione dei tradizionali sistemi considerati "obsoleti" con la moderna tecnologia di rete, il rischio di isolamento della rete diventa sempre più reale; e questo vale anche per il settore civile, che spesso anticipa quello militare[28]. Un'evoluzione che, di fatto, potrebbe imporre una modernizzazione della forza militare che la renderebbe incapace di operare efficacemente in un ambiente senza rete.

Le applicazioni militari dell'Intelligenza Artificiale e l'evoluzione della guerra: *swarming* e *machine teaming* nella rivoluzione degli affari militari

Le applicazioni militari dell'intelligenza artificiale (AI)[29]

Esiste un legame sempre più stretto tra *intelligence* e intelligenza artificiale (*Artificial Intelligence*, AI). Contrastare le minacce asimmetriche contemporanee richiederà progressivamente un uso sistemico dell'AI che, sul piano militare, potrà dare supporto, ad esempio, nel determinare l'entità, la natura e la posizione delle truppe e degli equipaggiamenti utilizzati, sia dagli alleati sia dai nemici; così come potrà aiutare nella valutazione di azioni militari e nella revisione della condotta delle operazioni a seconda delle evoluzioni sul campo di battaglia.

Due i livelli sui quali l'AI ha un impatto rilevante: quello operativo propriamente detto e quello concettuale/dottrinale, da cui derivano le applicazioni a livello operativo e tattico.

Il crescente ruolo dell'AI nel supportare i processi di *intelligence* – dalla raccolta dei dati all'analisi – conferma quanto lo strumento militare sia sempre più strettamente supportato dalla tecnologia a livello operativo. Lo è in tutti gli ambiti, terrestre e navale, ma è su quello aeronautico, in particolare, che il crescente dispiegamento della tecnologia è in grado di garantire una decisiva superiorità sul campo di battaglia. Per valutarne l'impatto complessivo, dobbiamo tenere in

[25] Crosston M.-, *The Millenials' war: dilemmas of network dependency in today's military*, "Defense & Security Analysis", 33:2, 2017, pp. 94-105.
[26] Ibid.
[27] Robinson T., *It's the Network, Stupid! Air Power and Network Centric Warfare – Trends and Challenges*, "Military Technology", 40–8, 2010.
[28] Matthew Crosston, art. cit.
[29] *The military applications of Artificial* ***Intelligence.*** *A focus on the 8th Beijing Xiangshan Forum (24-26 October 2018)*, START InSight, November 4th**,** 2018, in https://bit.ly/2EnPdfH.

considerazione le potenzialità dell'IA specificamente applicate sia ad aree delimitate, come aeroporti o altri *target* puntiformi e circoscritti, sia a spazi più ampi come le aree urbane; potenzialità che possono essere ulteriormente valorizzate attraverso sistemi integrati a livello nazionale o transnazionale.

Altro livello è quello concettuale/dottrinale, poichè lo sviluppo e l'adozione dell'AI ha la potenzialità di imporre un cambiamento radicale in termini di "Rivoluzione negli affari militari" (*Revolution in Military Affairs*, RMA, in altre parole, l'evoluzione della guerra): si tratta, insomma, di una vera rivoluzione che, per chi già non si è adeguato in termini di capacità offensive e difensive, avrà conseguenze micidiali. Lo stesso tradizionale "sistema meccanico" di combattimento sta subendo grandi e rapidi sviluppi grazie all'intelligenza artificiale, così come la guerra informatica. Ne consegue che i sistemi di comando e controllo saranno sempre più influenzati dalla tecnologia e dalle capacità dell'AI, imponendo così la necessità di un aggiornamento costante anche nell'ambito degli affari militari.

Inoltre, dobbiamo considerare le diverse prospettive di specifiche applicazioni militari dell'AI, in particolare lo "*swarming*" (sciame) e il "*machine teaming*" che indicano il dispiegamento (al momento ancora ipotetico) di elementi autonomi a basso costo – generalmente piccoli droni o robot – che agiscono in coordinamento tra loro per svolgere compiti senza un comando centralizzato. Una capacità di offesa sul piano operativo che apre a molte opportunità e scenari e che, al contempo, espone a nuove vulnerabilità.

Intelligenza artificiale ed evoluzione della guerra[30]

Quali considerazioni possiamo fare in merito al ruolo dell'AI nella prossima fase della *Revolution in Military Affairs*?

Due gli aspetti principali. Il primo: l'intelligenza artificiale ha, e avrà sempre di più, conseguenze dirette sul concetto stesso di guerra e sul processo decisionale (è fondamentale nel *problem solving*)[31]. Il secondo: l'AI, che rappresenta una piattaforma di lancio per future armi autonome, ha di fatto già imposto un cambiamento radicale all'RMA, anche sul piano operativo e dell'addestramento, condannando alla sconfitta chi non si sarà adeguato alle capacità offensive e difensive proprie dell'AI.

E in effetti l'intelligenza artificiale ha già imposto cambi di approccio sostanziale alla condotta della guerra, supportando in maniera rilevante il processo decisionale attraverso un'analisi tempestiva di tutti i fattori primari e secondari che potrebbero influenzare la pianificazione strategica e operativa. Inoltre, la combinazione di guerra elettronica e capacità cibernetica garantisce una straordinaria leva militare, sia offensiva che difensiva, in quanto consente un monitoraggio dettagliato e costante degli obiettivi nemici senza esporre le proprie unità e risorse a rischi e minacce[32]. La stessa cosa, sul piano difensivo, vale per le infrastrutture critiche, la cui sicurezza e incolumità può essere ora garantita con limitato dispendio di risorse, sia in termini di soldati che di equipaggiamento. In questo contesto, l'utilizzo di robot a controllo remoto o a controllo (totale o parziale) attraverso l'AI, diverrebbe funzionale al supporto delle truppe sul campo di battaglia (*boots on the ground*), senza sostituirle del tutto; un'evoluzione tecnologica e culturale che, in particolare nel caso di conflitti asimmetrici, garantirebbe alla componente umana un ruolo che ad oggi rimane essenziale e primario.

Sul piano virtuale, a supporto di quello reale, vi è un'attività di *wargaming* sempre più realistica e adeguata che gode di un sempre maggiore supporto da parte dell'AI, sia nella fase di *training* sia in quella di pianificazione. L'altra dimensione del campo di battaglia contemporaneo è alimentata dai

30 Bertolotti C. (2019), *Artificial Intelligence and the evolution of warfare. Report on 8th Beijing Xiangshan Forum*, START InSight, 6 novembre. In https://bit.ly/2zQeuLO.
31 *Ibidem*.
32 *Ibidem*.

social-media, che rappresentano una grande opportunità di controllo e analisi sebbene ciò possa rappresentare un potenziale rischio di controllo delle masse. In tale ampio quadro, in particolare quello relativo al *wargaming*, il ruolo del settore privato diviene fondamentale[33].

Il tradizionale "sistema meccanico" di combattimento, come abbiamo accennato, sta subendo notevoli accelerazioni e revisioni proprio grazie all'applicazione dell'AI, mentre quello *cyber* diviene sempre più efficace. In tale contesto, il sistema di comando e controllo sarà sempre più condizionato dalle capacità di impiego della tecnologia AI, imponendone uno sviluppo costante nell'ambito degli affair miltari. Ciò imporrà un ruolo sempre più prevalente dei sistemi automatici nei settori dell'addestramento e del combattimento diretto. È ormai evidente come «la supremazia del settore *intelligence* supportato dall'intelligenza artificiale dividerà in maniera netta gli attori sul campo di battaglia globale tra perdenti e vincenti»[34].

Anche sul piano dell'addestramento dello strumento militare convenzionale, proprio grazie al contributo dell'intelligenza artificiale, aumenta in maniera progressiva la componente virtuale attraverso la quale le attività di *wargame* sono sempre più realistiche. Così come sul piano della capacità di influire sulle opinioni pubbliche e sulle scelte politiche degli avversari, e ancora, della sorveglianza e dell'analisi, similmente alle altre dimensioni del campo di battaglia contemporaneo, i *social-media*, come abbiamo evidenziato, rappresentano una grande opportunità, pur a fronte del rischio tangibile di agevolare forme di controllo di massa[35].

L'intelligenza artificiale sta dunque assumendo un proprio ruolo nel combattimento: sarà all'altezza del compito? Questa è la *vexata quaestio*. L'evoluzione del processo *intelligence* basato sull'AI consentirà allo strumento militare di assumere un ruolo diverso da quello attuale, dando all'AI un posto di primo piano a livello tattico (sul campo di battaglia) ma non (ancora) sugli altri due: quello operativo e quello strategico; ma è un contributo che sarà sempre più importante e crescente. In relazione all'impiego bellico dell'AI, un aspetto di rilievo è l'esito del confronto diretto sul campo di battaglia tra due soggetti in possesso di capacità militari bilanciate: un'ipotesi in cui l'intelligenza artificiale cesserebbe di essere un fattore determinante alla vittoria. Si impone dunque come impellente e prioritaria la necessità di sviluppare continuamente lo strumento dell'intelligenza artificiale attraverso investimenti, ricerca e sperimentazione.

E ancora, dobbiamo considerare le implicazioni sociali dell'utilizzo dell'AI: come l'Intelligenza Artificiale potrebbe essere potenzialmente utilizzata per influenzare e alterare strutture e funzioni sociali e per indurre un cambiamento negli atteggiamenti e nelle opinioni degli individui? Si tratta di un tema che pone le basi per un'analisi critica sulle questioni etiche legate ad alcune applicazioni dell'IA all'interno dell'RMA. L'intelligenza artificiale contribuisce in maniera determinante all'applicazione della *cognitive imaging* (immagine cognitiva), ossia l'utilizzo di varie tecniche per influenzare e modificare in maniera significativa le strutture e le funzioni del sistema sociale. Con ciò ponendo le basi per un'analisi critica sulla questione etica dell'intelligenza artificiale nella RMA. In questo senso, l'uso allargato dell'AI indurrebbe a un cambio del comportamento sociale da parte della popolazione sottoposta all'azione di controllo remoto; un fenomeno che viene riscontrato sia nel caso di azione di controllo da parte di soggetto esterno (nemico/avversario/*influencer*), sia da parte del proprio governo: i cittadini sono condizionati dall'azione di controllo e pertanto tendono ad adeguare il proprio comportamento. Al tempo stesso l'utilizzo di AI induce a cambiamenti di atteggiamento da parte degli avversari anche a livello operativo e tattico, come dimostrato dai talebani in Afghanistan che hanno adattato le loro tecniche e tattiche anche in conseguenza dell'utilizzo dei droni. Possiamo immaginare cosa potrebbe provocare l'utilizzo di robot in una guerra asimmetrica? Cosa potrà accadere nella mente del nemico e delle popolazioni locali?

---

33 *Ibidem*.

34 Zeng Yi, vice direttore generale della *China North Industries Group Corporation Limited* (NORINCO GROUP), in occasione dell'8° Beijing Xiangshan Forum, 24-26 ottobre 2019. In Claudio Bertolotti, *Artificial intelligence*…, cit.

35 *Ibidem*.

Infine, è la stessa sfera etica del soggetto che implementa l'AI e che poi deve utilizzarla, a condizionarne lo sviluppo e l'applicazione dell'intelligenza artificiale; ma chi non tiene conto dell'aspetto etico ed è disposto ad utilizzare l'AI al massimo delle sue potenzialità sarà sempre avvantaggiato sul campo di battaglia[36].

***Swarming* e *machine teaming*: differenti prospettive**

Come abbiamo accennato, lo *swarming* (sciame) consiste nel dispiegamento di elementi autonomi a basso costo (generalmente piccoli droni o robot) che agiscono in coordinamento tra loro per svolgere compiti senza un comando centralizzato. I primi esempi di sciami commerciali (semi-autonomi) – come i droni che volano in formazione – sono già stati testati. L'uso militare è oggetto di ricerca attiva, ma attualmente è limitato a causa dei limiti di affidabilità e prevedibilità; inoltre, i sistemi autonomi sollevano anche questioni etiche, ampiamente dibattute sul piano politico.

Dato il rapido sviluppo della tecnologia, la comunità della sicurezza e della difesa insiste nell'evidenziare quanto sia prioritario acquisire una migliore comprensione delle sfide e dei rischi legati allo *swarming*, soprattutto perché ancora manca un efficace sistema di difesa contro tali ipotetici attacchi.

Sistemi autonomi e tecnologie derivate: lo stato di avanzamento[37]

I sistemi autonomi sono in grado di portare a termine un compito senza il diretto coinvolgimento umano grazie all'interazione con l'ambiente tramite sensori e programmazione digitale. A un livello di base, devono essere in grado di percepire l'ambiente ed elaborarlo in maniera tale che serva da *input* al processo decisionale; la parte critica nell'impiego dei sistemi autonomi e delle tecnologie derivate è la fase di pianificazione, che dipende da due variabili chiave: la complessità del compito e l'ambiente.

L'ambiente. La navigazione autonoma è molto dipendente dal contesto: ambienti aerei o sottomarini presentano meno ostacoli rispetto alla terraferma, dove deve essere presa in considerazione anche l'interazione con persone o macchine; e ancora, l'ambiente civile è meno impegnativo, più prevedibile o controllabile rispetto al campo di battaglia; possiamo poi avere veicoli per uso civile o militare autonomi, qualora vi sia la possibilità di mappare in via preliminare l'area. Un risultato importante è rappresentato dai droni autonomi per il rifornimento in volo, che dimostrano come sia possibile realizzare e condurre operazioni aeree complesse[38]. Va detto però che le macchine possono sì elaborare immagini e comprendere parole, ma non hanno buon senso; la più grande limitazione che tutt'ora riduce un più ampio impiego di tali sistemi è infatti data dalla cosiddetta "intelligenza percettiva": l'ostacolo all'uso dei sistemi robotici, soprattutto in campo militare, a causa della facilità di inganno a cui possono essere soggetti i sistemi.

La complessità del compito. Progettare il processo decisionale deve tener conto dei limiti del ragionamento sintetico: i computer possono calcolare ben oltre le capacità umane, sono potenti, veloci, precisi, ma non possono (ancora) generalizzare dalle esperienze precedenti e adattarsi a nuove situazioni. Inoltre, più i robot sono di ridotte dimensioni, più si riduce la loro potenza di calcolo e, dunque, di ragionamento e adattamento. Vediamo i due casi di coordinamento e impiego dei sistemi robotici e le loro potenzialità (*machine teaming*) e gli ambiti di impiego negli ambiti *intelligence* e operativo.

Teaming macchina-macchina: i sistemi possono condividere informazioni, comprese le informazioni dell'obiettivo, eseguire operazioni collaborative per compiti semplici (volare in

---

36 Bertolotti C. (2019), *L'intelligenza artificiale nella nuova fase della rivoluzione degli affari militari*, START InSight, 28 ottobre. In https://www.startinsight.eu/tag/intelligenza-artificiale-revolution-in-military-affairs/.

37 Vincent Boulanin, Stockholm International Peace Research Institute (SIPRI), in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on *Swarming and Machine Teaming*, Thun, Switzerland, November 21st, 2018.

38 *Ibidem*.

formazione, sorveglianza, ispezione di edifici in un ambiente non complesso); come evidenziato dai progetti di ricerca statunitensi per il *teaming* macchina-macchina in operazioni di attacchi distribuiti (LOCUST), il principale limite è la dipendenza dall'infrastruttura di comunicazione.

Teaming uomo-macchina: l'assenza di una comunicazione simmetrica tra macchina e uomo è una grande limitazione (nessun comando vocale per le funzioni critiche). Trovare il giusto equilibrio è difficile, poiché potrebbe rendersi necessaria la presenza di più di un operatore per sistema, in particolare in condizioni critiche.

Dominio dell'*intelligence*: i sistemi hanno la capacità di generare mappe, rilevare esplosivi, localizzare il fuoco delle armi e valutare le minacce. Possono altresì effettuare attività di ricerca attiva: sorveglianza automatizzata, fusione e analisi dei dati di *intelligence* e svolgere operazioni autonome[39].

Targeting: l'applicazione più critica dell'autonomia dei sistemi su cui è in corso un ampio dibattito, è quella relativa alla capacità di ingaggiare solo obiettivi materiali molto grandi e ben definiti, sebbene con il grande limite di non distinzione tra obiettivi civili e militari. L'attività di *targeting* si basa sull'attività di "ricerca attiva" (ad es. DARPA Trace).

Nel complesso, l'impiego efficace di sistemi autonomi in formazione di sciami che siano in grado di operare in maniera coordinata dipende dalla natura dell'attività: tanto più è complessa o generale, tanto più aumentano le complicazioni di pianificazione e impiego poiché l'interazione complessa con altri agenti, umani o macchine, potrebbe essere di difficile programmazione. L'autonomia è molto più facile da ottenere per le applicazioni commerciali che non per quelle militari.

Swarming ed evoluzione della strategia militare: conseguenze per la stabilità internazionale[40]

Ci sono quattro modi per l'uso della forza la forza in un confronto militare; da essi discendono le strategie militari[41]. Vediamoli.

1. Negazione: contrasta le forze nemiche e le distrugge. L'obiettivo è militare (esempio: la *Blitzkrieg* nella Grande Guerra);
2. Punizione: colpisce civili e infrastrutture per esercitare pressioni indirette (esempio: i bombardamenti indiscriminati degli Stati Uniti nella Seconda guerra mondiale);
3. Rischio: prevalere sugli avversari attraverso una minaccia di *escalation* (guerra psicologica; esempio: Guerra fredda);
4. Decapitazione: prende di mira la *leadership* nemica grazie alla tecnologia. Può compensare la mancanza/ritiro delle truppe, come è avvenuto con le operazioni militari e di anti-terrorismo condotte dalle presidenze statunitensi di George W. Bush e Barack Obama, che sono state combattute non solo attraverso i *boots on the ground* ma con la tecnologia (droni). I progressi tecnologici hanno portato a una nuova rivoluzione negli affari militari.

Lo *swarming* è considerato uno degli elementi importanti della quinta evoluzione della strategia militare per il modo in cui può concentrare massa, potenza di fuoco, velocità e forze in un modo mai visto prima nella storia dell'umanità. Ma lo *swarming*, per poter funzionare ed essere efficace necessita di alcuni requisiti: deve contare su un gran numero di piccole unità con capacità sensoriali, facili da manovrare, in grado di osservare, reagire e agire in coordinamento. In termini di tecnologia, questo è un risultato già raggiunto: la stampa 3D di componenti di armi da fuoco e la disponibilità e adattabilità di droni sfidano il monopolio degli stati nell'uso della forza da parte di attori non statali; durante la famigerata battaglia di Mosul (2017) diversi soldati iracheni sono stati uccisi da droni pilotati dal cosiddetto gruppo terroristico *Stato islamico* (già ISIS), in quello che è stato il primo caso in cui l'Occidente ha perso la supremazia aerea tattica. In tale contesto, le tattiche dello *swarming* si

[39] *Ibidem*.
[40] Jean-Marc Rickli, Geneva Center for Security Policy (GCSP), in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21st, 2018.
[41] *Ibidem*.

sono imposte come mezzo per la condotta delle guerre asimmetriche; sebbene prima di vedere la manifestazione fisica degli sciami dovremo attendere ancora del tempo, assisteremo però alle manifestazioni cibernetiche dello *swarming*, come dimostrato dall'esistenza di *malware* dotati di funzionalità autonome[42].

L'evoluzione e l'impiego di *Iron Dome* – il sistema d'arma mobile per la difesa antimissile progettato per la difesa puntiforme e di piccole città, in grado di intercettare razzi a media velocità e proiettili di artiglieria con traiettoria balistica – rappresenta il primo esempio dell'emergere di sciami difensivi. E se la reazione all'attacco multiplo con razzi (dunque non in grado di modificare la loro traiettoria in maniera autonoma) è ormai un fatto consolidato sul campo di battaglia contemporaneo, sono in corso ricerche sulla competizione tra sistemi di sciami autonomi, così come su macchine e robot ricomponibili. La guerra è così sempre più combattuta da surrogati umani e tecnologici.

