ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

20

ISSUE 2/2024

Milano 2024

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 20/2024

Direttore Responsabile:

Matteo Vergani (Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou (Lecturer at National Security School – Atene)
Cristian Barna ("Mihai Viteazul" National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti (senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies – Roma)
Valerio de Divitiis (Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio (Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel (London School of Economics – London)
Rovshan Ibrahimov (Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler (German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš (Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi (Università Cattolica del Sacro Cuore – Milano)
Anita Perešin (University of Zagreb – Croatia)
Giovanni Pisapia (Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj (University of Ljubljana)
Eman Ragab (Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli (Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick (University of Aarhus – Denmark)
Arturo Varvelli (Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz (Independent Researcher – Turkish National Police)
Munir Zamir (Fida Management&C7 – London)
Sabina Zgaga (University of Maribor – Slovenia)
Ivo Veenkamp (Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni (Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa (Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini (Università Cattolica del Sacro Cuore – Milano)
Marco Maiolino (Università Cattolica del Sacro Cuore – Milano)
Davide Scotti (Università Cattolica del Sacro Cuore – Milano)

© 2024 EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 979-12-5535-352-2

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

TERRORISM, WARFARE, INTELLIGENCE, STRATEGIC COMMUNICATION, CRISIS MANAGEMENT AND TECHNOLOGICAL ADVANCEMENTS AT THE CROSSROAD

FRONTIER PERSPECTIVES

Terrorism, warfare, intelligence, strategic communication, crisis management and technological advancements at the crossroad

Lo spazio tra esigenze strategiche e di sicurezza

Beatrice Cascone

Beatrice Cascone professionista nel settore spaziale, laureata con lode all'Università Cattolica del Sacro Cuore di Milano. Ha arricchito la sua formazione partecipando ad una Summer School presso l'ESA a Budapest, dove ha vinto il premio per il miglior paper. Successivamente, ha conseguito un master in politiche spaziali presso l'Agenzia Spaziale Italiana e SIOI, e un ulteriore master in imprenditoria spaziale presso l'EIIS. Attualmente, Beatrice ricopre il ruolo di project manager and control officer all'Agenzia Spaziale dell'Unione Europea (EUSPA) a Praga, contribuendo attivamente allo sviluppo di progetti innovativi in ambito spaziale.

Abstract

The space sector is characterized by the presence of several terminologies related to security outside the Earth's atmosphere. Militarization of space refers to the use of space-based devices to improve the military effectiveness of conventional forces, while weaponization of space refers to the placement of space-based weapons in orbit. Important steps have been taken throughout history to limit the use of weapons in space, but the concept of anti-satellite weapons continues to raise concerns for international relations.

Recent decades have seen an increase in the use of satellites for both military and civilian purposes. The use of satellites has made it possible to detect military secrets, monitor military installations and the presence of vehicles, and monitor possible ballistic missile deployment zones. In addition, satellites have provided real-time information and enhanced situational awareness to make decisions about potential risk factors and timely responses. The use of satellite data has proven essential for meteorological purposes, with the goal of preventing natural disasters, planning agricultural activities and monitoring natural resources. Remote sensing satellites, on the other hand, have made it possible to observe the Earth and detect data on the Earth's surface, helping to assess agricultural yields, monitor forests and the environment. These developments have shown how the use of satellites has become increasingly important in meeting global security and defense needs.

Satellite telecommunications allow communication between different geographical locations and are used for commercial and military purposes. Early warning satellites detect ballistic missile launches or nuclear explosions. Navigation satellites enable geolocation and remote munitions guidance. Europe developed the Eutelsat satellite system and the Galileo navigation system to provide independence in navigation. The integration of space into European policy and defense has been pursued through collaboration between the European Union and the European Space Agency, despite institutional differences. European space policy has focused on the security, defense and welfare of European citizens. Cooperation between civil and military space has been promoted to ensure greater security and prevent humanitarian crises.

Il settore spaziale si caratterizza per la presenza diverse terminologie legate alla sicurezza al di fuori dell'atmosfera terrestre. La militarizzazione dello spazio si riferisce all'utilizzo di dispositivi spaziali per migliorare l'efficacia militare delle forze convenzionali, mentre la weaponization of space si riferisce al posizionamento di armi spaziali in orbita. Nel corso della storia sono stati compiuti importanti passi per limitare l'uso di armi nello spazio, ma il concetto di armi anti-satellitari continua a suscitare preoccupazioni per le relazioni internazionali.
Negli ultimi decenni si è assistito a un aumento dell'utilizzo dei satelliti sia a scopi militari che civili. L'utilizzo di satelliti ha permesso di rilevare segreti militari, monitorare le installazioni militari e la presenza di veicoli, nonché di controllare le possibili zone di schieramento di missili balistici. Inoltre, i satelliti hanno fornito informazioni in tempo reale e una maggiore consapevolezza situazionale per prendere decisioni in merito a potenziali fattori di rischio e risposte tempestive. L'utilizzo dei dati satellitari si è dimostrato essenziale per scopi meteorologici, con l'obiettivo di prevenire catastrofi naturali, pianificare attività agricole e monitorare le risorse naturali. I satelliti di telerilevamento hanno invece consentito di osservare la Terra e rilevare dati sulla superficie terrestre, contribuendo alla valutazione delle rese agricole, al monitoraggio delle foreste e dell'ambiente. Questi sviluppi hanno dimostrato come l'utilizzo di satelliti sia diventato sempre più importante per soddisfare le esigenze di sicurezza e difesa globali.
Le telecomunicazioni satellitari permettono di comunicare tra diverse posizioni geografiche e sono utilizzate per scopi commerciali e militari. I satelliti di allarme precoce rilevano lanci di missili balistici o esplosioni nucleari. I satelliti di navigazione permettono di geolocalizzarsi e guidare munizioni a distanza. L'Europa ha sviluppato il sistema satellitare Eutelsat e il sistema di navigazione Galileo per garantire un'indipendenza nella navigazione. L'integrazione dello spazio nella politica e nella difesa europea è stata perseguita con la collaborazione tra l'Unione Europea e l'Agenzia Spaziale Europea, nonostante le differenze istituzionali. La politica spaziale europea si è concentrata sulla sicurezza, la difesa e il benessere dei cittadini europei. La cooperazione tra spazio civile e militare è stata promossa per garantire una maggiore sicurezza e prevenire crisi umanitarie.

Keywords

Spazio, armi, sicurezza, Unione Europea, difesa, space, weapons, security, European Union, defense

1. Introduzione: differenza tra Weaponization e Militarization

Nell'ambito spaziale ci sono diversi termini che vanno a identificare l'ambito sicurezza al di fuori della nostra atmosfera. In primo luogo, possiamo denotare le differenze tra i seguenti termini: *weaponization e militarization* dello spazio extra-atmosferico. La "militarizzazione dello spazio", in inglese militarization, fa riferimento all'utilizzo di diversi dispositivi che hanno base nello spazio allo scopo di aumentare l'efficacia militare di forze convenziona-

li, individuando gli usi militari attualmente ritenuti leciti[1]. La weaponization of space, invece, fa riferimento al posizionamento in orbita di "armi spaziali"[2]. Nel corso della storia sono stati compiuti importanti passi in termini di accordi bilaterali tra le potenze spaziali, Stati Uniti e Russia, in particolare in materia di difesa antimissilistica. Per comprendere al meglio la situazione, bisogna menzionare l'Anti-Ballistic Missile Treaty (ABM) del 1972, concluso alla fine dei negoziati SALT (Strategic Arms Limitation Talks), che vietava la sperimentazione e lo sviluppo di un sistema di difesa, volto a intercettare missili strategici nella traiettoria di volo, che si avvaleva di sistemi ABM collocati al di fuori dell'atmosfera per la difesa del territorio nazionale[3]. Venne successivamente denunciato dall'amministrazione Bush nel 2001[4] e successivamente da Mosca nel 2007. Tuttavia, il trattato anti-ABM aveva già vissuto un periodo di crisi in seguito all'annuncio dell'allora presidente statunitense Ronald Reagan di un sistema di difesa globale denominato SDI, Strategic Defense Initiative, detto anche Star Wars Program, successivamente abbandonato per gli enormi costi della sua realizzazione. Di conseguenza, vennero proposti altri trattati successivi all'ABM come il *Trattato per la proibizione dello stazionamento di armi di qualsiasi tipo nello spazio*, presentato nel 1981 all'Assemblea Generale dall'URSS, e il *Trattato sulla proibizione dell'uso e della minaccia dell'uso della forza nello spazio extra-atmosferico* del 1983.

Nel corso della storia ci sono stati altre limitazioni e divieti nei confronti dei sistemi anti-satellitari (ASAT), un tema che ha riscosso molta attenzione nella comunità internazionale la quale ha iniziato a interrogarsi sulla possibilità che il lancio di armi anti-satellitari, pur non esplicitamente vietato, possa comunque implicare una weaponization of space, rappresentando così un fattore altamente destabilizzante per quanto riguarda le relazioni internazionali. Più che una vera e propria arma questa va considerata come un'operazione meramente politica, il cui scopo è creare allarmismo ingiustificato verso il possibile uso di strutture spaziali come armi, ottenendo così uno

[1] Matthew Mowthorpe, The Militarization and Weaponization of Space, Lanham, Lexington Books, 2004. p. 3.

[2] Tuttavia, ad oggi non esiste una chiara definizione di cosa debba intendersi per veicolo spaziale militare. Natalino Ronzitti, "Problemi giuridici sollevati dalle iniziative in materia di disarmo spaziale", op. cit., p. 80. In questo senso anche la Commissione per il Disarmo delle Nazioni Unite, "Report of the Ad Hoc Committee on the Prevention of an Arms.

[3] Ibidem. V. anche Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-ballistic Missile Systems, opened to signature at Moscow, 26 May 1972, http://www.state.gov/www/global/arms/treaties/ abm/abm2.html.

[4] Con effetto dal 13 giugno 2002. Per il testo della nota diplomatica inviata dal governo Usa alle altre parti contraenti http://www.dod.gov/acq/acic/treaties/abm/ ABMwithdrawal.htm.

strumento di pressione tra Stati[5]. Le applicazioni satellitari utilizzate a scopi militari rappresentano temi attuali nel diritto internazionale dello spazio e che ancora oggi analizzati. Il punto principe delle diverse interpretazioni del concetto di "usi pacifici" sembra rappresentato dall'utilizzo di quello che le due superpotenze (Stati Uniti d'America e Russia) identificano come "mezzi nazionali di verifica" come, per esempio, gli strumenti satellitari per il riconoscimento dall'alto.

Per evitare una possibile militarizzazione dello spazio e conseguentemente una vera e propria "guerra spaziale", si fece riferimento all'importanza delle diverse attività di riconoscimento per mezzi satellitari dotati di natura essenzialmente difensiva e quindi militare. Solo in un secondo momento storico gli Stati riconobbero unanimemente l'assoluta liceità dell'uso di satelliti per il riconoscimento dall'alto. Da quel preciso momento l'osservazione via satellite ha avuto un ruolo fondamentale per il mantenimento degli equilibri strategico-militari, come accadde nella fase iniziale della crisi di Cuba. Lo status giuridico di tutte queste attività di monitoraggio e di controllo per diverse informazioni è stato oggetto di attenzione da parte delle Nazioni Unite, a partire dalla Conferenza sugli usi pacifici dello spazio extra-atmosferico tenutasi a Vienna nel 1968[6].

Se invece ora dovessimo prendere in considerazione il collocamento del satellite nello spazio, va rilevato in primo luogo che la sovranità dello Stato territoriale non si estende al di sopra dell'atmosfera. Lo spazio e tutti i corpi celesti, inclusa la Luna, hanno la possibilità di essere esplorati in maniera libera da parte di ogni Stato; come enunciato dall'articolo I del Trattato sullo Spazio Extra-atmosferico[7].

Gli usi militari dello spazio possono essere considerati leciti purché coerenti con l'articolo IV del Trattato sullo Spazio Extra-atmosferico e con l'articolo 2 paragrafo 4 della Carta delle Nazioni Unite. Sono quindi consentiti solo usi militari "passivi", ovvero uso di sistemi spaziali a sostegno di operazioni militari basate a Terra, mentre è vietata la weaponization of space.

[5] Bertrand de Montluc, "The New International Political and Strategic Context for Space Policies", in Space Policy, Vol. 25, No. 1 (February 2009), p. 22 nonché Giovanni B. Andornino, Dopo la muraglia. La Cina nella politica internazionale del 21. secolo, Milano, Vita e pensiero, 2008, pp. 302-307.

[6] Dal punto di vista del diritto consuetudinario è assente una norma precisa.

[7] Le parti di questa dichiarazione erano il Brasile, la Colombia, il Congo, l'Ecuador, l'Indonesia, il Kenya, l'Uganda e lo Zaire, che nell'esprimere tali rivendicazioni si ispirarono al "principio dell'hinterland" che, al tempo delle scoperte geografiche, attribuiva a chi possedesse la costa il diritto di rivendicarne le regioni interne. Editoriale, Assalto al cielo, in Limes n. 5/2004, p. 19.

Partendo dal lancio del primo Sputnik, i sistemi militari sono stati migliorati sia da un punto di vista quantitativo che qualitativo, fino al punto che nei successivi dieci anni, ossia fino all'entrata in vigore del Trattato sullo spazio Extra-atmosferico (Outer Space Treaty - OST), i satelliti erano già parte integrante del sistema di difesa USA e URSS.

Durante la Guerra Fredda vennero impiegati tali satelliti per identificare gli obiettivi nemici, monitorando, controllando e verificando gli armamenti attraverso modalità non "intrusive"[8]. I primi furono gli Stati Uniti che misero in pratica diversi programmi satellitari come il Corona, Samos (Satellite and Missile Observation System) e il Discover. Quest'ultimo aveva come obiettivo quello di rilevare segreti militari, ma in un secondo momento venne utilizzato anche per scopi civili. Successivamente moltissimi Stati cercarono di sviluppare propri sistemi satellitari per l'osservazione o di acquistare satelliti di osservazione commerciale. Bisogna anche sottolineare che i satelliti militari avevano una definizione molto più alta di quella per uso civile, caratterizzata da una risoluzione più bassa. Dagli anni Novanta in poi, grazie alla rivoluzione informatica e delle telecomunicazioni, si registrarono importanti investimenti nel settore privato per l'utilizzo commerciale di satelliti. Col passare del tempo i due sistemi si integrarono in satelliti dual use, utilizzati sia per scopi militari che per scopi commerciali.

Si iniziò a parlare di prima guerra spaziale solo successivamente alla Guerra del Golfo, che mise in evidenza le diverse potenzialità delle applicazioni spaziali per la condotta delle operazioni, dimostrando la loro centralità in tutte le tipologie di operazioni militari, veri "moltiplicatori di forza" a supporto di tutte le operazioni terrestri. I satelliti, infatti, riescono a rilevare dall'alto tutte le possibili installazioni militari, i diversi veicoli, movimenti di truppe e riescono a controllare le possibili zone di schieramento di missili balistici che potrebbero essere attivati da un momento all'altro, fornendo anche dei possibili ponti radio per mettere in comunicazione, in tempo reale e a lunghissima distanza, differenti paesi. Tutto questo consente una maggiore consapevolezza situazionale ed un efficace coordinamento delle informazioni sulle minacce[9].

Da un punto di vista politico, avere satelliti che controllano la Terra e le possibili minacce, avere informazioni e dati in tempo reale, permette di pren-

[8] William E. Burrows, "Imaging Space Reconnaissance Operations During the Cold War: Cause, Effect and Legacy", in Bodø Regional University, Cold War Forum, February 1997, http://webster.hibo.no/asf/Cold_War/report1/williame.html.

[9] Association aéronautique et astronautique de France (3AF) Strategy and Interna- tional Affairs Commission - Writers' Group, "The Militarization and Weaponization of Space: Towards a European Space Deterrent", op. cit.

dere decisioni su un quadro costantemente aggiornato dei potenziali fattori di rischio e di valutare globalmente tutte le possibili risposte tempestive.

Considerando il nostro periodo storico, notiamo come la flessibilità di utilizzo, l'accesso globale e il carattere intrusivo ha reso tutte queste applicazioni spaziali sempre più utili per le esigenze di sicurezza e difesa del XXI secolo. Non ci si può focalizzare esclusivamente sulla difesa del territorio nazionale dal momento che negli anni si sono moltiplicati i diversi impegni in teatri esterni funzionali alla tutelare degli interessi nazionali[10]. Di fronte a minacce sempre poco chiare e indefinite, ma soprattutto provenienti da attori non identificati come Stati, è essenziale poter contare sulle informazioni a disposizione sia sul proprio territorio nazionale che nelle aree esterne[11]. Non bisogna considerare i dati satellitari e tutte le informazioni che ci offre lo spazio come le migliori, considerando che in precisi scenari o determinate fasi di crisi di possono preferire altri strumenti che sono in grado di agire sul campo in maniera molto più immediata e con costi sicuramente inferiori. Ci sono diversi strumenti spaziali che sono essenziali per particolari situazioni e servizi come:

– *Meteorologia*: essa costituì uno dei primi veri e propri utilizzi di telerilevamento[12]. L'Assemblea Generale delle Nazioni Unite, una risoluzione del 1962, ne auspicò lo sviluppo in quanto strumento essenziale per il beneficio del genere umano, basti pensare all'agricoltore il quale deve essere a conoscenza del meteo futuro per poter pianificare le situazioni, agli operatori spaziali che hanno la necessità di pianificare per tempo i futuri lanci, ma agli stessi scienziati e studiosi che devono prevenire le possibili catastrofi naturali[13]. Un'attenzione particolare alla meteorologia si registrò a partire dalla Seconda Guerra Mondiale grazie all'incremento di nuovi strumenti come i radar. Fu proprio così che intorno agli anni Sessanta nacquero dei programmi specifici sia statunitensi che sovietici che riuscirono a migliorare sempre di più, fino ad oggi, la situazione climatica e l'accuratezza delle previsioni meteo.

[10] Ad esempio, per prevenire o mitigare i rischi per gli interessi nazionali, salvaguardare le direttrici commerciali e di approvvigionamento energetico. V. Michele Nones, Alberto Traballesi (a cura di), Applicazioni spaziali civili di possibile interesse della difesa, Roma, Informazioni della difesa, 1998 (Collana del Centro Militare di Studi Strategici [serie blu], 91), p. 21.

[11] Ibidem, p. 20. V. anche Report of the Panel of Experts on Space and Security, March 2005, pp. 8-10, http://ec.europa.eu/enterprise/policies/space/files/article_2262.pdf. V. anche Nina Louisa Remuss, Nato and Space: Why is Space Relevant for Nato?, op. cit.

[12] Pierre-Marie Martin, Droit des Activités Spatiales, op. cit., p. 173.

[13] UN General Assembly, Resolution No. 1802 (XVII), International cooperation in the peaceful uses of outer space, (A/RES/1802(XVII), 14 December 1962.

I satelliti meteorologici ruotano intorno all'orbita geostazionaria, confermando l'importanza di tale orbita fin da quando venne lanciato il primo satellite Applications Technology Satellite (ATS-1) da parte della NASA nel 1966[14]. Per quanto concerne i satelliti meteorologici, il primo fu Tiros 1 (Television and Infrared Operational Satellite), che inviò la prima immagine nel 1960, tre anni dopo il lancio del primo satellite Sputnik[15].

Il primo satellite meteorologico europeo denominato Meteosat sarà lanciato 17 anni dopo, nel 1977, e sarà il primo satellite europeo ad essere messo in orbita. Anche se di origine europea, tale satellite fu realizzato all'interno di un programma internazionale (Global Atmospheric Research Programme Garp) promosso dall'Organizzazione meteorologica mondiale che solo in un secondo momento l'Agenzia Spaziale Francese CNES decise di "europeizzare" con il progetto Meteosat, condotto ai tempi dall'Esro[16]. Ad oggi siamo arrivati fino alla terza generazione di Meteosat.

I satelliti meteorologici, inoltre, forniscono dati in grado di effettuare rilevamenti cartografici ad alta risoluzione della superficie terrestre[17]. Le immagini che vengono catturate sono importanti per comprendere al meglio la morfologia terrestre e le diverse condizioni, costituendo un elemento chiave per il soddisfacimento di tutte quelle esigenze di sicurezza, di gestione delle risorse e della sorveglianza, e per l'impiego di satelliti di telerilevamento. Questi sono importanti soprattutto nel campo dell'intelligence con scopi di ricognizione e sorveglianza della situazione, riuscendo a elaborare situazioni sempre aggiornate[18].

– *Telerilevamento*: i satelliti di telerilevamento sono in grado di osservare la terra e rilevare dati sulla superficie terrestre per mezzo di sensori ottici o radar. All'inizio erano semplicemente satelliti dotati di sensori ottici in grado di osservare l'energia riflessa attraverso varie lunghezze d'onda. Più

[14] Donald C. Ahrens, Meteorology Today. An Introduction to Weather, Climate, and the Environment, 8th ed., Thomson/Brooks/Cole, 2007, p. 18.