In questo scenario, la Cina e gli Stati Uniti stanno investendo molto nell'intelligenza artificiale, poichè offre molti vantaggi, *in primis* in termini di costi, essendo più economica e vantaggiosa in termini di ambizioni e risultati poiché consente di imporre la "negazione" all'avversario, cioè contrastare le forze nemiche e distruggerle.

Ma qual è l'impatto dello *swarming* sulla stabilità strategica? La stabilità esiste se non c'è incentivo ad attaccare: è il principio del vantaggio difensivo. In questo momento stiamo vivendo in un ambiente internazionale dominato dalla difensiva a causa delle armi nucleari; tuttavia, nel dominio informatico, l'offensiva è già prevalente. Se lo sciame si impone quale elemento strategico tradizionale, ci sarà un probabile cambiamento nell'equilibrio offesa-difesa in un ambiente internazionale più instabile, dove il conflitto diverrebbe la norma e non l'eccezione[43]; uno scenario che attribuirebbe ad autonomia e *swarming* il ruolo di elementi chiave del futuro campo di battaglia.

Manned-unmanned teaming (MUM-T) e *swarming*: opportunità e sfide nelle applicazioni militari[44]

Lo *swarming* è dunque un punto di svolta negli affari militari?

Si, lo abbiamo visto, ma va evidenziato che disporre di molti dispositivi non è un problema in termini di capacità di produzione e di gestione, ma l'obiettivo vero è la disponibilità di sottosistemi economici, affidabili e che richiedano un ridotto numero di operatori umani. Un altro aspetto rilevante è, come in parte abbiamo accennato, il contesto di impiego dei sistemi autonomi: la prospettiva militare è notevolmente diversa dalla prospettiva civile. Gli sciami si affidano alla comunicazione e alla navigazione satellitare e, in caso di scontro con avversari tecnologicamente superiori, vi è il rischio di "negazione" all'utilizzo del GPS che imporrebbe un'assenza, o una disponibilità parziale, di capacità di comunicazione. Una vulnerabilità che impone di aumentare la capacità di resilienza in ogni singola parte del sistema complesso; un processo che richiederà, a sua volta, ingenti investimenti economici per la ricerca e lo sviluppo. Molti sistemi strutturati sono relativamente costosi ed è per questo che probabilmente ci vorrà del tempo prima di vedere sciami nelle applicazioni militari, più probabilmente in ambienti non conflittuali (come le missioni di sorveglianza)[45].

Il *Manned-Unmanned Teaming* (MUM-T) per gli sciami è da tempo un tema di ricerca su cui è stato investito molto, ma ci sono ancora una serie di sfide da affrontare, in primo luogo la capacità di controllo di una flotta per missioni differenziate, che possa essere impiegata a diversi livelli operativi e molteplici configurazioni. Come raggiungere l'auspicato equilibrio che garantisca un elevato numero di sistemi/dispositivi per singolo operatore? E ancora, come aumentare e

42 *Ibidem*.
43 *Ibidem*.
44 Martin Hagström, FOI - Swedish Defence Research Agency, in Sulmoni Chiara, *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21st, 2018.
45 *Ibidem*.

velocizzare una capacità di interazione sempre più efficace tra l'operatore e il sistema? Quelle prospettate sono solamente le più rilevanti tra le sfide ancora aperte.[46]

Altre questioni da tenere in considerazione sono le regole e le politiche di sicurezza del volo (lo spazio aereo non è libero) e le difficoltà legate ai test. Stabilità e prevedibilità sono di primaria importanza nelle applicazioni militari, e poiché un sistema agisce all'interno di uno spazio definito e delimitato dal *software*, la capacità di autonomia consiste nel rendere tale spazio molto ampio, in modo da includere molti eventi potenziali. Ma al di fuori della simulazione, l'impiego di un sistema rimane complesso e l'imprevedibilità tende a prendere il sopravvento. Ciò che è importante sottolineare è che ci sono molte dimostrazioni su come controllare uno sciame per un singolo compito, ma una robusta interfaccia tra uomo e macchina è ancora un argomento di ricerca che necessita di essere approfondito e sviluppato.

***Swarming*, la Certain Conventional Weapons (CCW) e il Meaningful Human Control**[47]

I sistemi d'arma autonomi sollevano anche questioni etiche, ampiamente dibattute sul piano politico e che vengono discusse a livello di Organizzazione delle Nazioni Unite. L'UNIDIR (UN Institute for Disarmament Research) si occupa di UAV (veicoli aerei senza equipaggio) dal 2015 focalizzandosi principalmente sulla questione dei diritti umani e sull'impiego dei sistemi droni "*reaper*" e "*predator*".

L'UNIDIR, coerentemente con i suoi obiettivi istituzionali, incoraggia la comunità internazionale a riflettere sulle nuove sfide emergenti e sulle loro conseguenze, quali le implicazioni strategiche dei sistemi senza equipaggio che aprono, sì, a nuove opportunità ma che, al contempo, rappresentano fonte di nuovi rischi. A causa del dispiegamento a basso rischio di sistemi a controllo remoto e dal limitato impatto economico, potrebbero derivare pratiche militari problematiche.

In tale quadro, l'ampio dibattito sul tema potrebbe portare, almeno sul piano del diritto, a vietare o limitare l'uso di specifici tipi di armi che si ritiene causino sofferenze inutili o ingiustificabili ai combattenti o colpiscano indiscriminatamente i civili, così come accaduto per le mine, gli IED (*improvised explosive device*, ordigni esplosivi improvvisati), le munizioni a grappolo, ecc. Nel 2014 è stato istituito un gruppo di esperti governativi per affrontare i sistemi di armi letali autonome (LEG) con la partecipazione di 84 stati[48]. Da allora il tema cardine del dibattito tra tecnici ed esperti è la questione etica sulla capacità di controllo umano, poiché l'aumentare dell'autonomia potrebbe far crescere il distacco tra l'individuo e l'uso della forza letale.

Un dibattito non privo di ostacoli e di differenti punti di vista e approcci all'utilizzo dei sistemi militari a controllo remoto. Da una parte, si impongono le ragioni etiche a favore, in virtù delle esigenze di protezione del personale militare; dall'altra parte, sempre sulla base di ragioni etiche, i soggetti contrari al loro utilizzo, interessati a mantenere la primazia dell'azione umana nell'utilizzo della forza letale.

Nei primi due anni di lavoro dell'UNIDIR, un problema rilevante è stata la "tipizzazione" dei sistemi in esame, poiché la grande diversità delle capacità militari e tecnologiche dei singoli stati ha reso difficile classificare per tipologia i sistemi, che sono estremamente eterogenei, anche dal punto di vista terminologico. Ulteriori criticità sono state rilevate nella definizione del ruolo e della responsabilità dell'elemento umano nell'uso della forza letale, nel ruolo dell'interazione uomo-macchina nello sviluppo, nell'impiego e nell'uso della tecnologia emergente, e ancora, nell'esame delle potenziali applicazioni militari e delle relative tecnologie e, infine, nelle possibili opzioni per

---

46 *Ibidem*.

47 George Woodhams, UNIDIR Security and Society Programme, in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21st, 2018.

48 *Ibidem*.

affrontare le sfide umanitarie e di sicurezza internazionale poste, sul piano del diritto, dalle tecnologie emergenti[49].

In breve, ciò che l'UNIDIR pone in evidenza, è che sia necessario identificare le migliori pratiche e misure per incoraggiare la condivisione delle informazioni per aumentare il rispetto del diritto internazionale. Al di là della tecnologia, ci sono diverse prospettive nazionali che discendono da argomentazioni etiche. Lo *swarming* non è ancora stato menzionato specificamente, ma è l'area di autonomia che cattura di più l'immaginazione e che si pone sempre più al centro del dibattito sull'impiego della forza letale attraverso l'impiego di sistemi d'arma altamente tecnologici.

Analisi, valutazioni, previsioni

L'applicazione tecnologica associata all'AI ha dato due contributi chiave in campo militare e dell'*intelligence*: in primo luogo, si è imposta come piattaforma di lancio per future armi autonome; in secondo luogo, ha assunto un rullo primario nel *problem solving* e nei processi decisionali. Vanno poi consideraste le implicazioni sociali dell'AI, che potrebbe essere potenzialmente utilizzata per influenzare e alterare strutture e funzioni sociali, inducendo un cambiamento negli atteggiamenti e nelle opinioni degli individui.

Per quanto riguarda lo *swarming* e l'evoluzione della strategia militare, l'autonomia e lo sciame sono due caratteristiche chiave del campo di battaglia del futuro: la stampa 3D e lo *swarming* per applicazioni militari avranno enormi implicazioni. A proposito di *teaming* senza equipaggio (MUM-T) e *swarming*, considerando le possibilità e le sfide nelle applicazioni militari, ciò che è importante sottolineare è che, a fronte della dimostrata capacità di controllo e gestione di uno sciame per un singolo compito, l'implementazione di un'efficace interfaccia uomo-macchina è ancora argomento di ricerca che necessita di tempo e risorse. Infine, sul tema "*Swarming, the Certain Conventional Weapons (CCW) and Meaningful Human Control*", emerge quanto sia necessario identificare le migliori pratiche e gli strumenti legali per incoraggiare il rispetto del diritto internazionale e per adattarlo all'evoluzione tecnologica e a un'etica quanto più condivisa possibile.

La valutazione complessiva è che l'AI abbia già imposto un cambiamento radicale alla rivoluzione negli affari militari (RMA), sebbene il grado di sviluppo e dispiegamento dell'AI dipenda molto dai vincoli etici che ogni singolo attore saprà e vorrà imporsi e rispettare, pur nella consapevolezza che solo coloro che opteranno per trascurare l'aspetto etico e abbattendo i "confini" d'impiego dell'intelligenza artificiale, prevarranno sul campo di battaglia.

[49] *Ibidem*.

3. Il COVID-19 e la sicurezza del Mediterraneo

Le ripercussioni della pandemia da COVID-19 sulla sicurezza dei paesi "5+5" (Mediterraneo occidentale)

Come riportato nel recente documento di ricerca pubblicato dal CEMRES nell'ambito della "5+5 *Defense Initiative*" e presentato il 15 dicembre 2021 ai dieci ministri della Difesa dei paesi aderenti al forum per la sicurezza del Mediterraneo occidentale, di cui l'autore di questo contributo è il rappresentante italiano[50], le pandemie rappresentano un grave problema a livello mondiale e una seria minaccia alla sostenibilità e allo sviluppo. Gli effetti sono molteplici: dalla perdita di vite umane, alle malattie, al disagio sociale ed economico, alla perdita di capacità di fornire servizi. Inoltre, in un'economia mondiale sempre più integrata e costruita su reti globali di approvvigionamento, le pandemie in un paese possono facilmente impattare sugli altri.

Come la diffusione del virus Covid-19 ci ha dimostrato, un'epidemia è una nuova malattia che si diffonde all'interno dei confini nazionali, mentre una pandemia è un'epidemia che si diffonde in tutto il mondo, attraversando i confini internazionali e che va a colpire un numero molto elevato di persone. La diffusione di una malattia di questo tipo deriva dalla diffusione di un virus nuovo per l'umanità, in molti casi di origine animale, per il quale il corpo umano non è in grado di rispondere con efficacia o di ottenere l'immunità in maniera autonoma.

Le pandemie, come la storia recente ci ha dimostrato, non investono il mero campo della salute pubblica e dei sistemi sanitari nazionali, ma si impongono come sfide sociali e di sicurezza globale e hanno un impatto sulle dimensioni economica e politica dei paesi in cui si diffonde; la stessa diffusione del virus impone limitazioni ai trasferimenti delle persone da una regione all'altra, e questo a causa dell'elevato grado di contagiosità e diffusione del virus, con dirette ripercussioni sulla vita sociale dei cittadini. Quando le attività economiche vengono chiuse, il paese si trova di fronte a un deficit finanziario per soddisfare le esigenze della collettività, e così il blocco di una città o di un intero stato impone limiti allo sviluppo economico e sociale, portando a un aumento della pressione sui governi.

Il Covid-19

Il nuovo ceppo di virus all'origine della malattia da Covid-19, che è simile alla sindrome respiratoria acuta grave (SARS), ha portato l'OMS a dichiarare il 30 gennaio 2020 lo stato di epidemia di tipo PHEC (Public Health Emergency Concern) e il 12 febbraio 2020 la malattia è stata denominata Covid-19 (Coronavirus Disease 2019). Nell'arco di 30 giorni, il Covid-19 si è diffuso rapidamente a livello globale con un aumento di un numero di casi confermati con una prima massima concentrazione nella provincia di Wuhan, Hubei, Cina, attualmente considerato il possibile punto di origine. Secondo il rapporto sulla situazione dell'OMS del 13 marzo 2020, la malattia si è diffusa in più di 100 paesi del mondo e tra questi, i più colpiti sono l'Italia, gli Stati Uniti, la Spagna, la Germania, la Cina, la Francia e la Turchia. Per controllarne la diffusione, molti paesi, inclusa la regione dei paesi del Mediterraneo, hanno adottato alcune misure come il blocco delle città, meccanismi di *screening* negli aeroporti.

L'epidemia di COVID-19 rappresenta la peggiore pandemia sperimentata dalla generazione vivente a livello globale e con i più gravi riflessi in termini sanitari, sociali ed economici. Su scala globale, al 6 dicembre 2021, l'Organizzazione Mondiale della Sanità (OMS) ha confermato numeri pari a 267.865.289 pazienti infetti e 5.285.888 decessi in tutto il mondo.

[50] AA.VV. (a cura di) Salem Shanbr (2021), *The repercussions of natural disaster, epidemics and pandemics on the security of 5 + 5 countries: "means of cooperation and mutual support*, CEMRES, Tunis.

Impatto del Covid-19 sulla sponda sud dello spazio 5+5

La sponda meridionale dell'area "5+5" non è stata risparmiata dagli effetti dannosi della pandemia. La maggior parte dei paesi ha affrontato con successo l'impatto della prima ondata, mentre la seconda e la terza sono state più aggressive. Nonostante ciò, il numero di casi e vittime è inferiore a quello della costa settentrionale, come evidenzia la "Tabella 1":

State	*Confirmed Cases*	*Number of deaths*
Algeria	128,725	3,595
Libya	185,776	3,126
Mauritania	19,494	364
Morocco	519,108	9,143
Tunisia	345,474	12,654

***Table 1**: Confirmed COVID-19 cases & deaths in the Maghreb*

(source: Africa CDC & African Union June 2021)

I Paesi più colpiti sono stati il Marocco e la Tunisia mentre la Mauritania è stata meno afflitta per numero di casi e decessi. Tuttavia, i governi sono stati obbligati a mettere in atto misure restrittive per contrastare la diffusione della pandemia: tra questi il confinamento (*lock-down*), la chiusura delle frontiere e la chiusura delle scuole.

Le economie della regione del Maghreb hanno patito difficoltà a causa del Covid-19; secondo il Fondo monetario internazionale (FMI), la crescita reale del prodotto interno lordo (PIL) nella regione del Maghreb è diminuita dell'8,8 nel 2020. Tutti i paesi del Maghreb hanno registrato un calo della crescita del PIL reale nel 2020: Algeria (-6%), Libia (-59,7%), Mauritania (-2,2%), Marocco (-7%) e Tunisia (-8,8%). Il basso turismo e il calo delle rimesse sono fattori che hanno prevalentemente inciso sulla maggior parte delle economie, congiuntamente al crollo storico della domanda dei mercati petroliferi che ha danneggiato i paesi esportatori di petrolio. Nel caso della Libia, la cui economia è stata colpita dai conflitti politici a partire dal 2011, l'impatto della pandemia ha esacerbato i già persistenti problemi economici e sociali: il settore degli idrocarburi è il principale contribuente al PIL e il calo del prezzo del petrolio ha portato a un crollo senza precedenti dei proventi delle esportazioni.

Le prospettive di crescita del PIL della regione del Maghreb a medio termine, valutate in aumento del 14,7% e del 3,3% rispettivamente nel 2021 e nel 2022, sono positive ma la capacità di raggiungere i precedenti livelli di crescita e occupazione dipenderà dalla ripresa dell'economia mondiale, in particolare dalle economie dell'UE, e dall'evoluzione del turismo e della domanda di idrocarburi. Il persistente alto tasso di disoccupazione giovanile sembra essere una delle minacce alla pace sociale mentre la crisi sanitaria ha aumentato la necessità di finanziamenti per contrastare il deficit di bilancio (ad es. il FMI ha fornito alla Tunisia 753 milioni di dollari nell'aprile 2020).

Positive anche le prospettive economiche per Paese secondo il FMI (2021): Algeria (2,9%), Libia (3,1%), Mauritania (3,1%), Marocco (4,5%) e Tunisia (3,8%). Sebbene, pur a fronte di queste cifre, è valutato che i paesi del Maghreb avranno bisogno di nuovi modelli economici per risolvere i problemi finanziari tradizionali e per adattarsi alla fase globale post-Covid-19. Questa è la vera sfida a lungo termine per la regione del Maghreb.

Impatto del Covid-19 sulla sponda nord dello spazio 5+5

La pandemia di Covid-19 ha generato un impatto multidimensionale in tutti e cinque i paesi sulla sponda settentrionale dell'area 5+5; data la portata e l'impatto globale senza precedenti, ha posto sfide considerevoli alle autorità nazionali e ha accentuato le già presenti fragilità strutturali, imponendo risposte politiche coordinate a livello multinazionali (Greer, S.L.et al, 2020). I suoi effetti, tuttavia, non sono stati limitati ai "punti caldi" in termini di intensità o gravità inizialmente identificati. Infatti, mentre l'Italia è stata inizialmente indicata come uno dei principali epicentri dell'intera comunità internazionale, affiancata dalla Spagna che ha assunto anch'essa un ruolo di primo piano a causa dell'alta incidenza di contagio, le statistiche aggregate hanno definito dimensioni e popolazioni affette dal virus proporzionalmente diverse in Francia, Italia, Malta, Portogallo e Spagna.

I decessi e i casi di infezione registrati forniscono la rappresentazione più immediata e lampante del costo umano inerente a questa pandemia. Alla fine di aprile 2021, la Francia aveva raggiunto un totale di 5,37 milioni di casi di infezione e 102.000 decessi; l'Italia un totale di 3,9 milioni di casi di infezione e 117.997 morti; la Spagna 3,44 milioni di casi di infezione e 77.000 morti; il Portogallo 832.000 casi di infezione e 16.952 decessi; Malta 30.063 casi di infezione e 411 decessi. Questi numeri rimangono inevitabilmente provvisori quanto rappresentativi, mentre la crisi dilaga in tutto il mondo continuando a sottoporre a una condizione di elevato stress tutti i servizi sanitari pubblici nazionali e le capacità di far fronte a ondate consecutive di picchi nei tassi di infezione. Indipendentemente da ciò, la sponda settentrionale dello spazio 5+5 ha già totalizzato oltre 13,6 milioni di casi di infezione e oltre 314.000 decessi al mese di ottobre 2021.

La pandemia ha avuto un ruolo determinante anche a livello politico, come dimostrano i ritardi e i rinvii di diversi appuntamenti elettorali in tre dei cinque paesi europei, a causa del rischio di un ulteriore contagio. In Francia, ad esempio, il secondo turno delle elezioni locali originariamente previsto per il 22 marzo 2020 è stato spostato al 28 giugno 2020. L'Italia, dal canto suo, ha assistito al rinvio di un referendum nazionale oltre a numerose elezioni regionali e locali. Anche le elezioni regionali in Spagna, in particolare in Euskadi/Basco e in Galizia, originariamente previste per il 5 aprile 2020, sono state rinviate al 12 luglio 2020.

Tuttavia, l'impatto politico può essere valutato anche in termini di crescenti livelli di euroscetticismo, data l'interconnessione tra le risposte dei cinque paesi e l'approccio collettivo promosso dall'Unione Europea (UE) per affrontare la pandemia. L'Italia, in particolare, si è distinta all'inizio della pandemia con sondaggi che accreditavano il 55% della popolazione come scettica rispetto all'adeguatezza del sostegno dell'UE all'Italia (Fontana, O, 2020). I successivi problemi con l'introduzione della vaccinazione dall'inizio del 2021 hanno ugualmente contribuito a una diffusa percezione di "inadeguatezza" a causa dei problemi logistici e di distribuzione dei vaccini, portando così a una diminuzione complessiva dell'approvazione delle prestazioni dell'UE in tutti e cinque i paesi (Eurobarometro 2021). La perdita generalizzata di fiducia del pubblico nelle istituzioni è emersa quindi come una conseguenza chiave in questo particolare spazio.

Anche l'impatto economico complessivo è stato estremamente grave, con profonde crisi ancora non completamente chiare. Il PIL della Spagna è diminuito del 10,8% nel 2020, la recessione più profonda degli ultimi 80 anni e la più rilevante in Europa, mentre la disoccupazione è salita al 16,2% (Chislett 2021). Nel frattempo, il PIL del Portogallo si è contratto del 7,6% a causa di un calo significativo della domanda interna e dei consumi privati, ma anche a causa delle intense riduzioni delle esportazioni e delle importazioni di beni e servizi, con particolare riferimento al settore turistico (INE 2021). Allo stesso modo, la Francia ha assistito a una contrazione di quasi il 9%, con il governo che ha lanciato piani fiscali globali per il periodo 2020-22, per un totale di circa il 26% del PIL in misure di emergenza e di ripresa (FMI 2021). Anche l'economia maltese ha probabilmente registrato una contrazione senza precedenti del 6,6% nel 2020 (CBM 2020). Inoltre, le prospettive condivise per la ripresa sono state costantemente riviste alla luce degli effetti persistenti della pandemia in tutto il mondo.

Infine, tutti e cinque i paesi stanno attualmente sperimentando una certa misura di tensioni sociali, che mettono sotto stress i servizi pubblici e aumentano gli sforzi politici, dando allo stesso tempo spazio a visioni più estreme che si diffondono e consolidano sempre più ai margini della società (in particolare i movimenti antivaccinisti No-Vax e quelli complottisti che fanno riferimento al fenomeno statunitense di QANon), accentuando ulteriormente la complessiva percezione di crisi all'interno dei paesi della sponda nord dello spazio 5+5.

L'impatto dell'epidemia da Covid-19 nello spazio vicino: gli effetti nel Sahel

La regione del Sahel è stata meno colpita dalla pandemia rispetto ad altre regioni del mondo. Secondo i dati incompleti forniti da alcune organizzazioni internazionali, i casi e i decessi da Covid-19 in tutto il Sahel sono relativamente bassi. Alla fine di novembre 2020 erano riportati 17.891 casi e 551 decessi registrati dall'African Centers for Disease Control and Prevention (CDC). Gli ultimi dati riportati dalla stessa organizzazione al 1 giugno 2021 per il G5 Sahel sono i seguenti (*Tabella 2*):

State	*Confirmed Cases*	*Number of deaths*
Burkina Faso	13,431	166
Chad	4,929	173
Mali	14,265	----
Mauritania	19,494	463
Niger	5,410	517

***Table 2**: Confirmed COVID-19 cases & deaths in the Sahel*

(**source: Africa CDC & African Union June 2021**)

La *Tabella 2*, sopra, illustra come l'epidemia nella terza fase sia caratterizzata da un aumento del numero di casi (57.519) e di decessi (1.511). L'Organizzazione Mondiale della Sanità (OMS) ha sottolineato che la mortalità nei pazienti critici con Covid-19 è più alta nei paesi africani; in particolare all'interno della regione del Sahel i dati sulla mortalità sono superiori alla media globale.

L'evoluzione della pandemia e il suo impatto socio-economico è motivo di grande preoccupazione; la fragilità della maggior parte degli stati del Sahel e le deteriorate condizioni di vita sono messe alla prova dalla pandemia. La pandemia si è così imposta quale fattore extra-esogeno in gtrado di esacerbare le criticità tradizionalmente presenti della regione: mancanza di buon governo, povertà, difficoltà di accesso ai servizi pubblici (assistenza sanitaria, istruzione) e insicurezza.

	Burkina Faso	**Chad**	**Mali**	**Mauritania**	**Niger**
Original 2020 forecast	5.8%	3.2%	6.3%	5%	6%
COVID-19 2020 adjusted	-0.8%	-0.9%	-2.2%	-2%	1.2%
2021 projections	4.3%	1.8%	3.1%	4%	2.9%

***Table 3**: Adjusted economic growth forecast for G5 Sahel*

(**source: IMF World Economic Outlook (April 2020 & April 2021**)

La crescita economica nell'area "G5 Sahel" è stata gravemente colpita nel 2020, come mostra la *Tabella 3*, sopra. La sicurezza alimentare è minacciata dall'impatto della pandemia nel settore agricolo, che ha imposto una riduzione nell'accesso al settore agricolo da parte della manodopera. Inoltre, il numero crescente di sfollati e le loro condizioni di vita sono causa di crescenti conflitti intercomunitari. Secondo Save the Children, nel 2021 13 milioni di bambini non hanno accesso al Sistema scolastico a causa della crescente insicurezza. Inoltre, come evidenziato dal segretario generale delle Nazioni Unite, António Guterres, i gruppi terroristici stanno approfittando della pandemia di Covid-19 per intensificare i loro attacchi e sfidare le autorità statali nel Sahel.

Ripercussioni sulla sicurezza nell'area "5+5"

La sponda sud del Mediterraneo occidentale sta affrontando sfide di *governance*, socio-economiche, climatiche, ambientali e di sicurezza; molte di queste sfide derivano da tendenze globali e richiedono un'azione comune da parte dei paesi "5+5. I conflitti presenti nell'area del Mediterraneo continuano a infliggere terribili sofferenze umane, innescare significativi spostamenti forzati, pesare pesantemente sulle prospettive economiche e sociali di intere società, in particolare dei paesi che ospitano grandi popolazioni di migrant: elementi che sono al contempo causa e conseguenza della competizione geopolitica e dell'interferenza esterna[51].

La pandemia di Covid-19 sta avendo un impatto enorme su queste società[52]. Le principali minacce[53] alla sicurezza come il terrorismo, le minacce ibride, la criminalità informatica e la criminalità organizzata, compreso il commercio illegale di armi da fuoco, il traffico di droga, la tratta di esseri umani e il riciclaggio di denaro sono sempre più sfide fondamentali.[54]

Radicalismo ed estremismo violento

Analisi e studi di prove sui potenziali impatti della pandemia a supporto del reclutamento di estremisti violenti e nell'alimentare le forme di radicalizzazione. Ci sono evidenza a conferma dell'impatto di eventi straordinari sulla radicalizzazione e sull'estremismo violento. Nel complesso è valutato che l'impatto del Covid-19 sulla radicalizzazione avrà effetti differenziati a breve, medio e lungo termine.

Gli impatti a breve termine

Gli impatti a breve termine sulla radicalizzazione e sull'estremismo violento sono molteplici e complessi e derivano dall'impatto immediato della risposta alla pandemia, inclusi il distanziamento sociale e le restrizioni che vengono presi a pretesto da ideologi radicali per convalidare le loro visioni del mondo. Oltre a ciò, la limitata capacità o l'incapacità dei governi di raggiungere e supportare aree periferiche o gruppi minoritari contribuisce indirettamente a creare un *humus* favorevole al proliferare di forme di radicalismo e proselitismo. In breve[55]:

- I vuoti di *governance* possono emergere ed essere colmati da gruppi estremisti poiché le risorse nazionali sono limitate e la capacità di governare è messa in discussione;
- La pandemia può essere utilizzata per convalidare particolari visioni del mondo, ad esempio la decadenza dell'Occidente, la corruzione del governo;

51 European Commission (2021). *Joint communication to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions*, 9 February 2021. In https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021JC0002&rid=2.

52 PAM (2021). *Covid-19 Pandemic and Food Security in the PAM region*. In https://www.pam.int/welcome.asp?m=news&id=904.

53 European Commission (2021). *Cit.*

54 *Ibidem.*

55 Avis W. (2020). *The COVID-19 pandemic and response on violent extremist recruitment and radicalisation*, H4D, Helpdesk Report, University of Birmingham. In https://reliefweb.int/sites/reliefweb.int/files/resources/808_COVID19%20_and_Violent_Extremism.pdf.

- La pandemia può fornire un contesto in cui sono pianificati attacchi dettati dall'opportunità del momento;
- Le restrizioni sociali possono fornire un bacino ideale per la proliferazione del radicalism, pur tenendo conto del fatto che la radicalizzazione è un fenomeno a più stadi che in genere affligge individui e/o gruppi che si presentano come già essere ricettivi ai messaggi estremisti.

Gli impatti a medio termine

È probabile che gli impatti a medio termine del Covid-19 saranno influenzati dall'impatto a più ampio spettro della pandemia, ovvero dal modo in cui vengono percepite le risposte del governo, dalla ricaduta di tali risposte e dagli impatti socio-economici più ampi. In breve:

- La pandemia può comportare un calo della collaborazione internazionale poiché le nazioni privilegiano il supporto di alcune aree a discapito di altre;
- I paesi affrontano crescenti sfide nella fornitura di servizi: una condizione che tende a creare vuoti in cui possono muoversi i gruppi estremisti;
- Si possono creare tensioni tra i gruppi poiché la risposta del governo è percepita come diseguale;
- Se gli impatti socio-economici sono significative, la crisi può portare ad un'accentuazione delle disuguaglianze.

Impatti a lungo termine

Gli impatti a lungo termine sono più difficili da discernere e si verificheranno nel corso di mesi e anni. È chiaro che il modo in cui i governi risponderanno alla crisi iniziale si ripercuoterà nel medio e lungo periodo. In particolare, le risposte della politica, quando non ben ponderate, hanno il potenziale per consolidare le disuguaglianze o alienare particolari aree e gruppi. Se la pandemia imporrà una crisi economica prolungata a livello nazionale o internazionale, la cooperazione transfrontaliera ne risentirà consentendo la proliferazione di ideologie radicali.

Terrorismo

Il terrorismo e il suo finanziamento, la radicalizzazione, l'estremismo violento e il fenomeno dei combattenti terroristi stranieri (*Foreign Terrorist Fighters*) sono fenome ni che affliggono e colpiscono entrambe le sponde del Mediterraneo, spesso in un rapport di interconnessione.

La pandemia non poteva passare inosservata all'apparato mediatico di gruppi jihadisti come il cosiddetto gruppo terroristico *Stato Islamico* (IS) o *al-Qa'ida* (AQ).

Le attività di propaganda svolte durante la pandemia e gli attentati avvenuti in Europa e in Nord Africa, ricordano come il terrorismo dinamico sia associato al cosiddetto Stato Islamico e al-Qaeda soprattutto attraverso il *Web*. In particolare, l'IS ha confermato la sua narrativa aggressiva, identificando il Coronavirus come un "soldato di Allah". Un alleato, deciso a punire gli "infedeli", in primis le forze armate e di polizia, attualmente preoccupate nell'affrontare la pandemia e le misure di sicurezza imposte dai governi. Lo percepiscono come un'opportunità per impegnarsi in attacchi e "diffondere (...) caos e confusione".[56]

Migrazione irregolare, traffico e tratta di esseri umani ai tempi del Covid-19[57]

Il fenomeno migratorio ha dimensioni globali e come tale richiede risposte e azioni congiunte, solidarietà e condivisione delle responsabilità. La migrazione irregolare comporta importanti sfide,

[56] Van Ostaeyen P. (2020). The Islamic State and Coronavirus, Time for a Comeback? ISPI, Milan. In https://www.ispionline.it/it/pubblicazione/islamic-state-and-coronavirus-time-comeback-26166.

[57] INTERPOL (2020). *COVID-19 impact on migrant smuggling and human trafficking*, 11 June 2020. In https://www.interpol.int/News-and-Events/News/2020/COVID-19-impact-on-migrant-smuggling-and-human-trafficking.

in particolare il contrasto alle reti criminali che, grazie al traffic di esseri umani, aumentano sempre più il loro potere economico e, di conseguenza, le capacità di operare in maniera sempre più efficace.

Le dinamiche economiche – aumento del potere di acquisto delle fasce più deboli e impoverimento dei ceti medio-bassi – avranno un impatto significativo sul desiderio e sulla capacità delle persone di migrare, nonché sull'incentivo e sulle opportunità per le reti criminali di trarre profitto da un'immigrazione illegal sempre più in aumento.

Il traffico di migranti e la tratta di esseri umani sono particolarmente influenzati da fattori geo-politici e socio-economici, che variano notevolmente da regione a regione e nel modo in cui spingono a migrare le comunità più vulnerabili. La pandemia da Covid-19 sta influenzando e continuerà a influenzare questi fattori a livello globale. Inoltre, le misure adottate dai paesi per controllarne la diffusione stanno avendo un impatto sulla criminalità in tutto il mondo, compreso il traffico di migranti e la tratta di esseri umani.

L'Europa, l'area più afflitta dai fenomeni della migrazione irregolare e del traffico di migranti, è stata tra quelle più colpite dall'epidemia; nonostante ciò, i migranti non sono stati scoraggiati dal raggiungere, o tentare di raggiungerla, nonostante i rischi di contagio. E sebbene la maggior parte dei paesi africani abbia implementato restrizioni di viaggio per prevenire la diffusione di Covid-19, queste non sono state sufficienti per dissuadere i trafficanti o i migranti.

Migranti che continuano ad arrivare negli *hub* del contrabbando presenti nell'area del Sahel e che continueranno a muoversi verso l'Europa nonostante la pandemia. Poiché l'accesso alle mete desiderate è sempre più difficile, le reti di contrabbando cercheranno probabilmente nuovi mezzi di ingresso e applicheranno prezzi maggiorati per ognuno dei servizi offerti, aumentando così il *business* del traffico di esseri umani il quale, come in una sorta di circolo vizioso, sosterrà l'investimento in termini di ricerca di nuove rotte marittime alternative e potenzialmente più pericolose: l'aumento della domanda si accompagnerà sempre più, dunque, all'aumento dei prezzi.

I migranti in partenza principalmente dal Sahara occidentale, nel 2020, hanno continuato ad arrivare nelle Isole Canarie spagnole lungo la pericolosa rotta atlantica su navi non idonee alla navigazione mentre i migranti in partenza principalmente dall'area sub-sahariana, nel 2021, hanno portato a un aumento negli sbarchi in Italia lungo la rotta del Mediterraneo centrale, partendo principalmente da Tunisia e Libia. In tale contesto, l'aumento dell'attività delle milizie e dei gruppi armati in Libia, potrà portare a un aumento delle attività di contrabbando e di collaborazione con le organizzazioni criminali.

Analisi, valutazioni, previsioni

In termini di sicurezza e stabilità, la pandemia da Covid-19 ha reso più critica una già preesistente situazione problematica. In tale scenario, i paesi dell'area "5+5" sono chiamati a sviluppare ancora di più il partenariato in materia di sicurezza, tra di loro e con i paesi vicini, nonché a rafforzare la cooperazione sul piano operativo, *in primis* per la sicurezza marittima e la cooperazione con la guardia costiera. Partenariati che dovrebbero essere personalizzati, rispondere alle esigenze dei singoli partner e beneficiare di un concreto sostegno politico di alto livello per garantire risultati concreti. Fondamentale è anche la cooperazione con le organizzazioni regionali e internazionali.

Per quanto riguarda le migrazioni irregolari, è necessario che i "Paesi 5+5" intensifichino significativamente gli sforzi comuni per combattere la tratta di esseri umani e combattere le reti criminali che si arricchiscono attraverso lo sfruttamento dei flussi migratori. Il rafforzamento della *governance* in materia di migrazione e asilo, compresa la capacità di gestione delle frontiere, è un elemento chiave.

Si valuta inoltre come prioritaria una forma di cooperazione a livello regionale e multilaterale, anche attraverso la cooperazione triangolare e sud-sud, poiché alcuni partner del Mediterraneo meridionale sono paesi di origine, transito e destinazione dei flussi migratori.

A proposito di terrorismo e radicalismo, i recenti attacchi hanno sottolineato la necessità di approfondire i dialoghi strategici nel settore del contro/anti-antiterrorismo. Basandosi sulle forme di cooperazione già esistenti, in particolare sul piano legislativo, è necessario intensificare gli sforzi al fine della prevenzione del radicalismo e del contrasto al terrorismo, in particolare le forme di reclutamento online e la diffusione via Web di contenuti terroristici.

Le conseguenze di disastri naturali, epidemie e pandemie sulla sicurezza dei Paesi "5+5" (area del Mediterraneo occidentale): strategie di cooperazione e mutuo sostegno. I risultati del gruppo di ricerca internazionale presentati ai dieci ministri della Difesa

Come riportato nel recente documento di ricerca curato dal CEMRES nell'ambito della "5+5 Defense Initiative" e presentato ai ministri della Difesa della "5+5 Defense initiative" il 15 dicembre 2021, le conseguenze di disastri naturali, epidemie e pandemie sulla sicurezza del Mediterraneo occidentale è opportuno che vengano gestite dagli Stati aderenti all'iniziativa in cooperazione tra di loro.

La "5+5 Defense Initiative" è un *forum* di collaborazione nel settore della difesa e della sicurezza nato a fine 2004, che vede coinvolte dieci Nazioni del Mediterraneo occidentale: Algeria, Francia, Italia, Libia, Malta, Mauritania, Marocco, Portogallo, Spagna e Tunisia. L'obiettivo della " 5+5 *Defense Initiative*" è di migliorare, tramite la realizzazione di attività pratiche e attraverso lo scambio di idee e di esperienze, la reciproca comprensione e la fiducia nell'affrontare i problemi della sicurezza nell'area di interesse. L'Autore del presente contributo è il Ricercatore Senior e rappresentante unico per l'Italia presso il gruppo di ricerca internazionale della "5+5 Defense Initiative", che comprende un ricercatore per ogni paese. La missione del gruppo è fornire ai ministri della Difesa della "5+5" uno strumento di pensiero, analisi e previsione, che permetta loro di approfondire qualsiasi argomento relativo al Mediterraneo occidentale, con l'obiettivo di rafforzare l'azione comune dei partner e facilitare lo sviluppo di una nuova concezione della sicurezza regionale. Il CEMRES é per gli esperti e ricercatori provenienti da Europa e Maghreb uno spazio per lo scambio di esperienze e lavori sulle soluzioni ai problemi di sicurezza comune per aumentare il clima di fiducia producendo una attività di ricerca oggettiva che evidenzia le vere cause di insicurezza, i problemi e le sfide strategiche del Mediterraneo occidentale.

In linea con il tema di ricerca 2021 – *The repercussions of natural disasters, epidemics and pandemics on the security of 5+5 Countries (means of cooperation and mutual support)* – disastri naturali, epidemie e pandemie sono indicate quali sfide chiave a cui i governi (e le società) sono chiamati a rispondere con soluzioni che promuovano risultati efficaci e sostenibili, in grado di costruire una capacità di resilienza, nel rispetto dei diritti umani e della promozione del benessere economico, sociale e culturale in tempi e a costi complessivi ragionevoli.

I disastri assumono varie forme che vanno dai disastri naturali, come tempeste, incendi boschivi, a quelli causati dall'uomo. Indipendentemente dal tipo di disastro che colpisce individui, organizzazioni o paesi, i risultati comportano in genere perdite di vite umane, risorse, produttività e minacce alla sicurezza.

Inoltre, mentre la diffusione del virus Covid-19 sta avendo un impatto su scala globale, la risposta collettiva alla pandemia diventa la chiave per valutare le misure attuali e formulare previsioni future. L'intervento per affrontare i disastri si è evoluto nel tempo in un sottosistema politico complesso; la politica stessa, in caso di disastri, ha l'onere di implementare soluzioni e approcci funzionali noti come "gestione e risposta alle emergenze". I moderni approcci alla gestione e alla risposta alle emergenze implicano sforzi multidimensionali per ridurre la nostra vulnerabilità ai rischi, per diminuire l'impatto dei disastri e, ancora, per prepararsi, rispondere e riprendersi da quelli che si verificano.

Il mandato del gruppo di ricerca fornito dalle nazioni della "5+5" al gruppo di ricerca era quello di consegnare uno studio accademico che mettesse in evidenza le ripercussioni dei disastri naturali,

delle epidemie e delle pandemie sulla sicurezza dell'area mediterranea occidentale al fine di identificare, o quantomeno suggerire i mezzi di cooperazione e sostegno reciproco.