[15] La prima fotografia dallo spazio della copertura nuvolosa della Terra da parte di un satellite non dedicato era avvenuta invece già nel 1959, grazie al Vanguard II della Nasa, http://www.metoffice.gov.uk/science/creating/first_steps/obs_space_history.html.

[16] L'Esro, European Space Research Organisation, è stata formalmente stabilita da dieci paesi europei nel 1964, con l'Accordo di Parigi, allo scopo di sviluppare la collaborazione spaziale tra gli Stati Membri per la ricerca e la tecnologia spaziale, restando escluse le applicazioni pratiche della tecnologia spaziale. Per la costruzione di vettori di oggetti spaziali nacque invece l'Eldo (European Launcher Development Organisation).

[17] Introduzione, Esa Eduspace, http://www.esa.int/esaMI/Eduspace_IT/SEMWUWKXB1G_0.html.

[18] Michele Nones, Alberto Traballesi (a cura di), Applicazioni spaziali civili di possibile interesse della difesa, op. cit., pp. 29-30.

viene emessa l'energia adeguata attraverso la lunghezza d'onda più si ha la possibilità di penetrare le nubi e la foschia acquistando anche immagini notturne. Il più importante satellite per il telerilevamento è quello statunitense Landasat-1 del 1972, che venne utilizzato dalla Commissione delle Comunità Europee come strumento per osservare tutte le diverse esigenze collegate alla valutazione delle rese agricole e il monitoraggio dei boschi e foreste[19]. Da questo momento iniziarono diverse ricerche per un nuovo sviluppo tecnologico che vide la luce nel 2002 quando venne lanciato Envisat, il più grande satellite artificiale per l'osservazione mai costruito in Europa[20].

Tutte le diverse attività francesi nel campo dei sensori per l'Osservazione della Terra iniziarono intorno agli anni Settanta per ridurre la dipendenza dai satelliti americani. Il primo programma francese, il Samro (Satellite Militaire de Reconnaissance Optique), venne sostituito da un nuovo programma denominato HELIOS, il cui primo satellite venne lanciato nel 1995, la cui funzione principale era strategica e di intelligence[21]. Tale programma segnò la collaborazione tra Francia, Spagna e Italia. Quest'ultima iniziò ad interessarsi all'Osservazione della Terra attraverso mezzi satellitari. Ad oggi il sistema italiano per l'Osservazione della Terra, denominato Cosmo-SkyMed (Constellation of Small Satellites for the Mediterranean basin Observation), è nato con lo scopo di osservare interamente il suolo italiano e il bacino del Mediterraneo a causa del coinvolgimento delle forze armate italiane nei continui conflitti esterni collocati in quell'aerea. Vediamo quindi come il sistema Cosmo-SkyMed ha dimostrato di essere dual use, creato per ottimizzare le risorse disponibili di fronte al declino dei budget della Difesa e in un secondo momento si è rivelato una strategia vincente, in grado di fornire sostegno sia pubblico che privato all'industria spaziale[22].

[19] Raymond Klersy, "The Work and Role of the Commission of the European Com- munities", in International Journal of Remote Sensing, Vol. 13, Nos. 6-7 (1992), pp. 1035- 1058.

[20] Envisat Overview, ESA website, http://www.esa.int/export/esaEO/SEMWYN2VQUD _ index_0_m.html. V. anche Antonio Daniele, "Perfettamente riuscito il lancio di ENVISAT", in Rivista aeronautica, a. 78, n. 3 (maggio-giugno 2002), pp. 102-105.

[21] È significativo che quella che era iniziata come cooperazione industriale trilaterale tra Francia, Italia e Spagna, si è poi trasformata in cooperazione operativa in un campo in cui la cooperazione è tradizionalmente rara: quello dell'intelligence. http://www. assembly-weu.org/en/documents/sessions_ordinaires/rpt/2004/1881.php.

[22] Marco Cervino, Barbara Corradini, Silvio Davolio, "Uso pacifico dello spazio: un principio ormai accantonato?", in Scienza e Pace, paradigmi e pratiche a confronto, Workshop scientifico, Modena, 10 Novembre 2003, p. 33, http://www.bo.cnr.it/www- sciresp/OLD/GdL/SciMil/Workshop_Modena/ATTI/Atti_MO.pdf.

– *Telecomunicazioni*: le telecomunicazioni satellitari funzionano perché garantiscono un collegamento tra i diversi centri di comando e unità periferiche, assicurando la possibilità di comunicare tra persone e mezzi anche se la loro geolocalizzazione è differente[23]. Questa tipologia di satelliti riceve e trasmette una quantità esorbitante di segnali. Il sistema di telecomunicazioni che impiega satelliti è un vero e proprio ponte radio tra due stazioni terminali a terra.
  Durante il governo Kennedy, un consorzio di undici paesi si riunì per far nascere Intelsat (International Telecommunication Satellite Organization) con il fine ultimo di realizzare un sistema commerciale mondiale unico di comunicazioni[24]. L'Europa, che desiderava fortemente affermarsi in tale ambito, decise di dare vita ad un programma Eutelsat, nato nel 1959, primo sistema satellitare di telecomunicazioni in Europa.
– *Early Warning*: elemento fondamentale per le funzioni di intelligence[25], con la capacità globale e permanente di lanciare un allarme in modo tempestivo ed immediato in caso di azioni aero-terrestri dell'avversario, esplosioni nucleari o lanci di missili balistici[26]. I satelliti per l'allarme precoce, infatti, si avvalgono di sensori sensibili alle forti emissioni di energia proprio nella fase di combustione del lancio di missili balistici[27]
– *Navigazione*: un elemento fondamentale è geolocalizzarsi all'interno del globo terrestre, oltre alle che una delle più grandi esigenze militari. La geolocalizzazione è per tanto essenziale per la logistica, per tracciare armi o posizioni del nemico ma soprattutto permette di guidare munizioni a distanza aumentando così l'efficacia dell'attacco e minimizzando i danni collaterali[28]. Oltre alla possibilità di geolocalizzarsi, tali satelliti permetto-

[23] Francesco Borrini, La componente spaziale nella difesa, op. cit., p. 27.
[24] Pierre-Marie Martin, Droit des Activités Spatiales, op.cit., pp. 136-137. V. anche George Huang, "International Satellite Organizations Facing the Challenge: Intelsat and Inmarsat", in Singapore Journal of International and Comparative Law, Vol. 3, No. 1 (1999), p. 196.
[25] Intelligence Spazio E Trend2040.
[26] Anil K. Maini, Varsha Agrawal, Satellite Technology: Principles and Applications, UK, John Wiley & Sons, Ltd, Chichester, 2006, p. 536. V. anche Assemblée Européenne de Sécurité et de Défense, Assemblée de l'Union de l'Europe Occidentale, cinquantehuitième session, L'espace militaire: les satellites d'alerte avancée et de renseignement électromagnétique - Réponse au rapport annuel du Conseil, Rapport présenté au nom de la Commission technique et aérospatiale par M. Yves Pozzo di Borgo, rapporteur (France, PPE/DC), 17 juin 2010, Document A/2071, p. 13.
[27] Michele Nones, Alberto Traballesi (a cura di), Applicazioni spaziali civili di possi- bile interesse della difesa, op. cit.
[28] Gustav Lindström with Giovanni Gasparini, The Galileo Satellite System and its Security Implications, Paris, EU Institute for Security Studies, April 2003 (Occasional papers, 44), p. 7, http://www.iss.europa.eu/uploads/media/occ44_01.pdf.

no di identificare in maniera precisa gli oggetti fissi o in movimento, sia sulla superficie ma anche in atmosfera. Uno dei satelliti più importanti della navigazione satellitare è il GPS Navstar, che si compone di 24 satelliti in orbita circolari, posti su sei diversi piani orbitali, permettendo così di avere cinque o più satelliti visibili da ogni punto della Terra[29]. All'interno di ogni satellite, possiamo trovare quattro differenti orologi atomici che permettono di misurare in maniera precisa il tempo. I Navstar lanciati nel 2003 avevano all'interno un codice militare, detto anche M-code che era molto resistente ed era stato progettato per utilizzatori legati alla difesa, in grado di garantire un sistema di posizionamento preciso (PPS). Sul suolo terrestre è nata la necessità di costruire una base che permettesse di raccogliere tutti i dati delle stazioni e di compensarli tenendo conto dei possibili errori degli orologi all'interno dei satelliti. Contestualizzando la situazione, il primo vero sistema satellitare a fornire un posizionamento tridimensionale a livello mondiale è stato il GPS che ancora oggi è l'unico sistema di navigazione operativo poiché il programma russo Glonass è parzialmente disponibile[30]. Glonass (Globalnaya Navigatsionnaya Sputnikovaya Sistema) nacque nel 1976 per fornire la posizione e la velocità dei missili balistici russi[31]. I primi satelliti vennero lanciati nel 1982 e la sua operatività iniziò nel 1996. Erano 21 satelliti che erano dotati di una vita operativa in orbita di solo tre anni. Nel corso del periodo storico che gira intorno gli anni Novanta: GPS, Galileo e Glonass divennero interoperabili grazie a ricevitori comuni sintonizzati su due differenti sistemi. I russi si accorsero dell'immenso valore che aveva Glonass, tanto che nel 2001 approvarono un programma per ripristinare l'intero sistema.

Glonass venne originariamente costruito in contrapposizione al GPS americano e del sistema di posizionamento Galileo e analogamente a quest'ultimo contemplava un utilizzo civile, ma a causa di minor disponibilità economica il programma finì con il ridursi progressivamente fino ai pochi satelliti ancora attualmente attivi[32].

Relativamente all'Europa il programma Galileo, lanciato dalla Commissione Europea e dall'ESA nel 1999, permise un'indipendenza nella navi-

[29] Gustav Lindström with Giovanni Gasparini, The Galileo Satellite System and its Security Implications, op. cit., p. 10.

[30] Ferdinando Sguerri, "Galileo e la modernizzazione del Gps e del Glonass", in Rivi- sta aeronautica, a. 80, n. 3 (maggio-giugno 2004), p. 110.

[31] V. Bernd Eissfeller et al., "Performance of GPS, GLONASS and Galileo", op. cit., p. 190.

[32] Bastian Giegerich, "Navigating Differences: Transatlantic Negotiations over Galileo", in Cambridge Review of International Affairs, Vol. 20 No. 3 (September 2007), p. 492.

gazione satellitare[33]. Galileo è un sistema di costellazioni di 30 satelliti[34] distribuiti su tre differenti orbite medie, permettendo bassi rischi tecnici. Inoltre, è un servizio aperto, preciso e affidabile, integrando l'attività di ricerca e salvataggio per l'assistenza in caso di emergenza; con un servizio criptato e resistente ad interferenze riservato alle esigenze delle istituzioni pubbliche[35]. Il sistema Galileo è perfettamente integrabile con il sistema GPS e questo elemento è un punto di forza grazie ai diversi ricevitori pluri-banda, permettendo di basarsi su entrambe le costellazioni, nonché sugli stessi sistemi Glonass.

2. Integrazione dello spazio nella politica e nella difesa europea

Nel corso della storia le diverse istituzioni europee hanno mostrato interessi non sempre coincidenti riguardo attività spaziali pur riconoscendone sempre l'importanza economica come le telecomunicazioni e i trasporti, ma soprattutto mantenendo un focus per la difesa e la sicurezza nazionale e internazionale. Tutte le diverse normative e politiche adottate nel corso dei diversi avvenimenti storici, ha fatto si che le politiche europee, venissero indirizzate verso una sicurezza e una difesa comune, allo scopo di far affermare una leadership europea all'interno dello scenario globale.

L'avanzamento tecnologico e la consapevolezza strategica dello spazio hanno permesso di sviluppare nuove iniziative sia per scopi civili ma soprattutto militari[36] evitando di soccombere a possibili minacce future, valutando una corretta pianificazione operativa delle missioni e l'assunzione di decisioni strategiche di capacità di intelligence. Tutto questo ha permesso di avere a che fare con una maggiore sicurezza nei confronti dei cittadini europei, garantendo il controllo delle frontiere e la lotta al crimine internazionale al terrorismo, prevenendo possibili crisi umanitarie[37].

[33] Asi and the Galileo programme, A European navigation and positioning system" http://www.asi.it/en/flash_en/telecommunications/asi_and_the_galileo_ programme.

[34] Bruno Picerno e Francesco Brindisi (a cura di), Galileo vs Gps: collaborazione o confronto? Supplemento all'Osservatorio strategico No.7/2005, Centro militare di studi strategici, Roma, 2005, p. 33.

[35] Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Stato di avanzamento del programma Galileo, Gazzetta ufficiale delle Comunità europee 15.10.2002, [COM(2002) 518 def.], (2002/C 248/02).

[36] Gérard Brachet and Bernard Deloffre, "Space for Defence: A European Vision", in Space Policy, Vol. 22, No. 2 (May 2006), pp. 92-99.

[37] Fabrizio Minniti, La politica estera di sicurezza e difesa dell'Ue: tendenze e prospettive future, Roma, Centro Militare di Studi Strategici, dicembre 2009 (Ricerche Ce- MiSS), p. 123,

Per quanto concerne le diverse istituzioni europee, la prima a mostrare maggiore interesse per lo spazio fu la Commissione europea, che partecipando intorno agli anni Settanta alla presentazione dei primi risultati del primo lancio per il telerilevamento statunitense Landsat-1, si rese conto che tale tecnologia poteva risultare essenziale anche per l'Europa, perché avrebbe permesso una maggiore resa agricola e monitoraggio dei boschi e delle foreste[38]. Nel 1979 il Parlamento Europeo adottò la "*Proposta di risoluzione sulla partecipazione della Comunità Europea nella ricerca spaziale*", nel 1981 venne adottata la risoluzione sulla "*Politica spaziale europea*" e in seguito nel 1987 la Commissione contribuì allo sviluppo della codificazione del diritto spaziale[39]. Il vero quadro spaziale europeo iniziò a delinearsi solo intorno al 1999, permettendo così di iniziare una nuova formulazione della politica spaziale grazie ad una forte cooperazione con l'ESA per una nuova strategia spaziale europea[40]. La nascita e lo sviluppo dell'ESA, permise una progressiva integrazione dello spazio nei confronti delle future politiche europee spaziali, dimostrando che in futuro ci sarebbe stata la possibilità di una forte cooperazione europea in materia spaziale. L'interesse della Commissione europea, grazie alla spinta di Francia e Germania, era quello di definire una politica spaziale a sostegno dell'allora, politica europea di sicurezza e difesa[41].

Nel 2001, la Commissione europea e l'ESA istituirono una task force congiunta per cooperare verso nuovi scenari futuri e per consolidare il loro legame. Il primo loro rapporto "*verso una politica spaziale europea*" includeva la possibilità di una "*cooperazione spaziale nella politica esterna dell'Unione Europea*". Tale politica aveva come focus principale la sicurezza dell'Unione. L'importanza spaziale per l'UE venne ribadita nel gennaio del 2002 dal Parlamento europeo, attraverso l'adozione di una risoluzione intitolata "*l'Europa e lo spazio*", evidenziando che lo spazio deve essere utilizzato solo per

http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Pubblicazio-ni/News206/2009-12/Pagine/La_politica_estera_di_sicurezza_e_11785future.aspx.

[38] Raymond Klersy, "The Work and Role of the Commission of the European Com- munities", op. cit., pp. 1035-1058.

[39] Nina-Louisa Remuss, Space and Internal Security. Developing a Concept for the Use of Space Assets to Assure a Secure Europe, Vienna, European Space Policy Institute, September 2009 (ESPI Report, 20), http://www.espi.or.at/images/stories/dokumente/ studies/espi%20 report%2020_final.pdf.

[40] Marco Cervino, Barbara Corradini, Silvio Davolio, "Uso pacifico dello spazio: un principio ormai accantonato?", op. cit., p. 29.

[41] Michele Nones et al. (a cura di), La dimensione spaziale della politica europea di sicurezza e difesa, op.cit., p. 11.

"*usi pacifici*", includendo anche "*applicazioni militari per attività di mantenimento della pace*"[42].

Bisogna però tenere in considerazione le differenze tra ESA e Unione Europea e la loro forma di cooperazione istituzionale, necessaria, fondamentale ma a tratti problematica principalmente a causa delle diverse strutture istituzionali. L'Unione Europea è un'organizzazione internazionale a carattere sovranazionale, mentre l'ESA si fonda su una cooperazione intergovernativa con tutti i paesi membri i quali non coincidono con quelli dell'Unione. Inoltre, l'UE si basa sui principi del libero mercato e della libera circolazione di beni e servizi tra i paesi membri, mentre l'ESA promuove una politica industriale concentrata sul ritorno industriale nazionale. Ovviamente la tensione tra le due istituzioni ha creato la condizione per istituire una regolamentazione adeguata, evidenziando che il principale problema resta il potere decisionale ovvero lo stabilire chi decida politicamente. Per risolvere tale problema e per cooperare in maniera più efficace si sono delineati diversi modelli:

1. L'accordo quadro del 2004 che prende in esame la possibilità di cooperazione comune, pur rimanendo indipendenti, e di partnership specifica. Ai sensi di tale accordo l'UE è designata come responsabile delle decisioni politiche mentre l'ESA è incaricata di svilupparle, ma ognuna con i propri programmi economici ed industriali in maniera autonoma.
2. Alto livello di integrazione: l'UE aveva il diritto di stabilire la politica dello spazio e l'ESA poteva eseguire ed attuare tale politica, pur con il controllo da parte della Commissione Europea.
3. L'UE sarebbe potuta diventare membro dell'ESA e ottenere lo status di "membro associato"[43]

Nel luglio 2002, la Strategic Aerospace Review for the 21th Century, tramite un rapporto consultivo di alto livello della Commissione, denunciò la non esistenza di scopi comuni tra stati dell'UE e la mancanza di un approccio integrato a livello multidisciplinare. Venne così pubblicato il Libro Verde della Commissione sulla politica spaziale europea, aprendo un confronto sul futuro dello spazio e sui possibili benefici per cittadini europei. Esse venne seguito da un Libro Bianco nel novembre 2003, che mise in luce l'importan-

[42] Commissione delle Comunità Europee, L'Europa e lo spazio: comincia un nuovo capitolo (COM (2000) 597 definitivo, Bruxelles, 27.9 2000, http://eur-lex.europa.eu/ LexUriServ/ LexUriServ.do?uri=COM:2000:0597:FIN:IT:PDF.

[43] Stephan Hobe, "Prospects for a European Space Administration", in Space Policy, Vol. 20, No. 1 (February 2004), p. 25-29. V. anche Frans G. von der Dunk, "Towards One Captain on The European Spaceship. Why the EU Should Join ESA", in Space Policy, Vol. 19, No. 2 (May 2003), pp. 83-86, http://digitalcommons.unl.edu/cgi/viewcontent.cgi? article=1055&-context=spacelaw.

za strategica dello spazio per l'attuazione della politica estera e di sicurezza comune (PESC) e della politica europea di sicurezza e difesa (PESD)[44]. Insieme a questa regolamentazione fu approvato un piano dell'Eums, ovvero l'European Union Military Staff, denominato Space Systems Needs for Military Operations, un vero e proprio primo documento ufficiale redatto da un organo del Consiglio sui requisiti PESD per le applicazioni spaziali[45]. A fine 2003 venne firmato un accordo quadro tra UE-ESA che determinò la creazione di un organo congiunto: il Consiglio Spazio anche detto Space Council, composto dal Consiglio europeo e dal Consiglio ministeriale dell'ESA. Il Consiglio Spazio è composto da 27 stati membri dell'UE e da 18 stati membri dell'ESA. Il suo scopo primario è quello di coordinare le attività spaziali di entrambe le organizzazioni[46]. Dopo la pubblicazione del Libro Bianco nel 2003, la Commissione istituì un gruppo specifico per la politica spaziale, anche detto High Level Space Policy Group, con lo scopo di stilare un "programma spaziale europeo" per la fine del 2005. Lo stesso Consiglio europeo affermò la necessità di elaborare una strategia di sicurezza europea per un'Europea più coerente, attiva e capace di affrontare in modo veloce tutte le possibili minace meno visibili e meno prevedibili, come quella terroristica e di proliferazione di armi di distruzione di massa. Successivamente nel 2006 il Direttore Generale dell'ESA rilasciò l'Agenda 2011 in cui si richiedeva un coinvolgimento tra le diverse sinergie dei servizi spaziali civili e di difesa; contemporaneamente il Working Group sullo spazio e la sicurezza (Space and Human Security Working Group) sviluppò un rapporto che riconosceva l'importanza del satellite Galileo per la sicurezza. Un altro elemento fondamentale dell'Agenda era quello di richiedere un rafforzamento della cooperazione tra i diversi programmi e tecnologie spaziali e civili.

Con la presidenza francese nel 2008 sono stati compiuti passi avanti in relazione al valore delle tecnologie spaziali per la difesa e la sicurezza in Europa, ridefinendo quattro priorità: le applicazioni spaziali per la sicurezza, i cambiamenti climatici, l'economia e l'esplorazione.

Il Trattato di Lisbona, che entrò in vigore il 1° dicembre 2009, introdusse nuove aree di competenza per l'UE aprendo le strade verso una cooperazio-

[44] Commissione Europea, Libro bianco, Spazio: una nuova frontiera europea per un'Unione in espansione. Piano di azione per attuare una politica spaziale europea, COM(2003) 673 definitivo, Bruxelles, 11.11.2003, p. 5, http://eur-lex.europa.eu/Lex UriServ/site/it/com/2003/com2003_0673it01.pdf.

[45] Alexandros Kolovos, The European Space Policy. Its Impact and Challenges for the European Security and Defence Policy, op. cit., p. 7.

[46] Wolfgang Rathge- ber, The European Architecture for Space and Security, Vienna, European Space Policy Institute, August 2008 (ESPI Report, 13), p. 22, http://www.espi.or.at/images/stories/ dokumente/studies/espi_report_13.pdf.

ne tra Stati membri e paesi terzi[47]. Questo permise all'UE di condurre una politica spaziale europea, inserendo lo spazio tra le materie di competenza concorrente tra Unione Europea e Stati membri[48]. Pertanto, il Parlamento Europeo e il Consiglio possono stabilire una procedura legislativa, ovvero istituire delle misure necessarie per iniziare un nuovo programma spaziale europeo, prevedendo una collaborazione strutturata permanente in materia di sicurezza e difesa di una cooperazione rafforzata, principalmente in ambito civile.

3. Spazio: attività politico-strategica

Durante il periodo della Guerra Fredda le due superpotenze, Stati Uniti e Unione Sovietica, si contestavano il prestigio su due campi principali: il possesso di armamenti nucleari e la conquista dello spazio. Nel corso della storia, esattamente cinquanta anni dopo, lo spazio è diventato di importanza principalmente economica, politica, militare e culturale, rivelandosi uno strumento fondamentale per la diplomazia e la politica internazionale, garantendo benefici diretti e indiretti per ogni singolo stato.

Si iniziò a parlare di potere spaziale nel 1995 con Space Power 2010, identificandolo come la "*capacità di un attore statale o non-statale di realizzare i propri scopi e obiettivi in presenza di altri attori sullo scenario internazionale attraverso il controllo e lo sfruttamento dell'ambiente spaziale*"[49]. Per comprendere al meglio la teoria del potere spaziale bisogna menzionale il famoso discorso del presidente americano Ronald Reagan nel 1983 in cui, trattando del funzionamento e della struttura di "potenza spaziale", evidenziò dei requisiti di base per potersi identificare sotto questa denominazione: disporre di siti e veicoli di lancio, avere dei satelliti in orbita, avere il capitale umano adeguato e detenere un numero medio grande di seggi, all'interno delle organizzazioni internazionali e altri organi[50]. Bisogna tenere presente che lo space

[47] Jean-François Mayence, "Entry Into Force of the EU Lisbon Treaty. A New Era in the European Space Cooperation?", in ECSL. Bulletin of the European Centre for Space Law, n. 37 (February 2010), pp. 10-11, http://download.esa.int/docs/ECSL/12102010_ ECSL_37_preview.pdf.

[48] Gazzetta ufficiale dell'Unione europea del 3.12.2009, C 294 E/69, Spazio e sicurezza, Risoluzione del Par- lamento europeo del 10 luglio 2008 su spazio e sicurezza (2008/2030(INI)), http:// eur-lex.europa.eu.

[49] James L. Hyatt et al., Space Power 2010, Maxwell AFB, US Air Command and Staff College, May 1995 (Research Report, 95-05), p. 9, http://www.fas.org/spp/eprint/95- 010e.pdf.

[50] Nicolas Peter, Space Power and Europe in the 21st Century, Vienna, European Space Policy Institute, 28 April 2009 (ESPI perspectives, 21), p. 4, http://www.espi.or.at/images/ stories/ dokumente/Perspectives/ESPI_Perspectives_21.pdf.

power è considerato una forma indipendente di potere che viene utilizzato, da solo o in concorrenza, per il raggiungimento finale di scopi prefissati. Inoltre, è uno strumento diplomatico all'interno delle relazioni internazionali che rispecchia i rapporti di forza tra i paesi.

Lo Space Power comporta, inoltre, dei benefici come la capacità di identificarsi in un mercato in continua evoluzione, permettendo così cooperazioni sia a livello nazionale che globale. La capacità di realizzare un programma spaziale nazionale mette costituisce la prova di come si possa sviluppare il livello tecnologico di un paese e induce la realizzazione di uno sviluppo sempre più alto per quanto riguarda il settore industriale.

Lo spazio è identificato dal Trattato sullo Spazio Extra-atmosferico come un bene comune globale che deve essere utilizzato per scopi pacifici, mettendo in evidenza la cooperazione internazionale e la consultazione essenziali per interessi globali. Lo spazio, dunque, diventa uno strumento fondamentale di politica estera, capace di rafforzare le relazioni tra paesi e sviluppare cooperazione internazionale[51].

Uno stato che ha fatto dello spazio una della sua arma più potenti sono gli Stati Uniti che hanno assunto, nel corso della storia, un ruolo pioneristico nei confronti di tutte le attività spaziali per scopi geostrategici. Proprio gli americani vantano il programma spaziale più grande e avanzato del mondo. La spesa pubblica per tutte le attività spaziali nel 2010 era all'incirca 47 miliardi di dollari, rappresentava all'incirca il 75% del budget totale della spesa pubblica mondiale[52]. La cooperazione con gli altri paesi resta sempre un punto molto delicato, perché l'idea americana è quella di cooperare, ma rimanendo pur sempre il paese dominante, aumentando il budget a disposizione e assumendosi la responsabilità esclusiva della gestione del progetto. Avendo così una cooperazione che si concentra caso per caso in base ai progetti[53].

Nel corso della storia l'America non è sempre stata l'unica superpotenza, avendo nell'Unione Sovietica la sua più grande rivale sin dal primo lancio del primo satellite artificiale nel 1957. Fu proprio durante la corsa allo spazio che l'Unione Sovietica riuscì ad acquisire capacità e competenze uniche nel loro genere, ma dopo la crisi del rublo nel 1998 le attività spaziali furono elimi-

[51] Enrico Saggese, Gabriella Arrigo, "La nuova strategia decennale dell'Agenzia spaziale italiana", in La comunità internazionale, a. 65, n. 4 (2010), p. 522, http://www.sioi.org/Sioi/3saggese-arrigo.pdf.

[52] Bertrand de Montluc, "The New International Political and Strategic Context for Space Policies", op. cit., p. 23.

[53] Roger D. Launius, "United States Space Cooperation and Competition: Historical Reflections", in Astropolitics, Vol. 7, No. 2 (May 2009), p. 97.

nate dall'agenda di Mosca per circa un decennio[54]. Successivamente Mosca recuperò la sua capacità tecnologica ed innovativa per rimettersi in piedi e assumere un ruolo chiave sullo scacchiere geopolitico, diventando così una superpotenza energetica e riconoscendo alle risorse spaziali il ruolo di strumento per l'indipendenza nazionale. Lo stesso presidente Vladimir Putin nel 2008 ha riconosciuto lo stretto collegamento tra la capacità spaziale e lo status di superpotenza. Proprio su impulso da Putin iniziò un vero e proprio riammodernamento del settore spaziale impostosi sull'agenda strategica del Cremlino, per motivi politici ed economici. La cooperazione internazionale in ambito spaziale condotta dalla Russia si è sviluppata con partnership che promuovessero gli interessi di Mosca mantenendo sempre come interesse principale l'esaltazione della nazione. Le partnership più importanti della nazione russa sono state l'Europa con la quale è stato stretto un accordo per tutti i servizi di telecomunicazione e di lancio, e potenze emergenti come la Cina e l'India[55]. Dobbiamo però specificare che la Russia è sempre stata affascianata dall'economia cinese e dal suo mercato e avendo inoltre quasi sempre interessi geopolitici strategici comuni, come quello di mitigare l'influenza degli Stati Uniti.

Negli ultimi anni lo spazio è diventato sempre di più una materia importante, ma soprattutto strategica per tutti i paesi emergenti, convinti di poter trasformare in tal modo il proprio paese da un punto di vista economico e tecnologico e ottenere, in un secondo momento, il prestigio internazionale[56]. Ciò dimostra come lo spazio costituisca un palco importante per tutti i paesi con economie in espansione e desiderosi di entrare a far parte dei paesi industrializzati.

Quando si parla di paesi emergenti, uno dei più importanti è sicuramente la Cina. Pechino occupa oramai un posto di rilievo all'interno di tutta la comunità internazionale spaziale e ci mostra, inoltre, come un paese emergente sia entrato nel mondo dell'economia spaziale grazie a forte dinamismo economico con l'interesse primario di diventare una delle più grandi potenze internazionali. Proprio la vicenda cinese mostra come far parte di un programma spaziale sia in realtà un atto meramente politico, con l'intento di

[54] Charlotte Mathieu, "Assessing Rus- sia's Space Cooperation with China and India-Opportunities and Challenges for Europe", in Acta Astronautica, Vol. 66, Nos 3-4 (February-March 2010), p. 355.

[55] Enrico Saggese, Gabriella Arrigo, "La nuova strategia decennale dell'Agenzia spaziale italiana", op. cit., p. 528. V. anche Bertrand de Montluc, "Russia's Resurgence: Prospects for Space Policy and International Cooperation", in Space Policy, Vol. 26, No. 1 (February 2010), p. 21.

[56] Valérie Niquet, La recherche spatiale en Chine: saut technologique et capaci- tés militaires, Paris, Institut français des relations internationales (Ifri), Juin 2007 (Asie Visions, 1), p. 6, http://www.ifri.org/downloads/visionasie1.pdf.

raggiungere scopi ulteriori di carattere politico-diplomatico ma soprattutto simbolico[57]. Tutto ciò comporta dei benefici in termini tecnologici e occupazionali all'interno del paese, imprimendo un'accelerazione allo sviluppo economico in generale all'interno della Cina. L'obiettivo rimane comunque quello di avere influenze geostrategiche con la finalità di diventare una potenza mondiale[58]. Negli ultimi anni, infatti, la Cina ha sviluppato nuovi lanciatori, nuovi satelliti e programmato nuovi voli umani, mostrando di concentrarsi ulteriormente sulla cooperazione spaziale regionale.

Un altro paese emergente è l'India, che guarda allo spazio come ad un vero e proprio strumento di sviluppo, economico e sociale, dal momento con i satelliti si ha la possibilità di diffondere informazioni e trasmissioni televisive culturali e comunicative in tutto il paese, riducendo il digital divide. Un altro elemento particolarmente importante è che grazie ai satelliti possono essere controllati e gestite utte le risorse idriche, la meteorologia e la prevenzione dei disastri naturali[59]. Tuttavia, tutti questi sistemi hanno sempre delle potenzialità duali, sia civili che militari. Dal punto di vista internazionale, non sono mancate collaborazioni con la Russia e l'Europa. L'India ha ricevuto assistenza da parte dell'Unione Sovietica, ma più recentemente dall'Europa grazie a specifici accordi di cooperazione.[60]

Un altro paese emergente che si fa spazio sulla scena internazionale è proprio Israele, che nel corso della storia ha sviluppato un suo personale programma spaziale all'inizio degli anni Ottanta per rispondere alla sua situazione di sicurezza e difesa[61]. Rispetto agli paesi menzionati, il programma spaziale israeliano nacque in conseguenza diretta della situazione geopolitica e geostrategica in cui si trovava, soprattutto dopo l'accordo di pace con l'Egitto alla fine degli anni Settanta. In un'epoca in cui i classici strumenti tradizionali come l'uso della forza militare non sono più sufficienti, per evidenziare la forza e la capacità di un paese è necessario sviluppare strategie spaziali

[57] Serge Grouard et Odile Saugues, Rapport d'information déposé... par la Commis- sion de la défense nationale et des forces armées sur les enjeux stratégiques et indus- triels du secteur spatial, op.cit.

[58] Joan Johnson-Freese, China's Space Ambitions, Paris, Institut français des relations internationales (Ifri), Summer 2007 (Proliferation Papers, 18), p. 7, http://www.ifri.org/ downloads/ China_Space_Johnson_Freese.pdf.

[59] K.R. Sridhara Murthia, H.N. Madhusudan, "Strategic Considerations in Indian Space Programme - Towards Maximising Socio-Economic Benefits", op. cit., p. 507.

[60] Angathevar Baskaran, "Technology Accumulation in the Ground Systems of India's Space Program: The Contribution of Foreign and Indigenous Inputs", in Technology in Society, Vol. 23, No. 2 (April 2001), p. 206.

[61] Deganit Paikowsky and Isaac Ben Israel, "Science and Technology for National Development: The Case of Israel's Space Program", in Acta Astronautica, Vol. 65, Nos. 9- 10 (November-December 2009), p. 1466.

indipendenti e ciò rende Israele un paese dotato delle potenzialità adatte per accrescere, da un punto di vista internazionale il suo status sia in termini di controllo di informazioni che di deterrenza nei confronti dei paesi ostili[62]. Tutto questo ha permesso l'affermazione di Israele all'interno di un settore ad alta tecnologia a livello internazionale, dominando insieme ad un gruppo di nazioni il campo dell'esplorazione spaziale. Ciò, però, è soprattutto dovuto alla forte collaborazione che si è sviluppata nel corso degli anni insieme a Stati Uniti, ESA, Russia e Ucraina.

4. La responsabilità internazionale per danni prodotti da oggetti internazionali

L'immissione in orbita costituisce un momento molto delicato per tutte le attività spaziali, un momento complesso sia dal punto di vista tecnico che scientifico Avere la capacità di accedere in modo autonomo allo spazio attraverso veicoli spaziali propri è indispensabile, ad oggi, per ogni singola politica spaziale che si voglia considerare indipendente. Lanciare in orbita non è così semplice come potrebbe sembrare tanto che il lancio di oggetti spaziali costituisce un'attività complessa e molto pericolosa che solleva molti problemi di responsabilità internazionale. Un tema centrale di tale situazione sono i danni che possono essere provocati, sia alle singole persone che agli oggetti costruiti e pagati da più stati. La regolamentazione relativa lancio di satelliti è stabilita dal Trattato sui principi che governano le attività degli Stati nella esplorazione e utilizzo dello spazio extra-atmosferico, compresi la Luna e gli altri corpi celesti del 1967 e anche nella Convenzione sulla responsabilità internazionale per danni prodotti da oggetti spaziali del 1972. Anche se i razzi o i veicoli spaziali dovessero essere realizzati da privati, le attività spaziali sono comunque oggetto di responsabilità internazionale dei rispettivi Stati, su cui grava l'obbligo di controllare e monitorare tutto quello che viene lanciato, sviluppato e creato. La privatizzazione delle attività spaziali, novità degli ultimi decenni, ha determinato che le imprese sottraessero agli Stati il monopolio di determinati settori come quello delle telecomunicazioni o dell'osservazione della Terra. Da ciò è derivata la necessità di prevedere norme nazionali che introducessero nell'ordinamento nazionale il diritto internazionale dello spazio. Ai sensi dell'articolo VI del Trattato sullo Spazio Extra-atmosferico, in caso di attività svolte da organizzazioni internazionali, la responsabilità viene condivisa tra l'organizzazione e tutti gli stati partecipanti al trattato presenti in tale organizzazione. Il tema della responsabilità delle organizzazioni internazionali è stato oggetto di studio della Commissione per il Diritto Internazio-

[62] Deganit Paikowsky, "Israel's Space Program as a National Asset", op. cit.

nale nel 2002 e da quel momento sono stati approvati 66 articoli trasmessi al Segretario Generale delle Nazioni Unite e poi ai governi.

In quest'ambito è rilevante l'articolo XXII della Convenzione sulla responsabilità per danni derivati da oggetti spaziali del 1972, dove l'articolo specifica che ogni domanda di risarcimento del danno dovrà essere presentata in primo luogo all'ente internazionale entro sei mesi successivi all'avvenimento e ci sarà la possibilità di chiedere e di invocare la responsabilità degli Stati membri da parte della Convenzione sulla responsabilità per danni causati da oggetti spaziali[63].

5. Sicurezza spaziale

Quando si parla di sicurezza spaziale, si può in primo luogo far riferimento alla salute e la salvaguardia dei nostri astronauti, la sicurezza dei vettori e satelliti. Ma il concetto di sicurezza non può essere a ciò limitato, in quanto, bisogna anche considerare che lo spazio potrebbe rappresentare una nuova frontiera di conflitti.

L'utilizzo dei satelliti ha cambiato, come detto in precedenza, le nostre società che si sono evolute sia economicamente, politicamente e militarmente rappresentando un asset fondamentale per le diverse nazioni. È difficile classificare lo spazio come ambiente sicuro a causa di diverse minacce, tra cui le principali sono costituite da:

– Il rischio di una corsa agli armamenti nello spazio;
– La degradazione naturale delle condizioni di sicurezza dello spazio orbitale.

Diversi Stati hanno già sviluppato un nuovo sistema d'arma anti-satellitare, meglio detto ASAT, come la Cina, gli Stati Uniti e la Russia, con cui si è in grado di distruggere o disabilitare oggetti orbitanti. Altri Paesi in via di sviluppo, come l'India, stanno cercando di creare anch'essi tali armamenti. Lo sviluppo di capacità ASAT conferisce la capacità, soprattutto strategica, di infliggere danni con poca spesa. Oltre ai nuovi sistemi d'arma, lo spazio mantiene uno strettissimo legale con le armi nucleari tanto che USA e Unione Sovietica durante il periodo della Guerra Fredda hanno testato la capacità anti-satellitare per sfruttarla e utilizzarla come forma di deterrenza contro i possibili attacchi reali dei sistemi spaziali. La situazione poi si è poi prolungata nel corso del tempo, con lo sviluppo e l'implementazione di nuovi sistemi di capacità offensiva antisistemi spaziali per distruggere i satelliti di altri paesi,

[63] Convention on International Liability for Damage Caused by Space Objects, opened to signature at London, Moscow and Washington, 29 March 1972, http://www.oosa. unvienna. org/pdf/publications/STSPACE11E.pdf.

permettendo così un vero e proprio confronto nello spazio con il possibile utilizzo di armi spaziali. Le armi ASAT[64] costituiscono una categoria eterogena e possono produrre effetti immediati fino a giungere a sistemi sempre più complessi e allo sviluppo di nuove armi ASAT. Possiamo distinguere ben sei diverse classi di intensità di ASAT:

1. Attacchi elettronici, disturbando o eliminando totalmente il segnale.
2. Attacchi cibernetici, direttamente sugli oggetti nello spazio.
3. Attacchi energetici diretti, tramite laser o microonde per danneggiare le apparecchiature dello spazio.
4. Sistemi co-orbitali, con la capacità di colpire oggetti spaziali per danneggiarli.
5. ASAT cinetici fisici, con la distruzione ad impatto ad alta velocità con possibili esplosioni.
6. Detonazioni nucleari con effetti elettromagnetici o radioattivi.

Queste armi appena elencate sono state testate in diversi paesi del mondo, con un focus principale sugli ASAT cibernetici che comportano la capacità di prendere il completo controllo del bersaglio e ciò principalmente perché queste armi sono quelle più economicamente abbordabili gli Stati.

Lo spazio è anche soggetto a degradato, a seconda del numero di Stati che lo utilizzano, comporta problematiche quali l'aumento di collisioni tra oggetti spaziali e il grande aumento di detriti (debris) che ancora oggi, a inizio 2024, non sono ancora controllabili e che anche se di piccole dimensioni possono provocare davvero grandi danni se dovessero impattare su un satellite attivo.

Non risulta possibile, secondo nessuna regolamentazione, stipulare un trattato per la prevenzione di una possibile corsa agli armamenti nello spazio. Esiste tuttavia un codice di condotta[65] per tutte le attività spaziali, sviluppato dall'Unione Europea su impulso italiano, detto anche sistema per la Space Situational Awareness (SSA)[66] per il monitoraggio dell'ambiente spaziale e degli oggetti orbitanti. Questo sistema è in grado di prevedere possibili collisioni in anticipo, riuscendo a preannunciare la traiettoria e se necessario deviarla. In questo progetto l'Italia è leader nel campo della Near Earth Objects, ovvero asteroidi e comete la cui orbita passa vicino alla Terra.

[64] Armi Antisatellite: La Nuova Corsa Agli Armamenti Spaziali p. Aspenia Online. https://aspeniaonline.it/armi-antisatellite-la-nuova-corsa-agli-armamenti-spaziali/.

[65] "Codice Di Condotta UE." v. https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015D0203&from=EN.

[66] "SSA: Five Questions with ESA's Nicolas Bobrinsky.", https://www.esa.int/Enabling_Support/Operations/SSA_Five_questions_with_ESA_s_Nicolas_Bobrinsky2.