Coerentemente con il compito assegnato, i ricercatori hanno individuato e sviluppato due assi di ricerca principali attraverso l'analisi delle ripercussioni sulla sicurezza e la capacità di risposta collettiva in merito alle questioni (leggasi sfide e minacce) rilevanti.

Il rapporto offre le conclusioni di ciascun asse di ricerca e un capitolo dedicato a un'illustrazione sintetica delle raccomandazioni in termini di cooperazione, all'interno dello spazio "5+5", da cui si sottolinea l'opportunità di procedere a:

- Creazione di un centro di allerta preventiva all'interno della "5+5" per promuovere lo scambio di esperienze e competenze;
- Incoraggiare a sostenere la cooperazione, il coordinamento e lo scambio di informazioni tra i paesi della "5+5";
- Sviluppare materiale didattico e di sensibilizzazione che possa essere tradotto e utilizzato in iniziative nazionali;
- Promuovere iniziative di formazione ed esercitazioni;
- Promuovere progetti di ricerca scientifica;
- Promuovere lo sviluppo e la capacità di acquisizione e condivisione delle lezioni apprese;
- Sostenere lo sviluppo di piani di risposta alle emergenze (disastri/epidemie).

Dallo studio di ricerca 2021 potranno inoltre essere tratte altre raccomandazioni a livello nazionale, mentre ulteriori iniziative di ricerca potranno essere sviluppate coerentemente alla vasta bibliografia utilizzata e ad argomenti che non sono stati affrontati in modo approfondito ma indicati quali temi di interesse collettivo.

BIBLIOGRAFIA

- *AA.VV. (2018) Al Qaeda and Islamic State Affiliates in Afghanistan*, Congressional Research service, In Focus 7-5700, 23 agosto 2018.
- *AA.VV. (2021) Terrorist Groups in Afghanistan*, Congressional Research service, In Focus IF10604, 17 agosto 2021
- AA.VV. *The Human Cost, The consequences of insurgent attacks in Afghanistan*, Human Rights Watch, Vo. 19, N. 6(C), aprile 2007, p. 14.
- Alberts D.S., Garstka J.J., and Stein F.P. (1999)*, Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised).
- Avis W. (2020), *The COVID-19 pandemic and response on violent extremist recruitment and radicalisation*, H4D, Helpdesk Report, University of Birmingham. In https://reliefweb.int/sites/reliefweb.int/files/resources/808_COVID19%20_and_Violent_Extremism.pdf.
- Basileo Deborah (2020), *Tra Cyberterrorism e guerra dell'informazione. Scarsa consapevolezza e limiti normativi*, in #ReaCT2020, 1° rapporto sul terrorismo e il fondamentalismo in Europa, ed. START InSight.
- Bertolotti C. (2015), *NIT: Il 'Nuovo Terrorismo Insurrezionale'. Dalla '5+5 Defense Initiative 2015' il cambio di approccio alla minaccia dello Stato islamico*, Analysis ISPI n. 292.
- Bertolotti C. (2021), *Introduction: terrorism at the time of Covid-19*, in #ReaCT2021 – 2nd Report on Radicalization and Counter Terrorism, START InSight & Formiche. In https://www.startinsight.eu/en/react2021-2report-en/.
- Bertolotti C. (2022) *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).
- Bertolotti C., Sulmoni C. (2021), *How the Twenty-Year Afghanistan War Paved the Way for New Insurrectional Terrorism*, in Carenzi S., Bertolotti C. (2021) "Charting Jihadism Twenty Years After 9/11", Dossier ISPI, 11 settembre 2021.
- Bertolotti Claudio (2018), *Artificial Intelligence and the evolution of warfare. Report on 8th Beijing Xiangshan Forum*, START InSight, November 6th, in https://bit.ly/2zQeuLO.
- Bertolotti Claudio (2018), *The military applications of Artificial Intelligence. A focus on the 8th Beijing Xiangshan Forum (24-26 October 2018)*, START InSight, November 4th, in https://bit.ly/2EnPdfH.
- Bertolotti Claudio (2021), *Immigrazione e terrorismo: legami e sfide*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Bertolotti Claudio (2021), *Numeri e profili dei terroristi jihadisti in Europa*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Boulanin Vincent (2018), Stockholm International Peace Research Institute (SIPRI), in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on *Swarming and Machine Teaming*, Thun, Switzerland, November 21st.
- Bressan Matteo (2021), *L'esperienza del Kosovo nel rimpatrio dei foreign fighters: lessons learned*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Casini Enrico (2021), *L'attacco di Vienna e la pista balcanica*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- cellphones of journalists, activists worldwide, The Washington Post, July 18.
- Cochi Marco (2021), *Il jihadismo femminile in Africa. Il ruolo delle donne all'interno di Boko Haram e al-Shabaab*, START InSight, Lugano – Svizzera.

- Crosston M., *The Millenials' war: dilemmas of network dependency in today's military*, "Defense & Security Analysis", 33:2, 2017, pp. 94-105.
- Danzig Richard (2014) 'Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies', Center for a New American Security.
- European Commission (2021). *Joint communication to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions*, 9 February 2021. In https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021JC0002&rid=2.
- Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.
- Giustozzi A. (2009), Decoding the New Taleban, C. Hurst & Co. Publishers Ltd, London.
- Hagström Martin (2018), FOI - Swedish Defence Research Agency, in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21*st*.
- INTERPOL (2020). *COVID-19 impact on migrant smuggling and human trafficking*, 11 June 2020. In https://www.interpol.int/News-and-Events/News/2020/COVID-19-impact-on-migrant-smuggling-and-human-trafficking.
- Mazoomdaar Jay (2021), Explained: Here's how NSO Group's spyware Pegasus infects your device, The Indian express July 22, New Delhi.
- PAM (2021), *Covid-19 Pandemic and Food Security in the PAM region*. In https://www.pam.int/welcome.asp?m=news&id=904.
- Priest Dana, Timberg Craig, Mekhennet Souad (2021), Private Israeli spyware used to hack
- Rickli Jean-Marc (2018), Geneva Center for Security Policy (GCSP), in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21*st*.
- Robinson T. (2010), *It's the Network, Stupid! Air Power and Network Centric Warfare – Trends and Challenges*, "Military Technology", 40–8.
- Ruttig T. (2012) *How tribal are the Taleban*, in Bashir S. and Crews R.D., "Under the Drones. Modern Lives in the Afghanistan-Pakistan Borderlands", Harvard 2012.
- Schneider Jacquelyn (2019) The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war, Journal of Strategic Studies, 42:6, 841-863, DOI: 10.1080/01402390.2019.1627209. In: https://doi.org/10.1080/01402390.2019.1627209.
- Sulmoni Chiara (2021), *Estremismo di matrice jihadista in Europa. Il concetto e l'importanza della prevenzione e del contrasto*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Tor Uri (2017) 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, Journal of Strategic Studies, 40:1-2, 92-117, DOI: 10.1080/01402390.2015.1115975. In: https://doi.org/10.1080/01402390.2015.111597
- Van Ostaeyen P. (2020), The Islamic State and Coronavirus, Time for a Comeback? ISPI, Milan. In https://www.ispionline.it/it/pubblicazione/islamic-state-and-coronavirus-time-comeback-26166
- Woodhams George (2018), UNIDIR Security and Society Programme, in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21*st*.
- Xinhua, *Number of Afghan Insurgent Grow Rapidly Since 2006*, in Daily outlook Afghanistan, 11 ottobre 2009.

Year 2021
Strategic Analysis

Challenges and unconventional threats

Year 2021, Strategic Analysis
Challenges and unconventional threats

DISCLAIMER

The opinions expressed in this volume are of the Authors; they do not reflect the official opinion of the Italian Ministry of Defence or of the Organizations to which the Authors belong.

NOTES

The articles are written using open source information.

The "Osservatorio Strategico" is available also in electronic format (file.pdf and ebook) at the following link: http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OsservatorioStrategico/Pagine/default.aspx

Osservatorio Strategico 2021

This book has been edited by
Defense Analysis and Research Institute

Director
Col. Gualtiero Iacono

Deputy Director
Col. (A.F.) Loris Tabacchi

Editor-in-Chief
Magg. A.A.r.a.s. Luigi Bruschi

Editorial staff
CWO Massimo Lanfranco – WO Gianluca Bisanti – 1° Aviere Capo Alessandro Del Pinto

Graphic and layout
Mr. Massimo Bilotta – CWO Massimo Lanfranco – WO Gianluca Bisanti – Serg. Nello Manuel Santaniello

Author
Claudio Bertolotti

Printed by
Typography of the Center for High Defence Studies

Military Center for Strategic Studies
Strategic Monitoring Department
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – ROME- ITALY
tel.00 39 06 4691 3204 fax 00 39 06 6879779
e-mail: dipms.cemiss@casd.difesa.it

Closed in May 2022 – Published in August 2022

ISBN 979-12-5515-015-2

Index

Introduction

Twenty years after 9/11: who are the “new” Taliban and other groups in Afghanistan? Twenty years ago today, the US was struck by the 11/9 attacks. Those attacks had a profound effect on many different levels and marked the beginning of the War on Terror – ushering in a US-led military intervention in Afghanistan in 2001 and Iraq in 2003. Two decades later, the withdrawal of US troops from Afghanistan has come to an end, as US President Joe Biden has announced the end of America's "longest war" while the Taliban have taken control of Afghanistan once again. Twenty years after 9/11, who are the Taliban leading the country?

After the fall of Kabul: what’s next? The threat evolves into "New Insurrectional Terrorism" (NIT). What we are facing today has already been dubbed “New Insurrectional Terrorism” (NIT), a concept which essentially includes all attempts at disrupting the national and/or international political order through violence. NIT is revolutionary and utopian, and whereas terrorism is functional, insurrectional terrorism continuously evolves.

Numbers and profiles of jihadist terrorists in Europe: analysis by the Observatory on Radicalisation and Counter-Terrorism (ReaCT). 436 terrorist attacks, including failed and foiled ones, were recorded on European soil from 2017 to 2019 (895 in the 2014-2017 period): 63 percent were attributed to separatist and ethno-nationalist groups: 16 percent to radical leftist and anarchist groups (on the increase); 2.8 percent to far-right groups (decreasing); while 18 percent were jihadist. Although jihadist attacks are a marginal number, they were responsible for all deaths from terrorism in 2019 and 16 killed in 2020 (see START InSight’s database on www.startinsight.eu.

Increase of threats in cyberspace. Cyber threats may be generated by at least three distinct classes of actors: ‘the lone hacker,’ the ‘Hacktivists’ and the nation states. The most recent cyber-attacks, such as “WannaCry” and “Pegasus” cases, are just examples from which clearly emerge how the problem of the security of one's data and, by extension, of mobile devices and computer networks is underestimated. An evolving scenario in which the capacity/vulnerability paradox is placed.

The U.S. dependence on the network: vulnerabilities, critical issues and weaknesses of the Network Centric Warfare (NCW). Network Centric Warfare translates information superiority into combat power by effectively linking disparate capabilities in the "battle space". But the U.S. military capability is actually dependent on a network technology to the point that the very doctrine upon which the employment of the military instrument is based mandates the integration of network technology in almost every domain, most notably Network Centric Warfare.

The military applications of Artificial Intelligence and the evolution of warfare: Swarming and Machine Teaming There is an increasingly tight interconnection between intelligence and Artificial Intelligence (AI). Countering contemporary asymmetric threats will progressively require a sound use of AI, which can help, for instance, determine the size and position of troops and armaments belonging either to allies or enemies; evaluate the feasibility of military actions; alter the conduct of operations depending on the evolving battlefield context. The assessment is that AI potentially imposes a radical change onto Revolution in Military Affairs (RMA): The degree of development and deployment of AI is contingent upon an individual actor's ethical issues and constraints. But it's those who overlook ethics and push the boundaries of AI, who will take the lead on the battlefield.

The repercussions of natural disasters, epidemics and pandemics on the security of "5+5" Countries (West Mediterranean area): means of cooperation and mutual support. The results of the international research group: as reported in the recent research document edited by the CEMRES within the "5+5 Defense Initiative" and presented to the "5+5" Defense Ministry on the 15th of December 2021, Pandemics are a major problem worldwide and a serious threat to sustainable development. Their impacts are diverse: loss of life and disease can also cause social and economic disruption, loss of capability to provide services. In an increasingly integrated world economy built on networks of global supply chains, pandemics in one country can easily affect others.

1. The New Insurrectional Terrorism

Twenty years after 9/11: who are the "new" Taliban and other groups in Afghanistan?

A conflict shaped by two fronts

The twenty-year war in Afghanistan (2001 to 2021) has come to an end. This latest conflict was shaped by two fronts: a more explicit one, pitting a long-lasting Taliban insurgency against foreign armies and a national government that the fundamentalist movement deemed illegitimate; and another, less manifest one, embodied in the struggle to counter jihadist terrorism which has taken root in the country, and which is pursued by different groups and acronyms.

Today, the world must find a way to deal with a victorious Taliban who not only gained the upper hand on the battlefield, yet also learned how to efficiently exploit the digital ecosystem with a view to influencing public opinion within and outside Afghanistan. However, the group now faces the hurdle of running a country and the outcome of this latest endeavor is still uncertain. One of the main difficulties resides in the movement's heterogeneous make-up. With Kabul under the nominal control of the Taliban, internal divisions are becoming more evident, with factions competing over a power-sharing deal which is expected to accommodate personal and group ambitions. A further question mark hovers over the Taliban's ability to acknowledge a profoundly changed Afghan civil society and the extent to which the Taliban political arm will be able to rein in a younger generation of fighters who have been exposed to global jihadist ideologies, brands, objectives and tactics.[1] Their ranks could swell with a Taliban diaspora, depending on Taliban choices in matters of politics and security[2] – i.e., as pertains to preservation of women's rights and roles, ethnic and religious inclusiveness, overt or covert alliances with former enemies in the war against the so-called Islamic State.

However, the Taliban – who have not shied away from crushing dissent within their own ranks[3] – essentially retain the characteristics of a coherent and internally collaborative movement. A characteristic which stands in stark contrast to a galaxy of other jihadist groups enlisting an increasing number of veteran foreign fighters from Syria and Iraq.

In practical terms, the insurrectional front is estimated to include about forty different militant groups, some organized into political factions, others based on tribal or ethnic affiliations. Hence, the difficulty in being able to evaluate how many mujahideen actually operate on the battlefield. In 2007, military intelligence sources provided a figure ranging from 5,000 to 7,000 elements – swelling to 15,000 as per Pakistani sources, who included Pashtun tribal militias in their calculations. In February 2009, the Afghan Ministry of Interior estimated that overall, anti-government and jihadi groups' fighters could number 10-15,000.[4]

According to U.S. intelligence, prior to the final offensive which led to the fall of Kabul, the figure stood at around 60,000 active militants out of about 200,000 total elements. A number thought to have increased by a few tens of thousands over the months preceding the Taliban conquest, through the recruitment of new mujahideen among both Pashtun and non-Pashtun communities and thanks to an efficient, de-centralized organization based on an autonomous, "compartmentalised" and tactically flexible approach.

The Taliban's DNA: supra-tribal ideology and tradition

The Taliban is a predominantly Pashtun movement yet, thanks to ties and agreements at the local level, it has managed to involve other ethnic groups as well. Based on a dense network of affiliations, rooted in a form of Islamism steeped in tribal tradition and with a generic reference to the

1 CBC, *Can a divided Taliban rule a modern Afghanistan? Time will tell, says journalist*, 20 agosto 2021
2 France24, *Afghanistan: Do Islamic State group jihadists pose a real challenge to the Taliban?* 31 agosto 2021
3 Watkins, A. *Taliban fragmentation: a figment of your imagination?,* War on the Rocks, 4 settembre 2019
4 Xinhua, *Number of Afghan Insurgent Grow Rapidly Since 2006*, in Daily outlook Afghanistan, 11 ottobre 2009.

experience of Islamic jihad against the Soviets, the Taliban movement has fought with the objective of returning to power in Afghanistan.

According to experts Thomas Ruttig[5] and Antonio Giustozzi[6], the Taliban movement rests on a dualistic nature: that is, structural and ideological. It can be described as an organization characterised by a vertical structure, which over the years morphed into a central "shadow" state, defined by a supra-tribal and supra-ethnic ideology which can accomodate "nationalistic" aspirations. But the movement is also defined by a horizontal network structure deeply rooted in the segmented Pashtun tribal society.

The movement can be viewed as a 'network of networks'[7]; religious, tribal and regional factors merge with the organizational principles of the Taliban who, politically, aim at building a state which overcomes tribal limitations in favour of "national" outreach and the re-establishment of the Islamic Emirate (the official name by which they always went by). If the Taliban share a nationalist drive, they are, however, no irredentist Pashtuns seeking re-unification of Pashtun areas: their supra-tribal ideology leaves room for inclusion of non-Pashtun communities, an approach which has helped them win "hearts and minds" of non-Pashtun peoples, such as those living in the Northern and Western provinces.

For the Taliban, unlike for other jihadist groups whose progressive growth represents a forthcoming challenge for Afghanistan- Islam is an umbrella accomodating different communities; the combination of vertical (religious/ideological) and horizontal (tribal) structures is supposed to have in this way given the Taliban a high level of cohesion and strong organizational effectiveness[8].

Al-Qaeda, Islamic State-Khorasan Province (ISKP) and other terror groups operating in Afghanistan [9]

Afghanistan risks becoming a haven for extremist groups, including Pakistani Jaish-e-Mohammad and Lashkar-e-Taiba, which carried out the devastating 2008 Mumbai terror attacks and could continue their offensive against Indian targets in Afghanistan. Other terror groups are or will likely be operating in and from the country, above all the so-called Islamic State Khorasan Province (ISKP) and al-Qaeda, which can also count on its regional franchise, al-Qaeda in the Indian Subcontinent.

Al-Qaeda (AQ)

As periodically reported by the U.S. Congressional Research Service, the top echelon or "core" AQ leadership has been a primary U.S. target in Afghanistan since 2001. This includes AQ leader Ayman al-Zawahiri and his deputies. In September 2019, the White House announced that U.S. forces had killed Hamza bin Laden, son of AQ founder Osama bin Laden and a rising leader in the group, "in the Afghanistan/Pakistan region." U.S. officials have argued that U.S. raids and airstrikes on AQ targets, including a large training camp uncovered in Kandahar province in 2015, have reduced AQ presence in Afghanistan. An April 2021 report from the Department of Defense (DoD) estimated that AQ core leaders in Afghanistan "pose a limited threat" because they "focus primarily on survival".

The U.S.-Taliban agreement commits the Taliban to prevent any group, including al-Qaeda, from using Afghan soil to threaten the security of the United States or its allies. Taliban-AQ links have been reinforced by their shared battle against international forces in Afghanistan as well as

5 Ruttig T., *How tribal are the Taleban*, AAN, Kabul 2012.
6 Giustozzi A., *Decoding the New Taleban*, C. Hurst & Co. Publishers Ltd, London 2009.
7 Ruttig T., *How tribal are the Taleban*, in Bashir S. and Crews R.D., "Under the Drones. Modern Lives in the Afghanistan-Pakistan Borderlands", Harvard 2012.
8 Ruttig T., *How tribal are the Taleban?...*, cit.
9 *Al Qaeda and Islamic State Affiliates in Afghanistan*, Congressional Research service, In Focus 7-5700, 23 agosto 2018; and *Terrorist Groups in Afghanistan*, Congressional Research service, In Focus IF10604, 17 agosto 2021

through intermarriage and other personal bonds among members of the two groups. As reported in a United Nations (UN) report in April 2021, AQ and the Taliban "remain closely aligned and show no indication of breaking ties." The Taliban reportedly issued orders in February 2021, barring their members from sheltering foreign fighters, but do not otherwise appear to have taken tangible steps in the direction of severing ties with AQ.