L'Italia e l'Unione Europea stanno svolgendo una intensa ricerca per giungere ad una soluzione comune e condivisa da un punto di vista internazionale per la prevenzione della corsa agli armamenti e contro il degrado causato e dai detriti spaziali in orbita e dai NEO. Inoltre, l'UE sta cercando di studiare un nuovo sistema che possa rafforzare i propri satelliti contro ogni possibile minaccia sia accidentale che intenzionale. Il lavoro comune di collaborazione contribuirà, da un punto di vista diplomatico ed economico, al raggiungimento di un obiettivo comune, garantire maggiore sicurezza sia terrestre ma soprattutto spaziale. Bisogna tenere in considerazione che lo spazio sta diventando sempre di più un ambiente poco sicuro; tuttavia, è necessario avere una panoramica delle diverse minacce che lo spazio orbitale può porci.

Avendo preso in considerazione la sicurezza spaziale[67] e la possibile integrità dei satelliti, evidenziamo come possono essere messi a rischio a causa da:

1. Atti internazionali o azioni aggressive da parte di attori poco propensi ad una pace comune.
2. Diversi avvenimenti casuali causati dallo spazio orbitale come per esempio l'inquinamento spaziale.

Per quanto concerne il primo problema, bisogna tenere in considerazione che tutti i satelliti hanno un uso duale. Questo richiede una maggiore attenzione considerando che i satelliti rappresentano bersagli privilegiati per eventuali azioni ostili. Inoltre, i satelliti sono oggetti delicati e molto facili da colpire dal momento che seguono costantemente una traiettoria prestabilita e difficilmente modificabile.

Attualmente tutti i satelliti che abbiamo in orbita possono essere disabilitati dalla superficie terrestre. Oltre a questa metodologia esistono diverse modalità di attacco anti-satellitare come l'Anti-Satellite Attack ASAT, che possono colpire e distruggere fisicamente il satellite che viene preso di mira, sia disintegrandolo che interrompendo solo i collegamenti a terra. Queste tecnologie sono disponibili da decine di anni: basti pensare che durante la Guerra Fredda gli Stati Uniti e l'Unione Sovietica possedevano armi, missili balistici in grado di distaccarsi dal vettore del proprio satellite e bersagliarne un altro, distruggendosi all'impatto. Oltre al classico impatto e distruzione del satellite, oggigiorno esistono anche degli attacchi che includono l'uso del laser per offuscare o danneggiare, perfino distruggere, il satellite bersagliato tramite surriscaldamento dei sensori. Come la tecnologia precedente, anche questa è stata già utilizzata e testata nel 2006

[67] Presidenza del Consiglio dei Ministri. "Strategia Nazionale Di Sicurezza Per Lo Spazio".

quando gli Stati Uniti annunciarono che un loro satellite era stato colpito tramite un laser cinese. È possibile quindi utilizzare diversi sistemi di interferenza elettronica per disturbare la connessione e la comunicazione con i satelliti e le stazioni di terra, anche dette "*jamming*". Per quanto riguarda armi in orbita che abbiano la capacità di colpire sistemi ASAT o bersagli a terra, va specificato che non si tratta ancora di realtà dal momento che non esistono ancora delle tecnologie concrete per utilizzare un satellite come una vera e propria arma.

I nuovi paesi emergenti, che stanno a mano a mano entrando nello scenario spaziale, hanno iniziato a cambiare le carte in tavola: la Cina ha effettuato nel 2007 un primo test ASAT, facendo preoccupare e provocando una reazione degli Stati Uniti; anche l'India, come il Pakistan, ha l'idea di dotarsi di tali sistemi per potersi difendere e proteggere da qualsiasi minaccia esterna.

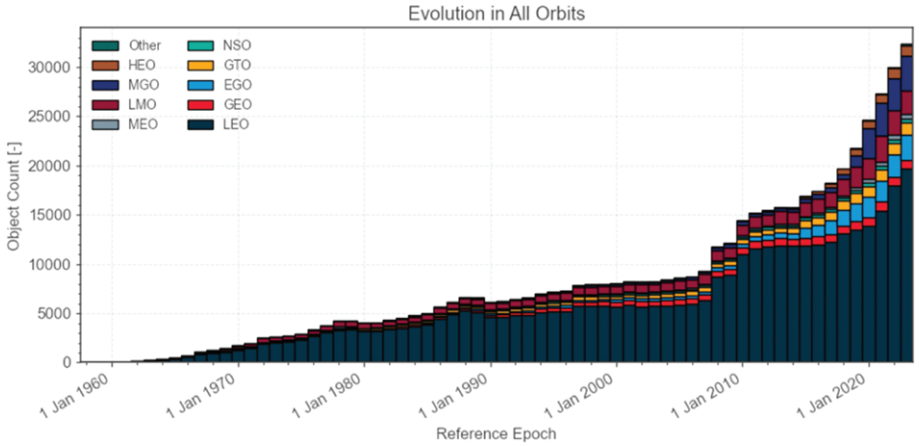
La seconda minaccia richiamata in precedenza, fa riferimento all'accrescimento dei detriti spaziali che crea un inquinamento spaziale, rischiando di provocare pericolosi incidenti. Questo problema è venuto alla luce solo nell'ultimo periodo storico quando c'è stato un incremento di applicazioni e di lanci satellitari, che hanno portato ad un aumento costante e continuo di satelliti in orbita. Ad oggi abbiamo un sovraffollamento di tutte le orbite, dalla geostazionaria all'orbita più alta, dove attualmente troviamo più di 957 satelliti attivi, oltre ad molti altri spenti e residuati da missioni passate, vaganti per lo spazio, che possono provocare collisioni molto importanti a satelliti ma perfino alla Stazione Spaziale Internazionale che ospita esseri umani. Secondo una stima, ci sarebbero all'incirca 19 mila oggetti grandi più di 10 centimetri e circa 500 mila tra 1 e 10 centimetri. Bisogna considerare che i frammenti più piccoli si aggirano intorno alle decine di milioni. La più grande concentrazione di detriti è tra gli 800 e gli 850 chilometri di altitudine[68].

Tutta questa spazzatura spaziale rappresenta una vera e propria minaccia per i satelliti considerando che i detriti che si trovano nell'orbita bassa e in quella geostazionaria ruotano alla velocità di 7-8 km al secondo e un singolo impatto potrebbe provocare danni gravi fino alla disabilitazione completa del satellite.

Lo schema sottostante ci mostra come il sovraffollamento delle orbite sia aumentato durante l'arco temporale preso in esame.

[68] Luca Del Monte, Understanding the Physics of Space security, discorso alla Space Security Conference 2010.

Figure 1 – *Evolution in All Orbits dal 1960 al 2023*



Fonte: https://www.esa.int/Space_in_Member_States/Italy/Space_Environment_Report_2023_dell_ESA

Non sono solo i detriti spaziali a provocare enormi danni, ma abbiamo anche considerare la meteorologia spaziale che va costantemente monitorata a causa delle possibili tempeste magnetiche che possono danneggiare in maniera importante tutte le diverse apparecchiature elettroniche e pannelli dei satelliti. Tali tempeste possono addirittura interrompere o distruggere tutti i segnali dei moderni sistemi di navigazione e comunicazione spaziale.

Infine, ci sono le piogge di asteroidi che costituiscono una minaccia molto impattante per il nostro pianeta. Proprio per questa possibile situazione si stanno creando delle apparecchiature che grazie allo scontro tra asteroide e sonda possono modificare l'orientamento e la rotazione dell'asteroide, impedendo di andare che questo colpisca l'atmosfera terrestre e impatti il suolo del pianeta Terra. Proprio l'ESA ha dei programmi di sicurezza spaziale che sviluppano satelliti e sensori in grado di captare possibili minacce come il tempo meteorologico spaziale o possibili traiettorie di asteroidi. Tutto questo, però, comporta una maggiore osservazione della Terra e un sistema di allerta all'avanguardia con tecnologie innovative.

Inoltre, la sicurezza spaziale è considerata un elemento strategico nazionale dagli Stati Uniti che è attualmente la principale potenza spaziale del mondo. Washington ha dichiarato la propria disponibilità a considerare tutti gli strumenti giuridici per limitare e controllare gli armamenti spaziali a condizione che siano garantiti dei trattamenti equi e verificabili tra i diversi paesi. Il problema sorge quando consideriamo tutti i satelliti o navicelle come strumenti duali, il che rende difficile, se non impossibile, determinarsi gli oggetti in questione sono utilizzati per scopi militari offensivi oppure no.

Bisogna comprendere come la natura duale di questi strumenti non vada a nuocere sugli stati in virtù di una sicurezza spaziale pronta a rispondere in maniera immediata sia da un punto terra centrico, ovvero tra i singoli stati che si contendono lo spazio o un piccolo elemento di terra, sia da un punto di vista esterno come una vera e propria difesa e sicurezza interplanetaria. Per poter porre rimedio a questa situazione bisogna creare una sinergia tra il pubblico e il privato, tra le istituzioni e le aziende e tra i paesi e le organizzazioni internazionali. Solo così si potrà arrivare ad avere una cyber-security, non solo da un punto di vista terrestre ma anche esterno. Per quanto effettivamente la minaccia cyber può essere controllata o gestita, l'impegno sinergetico di tutte quelle aziende del mondo accademico e di tutte le strutture di intelligence, possono coordinarsi per un impegno maggiore in ambito nazionale.

Dal punto di vista della situazione politica americana, va sottolineato come ci sia anche situazioni e posizioni di minoranza che rifiutano il concetto di limitazione degli armamenti, spingendo ad uno sviluppo molto rapido di essi e cercando di portare l'America ad una egemonia spaziale orbitale. Questa strategia era stata sviluppata durante gli anni di presidenza di George W. Bush. Diversamente Barack Obama ha sviluppato una politica spaziale nazionale[69], detta anche National Space Policy, NSP. Questa politica pone al centro la sostenibilità dell'ambiente spaziale, cercando di limitare i detriti spaziali creando misure che favoriscono la responsabilità spaziale ma soprattutto la trasparenza delle operazioni spaziali. Tuttavia, per poter ottenere il miglior risultato nel minor tempo possibile, è necessaria una cooperazione a livello internazionale. Con la presidenza Trump nel 2020 dove è stata attuata la nuova Space Policy Directive-5 (SPD-5)[70] in tema di Cybersecurity. L'SPD-5 applica la strategia di sicurezza informatica che attualmente è in uso nei sistemi terrestri con particolar attenzione alla protezione della sicurezza. Questa direttiva pone l'accento sulla necessità di incrementare e di conseguenza migliorare tutte le protezioni informatiche di una rete di controllo a terra, un controllo di un veicolo spaziale e di una rete utente o missione che fornisce tale servizio spaziale, cercando quindi di monitorare e di anticipare l'evoluzione delle attività informatiche dannose. Possiamo quindi dire che SPD-5 ordina alle agenzie governative statunitensi di collaborare con i proprietari e gli operatori di sistemi spaziali per sviluppare e implementare piani di sicurezza informatica, inclusa la possibilità di eseguire aggiornamenti e rispondere agli incidenti da remoto. Gli obiettivi di controllo sono:

[69] National Space Policy of the United States of America, giugno 2010, http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.

[70] "How does Space Policy Directive-5 Change Cybersecurity Principles for Space Systems?" Aerospace Security, last modified -09-14T14:49:19+00:00, https://aerospace.csis.org/how-does-space-policy-directive-5-change-cybersecurity-principles-for-space-systems/.

– Protezione dei collegamenti di comando e di controllo attraverso misure di autenticazione o crittografia efficaci;
– Misure di protezione fisica progettate per ridurre le vulnerabilità dei sistemi di comando di un veicolo spaziale;
– Protezione dei sistemi di terra, della tecnologia operativa e dei sistemi di elaborazione delle informazioni.

Oltre al rafforzamento della sicurezza informatica per i dispositivi spaziali è stata creata la nuova Space Force, la sesta branca delle forze armate statunitensi.

Per quanto riguarda invece l'ultima presidenza americana di Biden, questa ha mantenuto, per ora, la visione spaziale che ha avuto il precedente governo, non sbilanciandosi in maniera sostanziale.

L'Europa e l'Italia hanno sviluppato, a livello internazionale, una bozza del Codice di condotta (Coc) per tutte le attività nello spazio orbitale[71]. L'iniziativa italiana ha creato una strada verso uno strumento di sicurezza internazionale nello spazio. Tale Codice di condotta, quindi, si impegnerebbe a minimizzare ogni possibilità di incidenti, collisioni o interferenze con le attività spaziali altrui, cercando di danneggiare il meno possibile e provocando meno detriti spaziali. Il *Coc* oltre a non consentire nuovi test ASAT, contiene nuove misure di trasparenza e modalità di lanci spaziali, prevedendo un vero e proprio strumento di consultazione che dovrebbe essere utilizzato da tutti gli stati per mitigare gli eventi possibili. Non può essere considerato come vero e proprio strumento vincolante ma evidenzia come sia necessario vincolare e regolare determinati e possibili comportamenti, tanto che lo stesso strumento diviene pragmatico e concreto per affrontare tale problema comune. Per permettere una migliore e più veloce adozione del Codice di condotta, la diplomazia europea ha svolto diversi colloqui con rappresentati delle maggiori potenze spaziali come gli Stati Uniti, la Russia, la Cina e l'India.

Russia e Cina si sono mostrate favorevoli all'adozione ad un trattato vincolante e abbia la capacità di vietare il possibile schieramento di qualsiasi tipo di arma nello spazio orbitale. Nel 2008, infatti, questi due paesi presentarono una *bozza di un trattato sulla prevenzione del piazzamento di armamenti in orbita*, durante la Conferenza sul Disarmo. Successivamente, hanno chiarito che il trattato non restringeva la possibilità e il diritto di autodifesa né proibiva lo sviluppo di test ASAT. Tale bozza di trattato permette di constatare che c'è un ampio raggio di possibilità per poter infrangerlo, lasciando quindi la possibilità agli americani di definire tale trattato come un tentativo diplomatico di ridurre il vantaggio statunitense nella tecnologia spaziale e di conseguenza respingerlo.

[71] Disponibile a http://www.consilium.europa.eu/uedocs/cmsUpload/st14455.en10.pdf.

Possiamo quindi dire suddividere la sicurezza dello spazio consiste in due tendenze ben distinte ma soprattutto contrastanti:

– Il mantenimento della sicurezza dello spazio si sta sviluppando lungo una strada sempre più articolata e complessa. Ad oggi, la degradazione dello spazio orbitale raggiunge, livelli sempre più pericolosi mettendo a rischio l'integrità dei satelliti. I detriti spaziali sono in crescita giorno dopo giorno in maniera incondizionata.
– Dall'altro canto non possono negarsi tutti i progressi scientifici e tecnologici che si sono sviluppati in questi decenni. Dopo il governo Bush, l'America ha deciso di intraprendere una politica spaziale più collaborativa e di cooperazione, legata alla tutela e alla lotta della degradazione dell'ambiente orbitale. L'Unione Europea si è posta in prima linea per una politica spaziale internazionale proponendo un codice di condotta che, se adottato, potrebbe rappresentare un passo avanti per tutta la ricerca di governance nello spazio. Tale codice di condotta si pone come strumento propositivo attore propositivo allo scopo di evitare un possibile scenario di "guerre stellari". Siamo ancora lontani per una vera e definitiva adozione di tale CoC[72], sarà necessario un impegno politico diplomatico comune.

Un altro elemento fondamentale connesso alla sicurezza spaziale è il rischio cibernetico che nel corso degli anni è aumentato. Nel contesto dell'Unione Europea nel marzo 2022 è stato approvato lo *Strategic Compass*, una delle più importanti iniziative per la sicurezza e difesa dell'UE, che ha definito lo spazio e la cybersicurezza come pilastri strategici.

Appare evidente come lo spazio sia una delle fonti più attraenti per gli investimenti, ma è fondamentale valutare la sua vulnerabilità prima che ci verifichino pesanti danni economici che racchiudono incidenti su una serie di utenze che comprendono dalla mobilità marittima, terrestre, aerea, ed energetica, infrastrutturale e sicurezza pubblica.

Per salvaguardare ed evitare sgradevoli vicende nello spazio che sono poco controllabili, sorge la necessità che la situazione terrestre ma soprattutto quella spaziale venga sorvegliata per un continuo monitoraggio e controllo. In particolare, la sorveglianza spaziale è fondamentale per svolgere in sicurezza tutte le diverse attività e per assicurare un uso più sostenibile dell'ambiente spaziale. Tutto ciò è necessario perché la maggior parte delle infrastrutture spaziali sono concepite per uso duale e nella maggioranza dei casi non per uso scientifico, ma commerciale. Conseguentemente, alla luce dell'impor-

[72] Spazio: Ue Apre Negoziati Su Codice Di Condotta 2015. Affarinternazionali. https://www.affarinternazionali.it/archivio-affarinternazionali/2015/07/spazio-ue-apre-negoziati-su-codice-di-condotta/.

tanza che le applicazioni spaziali rivestono nella vita quotidiana e della gravità delle minacce provenienti dallo spazio, il programma di sicurezza spaziale dell'Unione Europea si pone come fine primario la protezione del nostro pianeta e di tutta l'umanità.

Sitografia

"Codice Di Condotta UE." v. https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015D0203&from=EN.

"How does Space Policy Directive-5 Change Cybersecurity Principles for Space Systems?" Aerospace Security., last modified -09-14T14:49:19+00:00, https://aerospace.csis.org/how-does-space-policy-directive-5-change-cybersecurity-principles-for-space-systems/.

"SSA: Five Questions with ESA's Nicolas Bobrinsky.", https://www.esa.int/Enabling_Support/Operations/SSA_Five_questions_with_ESA_s_Nicolas_Bobrinsky2.

Alexandros Kolovos, The European Space Policy. Its Impact and Challenges for the European Security and Defence Policy, ESPI, 2009.

Angathevar Baskaran, "Technology Accumulation in the Ground Systems of India's Space Program: The Contribution of Foreign and Indigenous Inputs", in Technology in Society, Vol. 23, No. 2 (April 2001).

Anil K. Maini, Varsha Agrawal, Satellite Technology: Principles and Applications, UK, John Wiley & Sons, Ltd, Chichester, 2006.

Antonio Daniele, "Perfettamente riuscito il lancio di ENVISAT", in Rivista aeronautica, a. 78, n. 3 (maggio-giugno 2002).

Armi Antisatellite: La Nuova Corsa Agli Armamenti Spaziali p. Aspenia Online. https://aspeniaonline.it/armi-antisatellite-la-nuova-corsa-agli-armamenti-spaziali/.

Assemblée Européenne de Sécurité et de Défense, Assemblée de l'Union de l'Europe Occidentale, cinquantehuitième session, L'espace militaire: les satellites d'alerte avancée et de renseignement électromagnétique - Réponse au rapport annuel du Conseil, Rapport présenté au nom de la Commission technique et aérospatiale par M. Yves Pozzo di Borgo, rapporteur (France, PPE/DC), 17 juin 2010, Document A/2071.

Association aéronautique et astronautique de France (3AF) Strategy and Interna-tional Affairs Commission - Writers' Group, "The Militarization and Weaponization of Space: Towards a European Space Deterrent".

Bastian Giegerich, "Navigating Differences: Transatlantic Negotiations over Galileo", in Cambridge Review of International Affairs, Vol. 20 No. 3 (September 2007).

Bertrand de Montluc, "The New International Political and Strategic Context for Space Policies", in Space Policy, Vol. 25, No. 1, February 2009.

Bruno Picerno e Francesco Brindisi (a cura di), Galileo vs Gps: collaborazione o confronto? Supplemento all'Osservatorio strategico No.7/2005, Centro militare di studi strategici, Roma, 2005.

Charlotte Mathieu, "Assessing Rus- sia's Space Cooperation with China and India- Opportunities and Challenges for Europe", in Acta Astronautica, Vol. 66, Nos 3-4 (February-March 2010), p. 355.

Commissione delle Comunità Europee, L'Europa e lo spazio: comincia un nuovo capitolo (COM (2000) 597 definitivo, Bruxelles, 27.9 2000, http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=COM:2000:0597:FIN:IT:PDF.

Commissione Europea, Libro bianco, Spazio: una nuova frontiera europea per un'Unione in espansione. Piano di azione per attuare una politica spaziale europea, COM(2003) 673 definitivo, Bruxelles, 11.11.2003, p. 5, http://eur-lex.europa.eu/Lex UriServ/site/it/com/2003/com2003_0673it01.pdf.

Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Stato di avanzamento del programma Galileo, Gazzetta ufficiale delle Comunità europee 15.10.2002, [COM(2002) 518 def.], (2002/C 248/02).

Convention on International Liability for Damage Caused by Space Objects, opened to signature at London, Moscow and Washington, 29 March 1972, http://www.oosa. unvienna.org/pdf/publications/STSPACE11E.pdf.