AQ reacted positively to the agreement with the U.S., with statements from its acolytes celebrating it as a victory for the Taliban's cause and consequently, for global militancy; AQ sympathizers celebrated the Taliban's takeover, while the Taliban reportedly freed prisoners, including AQ members. Following the fall of Kabul, the al-Qaeda leadership issued a dense, two-page statement on Afghanistan, congratulating the Islamic Emirate and framing it as an achievement for Afghans and the 'umma' (the global Muslim community); a result which, according to their propaganda, "proves" jihad is the right strategy to pursue, while "predicting" more victories ahead. What emerges from AQ affiliates' statements all over the world is the belief that the establishment of the Islamic Emirate in Afghanistan heralds wider triumphs and a new era of Islamic rule, validating jihad as the way forward and exposing the "democracy game" and peaceful means as illusory.

In addition, with the return of the Taliban in the wake of the U.S. withdrawal, it is assessed that al-Qaeda could exploit the situation to regroup, enhancing the risk that Afghanistan will once again turn into a recruitment and training ground for jihadi terror groups. A fear which is corroborated by the recent return of Amin-ul-Haq, a major al-Qaeda leader in Afghanistan and former aide of Osama bin Laden, to his native Nangarhar province.

Last but not least, relations between the Taliban -especially the Haqqani Network (HQN, see below)- and AQ remain close, based on friendship, a history of shared struggle, ideological sympathy and intermarriage.

Al Qaeda in the Indian Subcontinent (AQIS)

Al Qaeda in the Indian Subcontinent has reportedly solidified its presence in Afghanistan by embedding fighters in the Taliban. In September 2014, AQ leader al-Zawahiri announced the creation of this formal, separate AQ affiliate in South Asia.

According to the Congressional Research Service, differentiating between AQ and AQIS is a difficult task, but some key distinctions do exist. Essentially AQIS, in compliance with the 'franchise' model, establishes itself as an attempt by AQ to maintain a more durable presence in the region by enhancing links with local actors, prompted in part by the relocation of some AQ leaders to Syria. Former AQIS leader Asim Umar, who was being "sheltered" by Taliban forces when he was killed in a joint U.S.-Afghan operation in Afghanistan (September 2019), was an Indian national with deep roots in Pakistan; AQ core leaders are predominantly Arab.

According to the April 2021 U.S. DoD report, AQIS threatened U.S. forces in Afghanistan, a reflection of the group's cooperation with the Taliban, but likely lacked the means to conduct attacks outside the region.

Islamic State - Khorasan Province (IS-K, IS-KP)

The Islamic State announced the creation of its Afghan affiliate in January 2015, but steps in this direction had already been taken in late 2014. IS-KP once concentrated in Nangarhar, an Eastern Afghanistan province bordering Pakistan's Khyber Pakhtunkhwa. There, IS-KP was mostly comprised of former Tehrik-e-Taliban Pakistan (TTP, see below) militants who fled Pakistani army operations in the Khyber Pakhtunkhwa after mid-2014. Arguably one of the Islamic State's most successful affiliates, IS-K was "nearly eradicated" from its main base in Eastern Afghanistan in late 2019 by U.S. and Afghan military offensives and, separately, the Taliban. An IS-K contingent in Northern Afghanistan was similarly defeated in 2018. These territorial losses have forced the group to "de-centralize" according to UN sanctions' monitors, who assess the group has around 2,000

fighters located primarily in the East but also in Northern Afghanistan. A number of IS-K leaders were killed in U.S. strikes or captured by Afghan forces since 2016. IS-K remains a threat, and recent attacks attributed to the group, in particular, the Kabul airport attacks in late August 2021, indicate a high level of operational resilience and capabilities. In addition to attacks against civilians, U.S. and Taliban during the US withdrawal from Kabul, IS-K has claimed previous large-scale bombings, mainly targeting Afghanistan's Shia minority.

IS-KP and Taliban forces have sometimes fought over control of territory or for political and other differences; currently, the two groups oppose each other both on the ideological level and on the battlefield. Upon taking power, in August 2021 the Taliban reportedly executed an imprisoned former IS-K leader. It is assessed that Taliban hardliners – in particular, elements belonging to the HQN and young radicals – might defect to IS-KP if Taliban leaders compromise on certain issues as they transition to governance.

Haqqani Network (HQN)

The Haqqani Network is an official, semi-autonomous branch of the Afghan Taliban with solid ties to AQ. It was founded by Jalaluddin Haqqani (who died in 2018), a leading anti-Soviet Islamist commander who became a prominent Taliban official and a key leader in the post-2001 insurgency.

The group's current leader is Sirajuddin Haqqani (son of Jalaluddin) who also served as deputy leader of the Taliban since 2015. Sirajuddin's appointment to lead the network likely strengthened cooperation between the Taliban and AQ; the HQN is thought to be a "primary liaison" between the Taliban and AQ and according to reports, there might have been some recent form of cooperation between the HQN and IS-K elements in conducting complex suicide attacks in Kabul. It should be borne in mind that the HQN was the main driving force behind the deadliest attacks which took place during the war in Afghanistan.

Tehrik-e Taliban Pakistan (TTP)

Tehrik-e-Taliban Pakistan (TTP), also known as the Pakistani Taliban, has distinctive anti-Pakistan objectives. As confirmed by the Congressional Research Service, TTP is reportedly operating in and from Afghanistan, with thousands of fighters, alongside the Afghan Taliban. In 2014, some TTP members pledged allegiance to the Islamic State and subsequently relocated to Eastern Afghanistan in response to Pakistani army operations that mostly drove the group from its safe havens in the Pakistani Khyber Pakhtunkhwa province. Reunification between core TTP and some former splinter groups (possibly facilitated by AQ) since 2020, has swelled the group's ranks; some TTP members operating in Syria under the IS-K umbrella returned to Afghanistan together with Arab jihadist elements: this possibly substantiates the risk that Afghan soil might turn into a safe haven for global jihadi groups. It is assessed that the TTP may further benefit from the Taliban takeover and release of TTP prisoners held in Afghanistan.

Other minor groups

***Islamic Movement of Uzbekistan* (IMU)**

The Islamic Movement of Uzbekistan (IMU) was once a prominent ally of AQ. Formed by Uzbeks who fought with Islamist forces in the Tajikistan 1992-1997 civil war, IMU allied with the Taliban and launched attacks on other Central Asian states. After U.S. operations began in 2001, the group's focus shifted to Afghanistan and Pakistan. IMU forces operate in Northern Afghanistan under the control of the Taliban. In 2014, some IMU members pledged allegiance to the Islamic State and, similarly to former TTP members, started operating in Afghanistan and Syria under the IS-KP: some veterans returned to Afghanistan with other Arab jihadist elements.

***ìEast Turkestan Islamic Movement* (ETIM)**

The Eastern Turkestan Islamic Movement (ETIM) aims to establish an independent Islamic State for the Uyghur Muslim minority, the Turkic-speaking people in Western China. The group has ties to AQ. As recently reported, as a result of the China-Taliban talks and agreements, the latter has committed to eliminating ETIM from Afghanistan. At present, the group is still operating with hundreds of fighters in the Northeast of Afghanistan and it maintains a larger presence in Idlib, Syria, moving its fighters between the two areas. ETIM in Afghanistan is reportedly focused on China; the Syrian contingent has "a more global outlook," in line with IS-K's global vision of jihad. It is assessed that, if the Taliban breaks off relations with ETIM (in accordance with the agreement with China), ETIM fighters will likely switch to IS-K.

After the fall of Kabul: what's next? The threat evolves into "New Insurrectional Terrorism" (NIT)

The ideological and territorial spread of the Islamic State in Iraq and Syria has triggered a latent global jihadist violence. The Taliban triumph in Afghanistan has given new vital impetus to international jihadism and it is now presented by jihadist propaganda as the victory of Islam over the West and its corrupt values. This happens in contrast to the Taliban approach to jihad, which is limited to bless their national success: a national liberation war, in opposition to the IS-K and other groups who are looking for a global triumph.

But regardless of this, the victory of the Taliban and the opposition to the post-Islamic state terrorist galaxy it's already having direct effects on the will and the operational capacity of jihadist terrorist groups and individuals at a global level: from the communicative-propaganda aspect to the tactical and operational one.

Over the past 20 years terror groups, cells and individual jihadi fighters alike have begun to increasingly display new tactics, which they exported to, and adapted for, the contemporary and the future jihadi war. A first, bitter taste of things to come was the Mumbai attacks of 2008 when a group of ten terrorists divided into smaller groups mounted a siege which lasted for almost three days. Western cities have since occasionally become the set of complex suicide attacks and team-raids, and more often of individual assaults where the perpetrator efficiently exploits techniques learned in Middle Eastern war theaters. "Islamic State" or al-Qaeda militants and sympathizers have proven widely capable of carrying out deadly attacks and posing a direct threat to the security of citizens and national institutions. As such, contemporary terrorism can be described and must be recognized as a phenomenon with military characteristics or inspiration, particularly since IS with its external operations came onto the stage.

"New Insurrectional Terrorism" (NIT): is revolutionary, subversive and utopian[10]

Today, after the fall of Kabul and the success gained by the Taliban, the specter of terrorism hangs over the space of the Afghan, or Syrian, or Libyan, or Sahel battlefields. Can we claim that the significant increase in jihadi-terror-linked violence recorded in the world and Europe in the last 20 years is consistent with the classical concept of terrorism?

Terrorist attacks occurring between 2015 and 2018 in Europe, the United States, as well as in North African or Middle Eastern countries do confirm the effective operational capability of the terror groups, in particular the Islamic state, whose nature shifted over time from a proto-state reality with territorial control, to what we can deem a de-nationalized, borderless phenomenon. "Leaderless jihad", which anticipates IS, was perfected by the latter, as "aspiring" fighters were prevented from

[10] Bertolotti C., Sulmoni C. (2021), How the Twenty-Year Afghanistan War Paved the Way for New Insurrectional Terrorism, in Carenzi S., Bertolotti C. (2021) "Charting Jihadism Twenty Years After 9/11", Dossier ISPI, 11 settembre 2021

travelling and therefore chose to strike their home countries. What we are facing today has already been dubbed “New Insurrectional Terrorism” (NIT),[11] a concept which essentially includes all attempts at disrupting the national and/or international political order through violence. NIT is revolutionary and utopian, and whereas terrorism is functional, insurrectional terrorism continuously evolves. The aim of this new “breed” does not consist in instigating the masses with a view to overthrowing governments, rather in persuading a large number of Muslims all over the world to join the fight against the “infidels” insisting on a narrative supported by the victory of [their interpretation of] Islam in Afghanistan and at the same time presenting that victory as a reason to avoid any compromise with western countries.

This emerging "New Insurrectional Terrorism" has therefore nothing to do with the political terrorism of the ‘70s and ‘80s. It surfaced in the Middle East following the US invasion of Iraq (2003) and developed in the mid-2000s. It attracted world attention in 2014, due to its battlefield victories in Iraq and Syria (and then in Afghanistan). Today, however, IS – which main affiliate group is still fighting in (and possibly from) Afghanistan – has lost most of what it conquered over the past ten years: territories, energy resources, access to trade and finance channels. Its media appeal, though, is still strong and will utilize the Afghan success and the ongoing campaign as a “clear example”, also directed against the Taliban described as corrupted.

The loss of "territory" forced IS to concentrate on the one hand, on its *franchise* activities abroad, especially in areas of crisis, with a new social approach which includes outsourcing violence based on the reciprocal recognition between the IS central organization and local groups and opposition movements. Its message tries to turn thousands of radicalized individuals and dozens of young people and armed opposition groups into smart and ready "proximity weapons" prepared to “kill and die” in the name of the Caliphate.

In brief, “New Insurrectional Terrorism" consists in the use of violence, or threatened use of intentional, calculated, rational, self-justified violence in order to achieve political, religious and ideological goals. NIT is characterized by characterizing elements. The nature of the terrorist activity consists in using (or threatening to use) violence in order to reach a political objective. It is complex and, above all, unpredictable, revolutionary, subversive and with a view to establish a proto-state aiming to obtain the “monopoly of force” within a geographical area. Furthermore, it contains political, socio-economic and religious aspects (justified on religious and apocalyptic grounds) and can be described as "stra-ctical" because its strategic nature is being conveyed through tactics which must not necessarily be interconnected. Its nature is "glo-cal", transnational, borderless and based on "flexibility and adaptability". Its targets are represented by political, civilian, military, religious and symbolic combatants, as well as non-combatants. It is symbiotic: it “outsources” violence supported by emulative effects, and as a response to the “call to jihad”.

We can find all these elements in the (re)emerging phenomenon of the *Islamic state* which is findings new energies in the defeat of the United States in Afghanistan. What emerges from this description, is a threat to security represented by a contemporary, new form of terrorism: a phenomenon which adapts and evolves without a temporal or geographically-defined goal. NIT simply wants to impose a new societal model (the Caliphate) by tearing down alternatives and will use the symbolism associated with the Afghan war to exalt the “victory of Islam” obtained thanks to the sacrifice of “martyrs” and the “divine blessing”.

[11] Bertolotti C. (2015), *NIT: Il ‘Nuovo Terrorismo Insurrezionale’. Dalla ‘5+5 Defense Initiative 2015’ il cambio di approccio alla minaccia dello Stato islamico*, Analysis ISPI n. 292. In https://www.ispionline.it/sites/default/files/pubblicazioni/analisi292_bertolotti_16.12.2015.pdf.

Numbers and profiles of jihadist terrorists in Europe: analysis by the Observatory on Radicalisation and Counter-Terrorism (ReaCT)

The new terrorism in Europe, in numbers

As reported by Europol and the European Union Agency for Law Enforcement Cooperation in the Te-Sat report 2021, European Union Member States reported a total of 57 completed, failed and foiled terrorist attacks in 2020. The UK reported 62 terrorist incidents and Switzerland reported two probable jihadist terrorist attacks. The number of terrorist attacks in the EU Member States in 2020 is comparable to 2019 (119, 64 of which were in the UK) but decreased compared to 2018 (129, 60 of which were in the UK). A total of 21 people were killed in terrorist attacks in the EU in 2020. Three people died in the UK and one in Switzerland. With the exception of the targeted murder of a school teacher in France, the fatal victims appear to have been chosen at random as representatives of populations identified as enemies on ideological grounds.[12]

436 terrorist attacks, including failed and foiled ones, were recorded on European soil from 2017 to 2019 (895 in the 2014-2017 period): 63 percent were attributed to separatist and ethno-nationalist groups: 16 percent to radical leftist and anarchist groups (on the increase); 2.8 percent to far-right groups (decreasing); while 18 percent were jihadist. Although jihadist attacks are a marginal number, they were responsible for all deaths from terrorism in 2019 and for 16 killed in 2020.

The long wave of terrorism which hit Europe following the emergence of the "Islamic State" phenomenon recorded 158 jihadist attacks from 2014 to 2021: 200 terrorists took part in these attacks (60 among them died in action); 421 people lost their lives; 2,439 were injured (START InSight's database).

Twice as much emulative actions

The number of completed jihadist attacks in Europe (EU, Switzerland and the UK) in 2020 is more than doubled in comparison with the number in the EU (including the UK) in 2019. In 2020, unlike 2018 and 2019, the number of completed attacks exceeded that of foiled plots (four in the EU, two in the UK). Whether this was linked to the effects of the COVID-19 pandemic cannot be ascertained on the basis of the information available.[13]

According to START InSight's database, in 2020 a total of 25 completed jihadist terrorist attacks occurred in Europe compared to 19 in the previous year, with a substantial rise in the "emulative effect". "Emulative" and autonomous actions by *self-starters,* which are inspired or triggered by the main event and which occur within the following 8 days, represent 48 percent of the total attacks in 2020 (up from 21 percent in 2019). The period 2017-2021 was characterized by a progressive decrease in structured and coordinated actions; the now prevailing individual, unorganized, often improvised and unsuccessful actions have taken over the European urban "battlefield".

The number of completed jihadist attacks in Europe in 2021 (January-November) is 18.

Personal data of "European" terrorists

Terrorism and gender: terrorist attacks are a male prerogative as indicated by the 97 percent of male attackers (201 terrorists), although in 2020 there were 3 events conducted by women (12 percent of the total in 2020). Furthermore, the number of terrorist attacks increases as the stock of male immigrants increases too.

The median age of the 201 terrorists who carried out attacks is 26: this figure varies over time (24 in 2016, 26 in 2017, 25.5 in 2018, 30 in 2019, 25 in 2020 and 31,5 in 2021). The personal data

[12] Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.
[13] *Ibidem*.

of the 144 terrorists who were identified, allow us to draw a very interesting picture, showing that 10 percent of the subjects are under the age of 19, 36 percent are aged between 19 and 26, 39 percent between 27 and 35 and, finally, 15 percent are over the age of 35.

Increase in recidivism and individuals known to intelligence

Cases of recidivism are on the rise – individuals already convicted for terrorism who carry out attacks at the end of their prison term and, in some cases, within prison walls: from 3 percent in 2018 (1 case) to 7 percent (2) in 2019, to 27 percent (6) in 2020. This data highlights the social danger of convicted individuals who do not abandon their violent intent; this evidence suggests a potential increase in terrorist actions over the coming years, concurrently with the release of currently detained terrorists.

START InSight also spotted an increase in actions carried out by terrorists already known to European police forces or intelligence services: 54 percent of the total in 2020, compared to 10 percent in 2019 and 17 percent in 2018.

Also on the increase is the percentage of individuals already convicted and detained (for crimes not necessarily associated with terrorism): 33 percent in 2020 - they were 23 percent in 2019, 28 percent in 2018 and 12 percent in 2017. This evidence confirms the hypothesis that prisons can be conducive to radicalization.

Terrorism and immigration: links and challenges

89 percent of terror attacks in Europe were carried out by second and third-generation "immigrants" and first-generation immigrants, both regular and irregular. A statistical correlation between immigration and terrorism does therefore exist; however, the number of terrorists compared to the total number of immigrants is so marginal that it makes such correlation insignificant: the order of measurement is one unit per million immigrants.

The origins of terrorists: immigrants or Europeans?

65 (47 percent) out of 138 terrorists registered in START InSight's database are regular migrants; 36 (26 percent) are second or third generation immigrants; 22 (16 percent) are irregular immigrants. The latter figure is on the rise and represents 25 percent of perpetrators in 2020. Also significant is the number of European converts to Islam, who amount to 8 percent of attackers. Overall, 73 percent of terrorists are legal residents, while the ratio of irregular immigrants is 1 to every 6 terrorists.

Is there a link between immigration and terrorism? Are immigrants terrorists?

Immigration does "contribute" to the spread of terrorism from one country to another, but immigration *per se* is unlikely to be a direct cause of terrorism. There's no empirical evidence so far that first generation immigrants are more inclined to become terrorists. However, migratory flows from Muslim majority countries where terrorism is an occurrence, are thought to exercise a significant influence on attacks in the country of destination.

It's difficult to argue the existence of a causal link between the two phenomena: therefore, being a migrant would not be a triggering factor for joining terrorism.

However, there are other multiple links between immigration and terrorism and between immigrants and terrorists, in particular: 1) organized crime - terrorist groups - irregular migrants; 2) terrorist returnees - European terrorists who went to Syria are in fact "migrants": Europe can therefore be considered an "exporter" of terrorists; 3) economic migrants who join terrorism over the course of their journey; and 4) migrants joining jihad or migrating with the intention of carrying out attacks, as evidenced by the terrorist attacks France: Nice, on 29th October 2020, and Cannes on 8th November

2021, which were perpetrated by irregular immigrants who had previously landed in Italy from Tunisia and Algeria.

Ethno-national map of terrorism in Europe

Jihadist radicalization fuelling terrorism in Europe affects some specific national/ethnic groups. There is a proportional relation between major immigrant groups and terrorists. The terrorists' nationalities, or their families of origin, are in line with the dimensions of foreign communities in Europe. Maghrebi origins prevail: the ethno-national groups which are mostly afflicted by a link to terrorism are the Moroccan (in France, Belgium, Spain and Italy) and Algerian (in France).

An increase in the number of irregular migrants heightens the potential risk of terrorism

16 percent of terrorists are irregular immigrants (2014-2021). 25 percent in 2020.

In France, the number of irregular immigrants involved in terrorist attacks is growing. Until 2017, no attack had seen the participation of irregular immigrants; in 2018, 15 percent of terrorists were irregular immigrants: in 2020, they reached 33 percent. Belgium reported that in 2019 they identified asylum seekers linked to radicalism or terrorism (Europol).

There's therefore a statistical risk, as more immigrants mean greater chances that some terrorists might hide among them or join jihadist terrorism at a later stage. But despite this correlation, there is no manifest causal link: the choice of becoming a terrorist is not determined or influenced by one's status as a migrant, but by a series of factors such as individual experiences; living conditions at the time of arrival; voluntary or involuntary contacts with criminal or jihadist networks can all play a role.

Analysis, assessment, forecast

Increase in the "functional blockade": an indirect success of terrorism. The "functional blockade" represents the most significant outcome for terrorism on European soil; one which is obtained regardless of tactical success (death or destruction of a target): security forces' operational activities, transport, urban mobility, emergency health services, everyday life were all impacted.

Compared to a 34 percent of "success" obtained by terrorists from 2004 onwards, terrorism has proven its "effectiveness" by causing a "functional blockade" in 82 percent of the cases (2004-2020); in 2020, 92 percent of attacks led to a "functional blockade": an impressive result, despite the attackers' access to limited resources.

2. The cyberspace

Increase of threats in cyberspace

Will the information revolution lead to war?

As evidenced by Jacquelyn Schneider (2019), the proliferation of digital technology has created a new terrain for warfighting. As digitally-enabled militaries increase their dependency on information, so also do the vulnerabilities of information proliferate. Indeed, what makes offensive cyber weaponry (or any other cross-domain warfare that targets digital capabilities) a potential game changer for modern conflict is the connection that states have built between digital capabilities and conventional warfare.[14] As Richard Danzig (2014) points out: *«digital technologies... are a security paradox: even as they grant unprecedented powers, they also make users less secure… their concentration of data and manipulative power vastly improves the efficiency and scale of operations, but this concentration in turn exponentially increases the amount that can be stolen or subverted by a successful attack. The complexity of their hardware and software creates great capability, but this complexity spawns*»[15].

Cyber threat?

According to Uri Tor (2017), cyber threats may be generated by at least three distinct classes of actors[16].

The first is 'the lone hacker,' which may sound a bit of a cliché, and usually in reality includes several individuals working in some sort of coordination. Today, single individuals are very limited in their ability to inflict damage of strategic national impact through cyberattacks.[17]

The second class of actors includes non-state groups ranging from 'Hacktivists' to organized crime and terrorist groups. These groups can inflict substantial economic damage and public fear, for instance, by targeting banks or taking down government websites, but they lack the capability to target a specific high-value target, break into its core and damage it. Typically, the level of attacks these actors can generate ranges from Denial of Service attacks to cyber fraud and identity theft. This type of actor usually lacks the capabilities to identify and exploit complex code vulnerabilities, and would therefore seek to exploit human errors instead, by using 'spear-fishing' tactics, typically by sending malware via widespread social-engineered emails. Their attacks can be costly, but do not pose a strategic national threat.[18]

A third class of actors, typically nation states with extensive human, scientific, and economic resources. Such actors are capable of maintaining a long term, the multi-stage cyber campaign against a variety of targets, over a vast geographical area. Actors of this type are often referred to as Advanced Persistent Threats (APT), and usually aim at high value targets requiring complex degrees of covertness over a long period of time, sophisticated intelligence gathering, exploitation of code and technical vulnerabilities, and penetration of air-gaped networks not attached to the internet.[19]

According to Uri Tor (2017) "when dealing with the level of threat posed by this third class of actors in cyberspace, one can distinguish between attacks on information technology (IT) systems

---

14 Schneider Jacquelyn (2019) *The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war*, Journal of Strategic Studies, 42:6, 841-863, DOI: 10.1080/01402390.2019.1627209. In: https://doi.org/10.1080/01402390.2019.1627209.

15 Danzig Richard (2014) '*Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*', Center for a New American Security.

16 Tor Uri (2017) *'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence*, Journal of Strategic Studies, 40:1-2, 92-117, DOI: 10.1080/01402390.2015.1115975. In: https://doi.org/10.1080/01402390.2015.1115975

17 *Ibidem*.

18 *Ibidem*.

19 *Ibidem*.

and databases on the one hand, and attacks on industrial control systems (ICS) on the other. Although both types of attacks may have significant consequences, the distinction between them remains useful. Indeed, the spectrum of the threat to IT systems ranges from mere annoyance, through psychological warfare (e.g., defacing Internet sites or interfering with their time schedule), to functional and economic damage extensive enough to be considered a strategic threat. Yet in recent years, cyber-attacks have begun to pose another threat, which may be even more destructive than the one they pose to IT infrastructure. This is the threat of a takeover of, or severe damage to, industrial control systems, with the aim of causing an actual kinetic impact".[20]

From "WannaCry" to the case "Pegasus"

Four years ago (May 2017), more than 200,000 computers in 150 countries around the world were simultaneously affected by a ransomware virus called "WannaCry", which, exploiting a vulnerability in the Windows system, was able to infect computers and encrypt all files on the hard drive. Only by paying a ransom (in bitcoins) was it possible to obtain the return of one's data. The paradox is that Windows had made available to users a software update capable of resolving the vulnerability of the system one month before the spread of the virus; but most users, ignoring the update, exposed themselves to large-scale contamination. But there is more: four years later, more than 1,700,000 terminals are still vulnerable, of which almost 7,000 in Italy, and "Wannacry" continues to spread occasionally.

The "Wannacry" case is just one of the examples from which it clearly emerges how the problem of the security of one's data and, by extension, of computer networks is underestimated.[21]

Furthermore, as reported by *The Washington Post*, military-grade spyware licensed by an Israeli firm to governments for tracking terrorists and criminals was used in attempted and successful hacks of smartphones belonging to journalists, politicians, policy-makers, influencers, and human rights activists. The phones appeared on a list of more than 50,000 numbers that are concentrated in countries known to engage in surveillance of their citizens and also known to have been clients of the worldwide leader Israeli firm NSO Group.[22] What is the Project Pegasus? As reported by Mazoomdaar Jay (2021), the Israeli spyware, revealed to have been used to target thousands of phones, has grown less reliant on clicks. Pegasus can infect a device without the target's engagement or knowledge. It is a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract data from virtually any mobile device. Until early 2018, NSO Group clients primarily relied on SMS and WhatsApp messages to trick targets into opening a malicious link, which would lead to infection of their mobile devices. When a malicious link packaged as Enhanced Social Engineering Message (ESEM) is clicked, the phone is directed to a server that checks the operating system and delivers the suitable remote exploit.[23]

U.S. dependence on the network: vulnerabilities, critical issues and weaknesses of the Network Centric Warfare (NCW)[24]

Network-centric warfare (NCW) is defined as «an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, the higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In

[20] *Ibidem*.

[21] Basileo Deborah (2020), *Tra Cyberterrorism e guerra dell'informazione. Scarsa consapevolezza e limiti normativi*, in #ReaCT2020, 1° rapporto sul terrorismo e il fondamentalismo in Europa, ed. START InSight.

[22] Priest Dana, Timberg Craig, Mekhennet Souad (2021), *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, The Washington Post, July 18.

[23] Mazoomdaar Jay (2021), *Explained: Here's how NSO Group's spyware Pegasus infects your device*, The Indian express July 22, New Delhi.

[24] Bertolotti C. (2022), *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).

essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace». [25]

The U.S. military capability is de facto dependent on a network technology to the point that the very doctrine on which the use of the military instrument is based requires the integration of network technology in almost all areas, in particular Network Centric Warfare (NCW). And although the general orientation is to employ highly specialized personnel and systems, there is a growing need for human capital capable of operating within the "old analog dimension" in the event that computer systems should cease to be functional, in whole or in part. This is what Matthew Crosston, in his insightful article "*The Millenials' war: dilemmas of network dependency in today's military*", calls the "MacGyver effect", i.e. the ability to develop and dispose of talents and solutions that allow to effectively conduct military operations even when the main systems are offline and there is no possibility to access or activate alternative network systems.

The growing threat associated with network dependency is a relatively unstudied topic that is still not given due consideration, both from a policy and military perspective. While some concerns have already been highlighted in academia, as well as in operations, they are overshadowed by the vast array of benefits associated with integrating technology into every aspect of the military, from individual combatants on the battlefield to the command-and-control system to leadership at the operational and strategic levels. The U.S. has the most technologically advanced armed forces globally, and this is the result of large investments and growing reliance on the development of Network Centric Operations (NCO) with which, in fact, both routine and extraordinary activities are inextricably associated through network integration and proliferation. But the system, created to guarantee defense, offense and deterrence capabilities, brings with it - Crosston points out - some potentially lethal vulnerabilities from the highest (strategic) to the lowest (tactical) level.

The first of these vulnerabilities is represented by the conceptual approach at the strategic level - adopted by political and military leadership, and corroborated by the conceptual and academic theories of Network Centric Warfare and the Revolution in Military Affairs - which in itself represents the first truly great system vulnerability because it is based on an unconditional trust in cyber tools that are widely vulnerable.

The second degree of vulnerability is found at the tactical level, where operators and users of networked systems are becoming dependent on computer systems to a degree that we can assess as alarming given that, on the one hand, most military operators intervene through a computer connected to the system and, on the other hand, techniques, tactics, and procedures have all evolved around the availability and real-time processing capability of networked information. The current generation of the military is digital native, having grown up immersed in the network system, with a residual "analog" component at the middle and upper hierarchical levels that has in fact doctrinally adapted to the exclusive use of the network system leading to substantial dependence on it. Efforts at the policy level have been made with the intent to mitigate cyber threats, but placing the option of warfare in a post cyber-attack environment characterized by the availability of damaged, unreliable networks or even complete network isolation on the back burner. The most senior military personnel currently serving have operational experience from the late 1980s to the early 1990s, a time when very few areas were managed through networking. This generation is rapidly being replaced by the Millennials, the Internet savvy generation who know the digital world, who have never lived without a reliable and readily available Internet connection on which they are heavily dependent; and within the next decade, all branches of the military will be completely staffed by the Internet generation.[26]

---

[25] Alberts D.S., Garstka J.J., Stein F.P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised).

[26] Crosston M. (2017), *The Millenials' war: dilemmas of network dependency in today's military*, "Defense & Security Analysis", 33:2, pp. 94-105.

We can thus increasingly consider the level of dependence on the network system as critical because, when a network fails, work stops, and when work stops in the military, operational objectives cannot be pursued. Today, as Crosston well points out when the network is not operational and operators are offline, the only solution is to ask for help desk intervention and wait, queuing up; in the meantime, operators are unable to complete their tasks. In the meantime, operators are unable to complete their tasks. This is due to organizational and management choices that, in an attempt to reduce costs, have led to the transfer of support services away from operators, effectively transforming a proven and efficient decentralized model for network support into a centralized one. Can we imagine what would happen if the network connection was interrupted for a unit engaged in combat and under fire while artillery bombs were raining all around, or during a targeting operation carried out with a remote-controlled aircraft that could not be operated? What could the help desk do?

This growing and increasingly entrenched culture of network dependency is an unintended side effect of the race for efficiency and cost reduction.[27] The United States can be called the champion of network management and NCW but, paradoxically, while countries lagging behind in technological progress are weaker and slower in their decision-making and operational processes, they will also benefit from a lower level of vulnerability to networked cyber-attacks. And as the US military proceeds in forced stages to replace traditional systems considered "obsolete" with modern network technology, the risk of network isolation becomes more and more real; and this also applies to the civilian sector, which often anticipates the military one. An evolution that, in fact, could force the modernization of the military force that would render it incapable of operating effectively in a networkless environment.

The military applications of Artificial Intelligence and the evolution of warfare: Swarming and Machine Teaming

The military applications of Artificial Intelligence[28]

There is an increasingly tight interconnection between *intelligence* and AI. Countering contemporary asymmetric threats will progressively require a sound use of AI, which can help, for instance, determine the size and position of troops and armaments belonging either to allies or enemies; evaluate the feasibility of military actions; alter the conduct of operations depending on the evolving battlefield context.

The role of AI in supporting *intelligence* processes – from data gathering to analysis – and reiterated in his turn that never before has the military been so tightly supported by AI. Specifically, the increasing deployment of aircraft technology can be rewarding indeed for investors, as it affords them a decisive, battlefield superiority.

We must take into consideration the potential of AI specifically applied to delimitated areas, such as airports or other targets, or wider areas such as urban areas, which can be further enhanced by means of integrated systems at the national or transnational level.

Furthermore, we must consider that AI potentially imposes a radical change onto the *Revolution in Military Affairs* (RMA): it is, in brief, a true revolution to the deadly detriment of those who do not adjust to AI's offensive and defensive capacities. The traditional, combat 'mechanic system' is undergoing great and rapid developments thanks to AI, while cyberwarfare also grows in efficiency. As a consequence, command and control systems will increasingly be influenced by AI technology and capabilities, thus also requiring a regular updating in the field of military affairs.

---

27 Robinson T. (2010), *It's the Network, Stupid! Air Power and Network Centric Warfare – Trends and Challenges*, "Military Technology", 40–8, 2010.

28 *The military applications of Artificial* ***Intelligence.*** *A focus on the 8th Beijing Xiangshan Forum (24-26 October 2018)*, START InSight, November 4th**,** 2018, in https://bit.ly/2EnPdfH.

In addition, we must consider the different perspectives of specific military applications of the AI, in particular, the "swarming and "machine teaming". Swarming indicates the deployment of low-cost, autonomous elements (generally small drones or robots) acting in coordination with one another to carry out tasks without central command. Given the rapid development of technology, the security and defense community wished to gain a better understanding of the challenges and risks related to swarming, especially as an effective defence system against such hypothetical attacks is still lacking.

Artificial Intelligence and the evolution of warfare[29]

What can we assess about the role of AI in the next phase of *Revolution in Military Affairs* (RMA – in other words, the evolution of warfare) which bears direct consequences on the very same concept of war and the decision-making process? The assessment is that AI potentially imposes a radical change onto RMA: it is, in brief, a true revolution to the deadly detriment of those who do not adjust to AI's offensive and defensive capacities.

For instance, it can aptly support the decision-making process by providing a prompt analysis of all primary and secondary factors that could affect strategic and operational planning. Furthermore, the combination of electronic warfare and cyber capacity grants an extraordinary offensive and defensive military leverage, as it allows thorough monitoring of enemy targets without exposing one's own pilots and recognition assets to risks and threats.[30]

The same thing applies to critical infrastructures, whose security and safety can still be guaranteed with limited resources, be it in terms of soldiers or equipment. Within this context, the deployment of (partially or totally) remote controlled or AI controlled robots, without entirely replacing troops on the battlefield, nevertheless becomes instrumental in supporting them; and represents a technological and cultural development which, in asymmetric conflicts above all, can still safeguard the human component's primacy.[31]

On the virtual level, an ever more realistic wargaming activity takes place, which greatly benefits from AI in terms of both training and planning. And as yet another dimension of the contemporary battlefield, social media represent a great opportunity for surveillance and analysis, in spite of the looming threat of mass control. It is important to underline how, with specific reference to wargaming, the private sector plays a fundamental role.[32]

The traditional, combat 'mechanic system' is undergoing great and rapid developments thanks to AI, while cyberwarfare also grows in efficiency. As a consequence, command and control systems will increasingly be influenced by AI technology and capabilities, thus also requiring a regular updating in the field of military affairs. Automatic systems will also increasingly play a leading role, particularly in training and direct combat. It's now clear that what separates winners from losers on the global battlefield is supremacy in the intelligence sector, where the support of Artificial Intelligence is becoming paramount.

Artificial Intelligence is about to play its part in combat. But is it up to the task? Such is the *vexata quaestio*. We must consider the rapidly progressive evolution of intelligence on the contemporary battlefield, and the forthcoming, tactical role of AI (which essentially translates as 'battlefield-bound'); as far as the strategic and operational ones, we are not there just yet, despite progress being made. Should a direct, ground confrontation between two actors with equal military capabilities take place, AI would cease to represent a crucial factor.

---

29 *Artificial Intelligence and the evolution of warfare. Report on 8th Beijing Xiangshan Forum*, START InSight, November 6th, 2018, in https://bit.ly/2zQeuLO.

30 *Ibidem*.

31 *Ibidem*.

32 *Ibidem*.

AI made two key contributions to the military and intelligence fields: in the first place, it represents a launching platform for future, autonomous weapons; secondly, it's fundamental in *problem solving* and *decision-making* processes[33].

Furthermore, we must consider the social implications of AI: how Artificial Intelligence could potentially be used to influence and alter social structures and functions, and to induce a change in individuals' attitudes and opinions? It is an issue which clearly paves the ground for a critical analysis of ethical issues linked to certain applications of AI within RMA.

AI's diffuse application does indeed induce changes in the social behavior of populations which are subjected to remote-controlled surveillance. And it doesn't make a difference whether such control is exercised by an external actor (like an enemy or an influencer) or by one's own government: citizens simply adapt their behavior to the new situation. In the same way, AI can bring about shifts in the enemy's attitude, specifically in operational and tactical terms; the Taliban in Afghanistan for instance reshaped their techniques and tactics as a result of the deployment of drones.

Can we figure out the impact of robots in asymmetric wars, in Iraq or Afghanistan for instance? How would that affect the mind of the enemy and of the local populations?

The degree of development and deployment of Artificial Intelligence is contingent upon an individual actor's ethical issues and constraints. But it's those who overlook ethics and push the boundaries of AI, who will take the lead on the battlefield.[34]

Swarming and machine teaming: different perspectives

Swarming indicates the deployment of low-cost, autonomous elements (generally small drones or robots) acting in coordination with one another to carry out tasks without central command. Early examples of (semi-autonomous) commercial swarms -like drones flying in formation- have already been on display. Military use is actively researched but currently restrained due to limitations in reliability and predictability. Autonomous systems also raise ethical issues which are being discussed at the UN-level.

Given the rapid development of technology, the security and defense community wished to gain a better understanding of the challenges and risks related to swarming, especially as an effective defence system against such hypothetical attacks is still lacking.

Autonomous systems and underlying technologies: the state of play[35]

Autonomous systems are systems that can complete a task without direct human involvement, interacting instead with the environment by means of sensors and computer programming. On a basic level, they must be able to perceive the environment and process it in a way that serves as an input to the decision-making process. The critical part is planning; designing autonomous systems in itself is not complicated and depends on 2 key variables: the complexity of the task and the environment.

For instance, autonomous navigation is very context-dependent, with air or underwater environments presenting fewer obstacles compared to land, where interaction with people or machines must also be taken into consideration. Also, the civilian environment is less challenging, more predictable or controllable, which might not be the case on the battlefield. We can have autonomous cars and military vehicles if we can pre-map the area but we need to unlock new possibilities in vision-based guidance. One major achievement is autonomous drones for refueling

33 *Ibidem*.
34 *Ibidem*.
35 Vincent Boulanin, Stockholm International Peace Research Institute (SIPRI), in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on *Swarming and Machine Teaming*, Thun, Switzerland, November 21st, 2018.

in flight, which demonstrate we can attain complex operations in air and detection. There have also been developments in resilience, as components can be discarded.[36]

The limitation of perception intelligence is the most important obstacle towards the use of robotics systems in predictable environments, especially in the military field, as systems can be easily tricked, and limitations exploited by enemies. Machines can process images and understand words but have no common sense.

Planning decision-making: there are limitations to synthetic reasoning. Computers can calculate far beyond human capabilities, they are powerful, fast, and precise, but they cannot generalise from previous experiences and adapt to new situations. Small robots don't have enough computer-power in them.

Machine-machine teaming: systems can share information including target information and perform collaborative operations for simple tasks (flying in formation, surveillance, inspecting buildings in an uncomplex environment). Research projects in the US for machine-machine teaming in distributed attacks operations (LOCUST). A major constraint is reliance on communication infrastructure.

Human-machine teaming: no symmetrical communication between machines and humans is a great limitation (no voice command for critical functions). Finding the right ratio is also difficult, as we might need more than one operator for one system, especially when things go wrong.

Intelligence domain: systems can generate maps, detect explosives and locate weapons fire, threat assessment. Actively researched: automated surveillance, intelligence data fusion and analysis. Or robots doing practical, autonomous operations.37

Targeting: most critical application of autonomy is being discussed at the UN-level as well. Can only engage very large material targets and specific signatures, but do not have the ability to make distinctions between civilian and military targets. Actively researched (e.g. DARPA Trace).