Deganit Paikowsky and Isaac Ben Israel, "Science and Technology for National Development: The Case of Israel's Space Program", in Acta Astronautica, Vol. 65, Nos. 9- 10 (November-December 2009), p. 1466.

Donald C. Ahrens, Meteorology Today. An Introduction to Weather, Climate, and the Environment, 8th ed., Thomson/Brooks/Cole, 2007.

Enrico Saggese, Gabriella Arrigo, "La nuova strategia decennale dell'Agenzia spaziale italiana", in La comunità internazionale, a. 65, n. 4 (2010), p. 522, http://www.sioi.org/ Sioi/3saggese-arrigo.pdf.

Envisat Overview, ESA website, http://www.esa.int/export/esaEO/SEMWYN2VQUD_index_0_m.html.

Evolution in All Orbits dal 1960 al 2023

Fabrizio Minniti, La politica estera di sicurezza e difesa dell'Ue: tendenze e prospettive future, Roma, Centro Militare di Studi Strategici, dicembre 2009 (Ricerche CeMiSS), http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/ Pubblicazioni/News206/2009-12/Pagine/La_politica_estera_di_sicurezza_e_11785future.aspx.

Ferdinando Sguerri, "Galileo e la modernizzazione del Gps e del Glonass", in Rivista aeronautica, a. 80, n. 3 (maggio-giugno 2004).

Francesco Borrini, La componente spaziale nella difesa, Centro Militare Studi Strategici, Roma.

Gazzetta ufficiale dell'Unione europea del 3.12.2009, C 294 E/69, Spazio e sicurezza, Risoluzione del Par- lamento europeo del 10 luglio 2008 su spazio e sicurezza (2008/2030(INI)), http:// eur-lex.europa.eu

George Huang, "International Satellite Organizations Facing the Challenge: Intelsat and Inmarsat", in Singapore Journal of International and Comparative Law, Vol. 3, No. 1 (1999), p. 196.

Gérard Brachet and Bernard Deloffre, "Space for Defence: A European Vision", in Space Policy, Vol. 22, No. 2 (May 2006), pp. 92-99.

Giovanni B. Andornino, Dopo la muraglia. La Cina nella politica internazionale del 21. secolo, Milano, Vita e pensiero, 2008.

Gustav Lindström with Giovanni Gasparini, The Galileo Satellite System and its Security Implications, Paris, EU Institute for Security Studies, April 2003 (Occasional papers, 44), http://www.iss.europa.eu/uploads/media/occ44_01.pdf.

James L. Hyatt et al., Space Power 2010, Maxwell AFB, US Air Command and Staff College, May 1995 (Research Report, 95-05), p. 9, http://www.fas.org/spp/eprint/95- 010e.pdf.

Jean-François Mayence, "Entry Into Force of the EU Lisbon Treaty. A New Era in the European Space Cooperation?", in ECSL. Bulletin of the European Centre for Space Law, n. 37 (February 2010), http://download.esa.int/docs/ECSL/12102010_ ECSL_37_preview.pdf.

Joan Johnson-Freese, China's Space Ambitions, Paris, Institut français des relations internationales (Ifri), Summer 2007 (Proliferation Papers, 18), p. 7, http://www.ifri.org/ downloads/China_Space_Johnson_Freese.pdf.

K.R. Sridhara Murthia, H.N. Madhusudan, "Strategic Considerations in Indian Space Programme - Towards Maximising Socio-Economic Benefits", Acta Astronautica, 2008.

Luca Del Monte, Understanding the Physics of Space security, discorso alla Space Security Conference 2010

Marco Cervino, Barbara Corradini, Silvio Davolio, "Uso pacifico dello spazio: un principio ormai accantonato?", in Scienza e Pace, paradigmi e pratiche a confronto, Workshop scientifico, Modena, 10 Novembre 2003, p. 33, http://www.bo.cnr.it/www- sciresp/OLD/GdL/SciMil/Workshop_Modena/ATTI/Atti_MO.pdf.

Marco Cervino, Barbara Corradini, Silvio Davolio, "Uso pacifico dello spazio: un principio ormai accantonato?", Edizione Nuova Cultura, Istituto Affari Internazionali, 2011.

Matthew Mowthorpe, The Militarization and Weaponization of Space, Lanham, Lexington Books, 2004.

Michele Nones, Alberto Traballesi (a cura di), Applicazioni spaziali civili di possibile interesse della difesa,

Roma, Informazioni della difesa, 1998 (Collana del Centro Militare di Studi Strategici [serie blu], 91).

Michele Nones, Alberto Traballesi (a cura di), Applicazioni spaziali civili di possibile interesse della difesa, op. cit.

Natalino Ronzitti, "Problemi giuridici sollevati dalle iniziative in materia di disarmo spaziale", in Francesco Francioni e Fausto Poca (a cura di), Il regime internazionale dello spazio, Milano, Giuffrè, 1993.

National Space Policy of the United States of America, giugno 2010, http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf

Nicolas Peter, Space Power and Europe in the 21st Century, Vienna, European Space Policy Institute, 28 April 2009 (ESPI perspectives, 21), p. 4, http://www.espi.or.at/images/ stories/dokumente/Perspectives/ESPI_Perspectives_21.pdf.

Nina Louisa Remuss, Nato and Space: Why is Space Relevant for Nato?, ESPI, 2010.
Nina-Louisa Remuss, Space and Internal Security. Developing a Concept for the Use of Space Assets to Assure a Secure Europe, Vienna, European Space Policy Institute, September 2009 (ESPI Report, 20), http://www.espi.or.at/images/stories/dokumente/ studies/espi%20report%2020_final.pdf.
Pierre-Marie Martin, Droit des Activités Spatiales, Masson, 1992.
Presidenza del Consiglio dei Ministri. "Strategia Nazionale Di Sicurezza Per Lo Spazio."
Raymond Klersy, "The Work and Role of the Commission of the European Communities", in International Journal of Remote Sensing, Vol. 13, Nos. 6-7 (1992).
Raymond Klersy, "The Work and Role of the Commission of the European Communities", Taylor & Francis, 2007.
Report of the Panel of Experts on Space and Security, March 2005. http://ec.europa.eu/enterprise/policies/space/files/article_2262.pdf.
Roger D. Launius, "United States Space Cooperation and Competition: Historical Reflections", in Astropolitics, Vol. 7, No. 2 (May 2009).
Serge Grouard et Odile Saugues, Rapport d'information déposé... par la Commission de la défense nationale et des forces armées sur les enjeux stratégiques et indus- triels du secteur spatial, op.cit.
Sergio Marchisio, "Organizzazione meteorologica mondiale (Omm)", postilla di aggiornamento, in Enciclopedia Giuridica, Aggiornamento XV, Roma, 2007. V. anche Wmo, http://www.wmo.int/pages/about/index_ fr.html.
Spazio: Ue Apre Negoziati Su Codice Di Condotta 2015. Affarinternazionali. https://www.affarinternazionali.it/archivio-affarinternazionali/2015/07/spazio-ue-apre-negoziati-su-codice-di-condotta/.
Stephan Hobe and Julia Neumann, "Global and European challenges for space law at the edge of the 21st century", in Space Policy, Vol. 21, No. 4 (November 2005).
Stephan Hobe, "Prospects for a European Space Administration", in Space Policy, Vol. 20, No. 1 (February 2004), p. 25-29. V. anche Frans G. von der Dunk, "Towards One Captain on The European Spaceship. Why the EU Should Join ESA", in Space Policy, Vol. 19, No. 2 (May 2003), pp. 83-86, http://digitalcommons.unl.edu/cgi/viewcontent.cgi? article=1055&context=spacelaw.
Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-ballistic Missile Systems, opened to signature at Moscow, 26 May 1972. http://www.state.gov/www/global/arms/treaties/ abm/abm2.html.
UN General Assembly, Resolution No. 1802 (XVII), International cooperation in the peaceful uses of outer space, (A/RES/1802(XVII), 14 December 1962.
V. Bernd Eissfeller et al., "Performance of GPS, GLONASS and Galileo", Wichmann Verlag, Heidelberg, 2007.
Valérie Niquet, La recherche spatiale en Chine: saut technologique et capaci- tés militaires, Paris, Institut français des relations internationales (Ifri), Juin 2007 (Asie Visions, 1), p. 6, http://www.ifri.org/downloads/visionasie1.pdf.

William E. Burrows, “Imaging Space Reconnaissance Operations During the Cold War: Cause, Effect and Legacy”, in Bodø Regional University, Cold War Forum, February 1997, http://webster.hibo.no/asf/Cold_War/report1/williame.html.

Wolfgang Rathge- ber, The European Architecture for Space and Security, Vienna, European Space Policy Institute, August 2008 (ESPI Report, 13), p. 22, http://www.espi.or.at/images/stories/ dokumente/studies/espi_ report_13.pdf.

Invisible Arsenals. Developing a Medical Intelligence Capability to Understand Current Biosecurity Threats

Ryan Clarke, LJ Eads, Xiaoxu Sean Lin, Robert McCreight, Hans Ulrich Kaeser

Dr. Ryan Clarke is a Senior Fellow at the Asia Center for Health Security, National University of Singapore and Co-Founder and Managing Director the CCP BioThreats Initiative and the Frontier Assessments Unit. His career has spanned leadership positions in defense, investment banking, biosecurity, strategic research units, and technology.

LJ Eads is a seasoned expert in research intelligence, data analytics, and technology development, currently leading research intelligence initiatives as Director at Parallax Advanced Research Corp. LJ's background includes service as a Space Network Warfare Analyst and SIGINT Analyst in the United States Air Force, where he conducted detailed intelligence analysis and provided critical support to high-level decision-makers. As the founder of Data Abyss, LJ develops innovative big data platforms focused on Chinese science and technology data, empowering intelligence analysts to identify emerging threats and adversary activities.

Xiaoxu Sean Lin is an assistant professor of Biomedical Science at Fei Tian College Middletown New York. He served in the U.S. Army as an officer and microbiologist, and was former laboratory director for Viral Diseases Branch at Walter Reed Army Institute of Research. He is also a member of the Committee of Present Danger China.

Robert McCreight served for 27 years in the US Army in combined active and reserve duty and served for 35 years in the US Department of State as an intelligence analyst, political-military affairs analyst and as the Deputy Director of Global Scientific Exchanges. This work is dedicated to his countless contributions and to his memory.

Hans Ulrich Kaeser is a management consultant providing government agencies and private companies with advice on managing strategic risks. He served as an intelligence officer in combined NATO missions and exercises before joining the private sector and holds Masters Degrees in International Relations from the Geneva Graduate Institute of International Studies, and Security Studies from Georgetown University.

Abstract

Biological warfare and bioterrorism have a long history, ranging from ancient times to the present, in which they have maintained their appeal to superpowers and lone wolf terrorists alike. Throwing a rotten camel into a water well illustrates their most convincing features: low cost of development, potentially devastating and large-scale effect, limited traceability.

For a while, international efforts culminating in the Biological Weapons Convention (BWC) of 1972, kept a lid on the development, production, and stockpiling of biological weapons. But the post-Cold War period witnessed significant shifts in the landscape of biological warfare and bioterrorism threats. As the world becomes more multipolar, biological warfare moves back to center stage of global security threats.

The development of asymmetric warfare capabilities, including biological weapons is experiencing a new surge. Meanwhile, an increasingly interconnected and globalized world with rapid transportation networks and growing urbanization present a target far more vulnerable to the devastating potential of biological warfare and infectious diseases.

Western countries are lacking fully integrated intelligence networks to properly assess the threat. Starting with the systematic collection of relevant epidemiological and medical information to the systematic integration with civil and military intelligence to the deployment of trained rapid reaction task forces to deal with public health emergencies.

The COVID-19 pandemic exemplifies this new reality. Heated debate lingers four years after the outbreak. Was it a naturally occurring disease or a synthetic agent? Was the outbreak an accident or deliberate? Maybe even state-sponsored? Are we looking at the once-in-50-years pandemic or a persistent global threat?

Much too little was known about the pathology of the virus, even though it had been studied for over two decades. Equally no common understanding of the challenges it posed to public health systems, which, in many cases, collapsed locally. Speculation, political meandering and conspiracy dominated the public debate. Assessing and responding to the current and future threat environment will require quite the opposite: A professional and fully integrated medical intelligence practice and a structural shift in the approach to strategic threat assessment.

This article tries to convey a cursory understanding of the current threat environment through the eyes of an intelligence analyst, looking for the confluence of capability and intent. It dives deep into scientific research programs developing deadly biological agents and molecular delivery methods to understand existing and future capabilities for biowarfare and bioterrorism. It will end incomplete, missing a critical piece to understanding the threat and devising the strategies to counter it. At this stage, the article can only offer a few recommendations on how to build the missing piece.

La guerra biologica e il bioterrorismo hanno una lunga storia, che va dall'antichità ai giorni nostri, in cui hanno mantenuto il loro fascino sia per le superpotenze che per i terroristi. Gettare un cammello in putrefazione in un pozzo d'acqua illustra le loro caratteristiche più convincenti: basso costo di sviluppo, effetto potenzialmente devastante e su larga scala, tracciabilità limitata.

Per un certo periodo, gli sforzi internazionali, culminati nella Convenzione sulle armi biologiche (BWC) del 1972, hanno tenuto sotto controllo lo sviluppo, la produzione e lo stoccaggio di armi biologiche, ma il periodo successivo alla Guerra Fredda ha visto cambiamenti significativi nel panorama delle minacce di guerra biologica e bioterrorismo. Con un mondo sempre più multipolare, la guerra biologica torna al centro delle minacce alla sicurezza globale.

Lo sviluppo di capacità di guerra asimmetrica, comprese le armi biologiche, sta vivendo una nuova impennata, nel frattempo un mondo sempre più interconnesso e globalizzato, con reti di trasporto rapide e crescente urbanizzazione, rappresenta un bersaglio molto più vulnerabile al potenziale devastante della guerra biologica e delle malattie infettive.

I Paesi occidentali non dispongono di reti di intelligence pienamente integrate per valutare adeguatamente la minaccia. Questo a partire dalla raccolta sistematica di informazioni epidemiologiche e mediche rilevanti, all'integrazione con l'intelligence civile e militare, fino al dispiegamento di task force di reazione rapida addestrate per affrontare le emergenze di salute pubblica.

La pandemia di COVID-19 è un esempio di questa nuova realtà. A quattro anni da quest'ultima, il dibattito è ancora acceso. Si è trattato di una malattia naturale o di un agente sintetico? Un incidente o un'azione deliberata? Forse addirittura sponsorizzata dallo Stato? Siamo di fronte a una pandemia che si verifica una volta ogni 50 anni o a una minaccia globale persistente?
La conoscenza della patologia del virus era troppo limitata, nonostante fosse stato studiato per oltre due decenni; allo stesso modo è mancata una comprensione comune delle sfide poste ai sistemi di sanità pubblica, che in molti casi sono collassati a livello locale. La speculazione, i meandri politici e le cospirazioni hanno dominato il dibattito pubblico. Per valutare e rispondere all'ambiente di minaccia attuale e futuro sarà necessario il contrario: una pratica di intelligence medica professionale e pienamente integrata e un cambiamento strutturale nell'approccio alla valutazione strategica delle minacce.
Questo articolo cerca di trasmettere una comprensione di alto livello dell'attuale ambiente di minaccia attraverso la lente di un analista di intelligence alla ricerca della confluenza di capacità e intenzioni. Esso si immerge in profondità nei programmi di ricerca scientifica che sviluppano agenti biologici letali e metodi di somministrazione molecolare per comprendere le capacità esistenti e future per la guerra biologica e il bioterrorismo.
Il testo si conclude in modo incompleto, mancando di un tassello critico per la comprensione della minaccia e l'elaborazione delle strategie per contrastarla, per il quale, allo stato attuale, l'articolo fornisce raccomandazioni su come costruirlo.

Keywords

Hybrid warfare, biological warfare, bioterrorism, intelligence, medical intelligence, Covid-19

1. Developing the Agent

In Israel, a badly wounded IDF Soldier, who recently returned from action in Gaza, died with a strange fungal infection, a rare occurrence in non-immunocompromised – otherwise healthy – individuals. Reports from across Israeli hospitals show a significant percentage of wounded soldiers returning from the battlefield with serious antimicrobial-resistant infections, they likely picked up through contact with contaminated soil, among other factors.

Meanwhile, on the battlefields of Ukraine, resistance to antibiotic treatments has become a particularly alarming phenomena, where the resistance is likely a consequence of the indiscriminate, life-saving use of antibiotic treatments by combat medics and in field hospitals. However, the spread of resistant bacteria goes far beyond battlefields and field hospitals. Seemingly isolated medical phenomena occurring within the general fog of war have far-reaching consequences for civil societies removed from warfare. Experts still seem far from understanding what these immunological phenomena mean for public health and decision makers are in the dark on how to respond. How serious is this threat? We may know far less than we think.

At the onset of the COVID-19 pandemic in early 2020, decision makers and experts were in the dark on every angle of the impending disaster, from its origin to its vectors of diffusion and the potential effect on humans and their societies. Public attention focused on Wuhan's wet markets, bat caves and pangolins. But when looking for capability and intent, the attention quickly shifts to the laboratory. Two recent reports show startling levels of at least the capability to engineer deadly pathogens in the vicinity of Wuhan's wet markets. What are those laboratories working on?

1.1 High-Risk Research on Deadly Corona Virus Continues in Wuhan

In August 2023, a new study was published in the American Society of Microbiology's *Journal of Virology*, announcing that a new mouse-adapted coronavirus strain named SMA1901 was generated by the Wuhan Institute of Technology, under Dr. Shi Zheng-Li. SMA1901 was generated by serial passaging the original virus strain (bat SARSr-CoV rRsSHC014S) in young and aged mice for 19 times and intentionally selecting more pathogenic strains at every passage.[1]

In this study, the young mice infected with SMA1901 showed a rapid loss of body weight, up to 10% of their body weight, 4 days post-infection. Viral RNA was detected in multiple organs, primarily in the lungs, trachea, and turbinates, but also in the heart, liver, spleen, kidneys, intestine, and brain. While the young, infected mice demonstrated robust weight loss, inflammation, and increased viral titers in the respiratory tract, no mortality was observed.[2]

However, aged mice infected with SMA1901 exhibited significant body weight loss starting at 2 days post-infection. Most of the aged mice demonstrated a 25% reduction in body weight. Within 3 days post-infection, the mice showed mortality and by 7 days post-infection, only about 15% of the aged mice survived (2 out of 15). The pathogenicity of SMA1901 in aged mice is comparable to the effects of COVID-19 observed in older human patients.[3]

This study appears to be just a study for bat coronavirus. However, the bat SARSr-CoV rRsSHC014S strain used to generate SMA1901 was known to strongly interacted with both human ACE2 and mouse ACE2 receptors. That is to say that the original virus before SMA1901 has the potential to infect human cells. In this regard, it obviously warrants an experiment to study SMA1901's infectivity in transgenic mice that express human ACE2 receptors. This component of the

[1] HF Lin, Zheng-Li Shi, et. al, 'Characterization of a mouse-adapted strain of bat severe acute respiratory syndrome-related coronavirus', *Journal of Virology*, Vol. 97, No. 9, 28 September 2023.
[2] Ibid.
[3] Ibid.

examination is very critical, indicating the potentially enhanced pathogenicity in humans. Yet, it is entirely missing in Shi Zheng Li's study.

Four years after the outbreak of the global COVID-19 pandemic, researchers in a Wuhan laboratory are developing more deadly variants of the same virus that probably killed millions worldwide. They test these variants on mice but publish no data on the pathogenicity for humans. The involvement of international scientists or institutions in these studies has simultaneously dropped significantly. Finally, the Gain-of-Function[4] method used in these studies are heavily regulated in the United States and European Union, due to biosafety and biosecurity risks and their dual-use potential. The alarm bells of the intelligence analyst looking for bioweapons capability are ringing.

1.2 New Lethal Virus by Design Under Military-Civil Fusion[5] Project in Beijing

Shi Zheng-Li's studies are no rarity, despite the high-risk methods used and international pressure to keep a lid on pathogen experiments in the aftermath of the COVID-19 pandemic. In fact, to the diligent observer it almost appears like a new competitive field of research. Another report recently surfaced on the pre-publication platform bioRxiv (bio-archive), offering a peak into a project involving similar levels of capability. The platform provides researchers the opportunity to receive initial feedback from the scientific community and make revisions to their reports before they are being published. Besides the alarming nature of the findings in this report, the revisions made shortly after it initially appeared are at least as concerning.

In January 2024, researchers from the Beijing Advanced Innovation Center for Soft Matter (BAIC-SM) Science and Engineering at Beijing University of Chemical Technology, the Research Center for Clinical Medicine at The Fifth

[4] Gain-of-Function (GoF) experiments are a controversial domain within biomedical science, defense and security fields. They are distinct from other scientific methods and approaches. These experiments are deliberately designed to enable pathogens to acquire and develop new properties including increased transmissibility, increased lethality, and resistance to drugs. It can also involve modifying pathogens to enable them to be transmitted between humans asymptomatically and/or to evade the human immune system response. Such lab-made chimera viruses are potentially more dangerous than viruses found in nature. GoF research has been subjected to episodic bans in the West while it has continued uninterrupted and virtually unregulated in China. During these prohibition periods in the West, some Western scientists have continued their GoF research with partners in China.