In brief: swarming is a means to an end. Feasibility depends on the task, with 'general' or ill-defined tasks being the most complicated. Complex interaction with other agents, humans or machines might be difficult to engineer. Autonomy is much easier to achieve for commercial applications.

Swarming and the evolution of military strategy: consequences for international stability[38]

Swarming is considered the 5th evolution of military strategy. There are four other ways to apply force (military strategies):[39]

1. Denial - breaks through the enemy forces and destroys them; the target is military; e.g. WWI – Blitzkrieg;
2. Punishment - hits civilians and infrastructure to exert indirect pressure; e.g. WWII bombings, terrorism;
3. Risk - tries to win over adversaries by threatening an escalation (psychological warfare); e.g. US USSR Cold War;
4. Decapitation: targets the enemy leadership thanks to technology. It can compensate for lack/withdrawal of troops, as was the case with Bush and Obama's counter-terror operations, which were fought not only through human beings but technology (drones). Technological advances brought about what is known as RMA (Revolution in Military Affairs).

Swarming is deemed the 5th evolution of military strategy because of the way it can concentrate mass, firepower, speed, and forces in a way that is unseen in human history.

---

36 *Ibidem*.
37 *Ibidem*.
38 Jean-Marc Rickli, Geneva Center for Security Policy (GCSP), in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21st, 2018.
39 *Ibidem*.

Requirements for a swarm to work: it must count on a large number of small units with sensory capabilities, be easy to maneuver, able to observe, react and act in coordination. In terms of technology, we are already there. 3D printing of gun components and drones challenges states' monopoly of the use of force (by non-state actors, open source access). During the notorious battle of Mosul (2017) several Iraqi soldiers were killed by drones operated by ISIS, in what is the first instance of the West losing tactical aerial supremacy. Swarming tactics is a means to wage asymmetric wars. Before we see the physical manifestation of swarms, however, we will witness cyber manifestations of a swarm. Malware equipped with autonomous capabilities already exists.[40]

Iron domes, on the other hand, represent an early example of the emergence of defensive swarms. Research is being conducted on swarms competing against swarms. And also on machines and robots which can be recomposed. War is increasingly being waged by human and technological surrogates. China and the US are investing heavily in AI, which provides many advantages as it's cheaper and allows States to deny an operation. A report by US DoD (2016) declares how autonomy is the new super-bullet in future armed conflict.

But what's the impact of swarming on strategic stability? Stability exists if there is no incentive to attack a neighbor (defensive advantage). Right now we are living in a defensive-dominant international environment because of nuclear weapons. In the cyber domain though, the offensive already has the advantage. If swarming becomes a mainstream strategy, there will be a likely shift in the offense-defense balance resulting in a more conflictual international environment, where conflict becomes the norm and not the exception.[41]

Concluding, autonomy and swarming are two key characteristics of the battlefield of the future; 3D printing and swarming for military application will have tremendous implications.

Manned-unmanned teaming (MUM-T) and swarming: possibilities and challenges in military applications[42]

Is swarming a game changer? Having 'many of something' is not a problem; what you want is to have cheap sub-systems with no single point of failure and a reduced number of operators.

The antagonist perspective is considerably different from the civil perspective. Swarms rely on communication and satellite navigation and should you clash with adversaries who can master a high technological command, you can end up being GPS-denied, with a lack of communication in a contested environment, having then to increase the robustness of each agent. Many robust systems are quite expensive and this is why it will probably take some time before we see swarms in military applications, more likely in non-antagonistic environments (like surveillance missions). Another limitation is that the battlefield requires predictability.[43]

Manned-unmanned teaming (MUM-T) for swarms has been a research topic for quite some time but there are a number of challenges to be addressed, the main question being: how to control a fleet for different missions, at different operational levels and with different fleet sizes? How to reach the 'one operator-many agents' balance? Teaming itself is quite complex, there must be a broad, dynamic interplay between the operator and the system, but machines understanding humans and *viceversa* is inherently difficult. Finding a solution which is robust for such interplay is a challenge. And robustness (which is desirable in many aspects, for instance when swarms lose agents, and in the military field), might lead to fragility in context.[44]

Other issues to take into account for flying objects are flight safety rules and policies (the air space is not free) and difficulties linked to testing. Stability and predictability are paramount in military

40 *Ibidem*.
41 *Ibidem*.
42 Martin Hagström, FOI - Swedish Defence Research Agency, in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21st, 2018.
43 *Ibidem*.
44 *Ibidem*.

applications, and because a system acts within its own software-designed space, autonomy is to make that design space very large, as to include many potential events. But outside of simulation, testing a system remains difficult and unpredictability takes over.

Concluding, what is important to underline is that there are many demonstrations on how to control a swarm for one single task but a robust interface between man and machine is still a research topic.

Swarming, the Certain Conventional Weapons (CCW) and Meaningful Human Control[45]

Autonomous weapons raise ethical issues which are debated at UN-level. UNIDIR (UN Institute for Disarmament Research) has been dealing with UAVs (un-manned aerial vehicles) since 2015, inheriting previous work started in New York around 2012 and considering the issue mainly from a human rights perspective, with concerns about the use of Reapers and Predators (drones). As part of its role, it encourages the international community to consider what new challenges may emerge (e.g. strategic implications of un-manned systems with the core question of whether their features enable new military practices). Un-manned nature creates new opportunities and risks, the risks being that if you don't put personnel in harm's way, the military is more likely to deploy lethal force. As part of internal research, UNIDIR tried to understand how it could encourage some of the states engaged with debates around the use of drones, to think about drivers for these systems to become smaller.[46]

Drivers for the acquisition of smaller systems: they are pilot-friendly (they do not put pilots out of job); they are affordable; they are expendable in combat (low-cost). An issue for the UN to consider in the long-term, is whether due to the low-risk and cheap deployment, these systems might lead to problematic military practices. Relevant to this debate and developments, is the Convention on Certain Conventional Weapons, a UN negotiating body designed to address certain weapons systems with implications on international humanitarian law. The framework is to ban or restrict the use of specific types of weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilians indiscriminately; mines, IED, cluster ammunitions, *etc*. A Group of Government Experts to address Lethal Autonomous Weapons s

Systems (LAWs) was established in 2014, with the participation of 84 states; experts and military advisors are regularly invited in.[47]

Since 2014, a key discussion is on meaningful human control: *Why is it an ethical concern that increasing autonomy might mean increasing detachment from the individual and the deployment of lethal force?* There are those with ethical reasons in favour of LAWs (protection of military personnel, for instance), others concerned with retaining human agency in decisions to use lethal force; the loss of human dignity, moral responsibility and human accountability. In the first two years of conversation, a major problem was the characterization of the systems under consideration. Key challenge: huge diversity of states and military capabilities. The level of insight is difficult. The point is that there is a different way of characterizing those systems and terminology. Further consideration of the human element in the use of lethal force – aspects of human-machine interaction in the development, deployment and use of emerging technology in the area of LAWs; review of potential military applications of related technologies in the context of the Group's work; possible options for addressing the humanitarian and international security challenges posed by emerging technologies in the area of LAWS.[48]

[45] George Woodhams, UNIDIR Security and Society Programme, in *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21st, 2018.
[46] *Ibidem*.
[47] *Ibidem*.
[48] *Ibidem*.

In brief, there's a need to identify best practices and practical measures to encourage info sharing for improving compliance with international law. Beyond technology, there are different national perspectives that come from underlying ethical arguments. Swarming has not been mentioned specifically over the last four years, but it is the area of autonomy that catches the imagination the most.

Analysis, assessment, forecast

What emerges from the observation of the evolution of the Artificial Intelligence applications is that AI made two key contributions to the military and intelligence fields: in the first place, it represents a launching platform for future, autonomous weapons; secondly, it's fundamental in problem solving and decision-making processes. Furthermore, we must consider the social implications of AI because it could potentially be used to influence and alter social structures and functions, inducing a change in individuals' attitudes and opinions.

Regarding Swarming and the evolution of military strategy, autonomy and swarming are two key characteristics of the battlefield of the future; 3D printing and swarming for military application will have tremendous implications.

About manned-unmanned teaming (MUM-T) and swarming, considering the possibilities and the challenges in military applications, what is important to underline is that there are many demonstrations on how to control a swarm for one single task but a robust interface between man and machine is still research topic.

On the topic of "swarming, the Certain Conventional Weapons (CCW) and Meaningful Human Control", in brief, there's a need to identify best practices and practical measures to encourage info sharing for improving compliance with international law. Beyond technology, there are different national perspectives that come from underlying ethical arguments. Swarming has not been mentioned specifically over the last four years but it's the area of autonomy that catches the imagination the most.

3. COVID-19 and the security of the Mediterranean area

The repercussions of the COVID-19 pandemic on the security of 5+5 countries (West Mediterranean area)

As reported in the recent research document edited by the CEMRES within the "5+5 Defense Initiative" and presented to the "5+5" Defense Ministry on the 15th of December 2021,[49] Pandemics are a major problem worldwide and a serious threat to sustainable development. Their impacts are diverse: loss of life and disease can also cause social and economic disruption, and loss of capability to provide services. In an increasingly integrated world economy built on networks of global supply chains, pandemics in one country can easily affect others.

An epidemic is a new disease that usually spreads within national boundaries. A Pandemic is an epidemic that spreads worldwide, crossing international boundaries and affecting a very large number of people. The outbreak of such a disease is caused by a virus that is new to mankind to which the human body is not immune. Viruses that are found in animals sometimes when transmitted to the human body mutate and become harmful causing deaths.

Pandemics are not the mere field of public health but a social issue and global security issue. It impacts on economic, social, and political conditions of the countries where it spreads. The movement of people from one region to another is highly restricted on account of the transmission of the virus and therefore the social life of citizens gets badly affected. When economic activities are shut down country faces a deficit in funds for meeting the needs of the people. The Lockdown of a city or entire state curtails development and so builds up the pressure on the governments. A country needs to be well equipped with medical infrastructure to sail through a pandemic situation.

A new strain of virus causes the disease COVID-19 which is similar to Severe Acute Respiratory Syndrome (SARS). Symptoms of the disease include fever, cough, and shortness of breath. In more severe cases, the infection can cause pneumonia or breathing difficulties (WHO). The outbreak of the disease was first reported in Wuhan, Hubei province, China in December 2019. WHO declared on 30th January 2020, the outbreak of PHEC (Public Health Emergency Concern), and on 12th February 2020, the disease was named COVID-19 (Coronavirus Disease 2019). In a span of 30 days, COVID-19 spread rapidly to the entire country with an increase in a number of confirmed cases where the first few were from Wuhan, Hubei, China which is also the possible point of origin of COVID-19 and later cases were through transmission from one person to another "7". As per the WHO"s situation report on 13th March 2020, the disease has spread in more than 100 countries of the world and among them, the most affected are the USA, Italy, Spain, Germany, China, France, and Turkey. To check the spread of pandemics many countries including the region of Mediterranean countries took certain measures such as lockdown of cities, screening mechanisms at airports to detect symptomatic people, and keeping them in isolation for 14 days to test them for the virus.

The COVID-19 outbreak represents the worst pandemic experienced by nearly all people currently living and has had severe medical, social, and economic tolls worldwide. On a global scale, as of December 6, 2020, the World Health Organization (WHO) published statistics of 267.865.289 infected patients and 5.285.888 deaths worldwide. As a part of the globe, both Mediterranean shores have experienced several difficulties during the spreading stages of COVID-19.

Covid-19 impact on the Southern shore of 5+5 space

The Southern shore of the 5+5 was not spared from the harmful effects of the pandemics. Most countries tackled successfully the impact of the first wave but the second and third waves have been

[49] AA.VV. editor Salem Shanbr (2021), *The repercussions of natural disaster, epidemics and pandemics on the security of 5 + 5 countries: "means of cooperation and mutual support*, CEMRES, Tunis.

more aggressive. Despite this fact, the number of cases and fatalities are lower than on the Northern shore as the following table shows:

State	*Confirmed Cases*	*Number of deaths*
Algeria	128,725	3,595
Libya	185,776	3,126
Mauritania	19,494	364
Morocco	519,108	9,143
Tunisia	345,474	12,654

***Table 1**: Confirmed COVID-19 cases & deaths in the Maghreb*

(source: Africa CDC & African Union June 2021)

The countries more hit by the pandemic have been Morocco and Tunisia while Mauritania is less affected by a number of cases and deaths. Nonetheless, governments were obliged to put in place restrictive measures to counter the spread of the pandemic like lockdown, borders shutdown and schools closure among others.

The economies in the Maghreb region have experienced hardship as a consequence of the COVID-19 pandemic. The real Gross Domestic Product (GDP) growth in the Maghreb region decreased by 8.8 in 2020 according to the International Monetary Fund (IMF) (2021). All Maghrebian countries experienced a decline in real GDP growth in 2020: Algeria (-6%), Libya (-59.7%), Mauritania (-2.2%), Morocco (-7%) and Tunisia (-8.8%). Low tourism and decline in remittances are factors that impact most economies together with the historical collapse of the demand in oil markets which harms the oil exporter countries. In the case of Libya, whose economy has suffered from political conflicts since 2011, the pandemic impact has exacerbated economic and social problems. The hydrocarbon sector is the main contributor to the GDP and the oil price depression led to an unprecedented slump in export revenues.

The prospects of GDP growth for the Maghreb region in the medium term, an increase of 14.7% and 3.3% in 2021 and 2022 respectively, are positive but the ability to reach previous levels of growth and employment will depend on the recovery of the world economy, especially the EU economies, and the evolution of tourism and hydrocarbon demand. The high rate of unemployment among youngsters remains and seems to be one of the threats to social peace. The health crisis has increased the need for funding to counter budget deficit, e.g. the IMF provided USD 753 M to Tunisia in April 2020.

Economic prospects by country are positive too according to IMF (2021): Algeria (2.9%), Libya (131%), Mauritania (3.1%), Morocco (4.5%) and Tunisia (3.8%). Despite these figures, Maghrebian countries will need new economic models for solving traditional economic problems and for adapting to the post-COVID-19 global stage like the rest of the World economies. That is the real challenge in the long term for the Maghreb region.

Covid-19 impact on the Northern shore of 5+5 space.

The COVID-19 pandemic has generated a multi-layered and multidimensional impact across all five countries on the Northern shore of 5+5 space. Given its unprecedented global reach and impact, it has posed considerable challenges to national authorities and heightened previous fragilities across the board, thus requiring coordinated multi-country policy responses (Greer, S.L.et al,2020). Its accumulated effects, however, have not been restricted to the hotspots of intensity or

severity that had been initially identified. Indeed, while Italy was first reported as one of the main epicenters for the entire international community, with Spain assuming a key prominence soon afterwards due to spiking numbers, the aggregated statistics have since then reflected the proportionally different sizes and populations of France, Italy, Malta, Portugal, and Spain, while still affecting each country accordingly.

Fatalities and infection cases provide the most immediate and glaring depiction of the human cost inherent to this pandemic. By the end of April 2021, France had reached a total of 5.37 million infection cases and 102,000 fatalities; Italy a total of 3.9 million infection cases and 117,997 fatalities; Spain a total of 3.44 million infection cases and 77,000 fatalities; Portugal a total of 832,000 infection cases and 16,952 fatalities; and Malta a total of 30,063 infections cases and 411 fatalities. These numbers remain understandably provisional as the crisis grasses through the world in as much as they also remain contingent on the stress put into each respective national public health service and capacities in the face of consecutive waves of spikes in infection rates. Regardless, when combined, the Northern shore of the 5+5 space has already totaled over 13.6 million cases of infection and over 314,000 fatalities thus far.

The pandemic also took its sizeable toll at a political level. This is best represented by the delay or postponement of several electoral acts in three of the five countries under analysis due to the risk of further contagion through the concentration of large gatherings. In France, for instance, the second round of local elections originally scheduled for 22 March 2020 was moved to 28 June 2020. Italy, for its part, witnessed the postponement of a national referendum in addition to numerous regional and local elections. Regional elections in Spain, namely in Euskadi/Basque and Galicia, originally scheduled for 5 April 2020, were also pushed back to 12 July 2020.

However, the political impact can also be assessed in terms of growing levels of Euroscepticism, given the interconnection between the five countries' responses and the collective approach promoted by the European Union (EU) to tackle the pandemic. Italy, in particular, stood out early on with polls crediting 55% of the population to deem EU support to Italy during the COVID-19 crisis as "inadequate" (Fontana, O, 2020). Successive problems with the vaccination roll-out since early 2021 have equally contributed to widespread blame of the bloc for multiple shipment shortcomings, thus leading to an overall decrease in approval of the EU's performance in all five countries (Eurobarometer 2021). Generalized loss of public confidence in institutions and leadership alike has therefore emerged as a key consequence across this particular space.

The overall economic impact has also been extremely severe, with full ramifications still unaccounted for. Spain's GDP shrank 10.8% in 2020, the deepest recession in 80 years and the harshest in Europe, while unemployment rose to 16.2% (Chislett 2021). Meanwhile, Portugal's GDP contracted by 7.6% due to a significant decline in domestic demand as well as in private consumption, but also owed to the intense reductions in exports and imports of goods and services, with a special focus on tourism (INE 2021). Likewise, France, witnessed a contraction of nearly 9%, with the government launching comprehensive fiscal plans for 2020–22, totaling about 26% of the GDP in emergency and recovery measures (IMF 2021). The Maltese economy also likely recorded an unprecedented contraction of 6.6% in 2020 (CBM 2020). Moreover, shared outlooks for recovery have been consistently pushed back in light of the lingering effects of the pandemic worldwide.

Finally, all five countries are also currently experiencing some measure of social tensions, placing public services under stress as well as elevating the political costs of omission and inefficiency, while at the same time giving room to more extreme views to take hold throughout the fringes of each society and further heightening the overall perception of crisis in the Northern shore of the 5+5 space.

Epidemics and Covid-19 impact on the neighboring space (Sahel)

The Sahel region has been less hit by the COVID-19 pandemic than other regions in the world. According to the uncertain figures provided by some international organizations, COVID-19 cases and fatalities across the Sahel are relatively low. By the end of November 2020, there were 17,891 cases and 551 deaths caused following the Africa, Centers for Disease Control and Prevention (CDC). The latest figures reported by the same organization on the 1st of June 201 for the G5 Sahel are the following:

State	*Confirmed Cases*	*Number of deaths*
Burkina Faso	13,431	166
Chad	4,929	173
Mali	14,265	----
Mauritania	19,494	463
Niger	5,410	517

***Table 2**: Confirmed COVID-19 cases & deaths in the Sahel*

(source: Africa CDC & African Union June 2021)

The above table shows that the epidemic in the third phase shows an increase in the number of cases (57,519) and fatalities (1,511). The World Health Organization (WHO) pointed out that the mortality in critically ill patients with COVID-19 is higher in African countries and particularly in the Sahel region showing case fatality ratios higher than the global ones.

The evolution of the pandemic and its socio-economic impact is the cause of major concern among the international community. The fragility of most Sahelian states and the deteriorated human life conditions are challenged by the pandemic. COVID-19 pandemic has become an extra-exogenous factor to exacerbate the traditional evils of the region: lack of good governance, poverty, difficult access to public services (health care, education) and insecurity.

	Burkina Faso	**Chad**	**Mali**	**Mauritania**	**Niger**
Original 2020 forecast	5.8%	3.2%	6.3%	5%	6%
COVID-19 2020 adjusted	-0.8%	-0.9%	-2.2%	-2%	1.2%
2021 projections	4.3%	1.8%	3.1%	4%	2.9%

***Table 3**: Adjusted economic growth forecast for G5 Sahel*

(source: IMF World Economic Outlook (April 2020 & April 2021)

Economic growth in the G5 Sahel has been seriously affected in 2020 as the above table shows. Food security is threatened by the impact of the pandemic in the agricultural sector by reducing inputs access and labor. The increasing number of displaced people, as well as their live conditions, is a cause of inter-communal conflicts. According to Save the Children 2021, 13 million children are out of school due to increasing insecurity. The UN Secretary General, António Guterres warned in May 2020 that terrorist groups were taking advantage of the Covid-19 pandemic to intensify their attacks and challenge state authority in the Sahel.