[5] For additional analysis of the Civil-Military Fusion Law, please see 'Alibaba and Ant Group: Involvement in China's Military-Civilian Fusion Initiative', RWR Advisory Group, 2 October 2020. https://www.rwradvisory.com/wp-content/uploads/2020/10/RWR-Report-Ant-MilCiv-Fusion-10-2020.pdf, accessed on 28 January 2024.

Medical Center of the PLA General Hospital (PLAGH), and State Key Laboratory of Pharmaceutical Biotechnology at Nanjing University claimed that a cell-culture passaged and adapted clone of a pangolin coronavirus isolate, GX_P2V C7, caused 100% mortality in a hACE2 transgenic mice model[6]. Lihua Song from the BAIC-SM was the lead and corresponding author for this shocking report. Very little is known about this researcher, which again raises suspicion for someone who is conducting such high-stakes research on a world-famous virus.

Based on previous studies conducted by Shi Zheng-Li from Wuhan Institute of Virology (WIV), prior to the COVID-19 outbreak, Lihua Song's group conducted further mouse model studies on the more deadly isolate, which may hint at the attempt to generate more viral mutants with higher pathogenicity for human infection.

Critically, they found that the GX_P2V(short_3UTR) clone can infect humanized mice with high viral loads detected in both lung and brain tissues. This infection resulted in 100% mortality in the humanized mice with these researchers assessing that the cause of death may be linked to the occurrence of late brain infection.[7] Although the high lethality in the human ACE2-transformed mice model might be due to high number of inserted copies of the hACE2 gene in the genome of this particular mouse model, the total killing within 8 days is still a shocking result and has triggered international concern. What is more, the GX_P2V(short_3UTR) mutant had not been previously studied to determine its adaptive mutations in cell cultures. To obtain a genetically homogenous clone for animal experiments, they cloned the serial passaged mutant through two successive plaque assays, a high-risk operation that is banned in the West.

Shortly after the report first appeared, it was revised and a new version appeared on the bioRxiv platform. The new version critically tunes down the 'lethal' tone of the initial report and gives it a new spin. The new narrative sells the study as an approach for vaccine or drug development. Yet, no scientific justification or reasoning was given for the serial passaging experiment that led to this new GX_P2V (short_3UTR) clone in the original January 4 study. In fact, many vaccine developers avoid doing serial passages of this novel virus, SARS-CoV-2, because still so little is known about this virus. The world continues to struggle with the challenges of its naturally generated variants. It is unclear as to why this research group decided to generate more risks with serial passages of this virus on animals that were not a natural reservoir for it. Given the level of protection against the development of severe disease provided by current vaccines, there is

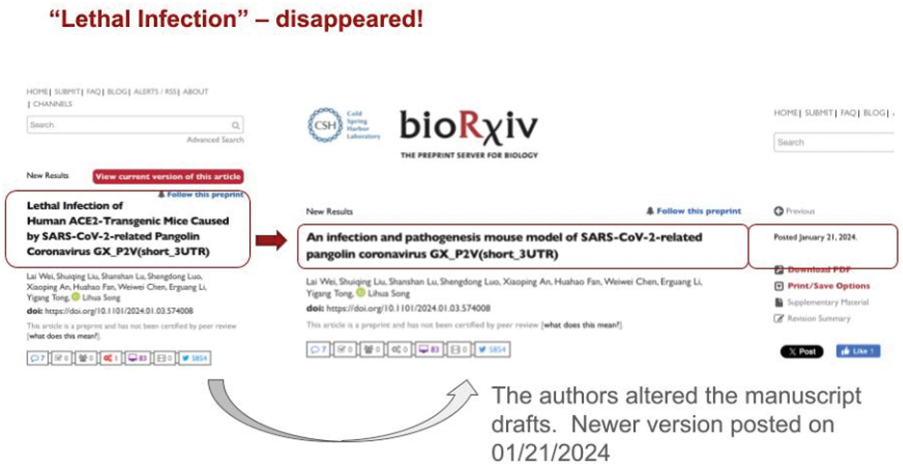
[6] Lai Wei, et. al., 'Lethal Infection of Human ACE2-Transgenic Mice Caused by SARS-CoV-2-related Pangolin Coronavirus GX_P2V(short_3UTR)', *bioRxiv*, 4 January 2024.

[7] Lai Wei, et. al., 'Lethal Infection of Human ACE2-Transgenic Mice Caused by SARS-CoV-2-related Pangolin Coronavirus GX_P2V(short_3UTR)', *bioRxiv*, 4 January 2024.

no clear civilian scientific justification to develop additional vaccines that protect against artificially enhanced SARS-CoV-2 viruses.

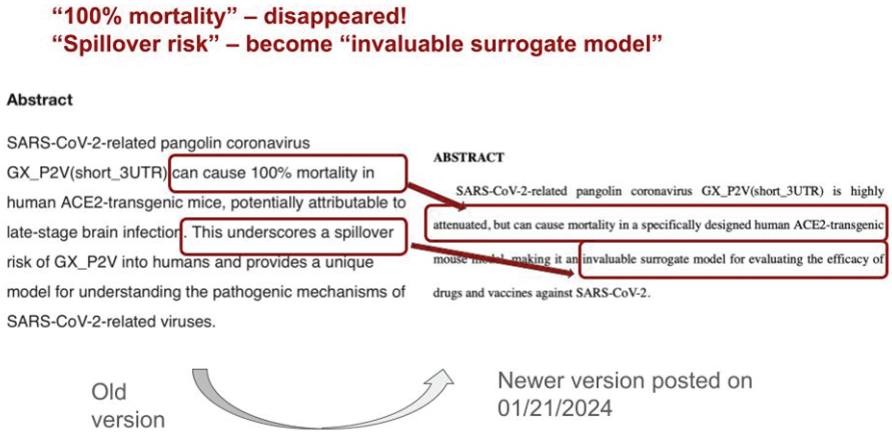
The following snapshots from the study show the contentious changes in Lihua Song's January 2024 report.

Figure 1



Screenshots from bioRxiv, accessed on 4 January and on 21 January 2024 respectively, showing Lai Wei, et. al., 'Lethal Infection of Human ACE2-Transgenic Mice Caused by SARS-CoV-2-related Pangolin Coronavirus GX_P2V(short_3UTR)'. The revised version omits the lethality of the infection with SARS-CoV-2.

Figure 2



Screenshots from bioRxiv, accessed on 4 January and on 21 January 2024 respectively, showing Lai Wei, et. al., 'Lethal Infection of Human ACE2-Transgenic Mice Caused by SARS-CoV-2-related Pangolin Coronavirus GX_P2V(short_3UTR)'. References to the 100% mortality and the serious spillover risk of the research are omitted in the revised version.

The point of sharing a report on the bioRxiv platform is to receive feedback from the scientist community prior to publication. Whatever the feedback the authors received on the initial version of the report, omitting spillover risks into humans and 100% lethality of a laboratory-engineered virus that was based on SARS CoV-2 clearly are not cosmetic changes.

Finally, the advances made by Dr. Shi Zheng-Li and a range of collaborators in reverse genetic engineering, render synthetic lab-created coronaviruses indistinguishable from coronaviruses originally found in nature. The implications of these developments are difficult to overstate.

For one, this injects a fundamental degree of uncertainty and unreliability into the countless investigations that are occurring across the world that seek to determine the origins of SARS-CoV-2, the virus that causes COVID-19.

Secondly, these advanced technologies enable a strong degree of plausible deniability in the event of a lab leak when engineering synthetic coronaviruses, conducting Gain-of-Function experiments on previously natural coronaviruses, and other high-risk pathogen research. The use of these technologies in laboratory settings has traditionally been confined to a relatively finite number of research groups in China and several Western countries.

1.3 BAIC-SM Emerges as a New Bioweapons Player in China

The bioweapons capability alarms are still ringing, even more so as these Chinese scientists seem to outcompete each other, using high-risk methods to develop deadly pathogens. The questionable revisions and obfuscation attempts raise a new level of concern to the intelligence analyst who tries to identify a threat. What are the reasons for the changes made to Song's study and ultimately, what is the true motivation of his research?

A closer look at the scientists' host institution may reveal just that. The mission statement of BAIC-SM Science and Engineering Center at the Beijing University of Chemical Technology explicitly lists 'novel research is at the core of our mission, and as such, high-risk research is encouraged wherever possible'.[8] It is questionable how a thorough bioethical review process can coexist with such a mission.

In addition, the Beijing University of Chemical Technology (BUCT) is completely committed to the Military-Civilian Fusion program that has been driven by the Chinese Communist Party (CCP) under Xi Jinping's leadership. A 2021 BUCT overseas talent recruitment program announcement stated that BUCT is 'treating industrial-academic fusion and military-civil

[8] 'About Us', Beijing Advanced Innovation Center for Soft Matter Science and Engineering (BAIC-SM), Beijing. https://en-baicsm.buct.edu.cn/388/list.htm, accessed on 28 January 2024.

fusion as key development opportunities, and to establish the BAIC-SM for Soft Matter Science and Engineering'.[9] This advertisement directly states that the BAIC-SM program could be an outcome of BUCT's engagement in the Military-Civil Fusion program.

Meanwhile, it is surprising that BUCT was actually selected to develop 'Biosafety' as a core competence in the list of Advanced Academic Programs to be established among higher education institutes in Beijing in 2021.[10] A chemical engineering and technology institute being chosen to develop core competence for 'Biosafety' is definitely unusual, especially considering that Beijing has many other institutions that have stronger biotechnology talent pools.

So far, the intelligence analyst confirms the existence of animate – if not competitive – research activity on lethal pathogens that have already wreaked havoc on humans worldwide. The reports are an unequivocal show of dual-use capability, encouraged and conducted under the scope of a Military-Civil Fusion, high-risk research program. This is far from a smoking gun but a clear indication of intent to accept high biosafety risks in the development of what turned out to be a deadly pathogen with devastating potential for public health. The attempts to frame it as an effort to develop a vaccine, years after several effective vaccines against the naturally occurring mutations are available on an industrial scale, only corroborates the analyst's suspicions.

2. Deploying the capability: Nanotechnology and the Weaponization of Deadly Agents

To get a better understanding of the intent, it often helps to investigate the sponsorship of these programs – ideological and pecuniary. Exactly what does a military-civil fusion program do? What does it fuse? And what are its objectives? As the intelligence analyst broadens the scope, a vast array of dual-use studies appear. The military research and development programs of the CCP and the People's Liberation Army (PLA), which is the armed wing of the CCP and the core military force in China, cover a range of advanced weaponry projects, distinctly focused on asymmetric warfare. This includes biological, biochemical and neurobiological weapons.[11]

[9] 'Notice of the Beijing Municipal Education Commission on Announcing the List of High-tech Disciplines in Beijing Colleges and Universities', Beijing Institute of Petrochemical Technology, 11 November 2021. https://www.bipt.edu.cn/pub/graduate/xkjs/xkjsdt/228207.htm, accessed on 28 January 2024.

[10] Ibid.

[11] For more in-depth analysis of these programs, please see Ryan Clarke, Xiaoxu Sean Lin and LJ Eads, *China's International Military-Civilian Virology Fusion: High-Risk Pathogen Re-*

2.1 Nanotechnology Platforms: A Transformative Capability?

The convergence of nanotechnology with various scientific disciplines offers particularly interesting options in the realm of asymmetric warfare, from nanoscale drugs to nanorobots using communication systems based swarm intelligence.

Nanoscale drug delivery systems might transport biological agents directly to target cells with deadly precision. Moreover, nanorobots could navigate the human body, delivering lethal payloads while evading conventional biological defenses. This is not a hypothetical concern.

Researchers from the Hefei Institute of Physical Science, Chinese Academy of Sciences, have made a 'breakthrough' in DNA nanotechnology, developing a smart DNA molecular nanorobot model. This model innovatively proposes a non-linear gathering 'siege' of biological targets, allowing for advanced signal amplification and intelligent targeted drug delivery.[12]

The nanorobot model consists of multifunctional robotic arms with optional accessories (such as drugs and signal tags), target validators, intelligent swarm path controllers, and self-assembling motors. It responds only to specific biological targets, forming a large aggregate through cooperative operations and achieving nonlinear cascade amplification or amplification of target signals.

The study suggests that this technology has potential applications in biosensing, bioimaging, and drug delivery. However, there are risks associated with this advancement. The ability of nanorobots to transport biological agents directly to target cells with deadly precision could be exploited for harmful purposes. It could be used to deliver biological agents with precision, making it a potential threat for biological warfare. Additionally, the close collaboration between the Hefei Institute of Physical Science and the PLA raises concerns about potential dual-use applications of this technology for military purposes.[13]

The nanorobot study is far from evidence of a credible threat. It is one amongst countless examples of research projects that will produce credible

search, Global Linkages and Strategic Implications, Broad Publishers, Taipei, March 2023.
LJ Eads, Ryan Clarke and Xiaoxu Sean Lin, 'In the Shadows of Science: Unravelling China's Invisible Arsenals of Nanoweapons', CCP BioThreats Initiative, August 2023. In+the+Shadows+of+Science+-+Unravelling+Chinas+Invisible+Arsenals+of+Nanoweapons.pdf (squarespace.com), accessed on 22 January 2024.

[12] 'The Chinese scientific research team proposes a model of intelligent nano-robots gathered to "siege" biological targets', *China News Network*, 19 May 2023. 中国科研团队提出云集"围攻"生物靶标智能纳米机器人模型-中新网 (chinanews.com.cn), accessed on 17 January 2024.

[13] Ibid.

dual-use applications for asymmetric warfare. There may not be a ready-to-deploy nanoplatform that can be weaponized with biological agents today and tomorrow. However, the immense challenge with fusion programs is that until the actual point of fusion its components are inconspicuous or seemingly benign. At the point of fusion these programs can generate an existential threat potential overnight. The intelligence analyst must therefore develop a muscle for cognitive fusion. Capabilities must be assessed in terms of their exponential fissile power when combined with other next-generation projects.

Through this lens, the intelligence analyst will see a vast invisible arsenal of deadly biological agents and untraceable delivery methods with molecular precision. What are these capabilities being developed for? What is the end game? The only thing that becomes clear from the evidence is that these developments occur independently of international cooperation or involvement of any sort. This reality has major strategic implications.

3. Strategic Implications

While the CCP and the PLA previously required intensive and targeted international connectivity to obtain the technology and specialized knowledge required to make advancements in fields such as bioweapons and nanoplatforms, recent evidence suggests that this is no longer the case. China now has robust domestic capabilities that provide Beijing with a range of asymmetric options against perceived adversaries. These developments have occurred while many strategic and intelligence analysts have focused more heavily on China's conventional military assets such as its aircraft carriers, submarine fleet and rocket forces. However, when arrayed against aggregated American and Western capabilities, the PLA has virtually no prospect for establishing any form of strategic parity, let alone overmatch. As such, Chinese advancements in the unconventional domain areas of bioweapons and nanoplatforms assume an even greater degree of relevance and criticality.

3.1 From Critical International Dependency to Domestic Self-Sufficiency

When the Chinese Communist Party (CCP) began its ambitious programs to become a world leader in strategic dual-use technology domain areas such as bioweapons and nanoplatforms, Beijing had critical dependency on continuous access to intellectual property, specialized knowledge and technical guidance from international sources. China's own domestic research and development and technology operationalization capabilities lagged far beyond key Western countries, Japan, South Korea and even Russia. However,

through continuous targeted engagement with specific international research institutes, scientists, engineers and companies, the CCP has been able to discreetly establish itself as a world leader with 'first-mover advantage' across several strategic technology domain areas.

In 2024, the CCP no longer requires international connectivity and access to continue to development its virology and nanoplatform dual-use research programs. China has absorbed the technology, knowhow and has trained and developed an adequate number of personnel domestically to have achieved self-sufficiency. China will of course still absorb international inputs if and when they become available but there are no longer the critical dependencies of the past.

The CCP's continued high-risk pathogen research on SARS-CoV-2 is particularly problematic and demonstrates that Beijing assigns a high degree of strategic importance to serial passaging experiments continuing to be done in China despite being banned across the West. This is in spite of the fact that the SARS-CoV-2 virus is directly responsible for the deaths of millions of people across the world. No SARS-CoV-2 serial passaging experiment has been credibly linked to any existing vaccine, therapeutic, prophylactic or diagnostic. The fact that this work continues, including in Wuhan itself, likely demonstrates that there is a broader strategic logic underpinning this continued high-risk pathogen research.

Chinese advancements in nanoplatforms also generates a new set of risks and strategic uncertainties. Nanoplatforms serve as a 'horizontal layer' that can miniaturize, massively decentralize and obfuscate origins across the full range of asymmetric capabilities of the CCP and the PLA. This includes, but is not limited to:

- Nanomedicine as a Weapon
- Nanorobotics and Autonomous Weapons
- Nano-Bioinformatics for Biowarfare
- Nano-Scale Chemical Sensors
- Nano-Cyber Biological Weapons
- Advanced Chemical Warfare
- Covert Surveillance and Assassination
- Non-Conventional Attacks
- Cyber-Biological Attacks
- Targeted Biological Warfare

The above domain areas have the potential to fundamentally and irreversibly transform the nature of next-generation medical intelligence collection, integration and distribution and the threat assessments. The CCP's deliberate decision to dedicate resources, personnel and national prioritization to the fields of bioweapons and nanoweapons provides insight into where Beijing as-

sesses its own unique strengths to lie and, possibly, where Beijing has assessed its adversaries to have weaknesses in their own intelligence and emergency response systems.

Two elements of this conclusion must not be overlooked. First, cutting-edge research in next-generation technology, including bio or nanotechnology are no longer the exclusive domain of Western countries. The establishment of independent domestic capabilities in China create a level of intransparency and uncertainty that complicates realistic threat assessments. Second, the fusion programs combining the capabilities of bio-engineering, neuroscience and nanotechnology will produce unimaginable novel offensive capabilities. The application of artificial intelligence to these research programs will potentiate their outcomes and erode the last shred of predictability on these domains.

4. Conclusion and Policy Recommendations

It is essential to recalibrate and refocus capabilities on the demonstrably highest probability source of the next pandemic: synthetic viruses that are increasingly being created in labs in China. American and other Western scientists were fundamental in the early stages of this process, but they have now been relegated to the sidelines. This structural shift needs to be broadly recognized and directly acted upon immediately.

Genetic engineering technologies, as seen in the SARS CoV-2 studies discussed earlier, introduce a compounding challenge to the strategic threat environment. Synthetic and naturally occurring pathogens become indistinguishable. Consequently, weaponized biological agents become practically untraceable. This makes current forensic assessment and attribution capabilities and tracking systems almost obsolete. Early warning and detection systems as well as rapid response and monitoring teams must broaden their scope and engage in intelligence fusion. True protective capability can no longer rely on bio forensics but must develop the muscle to integrate previously disparate pieces of information and data from various fields of scientific and military expertise.

In response to the outbreak of the COVID-19 pandemic, vast amounts of public resources were spent with countless dedicated clinicians, scientists, and others working tirelessly to protect public health. However, we do not presently have a pandemic risk surveillance system or rapid diagnostic tools commensurate to the current threat level, let alone a new and rapidly emerging one. This is not to suggest that the infectious disease surveillance and control work done for example by the U.S. Agency for International Development (USAID) and others is futile. However, it must be noted that the

majority of zoonotic pathogens that infect humans with the highest statistical frequency, such as malaria, dengue, scrub typhus, melioidosis, leptospirosis, and others are not transmissible between humans. Therefore, they don't pose a high risk of causing a global, or even regional, pandemic.

Key scientists and medical technicians were indispensable in fighting the devastating effect of the pandemic, they will also play a crucial role in building, operating and protecting biosecurity systems. Instead of leading government task forces and delivering press statements for political purposes they must build and operate the medical and epidemic intelligence networks, governed by rigorous intelligence processes.

Epidemic Intelligence (EI) primarily focuses on the surveillance and early detection of infectious disease outbreaks, whether they arise naturally or as a result of deliberate actions, such as bioterrorism. EI involves the systematic collection, analysis, and interpretation of health data from diverse sources, including hospitals, laboratories, public health agencies, media reports, and social media platforms. By monitoring trends in disease incidence, geographic spread, and population susceptibility, EI aims to identify potential outbreaks promptly and facilitate rapid response efforts to contain and mitigate their impact. Key components of Epidemic Intelligence include epidemiological surveillance systems, disease modelling techniques, and information-sharing networks.

Medical Intelligence (MI) encompasses a broader range of health-related threats, including infectious diseases, chemical and radiological exposures, bioterrorism, and other public health emergencies. MI integrates information from diverse sources, such as medical and scientific literature, intelligence reports, open-source data, and expert analysis, to assess the nature, magnitude, and implications of health threats for national security and public health preparedness. MI analysts evaluate the capabilities and intentions of adversaries, assess vulnerabilities in health infrastructure, and provide policymakers with timely and actionable insights to support decision-making and resource allocation. MI also encompasses medical surveillance, which involves monitoring the health status of key personnel, high value targets, persons of interests, military personnel, travelers, and populations at risk of exposure to health threats in operational settings, conflict zones or other zones of interests.

While Epidemic Intelligence focuses primarily on infectious disease surveillance and response, Medical Intelligence adopts a broader perspective, encompassing a wide range of health threats and vulnerabilities, including those related to chemical, radiological, and unconventional weapons. Both fields play complementary roles in safeguarding public health and national security. They must closely collaborate and integrate with national security

and intelligence agencies to assess the threat of emerging infectious diseases and the invisible arsenals of bioweapons.

References

'About Us', Beijing Advanced Innovation Center for Soft Matter Science and Engineering (BAIC-SM), Beijing.
https://en-baicsm.buct.edu.cn/388/list.htm

'Alibaba and Ant Group: Involvement in China's Military-Civilian Fusion Initiative', RWR Advisory Group, 2 October 2020.
https://www.rwradvisory.com/wp-content/uploads/2020/10/RWR-Report-Ant-Mil-Civ-Fusion-10-2020.pdf

HF Lin, Zheng-Li Shi, et. al, 'Characterization of a mouse-adapted strain of bat severe acute respiratory syndrome-related coronavirus', *Journal of Virology*, Vol. 97, No. 9, 28 September 2023.

Kristopher M. Curtis, Boyd Yount, Ralph S. Baric, Methods for producing recombinant coronavirus, US Patent US7279327B2, 2002-04-19.

Lai Wei, et. al., 'Lethal Infection of Human ACE2-Transgenic Mice Caused by SARS-CoV-2-related Pangolin Coronavirus GX_P2V(short_3UTR)', *bioRxiv*, 4 January 2024.

Li Shengsong, et. al, 'Core-shell quantum dot-nano-gold particle assembly for efficient detection of nerve agent mimics (**核壳型量子点**-纳米金颗粒组装体高效检测神经性毒剂模拟剂)', *Journal of Inorganic Materials*, Issue 8, 12 September 2019.

LJ Eads, Ryan Clarke and Xiaoxu Sean Lin, 'In the Shadows of Science: Unravelling China's Invisible Arsenals of Nanoweapons', CCP BioThreats Initiative, August 2023.
In+the+Shadows+of+Science+-+Unravelling+Chinas+Invisible+Arsenals+of+Nanoweapons.pdf (squarespace.com)

Mei-Qin Liu, et. al., 'A SARS-CoV-2-Related Virus from Malayan Pangolin Causes Lung Infection without Severe Disease in Human ACE2- Transgenic Mice', *Journal of Virology*, Vol. 97, Iss. 2, February 2023.

'Notice of the Beijing Municipal Education Commission on Announcing the List of High-tech Disciplines in Beijing Colleges and Universities', Beijing Institute of Petrochemical Technology, 11 November 2021.
https://www.bipt.edu.cn/pub/graduate/xkjs/xkjsdt/228207.htm, accessed on 28 January 2024.

Powerful information revealed about COVID ft. Dr. Reiner Fuellmich & Dr. David Martin | The last 16 months have been a rollercoaster of fears and facts, and we have seen the narrative behind COVID-19 change constantly, it was novel after... | By Randy Hillier | Facebook

Ryan Clarke, Xiaoxu Sean Lin and LJ Eads, *China's International Military-Civilian Virology Fusion: High-Risk Pathogen Research, Global Linkages and Strategic Implications*, Broad Publishers, Taipei, March 2023.

Ryan Clarke, 'Emerging Pandemic Risks Come From Engineered Viruses in Chinese Labs, Not the Jungle or Bat Caves', Epoch Times, September 4, 2021.
Emerging Pandemic Risks Come From Engineered Viruses in Chinese Labs, Not the Jungle or Bat Caves | The Epoch Times
'The Chinese scientific research team proposes a model of intelligent nano-robots gathered to "siege" biological targets', *China News Network*, 19 May 2023.
中国科研团队提出云集"围攻"**生物靶**标智能纳米机器人模型-**中新网** (chinanews.com.cn), accessed on 17 January 2024.
Qing Xiong, et. al., 'Close relatives of MERS-CoV in bats use ACE2 as their functional receptors', *Nature*, December 2022.

Challenges in Countering Domestic Terrorism in the Absence of Common Intelligence Instruments – Is Japan Closer to Establishing its Own Central Intelligence?

Rene D. Kanayama

Rene D. Kanayama, B.A. (Philosophy & Ethics), M.A. (International Relations), Postgraduate Diploma (Oil & Gas Technology), MBA (Oil & Gas Industry Management), has been professionally engaged in the region of post-Soviet republics, Western Balkans and Middle East since 2003. At Institute ITSTIME he participates in academic activities as a Senior Researcher for Electronic Warfare and Electromagnetic Spectrum Operations, as well as the Head of Central Asia Branch. In a capacity of multiple Government Advisory positions, he has counselled both the government agencies and investing international corporates on issues of direct investment, energy security and counter-terrorism. He has advised an overseas Diplomatic Mission of the Republic of Tajikistan on economic relations from 2009 to 2017, and from April 2022 acts as a Foreign Direct Investment Representative and Adviser to a Kyrgyz business federation.

Abstract

In the era when terrorism, in its multitude of shapes and forms, defines both the daily lives of ordinary citizens as well as briefing formats of countries' Commander-in-Chiefs, it is commonly perceived that every nation has already established several intelligence bodies, each equipped to deal with specific tasks and challenges that terrorism poses. Countries such as Israel or France have even created special intelligence bodies that address nuclear issues (both in its energy spectrum, as well as in its military applications) as one separate domain significant enough to warrant an exclusive attention. Sweden operates the Psychological Defense Agency to specifically counter foreign information influence directed towards the country by its adversaries.

While the global intelligence community and academia have grown accustomed that each nation operates at least three distinct intelligence entities (one tasking with collecting foreign intelligence, one focused on domestic issues and counter-intelligence, and at least one intelligence agency operating in the military realm), there are some national anomalies even among the G7 countries that defy the common sense when discussing a country's intelligence collection set-up, most notably Japan – which does have nominal government branches assigned to information and intelligence gathering but manages them in a manner significantly different than most other world powers. In a discourse about the intelligence gathering capabilities of any developed nation it is customary to highlight the equivalents of bodies such as the US Central Intelligence Agency, British Secret Intelligence Service, Israel's MOSSAD or France's DGSE – although in the case of Japan one needs to dig deeper to actually discover what bodies are tasked with intelligence issues.

The article aims at highlighting some of the challenges Japan faces when it comes tackling the many examples of both domestic-grown as well as potentially foreign-originated acts of terrorism – because of its very structure (or lack of it) in the country's intelligence apparatus. As part of the clarification of various factors involved, the author will discuss the constitutional constraints in Japan in relation to countering historical examples of religious-driven terrorism, and also will touch upon the issue of absence of full-fledged intelligence agencies (both domestic and foreign focused) in the understanding of Western intelligence mechanisms – which at large prevent the functioning of the state security apparatus in both preventing and counteracting the terrorism incidents.
Some attention is also given to the general inability to develop counter-terrorism policies in Japan because of the lack of classified/compartmented information mechanisms among Government agencies – whereby procurement and sharing the vital intelligence is of utmost significance. The conclusions made based on this brief outline could also lead to a discourse whether Japan could become the next soft target of international terrorism (not necessarily stemming from Islamic radicalism, but also various issues related to cyber security and the increasing number of international conflicts) and what factors can be identified to prevent such occurrences from happening.

Nell'era in cui il terrorismo, nella sua moltitudine di forme e forme, definisce sia la vita quotidiana dei cittadini comuni sia i formati di briefing dei comandanti in capo dei paesi, è comunemente percepito che ogni nazione ha già istituito diversi organi di intelligence, ciascuno attrezzato per affrontare compiti e sfide specifici posti dal terrorismo. Paesi come Israele o Francia hanno persino creato organismi di intelligence speciali che affrontano le questioni nucleari (sia nel suo spettro energetico, sia nelle sue applicazioni militari) come un dominio separato abbastanza significativo da meritare un'attenzione esclusiva. La Svezia gestisce l'Agenzia di difesa psicologica per contrastare specificamente l'influenza delle informazioni straniere diretta verso il paese dai suoi avversari.
Mentre la comunità dell'intelligence globale e il mondo accademico si sono abituati al fatto che ogni nazione gestisce almeno tre distinte entità di intelligence (una incaricata di raccogliere informazioni straniere, una focalizzata su questioni interne e controspionaggio e almeno un'agenzia di intelligence che opera nel regno militare), ci sono alcune anomalie nazionali anche tra i paesi del G7 che sfidano il buon senso quando si parla della struttura di raccolta di informazioni di un paese, in particolare il Giappone – che ha rami governativi nominali assegnati alla raccolta di informazioni e intelligence ma li gestisce in un modo significativamente diverso rispetto alla maggior parte delle altre potenze mondiali. In un discorso sulle capacità di raccolta di informazioni di qualsiasi nazione sviluppata è consuetudine evidenziare gli equivalenti di organismi come la Central Intelligence Agency degli Stati Uniti, il Secret Intelligence Service britannico, il MOSSAD israeliano o la DGSE francese – anche se nel caso del Giappone bisogna scavare più in profondità per scoprire effettivamente quali organismi sono incaricati delle questioni di intelligence.
L'articolo mira a evidenziare alcune delle sfide che il Giappone deve affrontare quando si tratta di affrontare i numerosi esempi di atti di terrorismo sia di origine nazionale che potenzialmente originati all'estero, a causa della sua stessa struttura (o della sua mancanza) nell'apparato di intelligence del paese. Nell'ambito del chiarimento dei vari fattori coinvolti, l'autore discuterà i vincoli costituzionali in Giappone in relazione alla lotta agli esempi storici di terrorismo di matrice religiosa, e toccherà anche la questione dell'assenza di agenzie di intelligence a pieno titolo (sia nazionali che focalizzato sull'estero) nella comprensione dei meccanismi

di intelligence occidentali – che in generale impediscono il funzionamento dell'apparato di sicurezza statale sia nel prevenire che nel contrastare gli episodi di terrorismo.
Una certa attenzione viene prestata anche alla generale incapacità di sviluppare politiche antiterrorismo in Giappone a causa della mancanza di meccanismi di informazione classificata/compartimentata tra le agenzie governative – per cui l'acquisizione e la condivisione di informazioni vitali è della massima importanza. Le conclusioni tratte da questo breve profilo potrebbero anche portare a discutere se il Giappone potrebbe diventare il prossimo bersaglio debole del terrorismo internazionale (non necessariamente derivante dal radicalismo islamico, ma anche da varie questioni legate alla sicurezza informatica e al crescente numero di conflitti internazionali) e quali fattori possono essere identificati per evitare che tali eventi si verifichino.

Keywords

Counter-Terrorism, Intelligence Services, Constitutional Constraints, Classified Information Mechanisms

1. Introduction – The Post-World War II Domestic Political Developments as a Precursor of Country's Intelligence Collecting Structure

Japan has had her own share of various societal upheavals after the World War II that often resulted not only in clashes between the ruling political elite and the discontented masses, but also to the forming of multiple right-wing and ultra-left groupings that contributed to the most violent assertion of the respective organization's political agenda. The establishment of these extremist political syndicates had roots in manifold post-war realities – from opposition to the United States – Japan Security Treaty, perception of a loss of national identity, to embracing some of the international political tendencies inclined to the left spectrum, especially in the 1960's among the Japanese youth.

Jo notes that in addition to the post-war development of Japan's security stratagem closely aligned with the US vision of Japan's role in Far East Asia at large, the institution of the Emperor, usually associated with all Japan's right-wing tendencies, had a role in shaping the today's security nexus of the country:

> In the 1970s, through approval of the US-Japan Security Treaty and peace constitution, the emperor's responsibility in the war was obscured. Enthroned in 1989, Emperor Heisei then came to symbolize peace in postwar Japan. Thus, one should now seek the Emperor System's agenda, not in the past war responsibility, but in its role of building trust for postwar Japan's peaceful image and taking responsibility for peace in the future. As East Asian nationalism

> continues to clash without any compromise and as Japan attempts to restore armament, even this 'image' of peace established by the symbolic Emperor System is at stake.[1]

The new regional conflicts, including the ones on the Korean peninsula and Vietnam also led to the polarization of both the Japanese intelligentsia and political parties. The formation of the entities such as Japanese Red Army and United Red Army – splinter groups after its predecessor Red Army Faction was merely a symptom of the turbulent post-war period and were responsible for several both domestic and international incidents that in today's terminology and perception can only be classified as the most violent terrorist acts recorded in history. Although these events are not a focal point of the article, let us recall the Lod Airport Massacre in 1972, hijacking of a Japan Airlines flight to North Korea in 1970, as well as domestic hostage and siege incidents or the series of local riots organized in protest of new Narita International Airport construction that lasted well into 1980's. The terrorism act at the Lod Airport was executed in particular with brutality rarely associated with the Japanese subjects in modern history:

> On May 30, 1972, three members of the Japanese Red Army, a terrorist offshoot of the Japanese New Left, arrived at Lod Airport in Tel Aviv on Air France flight 132 on the Paris–Rome–Tel Aviv route. In the airport's baggage claim area, they retrieved Kalashnikov assault rifles and hand grenades concealed in their luggage, opened fire, and threw the hand grenades at passengers in the baggage waiting area. They killed 25 people, most of them tourists from Costa Rica, and wounded 78 people in all. One of the terrorists was captured. Two were killed, one accidentally shot by his colleague, the other after landing on a hand grenade. An Israeli journalist wrote, "The scene here at Lod Airport is like after a pogrom. Broken glass panes, doors riddled with bullet holes and blood patches on every side." The attack was coordinated with the Popular Front for the Liberation of Palestine (PFLP). Aside from the destruction of the Swissair flight in 1970 that claimed 47 lives, the Lod Airport attack was the worst single attack in Israel in the post-1967 terrorist campaign carried out by a member organization of the PLO's Executive Committee.[2]

It would only be legitimate to assume that the nature of the events spanning over almost 80 years after the end of the World War II in Japan would create fertile environment for several full-fledged intelligence agencies to be established, operate and exert influence in both the law enforcement as well

[1] Jo G. (2015), The Revival of Japanese Right-Wing Thought and the Coincidental Collaboration of the Left and Right, p. 36.

[2] Herf J. (2016), Palestinian Terrorism in 1972: Lod Airport, the Munich Olympics, and Responses, Cambridge University Press, p. 1.

as prevention of terrorism – however to this date the debate of "when" the situation in Japan would be mature and favorable enough for the equivalent of the CIA, MI6 or MOSSAD to be instituted remains just a debate.

It is generally perceived that the long-term dependence of Japan notably on its major ally – the USA – has not created the environment in need of a powerful national intelligence agency (although looking at the neighboring South Korea, the US did contribute heavily to establishing an entity once known as K-CIA). In today's true globalization of the terrorism itself however, Japan is made to feel both the necessity and pressure in designing its intelligence apparatus to be capable of countering the most distressing threats coming from multiple directions. The article aims to address the structural and systemic issues that in Japan by large prevent the countering of terrorism as perceived by contemporary standards, and explains some of the underlining factors that contribute to this collective idiosyncrasy.

2. Constitutional constraints in Japan in countering religious-driven terrorism

Japan has not been immune to the religious radicalism, in particular after the World War II, when the religious monopoly of State Shinto has been abolished. Although it is yet to see any particular impact of internationally occurring examples of Islamic fundamentalism within Japan – making Japan as a country somewhat of an anomaly as the Islamic extremism is already thriving in neighboring regions of South-East Asia – Thailand, Bangladesh, Indonesia, Philippines or Central Asia – let us be clear that historically we can find acts of terrorism in most religious directions. Some of the examples we need to mention would include the actions of Reverend Jones's Christian cult in Guyana in 1978, the cult of Branch Davidian in Waco in 1993, a course of action against the Muslim population of Myanmar resorted to by Buddhist groupings, and of course the quasi-religious doomsday cult of Aum Shinrikyo which in its characteristics combines multiple Eastern religious streams with the obsession with Biblical prophecies. In fact, with regard to Islamic extremism in Japan – it is almost non-existent. Statistics state that in the country of 125 million inhabitants, only 250,000 are identified as Muslims, and 95% of these are composed of low-income migrating work force from countries such as Bangladesh, Indonesia or China. One of the reasons why the Muslims as a religious group do not congregate in Japan may be that Japan geographically represents a "dead end", and the migrant flows will not use the country as a platform to move to other countries if coming from the Eurasian continent. Another reason may be the low conversion rate of the local population (only about 5% of all Muslims in Japan are actually the Japanese).

For the purpose of examining the religion as a societal phenomenon and its relationship to acts perceived as threat from the national security perspective (shortly – terrorism), Japan finds its inability (or unwillingness) to surveil extremist religious groupings rooted in its post-war constitutional set-up. In 1945, the Imperial Japan's official ideology embedded in a religious-societal movement called "State Shinto" was abolished, together with the "divine origin of the Emperor" and the path was paved for literally any movement characterizing itself as "religious" by the new Constitution of 1947. As such, in 2023 there were more than 180,500 religious groups recorded in Japan, all of them enjoying the protection under the Constitution, as well as multiple fiscal and tax privileges. While the Article 20 of the Japanese Constitution guarantees the freedom of religion, together with Article 89 they are designed to separate the religion from the state and prevent the former State Shinto from gaining any dominant position in the society.

> Article 20 appears to guarantee absolute freedom of religion by not providing any explicit exceptions to that freedom. The only exceptions provided in the Article withhold power from the state in order to protect that religious freedom.[3]

It seems that the general perception of the State not protecting or providing exceptions to any of the organizations registered as "religious" creates the illusion that the State should not interfere with the activities of any such religious group, and as a result providing a fertile soil for either depraved or even potentially criminal pursuits of such groups to go unnoticed. While the State Shinto, having direct connotations with pre-World War II Japan is certainly of no threat to today's society, its former privileged standing is at the foundation of today's Constitution with regard to religious freedom for all organizations defining themselves as such.

> Without the threat of revived State Shintō, Article 20 only serves to protect free conscience in two very distinct forms. One form serves to shield the people from legislation that would impose religious laws, such as Canon Law or Shari'a Law, which is in no way a current threat. More pressing, Article 20 serves to protect religions from the people. Popular opinion in Japan distrusts religions and believes they should no longer enjoy tax privileges. In such a political climate, there simply exists no compelling reason to keep the government from engaging with religious groups to ensure their continued freedom.[4]

Only in the wake of Aum Shinrikyo's perpetrated sarin gas attack on the Tokyo subway in 1995, a year later the law was adopted to enable the Government

[3] Van Winkle A.B. (2012), Separation of Religion and State in Japan: A Pragmatic Interpretation of Articles 20 and 89 of the Japanese Constitution, p. 381.
[4] Ibid, p. 395.

to supervise certain religious groups – but the terrorist act itself did not lead to the religious group being banned, with authorities fearing backlash based on the constitutional guarantees.[5]

Although by early 21st century, the Islamic extremism and fundamentalism have been monitored internationally given its high-perceived risk to the national security of both developed as well as developing nations, it was only in 2011 that it emerged that the National Police Agency systematically collected personal data of Muslims of foreign origin only to be dismissed three years later by court as a "necessary step" in protecting national security interests. In other words, if there are any measures undertaken to counter any potential threat arising from international terrorism, such measures are very nascent in nature and by far inadequate compared to the scale of internationally perpetrated terrorism acts by extremists.

3. Various Perceptions on the Structure of the Japanese Intelligence Community

Professor Ken Kotani, in a podcast recorded in June 2024, summarized the key players of the Japanese intelligence community as follows:

> The size of the Japanese intelligence community is very small, but complicated. At present, the Cabinet Intelligence Research Office silo of the Cabinet Secretariat is a central intelligence machinery of the community, similar to the American CIA, but the number of staff is very small – only 500.
>
> There are also five ministry-embedded apparatuses. The Public Security Department of the National Police Agency, NPA, is close to the American FBI, which engages in counter-espionage and [counter-] terrorism in Japan. The defence

[5] In the morning of March 20, 1995 when the Tokyo subway gas attack was perpetrated, the author was in the epicenter of the incident between the subway stations Kasumigaseki and Akasaka Mitsuke, witnessing the chaos resulting from at that moment yet unknown cause. The event certainly resulted in the nation's most broadcasted and commented issues encompassing the religious freedom, principles of democracy as well as the capabilities (or the lack of) the law enforcement agencies countering the terrorist act. Even during the immediate days following the incident, observers were overwhelmed with the volume and diversity of auxiliary events, unable to either connect the dots or analyze them in a qualified manner – because of the very seemingly non-relatedness of the happenings. Let us just mention two – the debate why a chief Aum Shinrikyo cult member tasked with the "scientific research" succumbed immediately to a knife attack by a right-wing Korean national while the National Police Agency's Commissioner General Takaji Kunimatsu, shot by four rounds from a magnum revolver ten days after the sarin attack, not only survived but fully recovered and returned to duty. While it may have been speculated that the murder and attempted murder respectively were related to the doings of the cult itself, both motives and the relations of perpetrators to the cult remain inconclusive.