Repercussion on 5+5 space security

The Southern Mediterranean region is facing governance, socio-economic, climate, environmental and security challenges, many of which result from global trends and call for joint action by the "5+5 countries". Protracted conflicts in the Mediterranean region continue to inflict terrible human suffering, trigger significant forced displacement, weigh heavily on the economic and social prospects of entire societies, especially for countries hosting large refugee populations, and intensify geopolitical competition and outside interference.[50] The Covid-19 pandemic is having a tremendous impact on these societies. [51]

The urgency of addressing these challenges is further reinforced by the COVID-19 pandemic, which has illustrated starkly shared vulnerabilities.[52]

Major security threats such as terrorism, hybrid threats as well as cybercrime and organised crime, including the trade of illegal firearms, drug trafficking, human trafficking and money laundering are key challenges.[53]

Radicalism and violent extremism

Analysis and studies evidence on the potential impacts of the COVID-19 pandemic and response to violent extremist recruitment and radicalisation. There are pieces of evidence identified on the impact of disasters on radicalisation and violent extremism.

The impact of COVID-19 on radicalisation will play out differently over short-, medium- and long-term frames.[54]

The short term impacts

The short-term impacts of COVID-19 on radicalisation and violent extremism are multifaceted and complex, these result from the immediate impact of response to the pandemic. These include social distancing and restrictions.

Such responses have been seized on by radical ideologues to validate their world views. Further to this, the failure or inability of the government to reach certain areas or groups may lead to avoid in which violent extremists may step. In brief:[55]

a. Governance vacuums may emerge and be filled by extremist groups as national resources are stretched and the capacity to govern is challenged;
b. The pandemic may be used to validate particular world views i.e. the decadence of the west, and the corruption of big government;
c. The pandemic may provide a context in which opportunistic attacks are planned and accelerationist seek to act;
d. Social restrictions may provide a captive audience ripe for radicalisation. It is important to note that radicalisation is a multi-stage phenomenon and individuals must usually already be receptive to extremist messaging.

The medium term impacts

The medium term impacts of COVID-19 are likely to be influenced by the broader impact of the pandemic i.e. how government responses are perceived, the fall out of said responses as well

50 European Commission (2021). *Joint communication to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions*, 9 February 2021. In https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021JC0002&rid=2.
51 PAM (2021). *Covid-19 Pandemic and Food Security in the PAM region*. In https://www.pam.int/welcome.asp?m=news&id=904.
52 European Commission (2021). *Cit.*
53 *Ibidem.*
54 Avis W. (2020). *The COVID-19 pandemic and response on violent extremist recruitment and radicalisation*, H4D, Helpdesk Report, University of Birmingham. In https://reliefweb.int/sites/reliefweb.int/files/resources/808_COVID19%20_and_Violent_Extremism.pdf.
55 *Ibidem*.

as the broader socio-economic impacts. As such radical ideologies may be provided with a space and audience to propose violent extremism. In brief:[56]

a. The pandemic may result in declining international collaborationas nations seek to fund responses to COVID-19 at the expense of other areas;
b. Countries may face challenges in providing services, this may provide a void into which extremist groups can move;
c. Tensions may be created between groups as government responses are perceived to be unequal;
d. The crisis may result in deepening inequalities if the socio-economic impacts are significant

Longer term impacts.

The longer-term impacts are harder to discern and will play out over months and years. It is clear that how governments respond to the initial crisis will reverberate over the medium to long term. In particular decisions regarding how to respond have the potential to entrench inequalities or alienate particular areas and groups. If the pandemic leads to a sustained economic crisis at the national or international level – cooperation across borders may be reduced allowing radical ideologies to proliferate.[57]

Depending on the severity of the crisis a number of factors could influence radicalisation and violent extremism these, however, are uncertain.

Terrorism

Terrorism and its financing, radicalisation, violent extremism, and the phenomenon of Foreign Terrorist Fighters occur on and affect both shores of the Mediterranean and are often interlinked.[58]

As the novel COVID-19 was spreading like a bushfire, the pandemic couldn't go unnoticed by the media apparatus of jihadi groups like the so-called terror group *Islamic State* (IS) or al-Qaeda (AQ). Islamic State and al-Qaeda online terrorist propaganda during the Covid-19 emergency Propaganda activities carried out during the Covid-19 pandemic and the attacks which took place in Europe and North Africa, recall how dynamic terrorism associated with the so-called Islamic State and al-Qaeda remains, especially through the Internet. In particular, the IS confirmed its aggressive narrative, identifying the Coronavirus as a "soldier of Allah". An ally set out to punish the "infidels", above all the military and police forces[59], currently preoccupied with dealing with the pandemic and the extra security measures involved. They perceive this as an opportunity to engage in attacks and "spread (…) chaos and agitation".[60]

Irregular migration, migrant smuggling and human trafficking in the time of COVID-19[61]

Migration is a global phenomenon that requires joint responses, solidarity and global responsibility sharing. Irregular migration brings challenges, also by further increasing the economic power and destabilising the influence of criminal networks.[62]

The economic consequences will significantly impact peoples' desire and ability to migrate, as well as the incentive and opportunities for criminals to profit from illegal migration which is also expected to increase.

---

56 *Ibidem*.
57 *Ibidem*.
58 *Ibidem*.
59 Bertolotti C. (2021), *Introduction: terrorism at the time of Covid-19*, in #ReaCT2021 – 2nd Report on Radicalization and Counter Terrorism, START InSight & Formiche. In https://www.startinsight.eu/en/react2021-2report-en/.
60 Van Ostaeyen P. (2020). The Islamic State and Coronavirus, Time for a Comeback? ISPI, Milan. In https://www.ispionline.it/it/pubblicazione/islamic-state-and-coronavirus-time-comeback-26166.
61 INTERPOL (2020). *COVID-19 impact on migrant smuggling and human trafficking*, 11 June 2020. In https://www.interpol.int/News-and-Events/News/2020/COVID-19-impact-on-migrant-smuggling-and-human-trafficking.
62 European Commission (2021). *Cit*.

Migrant smuggling and human trafficking are particularly affected by geo-political and socio-economic factors which vary greatly by region and in the ways they drive vulnerable communities in those regions to migrate. The COVID-19 pandemic is, and will continue, to influence these factors across the globe. Furthermore, COVID-19, and measures being taken by countries to control its spread, are impacting crime around the world, including migrant smuggling and human trafficking.

Europe, the most frequent destination countries for irregular migration and migrant smuggling, have been amongst the most heavily impacted by the COVID-19 outbreak. Migrants have not been discouraged from reaching, or attempting to reach, these destinations despite the risks of contagion.

Most African countries have implemented travel restrictions to prevent the spread of COVID-19, however, these have not been sufficient to dissuade smugglers or migrants in certain regions.

Migrants are still arriving in smuggling hubs in the Sahel region: it is almost certain that attempts to migrate to Europe will continue in spite of the pandemic. With access to desired destinations being increasingly difficult, smuggling networks will likely be seeking new means of entry and charging premium prices for their so-called services.

- Alternative and potentially more dangerous, maritime routes will continue to be explored;
- Increased militia activity in Libya likely to see an increase in smuggling activities;
- Increased demand, and higher prices, for smuggling activities are expected in response to greater difficulty to enter destination countries.

Migrants departing mainly from Western Sahara, in 2020, have continued to arrive in the Spanish Canary Islands along the highly perilous Atlantic route in unseaworthy vessels.

Migrants departing mainly from sub-Sahara, in 2021, have increased their arrival in Italy along the Central Mediterranean route departing mainly from Tunisia and Libya.

Analysis, assessment, forecast

In terms of security and stability, the COVID-19 pandemic has made the pre-existing problematic situation more critical.

In this challenging scenario, “5+5 countries” need to develop further their partnership on security matters with their neighbouring countries, as well as enhance operational cooperation, including for maritime security and coastguard cooperation. Such partnerships should be tailor-made, correspond to respective needs and enjoy high-level political support in order to guarantee concrete results. Cooperation with regional and international organisations is also vital.

Regarding irregular migrations

It is required that the “5+5 countries” will significantly step up common efforts to combat trafficking and fight the criminal networks behind migrant smuggling and trafficking of human beings. Strengthening migration and asylum governance including border management capacity is a key element. Cooperation at the regional and multilateral level should be explored further, including through triangular and south-south cooperation, since some southern Mediterranean partners are origin, transit and destination countries.

Regarding terrorism and radicalism

Recent attacks have underscored the need to deepen high level strategic dialogues on counterterrorism. Building on existing cooperation, notably on law enforcement, it is needed to step up efforts to prevent radicalisation, including deepening interreligious and intercultural dialogues, and building capacity to address violent extremism, online recruitment, preventing the dissemination of terrorist content online.

The "5+5" Countries (West Mediterranean area): means of cooperation and mutual support. The results of the international research group.

As reported in the recent research document edited by the CEMRES within the "5+5 Defense Initiative" and presented to the "5+5" Defense Ministry on the 15th of December 2021,[63] the repercussions of natural disasters, epidemics and pandemics on the security of 5+5 Countries are a concern for States.

The "5+5 Initiative" is a defense and security forum established at the end of 2004. Ten western Mediterranean countries: Algeria, France, Italy, Libya, Malta, Mauritania, Morocco, Portugal, Spain and Tunisia participate in this initiative. The goal of the "5+5 Initiative" is to improve, through practical activities and through the exchange of ideas and experiences, mutual understanding and confidence in dealing with problems of security in the area of interest.

The author of the present synthesis is the Senior researcher as Italian representative at the "5+5 Defense Initiative" international research group which includes one researcher per country. The research group is aimed to provide the 5+5 Defense Ministers with an instrument of thinking, analysis and forecasting, allowing them to explore any issue related to the Western Mediterranean, aiming at reinforcing the common act of the partners, to facilitate the development of a new conception for regional security. CEMRES provides experts and researchers from Europe and the Maghreb a space to exchange experiences and works on solutions to common security problems, to contribute towards the strengthening of confidence-building measures by producing an objective research activity, highlighting the real causes of insecurity and the key issues and strategic challenges facing the Western Mediterranean.

A key challenge for the governments (societies) is how to respond to natural disasters and emergency cases in ways that foster just and sustainable outcomes that build resilience, respect human rights, and foster economic, social, and cultural well-being in reasonable timeframes and at reasonable costs.

Disasters take various forms ranging from natural disasters, such as windstorms, wildfire to man-made disasters, such as workplace violence, and happen on a far too frequent basis. No matter what type of disaster befalls individuals, organizations, or countries, the results are typically the same, i.e., substantial loss of life, assets, productivity, and security threats.

While the Covid-19 outbreak is making an impact on a global scale, the collective response to the pandemic becomes the key to, evaluating current measures and formulating future predictions. Intervention to address disasters has evolved through time into a complex policy subsystem, and disaster policy is implemented through a set of functions known as emergency management and response. Modern approaches to emergency management and response involve multidimensional efforts to reduce our vulnerability to hazards; to diminish the impact of disasters; and to prepare for, respond to, and recover from those that occur.

The mandate of the research team provided by 5+5 nations was to deliver an academic study highlighting the repercussions of natural disasters, and epidemics on the security of 5 + 5 countries: "means of cooperation and mutual support".

Consequently, two main axes were identified and addressed by the analysis of the repercussions on 5+5 space security, and collective response, to relevant issues.

The report offers conclusions from each axis and a dedicated chapter with a synthesis of recommendations in terms of cooperation, in the "5 + 5" space, from which the following should be stressed:

- Creation of a 5+5 early warning center to promote the exchange of experience and expertise;

[63] AA.VV. editor Salem Shanbr (2021), *The repercussions of natural disaster, epidemics and pandemics on the security of 5 + 5 countries: "means of cooperation and mutual support*, CEMRES, Tunis.

- Encourage to support cooperation, coordination, and exchange of information between 5+5 countries;
- Develop instructional and awareness material that can be translated and used in national initiatives;
- Promote training and exercises initiatives;
- Promote scientific research projects;
- Promote Lessons Learned capabilities;
- Support the development of [disasters/epidemics] Emergency Response Plans.

From this research study, other recommendations can be elicited at the national level and further research initiatives may be pursued from the extensive bibliography that was used or topics that were not thoroughly addressed.

BIBLIOGRAPHY

- *AA.VV. (2018) Al Qaeda and Islamic State Affiliates in Afghanistan*, Congressional Research service, In Focus 7-5700, 23 agosto 2018.
- *AA.VV. (2021) Terrorist Groups in Afghanistan*, Congressional Research service, In Focus IF10604, 17 agosto 2021
- AA.VV. *The Human Cost, The consequences of insurgent attacks in Afghanistan*, Human Rights Watch, Vo. 19, N. 6(C), aprile 2007, p. 14.
- Alberts D.S., Garstka J.J., and Stein F.P. (1999)*, Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised).
- Avis W. (2020), *The COVID-19 pandemic and response on violent extremist recruitment and radicalisation*, H4D, Helpdesk Report, University of Birmingham. In https://reliefweb.int/sites/reliefweb.int/files/resources/808_COVID19%20_and_Violent_Extremism.pdf.
- Basileo Deborah (2020), *Tra Cyberterrorism e guerra dell'informazione. Scarsa consapevolezza e limiti normativi*, in #ReaCT2020, 1° rapporto sul terrorismo e il fondamentalismo in Europa, ed. START InSight.
- Bertolotti C. (2015), *NIT: Il 'Nuovo Terrorismo Insurrezionale'. Dalla '5+5 Defense Initiative 2015' il cambio di approccio alla minaccia dello Stato islamico*, Analysis ISPI n. 292.
- Bertolotti C. (2021), *Introduction: terrorism at the time of Covid-19*, in #ReaCT2021 – 2nd Report on Radicalization and Counter Terrorism, START InSight & Formiche. In https://www.startinsight.eu/en/react2021-2report-en/.
- Bertolotti C. (2022) *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).
- Bertolotti C., Sulmoni C. (2021), *How the Twenty-Year Afghanistan War Paved the Way for New Insurrectional Terrorism*, in Carenzi S., Bertolotti C. (2021) "Charting Jihadism Twenty Years After 9/11", Dossier ISPI, 11 settembre 2021.
- Bertolotti Claudio (2018), *Artificial Intelligence and the evolution of warfare. Report on 8th Beijing Xiangshan Forum*, START InSight, November 6th, in https://bit.ly/2zQeuLO.
- Bertolotti Claudio (2018), *The military applications of Artificial Intelligence. A focus on the 8th Beijing Xiangshan Forum (24-26 October 2018)*, START InSight, November 4th, in https://bit.ly/2EnPdfH.
- Bertolotti Claudio (2021), *Immigrazione e terrorismo: legami e sfide*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Bertolotti Claudio (2021), *Numeri e profili dei terroristi jihadisti in Europa*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Boulanin Vincent (2018), Stockholm International Peace Research Institute (SIPRI), in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on *Swarming and Machine Teaming*, Thun, Switzerland, November 21st.
- Bressan Matteo (2021), *L'esperienza del Kosovo nel rimpatrio dei foreign fighters: lessons learned*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Casini Enrico (2021), *L'attacco di Vienna e la pista balcanica*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- cellphones of journalists, activists worldwide, The Washington Post, July 18.
- Cochi Marco (2021), *Il jihadismo femminile in Africa. Il ruolo delle donne all'interno di Boko Haram e al-Shabaab*, START InSight, Lugano – Svizzera.

- Crosston M., *The Millenials' war: dilemmas of network dependency in today's military*, "Defense & Security Analysis", 33:2, 2017, pp. 94-105.
- Danzig Richard (2014) 'Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies', Center for a New American Security.
- European Commission (2021). *Joint communication to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions*, 9 February 2021. In https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021JC0002&rid=2.
- Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.
- Giustozzi A. (2009), Decoding the New Taleban, C. Hurst & Co. Publishers Ltd, London.
- Hagström Martin (2018), FOI - Swedish Defence Research Agency, in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21*st*.
- INTERPOL (2020). *COVID-19 impact on migrant smuggling and human trafficking*, 11 June 2020. In https://www.interpol.int/News-and-Events/News/2020/COVID-19-impact-on-migrant-smuggling-and-human-trafficking.
- Mazoomdaar Jay (2021), Explained: Here's how NSO Group's spyware Pegasus infects your device, The Indian express July 22, New Delhi.
- PAM (2021), *Covid-19 Pandemic and Food Security in the PAM region*. In https://www.pam.int/welcome.asp?m=news&id=904.
- Priest Dana, Timberg Craig, Mekhennet Souad (2021), Private Israeli spyware used to hack
- Rickli Jean-Marc (2018), Geneva Center for Security Policy (GCSP), in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21*st*.
- Robinson T. (2010), *It's the Network, Stupid! Air Power and Network Centric Warfare – Trends and Challenges*, "Military Technology", 40–8.
- Ruttig T. (2012) *How tribal are the Taleban*, in Bashir S. and Crews R.D., "Under the Drones. Modern Lives in the Afghanistan-Pakistan Borderlands", Harvard 2012.
- Schneider Jacquelyn (2019) The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war, Journal of Strategic Studies, 42:6, 841-863, DOI: 10.1080/01402390.2019.1627209. In: https://doi.org/10.1080/01402390.2019.1627209.
- Sulmoni Chiara (2021), *Estremismo di matrice jihadista in Europa. Il concetto e l'importanza della prevenzione e del contrasto*, in #ReaCT2021, 2° rapporto sul radicalismo e il terrorismo in Europa, ed. START InSight e Formiche, Lugano-Roma 2021.
- Tor Uri (2017) 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, Journal of Strategic Studies, 40:1-2, 92-117, DOI: 10.1080/01402390.2015.1115975. In: https://doi.org/10.1080/01402390.2015.111597
- Van Ostaeyen P. (2020), The Islamic State and Coronavirus, Time for a Comeback? ISPI, Milan. In https://www.ispionline.it/it/pubblicazione/islamic-state-and-coronavirus-time-comeback-26166
- Woodhams George (2018), UNIDIR Security and Society Programme, in Sulmoni Chiara (2018) *12 perspectives on swarming*, Report START InSight for Armasuisse S+T, Workshop on Swarming and Machine Teaming, Thun, Switzerland, November 21*st*.
- Xinhua, *Number of Afghan Insurgent Grow Rapidly Since 2006*, in Daily outlook Afghanistan, 11 ottobre 2009.

L'*Osservatorio Strategico* è uno studio che raccoglie analisi e report sviluppati dall'Istituto di Ricerca e Analisi della Difesa (IRAD), realizzati da ricercatori specializzati.
Le aree di interesse monitorate nel 2021 sono:

- Balcani e Mar Nero;
- Mashreq, Gran Maghreb, Egitto ed Israele;
- Sahel, Golfo di Guinea, Africa Subsahariana e Corno d'Africa;
- Cina, Asia meridionale ed orientale e Pacifico;
- Russia, Asia centrale e Caucaso;
- Golfo Persico;
- Area Euro/Atlantica (USA-NATO-Partners);
- Politiche energetiche;
- Sfide e minacce non convenzionali.

Gli elaborati delle singole aree, articolati in analisi critiche e previsioni, costituiscono il cuore dell'"Osservatorio Strategico"**.**

The "Osservatorio Strategico" is a survey that collects, analyses and reports developed by the Defense Research and Analysis Institute (IRAD), carried out by specialized researchers.

The areas of interest monitored in 2021 are:

- The Balkans and the Black Sea;
- Mashreq, Gran Maghreb, Egypt and Israel;
- Sahel, Gulf of Guinea, sub-Saharan Africa and Horn of Africa;
- China, Southern and Eastern Asia and Pacific;
- Russia, Central Asia and the Caucasus;
- Persian Gulf;
- Euro/Atlantic (USA-NATO-Partners);
- Energy policies: interests, challenges and opportunities;
- Challenges and unconventional threats.

The heart of the "Osservatorio Strategico" consists of the scripts regarding the individual areas, divided into critical analyses and forecasts.

Stampato dalla Tipografia del Centro Alti Studi per la Difesa

———————————

Printed by Typography of the Center for High Defence Studies

ISBN 979-12-551-5015-2