> intelligence headquarters of the Ministry of Defense, MOD, specialises in technical intelligence, such as signals and geospatial intelligence, and the Ministry of Foreign Affairs, MoFA, has two intelligence services, the Intelligence and Analysis Service, IAS, and the Counter- Terrorism Unit, CTU-J. Both services specialise in intelligence analysis on overseas and terrorist affairs. Lastly, the Public Security Intelligence Agency, PSIA, of the Ministry of Justice, is a security service, like the British MI5. These six agencies form the Japanese intelligence community.[6]

Although nominal institutions as parts of Japan's small intelligence community may be in existence, the country certainly lacks the robust legal and technical mechanism that could utilize the existing entities to their full potential or perhaps consider "upgrading" some of the bodies to more mature intelligence agencies.

> Intelligence reform is an underappreciated arm in these security reforms, and in taking a direct modelling approach for intelligence infrastructure Japan risks neglecting a formative period in its intelligence development. Although the creation of a National Security Council has facilitated greater executive decision-making overall, the lack of whistle-blower safeguards in the Specially Designated Secrets Act [of 2013] allows mismanagement to go unnoticed by the Japanese public, stunting institutional growth.[7]

In general, it is only logical that the Japanese intelligence apparatus is observed to have similarities to the counterpart structure in the US – however the individual tasks, operations and end-results visibly differ.

> … Japan's current intelligence system is similar to that in the United States in many respects. First, the mission of Japan' s IC is to support the Prime Minister's office in making national security-related policy decisions. Consequently, an intelligence cycle is established starting from the prime minister's office as the primary intelligence customer. Second, the Cabinet Intelligence and Research Office (CIRO) in the Cabinet Secretariat – which directly reports to the Prime Minister's office – is the nexus between the IC and the policy sector. This mechanism is similar to how the United States established the Office of the Director of National Intelligence (ODNI) to enhance IC integration after the United States was attacked on September 11, 2001. Moreover, Japan's IC also includes civilian and military intelligence agencies, with the civilian agency responsible for community integration and coordination.[8]

[6] Japan's Intelligence Capabilities with Professor Richard Samuels, Professor Kotani Ken and Hosaka Sanshiro (2024), Transcript of the Podcast Episode, p. 4.
[7] Fishlock N. (2019), Policies to Please Political Partners: The Development of Japan's Intelligence Policy in the 21st Century, p. 8.
[8] Kobayashi Y. (2023), Re-assessing the Organizational Characteristics of Japan's Intelligence Community and Its Social and Political Backgrounds, p. 5.

One of the obvious reasons why the Japanese intelligence community (and their respective member organizations) does not exert both tangible and consequential influence on vital security issues, notably terrorism prevention, is that the country is yet to establish some kind of parliamentary oversight for activities of the individual bodies regarded as "intelligence gathering" subjects.

> … Japan is the only country in the G7 and Australia without an exclusively dedicated body, whether parliamentary or administrative, responsible for democratic oversight of the IC. As a bureau within its respective parent organization, each member organization in Japan's IC is subject only to the same level of administrative and parliamentary oversight as other non-intelligence bureaus. Such ordinary oversight lacks expertise in intelligence affairs and has no access to confidential IC information. Thus, it is highly likely that their effectiveness is limited.[9]

4. Common Intelligence Instruments – Are They Necessarily Repressive?

Engaging in foreign espionage is one of the essential attributes of an adequately functioning sovereign nation, together with the right of belligerency. It seems that together with the renouncement of act of war embedded in the Constitution as one of the sovereign rights, Japan has also quietly rejected the idea of deploying a full-fledged intelligence outfit especially in the country's foreign engagements. Such decision, whether made consciously by the ruling elites, or having risen out of the geopolitical development of the post-World War II era, has its price. While before the Aum incident of 1995 Japan did not witness on its own territory major acts of terrorism acts perpetrated by either an internal or foreign adversary, the Japanese citizens have regularly become "soft" targets overseas – in incidents either targeting Japan in particular or as part of terrorist acts aimed at the Western civilization at large.

Although the pledge "not to maintain land, sea and air forces" has been circumvented by establishing "self-defense" forces, the key point related to refraining from operating a major intelligence entity is probably in the Constitution's distancing from the use of military power – the mechanism usually associated with any major intelligence agency:

> Article 9 of Japan's postwar constitution subjects the nation to stringently worded constraints on its legal capacity to wage war. Although not the only constitution to include a renunciation of war, Japan's postwar constitution is unique in its prohibition of military forces that make war possible. The article reads:
> Aspiring sincerely to an international peace based on justice and order, the Japanese people forever renounce war as a sovereign right of the nation and the threat

[9] Ibid, p. 14.

> or use of force as means of settling international disputes. In order to accomplish the aim of the preceding paragraph, land, sea, and air forces as well as other war potential, will never be maintained. The right of belligerency of the state will not be recognized.[10]

It is somewhat of a paradox that at the same time, observations are made that Japan is equipped with the most modern warfare (both of national production as a result of state-of-the-art research and development capabilities as well as procured overseas), including the instrumentation designed for intelligence collection.

> Japan today possesses the most advanced anti-submarine, air defence, and intelligence-gathering equipment, including missile-mounted Aegis destroyers with advanced detection and analysis systems. Some of there were, in fact, deployed in the Indian Ocean in support of the U.S. coalition action against Afghanistan.[11]

Perhaps most striking in the characteristics of the overall Japanese intelligence community is a non-existence of a dedicated HUMINT organization, which across the board of international intelligence systems is the most crucial element in gaining vital intelligence especially in the realm of terrorism. It is often perceived that the memories of the repressive secret police in pre-war Japan (disbanded fully after the World War II) prevent the country from engaging in establishing a human-resource based spy organization that would effectively collect essential information for analysis, in particular overseas.

Table 1 – *Comparison of Characteristics of Japan's Intelligence Community with those of other G7 countries and Australia*[12]

International Comparison of IC Organizational Characteristics

	Japan	Australia	Canada	France	Germany	U.K.	U.S.
Organizations dedicated to IC integration and Coordination	DCI CIRO	DGNI ONI	NSIA	×	×	JIC	DNI ODNI
Organizations dedicated to external HUMINT activities	×	ASIS	×*	DGSE	BND	SIS	CIA
Organizations dedicated to domestic intelligence	×	ASIO	CSIS*	DGSI	BfV	SS	×
Parliamentary bodies dedicated to IC oversight	×	PJCIS	NSICOP**	DPR	PKGr	ISCP	Senate SCI HR PSCI

The members of the intelligence community worldwide, and of the individual entities tasked with intelligence operations in particular, often make a point to highlight whether their respective organization is an "information collecting agency" or a "secret service" – the latter having the direct conno-

[10] Haley J.O. (2005), Waging War: Japan's Constitutional Constraints, p. 18.
[11] Ibid, p. 19.
[12] Kobayashi Y. (2023), Re-assessing the Organizational Characteristics of Japan's Intelligence Community and Its Social and Political Backgrounds, p. 12.

tations to regular engagement in "active measures" and "covert operations". It is perhaps also a matter of education and adequate informational guidance to convince the nation that "information gathering with the aim of proper analysis" does not equal "wet jobs", to use a jargon of intelligence bodies.

5. Absence of full-fledged intelligence agencies (both domestic and foreign focused) in the understanding of Western intelligence mechanisms

Not only in the context of countering terrorism, but as part of a larger discussion of who should be safeguarding the constitutional and public order, it has been deliberated why Japan until today has not fully used the potential of already existing quasi-intelligence bodies or outright enacted the intelligence agencies on par with their Western counterparts (with both counter-intelligence focus as well as foreign intelligence gathering focused). While it is challenging to say that the institutions such as the CIA, FBI, MI6, Mossad or DGSE are always capable of preventing terrorism on their respective soil or targeting their nation's citizens, the instruments, methods employed and networks of operatives certainly enable mechanisms capable of detecting and countering some of the major terrorist plots.

As part of this discourse, we will examine the one extremist event perpetrated by the members of the Aum Shinrikyo cult in March 1995 in its attempt to sow death and chaos among population in Tokyo. While the common description of this incident usually mention "actions of a doomsday cult", was this an act based purely on religious beliefs or did it have hallmarks of a very specific national security threat? While not know to the wider public, let us state some of the facts related to Aum Shinrikyo in relation to their long-term activities that had very little in common with their official religious tenets:

1. Well before 1995 Tokyo subway attack, the group was implicated (and later proved) to have abducted and murdered the whole family of a lawyer representing parties against the group.[13]
2. In 1993, the group tried to disperse anthrax spores to cause mass poisoning in one of the Tokyo neighborhoods.[14]

[13] Murders of more than one person by a perpetrator carries mandatory death sentence in the Japanese penal code, and the disappearance of the family of three indicating that they have been murdered should have received attention of not only police but respective organization(s) dealing with subversive domestic activities.

[14] Japan, having pledged never to resort to use of any military weapons, let alone weapons of mass destruction, should have treated the mere occurrence of anthrax substance with heightened attentiveness.

3. In 1993 and 1994, the group's division in Western Australia started to manufacture both sarin and VX gas at a local property, testing it on sheep.[15]
4. In 1994 and 1995, the group's members used both sarin and VX to either kill groups of people or assassinate specifically designated individuals.[16]

> … due to the disproportionate public attention paid to the Tokyo attack, it is often overlooked that Aum's violence was not a one- off event: there was a period of about six years in which Aum became increasingly violent, not only towards outsiders but to its own members, especially against followers whose devotion to the guru was seen to be wavering. Regrettably, its various murders, murder attempts, and its first indiscriminate terrorist attack using sarin in June 1994 in Matsumoto – a midsize regional city in Nagano Prefecture, central Japan – have tended to be sidelined in academic and media debates about Aum. The causes and consequences of the Matsumoto sarin attack merit special attention not only as a historical milestone in Aum's turn to mass violence as a means of achieving religious ends, but also because of its lack of national impact in the immediate aftermath of the attack. The Matsumoto attack killed eight and injured more than 600 residents in a residential neighbourhood, in what was then one of the largest terrorist attacks in living memory.[17]

5. In 1994, the group's members broke into the factory of Mitsubishi Heavy Industries Company, attempting to steal blueprints for tanks and artillery.[18]
6. Following the Tokyo gas attack, explosives, firearms, a functioning Russian military Mi-17 helicopter and stockpile of chemicals to produce enough sarin to kill 4 million people were found in the group's compound. This particular find illustrated a clear picture that the group was in contact with foreign parties from whom the weapons and chemicals were procured.[19]

According to some accounts, the group internally designated a "new government" with having a list of people that were to replace the existing

[15] With any substantial international intelligence sharing agreements in place, such incident occurring at object managed by Japanese nationals should have triggered a response commensurate with the gravity of the findings.

[16] March 1995 Tokyo subway gas attack was preceded by the usage of the same mass destruction toxin in the previous year, targeting a judge. It is therefore safe to assume that the Tokyo subway attack could have been prevented if the precedent would be given due attention and treatment.

[17] Ushiyama, R. (2022), Aum Shinrikyo and Religious Terrorism in Japanese Collective Memory, p. 30.

[18] In a country governed by a pacifist Constitution, it is somewhat of a mystery why a clear attempt to target military technology would not be treated with adequate response from the authorities.

[19] If any conclusions were made upon the finding among the respective "intelligence" agencies, the informational outcome was certainly not shared with the public. It is alarming that a find of substances and military grade equipment did not obviously trigger a larger scale investigation and overall international repercussions were not tangible.

government personnel, leading to speculations that the ultimate motive of the gas attack was to execute a full-fledged coup d'etats.[20]

Some academic sources also point out the fact that most obviously, the Aum Shinrikyo religious group was aiming at a megalomaniac design to "take over Japan" and actually even for few months after the March 1995 subway attack, the cult's leader continued to plot various schemes to attack the Government. This illustrates that not only no substantial intelligence was in the hands of relevant authorities, but also even in the weeks following the subway attack, the Government grappled with making a sense of what was happening.

Public fears that Aum may commit another terrorist attack of a similar scale were justified and accurate, as Asahara [the cult's leader, ultimately executed only in 2018, 23 years after the subway gas attack was perpetrated] continued to give instructions to carry out terrorist attacks. The Vajrayāna Plan to take over Japan was still in effect. In April and May, Aum attempted to spray hydrogen cyanide from a briefcase at Shinjuku, one of Tokyo's busiest stations. On the day of Asahara's arrest, 16 May, Aum sent a letter-bomb to the Tokyo Metropolitan Government, seriously injuring a government employee. These violent plots came to an end only after the most senior disciples were arrested.[21]

And yet, there was no record of the group's activities being on a radar of National police or any of the government entities – or at least publicly not admitted. While some of the investigation after the terrorist act may have exposed a foreign related lead, none were reported to the public. In the wake of the sarin gas terrorist attack, one thing is certain – Aum Shinrikyo's fatal action had a profound effect on how both the society as well as the country's security establishment became to view the various religious groupings in general:

> … the Aum Affair also produced in its wake myriad cultural narratives, discourses, practices, and products that have transformed how people both inside and outside Japan conceptualise and interact with minority religions, millennialism, religious violence, and religious terrorism. One of the most transformative changes occurred in the Japanese religious field. In the wake of the Tokyo attack, religious organisations were left reeling as they confronted a sea

[20] An officer of the National Police Agency's Public Security Department, in a confidential conversation, did confirm the existence of "certain proofs" that a foreign power was partially supporting the preparations leading up to the deadly sarin attack. The gas attack itself may have been only a false flag operation designed to divert public attention from the attempt to subvert the legitimate Japanese Government.

[21] Ushiyama, R. (2022), Aum Shinrikyo and Religious Terrorism in Japanese Collective Memory, p. 57.

> change in public attitudes towards religions, from one of apathy and indifference to open distrust and sometimes active animosity.[22]

At the kernel of the issue is the intelligence community set-up in general and the lack of the corresponding tools that would have at least provided an indication for the nefarious activities the group had been undertaking totally under the radar of the authorities. While the National Police Agency and several ministries, including the office of the prime minister, have a rudimentary "intelligence" department, most domestic intelligence resources are directed towards perceived threats originating in China and North Korea, and 80% of the intelligence gathering efforts overseas are focused on economic issues – both safeguarding the domestic industrial base as well as obtaining foreign economic indicators vital to national interests. The only entity that comes close to the Western understanding of an "intelligence agency" probably is the Public Security Intelligence Agency (PSIA) of the Ministry of Justice which today engages in some of the internationally adopted practices of intelligence sharing (among G7 nations mostly) and has some of the instruments for both domestic and foreign intelligence operations at their disposal. Historically, however, PSIA has been largely focused on the domestic North Korean diaspora (about 150,000 people) in infiltrating their ranks to obtain North Korea originating intelligence, and lately to some extent focusing on China (both domestically as well as on foreign land). Even given the current diplomatic estrangement between Japan and Russia, the officers associated with the Japanese intelligence community admit that Russia is not as much in their focus as the Asian neighbors North Korea and China.[23]

Only given a predicament in the last three decades whereby the Japanese nationals have been targeted in countries such as Bangladesh, Algeria, Egypt, Indonesia, Iraq, Syria, Tajikistan or Kyrgyzstan as part of terrorist acts perpetrated by Islamic fundamentalists, a discussion has risen to address the need for full-fledged foreign intelligence gathering agency. In 2014 several Japanese nationals have been identified as ISIS sympathizers and were arrested immediately prior to leaving the country to join ISIS forces in Syria, although this was not a result of a concerted effort to monitor and curb Islamic extremism in Japan. Instead, Japan continues to rely on a "good-will"

[22] Ibid, pp. 2-3.

[23] Given the Japan's security apparatus proximity to those in the USA, it has been debated for some time should Japan join the Anglo-Saxon intelligence sharing network of "Five-Eyes" together with Germany, Singapore and South Korea, and as a result create a new "Nine-Eyes" alliance. Apart from the US, Japan does have bilateral intelligence sharing agreements with some of the G20 countries, including Australia or Italy.

gesture of the main international intelligence agencies to share some of the information about imminent threats if that concerns Japan directly.

6. Inability to develop counter-terrorism policies in Japan given the lack of classified/compartmented information mechanisms among Government agencies

In a conversation the author had in summer 2024 with one of the senior officers of National Police Agency's Public Security Department, the officer highlighted the following:

1. In the context of absence of a full-fledged foreign intelligence gathering entity, a timely procurement of an objective and proven intelligence from abroad pertaining to threats against the national security of Japan is limited. Reliance on other international agencies to obtain vital information does not correspond to the current needs nor imperatives that the threat of international terrorism presents.
2. Even with the development of any entity resembling those of CIA or MOSSAD, such agency will still be heavily limited in its span and authority given the Constitution renounces belligerency as a sovereign right, as well as use or threat of force as means of settling international disputes. This also relates to the right to conduct intelligence operations abroad commensurate with the level of threat to the national security – and so far it has been deemed that it is better not to have access to intelligence rather than being accused of violating its own Constitution.
3. In practice, there is no system of "security clearance" among the Japanese civil servants employed by the security apparatus or by the ministries delegated with threat assessment – and the notion of "Confidential", "Classified", "Top Secret" or "Compartmented" information is non-existent. As a result, when such intelligence is received from abroad as part of foreign Embassy or specific security briefing, it is up to the personnel present at the meeting to utilize such information later in government policies.

On the background of the above, some international incidents related to "Japanese intelligence agencies" may even appear to be grotesque. In September 2024, news outlets in the Republic of Belarus reported, accompanied duly with "evidence" and corresponding YouTube channel clips that a "Japanese intelligence officer employed by the PSIA" was apprehended near the Belarus-Ukraine border, who later "confessed" that his intelligence collecting activities "may have been of grave consequence to the national security of the Republic of Belarus". In Japan the story perspired as an anecdote, with relevant Japanese security apparatus personnel pointing to the numerous facts

highlighted by both Belarussian propaganda as well the concerned person's background that whatever the individual was doing "on the Belarus-Ukraine border", it was not for the benefit of the PSIA. On the other hand, with a record of real PSIA agents being arrested and incarcerated in China, the same security apparatus personnel pointed out that exposé of any real-life agent abroad (at least given the characteristics of how the PSIA operates) is possible only with the existence of internal mole within the PSIA itself. That, of course, is already another topic to be debated on a separate platform.

7. Conclusions

Given the fast changing tendencies on the international arena with regard to both definition of terrorism as well as the corresponding countermeasures, most certainly Japan, among the G7 nations, lags behind in having both instruments as well as opportunities "to be in the know" when it comes to timely reacting to the challenges this arena represents. In the world saturated with new conflicts, new players and new technologies that engage in both offensive and defensive mechanisms, the threat to fundamental principles of each state's national security is growing.

Given the relative frequency of international acts of terrorism to which Japanese nationals succumb, the amount of "food for thought" when it comes to serious deliberations whether or when to establish an intelligence agency capable of countering and neutralizing threats of terrorism both home and abroad is more than enough. Let us remember the In Amenas hostage crisis of January 2013 in Algeria where 10 of the Japanese nationals perished (the largest contingent among the foreigners, out of 40 dead) which had a grave fallout also with regard to how the operations in hydrocarbon industry overseas are to be conducted. 1997 Luxor massacre produced 10 Japanese casualties among the tourists, most of them newly-weds. The so-called "Bangladesh's 9/11" of July 2016 when 7 consultants of the Japan International Cooperation Agency lost their lives in Dhaka to a local Jihadist outfit was certainly one of the most painful reminders that even the non-military personnel abroad are targeted in the line of their duties. Realizing that not all loud terrorist acts are committed by Islamist radicals, the 1996 Japanese embassy hostage crisis in Peru which lasted for over 4 months is a reminder that actionable intelligence needs to be gathered 24/7, in every international location where the Japanese nationals and the country's vital interests are present. Abductions of Japanese nationals in Central Asia, leading to secreted negotiations with the terrorists and subsequent payment of ransom, also give us material to reconsider both the existing intelligence structures as well as mechanisms deployed to resolve the crisis. Execution of Japanese nationals by ISIS groupings in Syria and lat-

er propagated by the groups media is another painful moment to realize that any gathered intelligence needs to be shared with the relevant individuals to prevent such occurrences.

Answering the initial rhetorical question whether Japan is close(r) to establishing its own Central Intelligence body, it is probably a cynical "not until a Japanese 9/11 takes place in the country's territory". With the world in a new wave of geopolitical polarization, with multitude of regional wars and political conflicts just a step away from full-fledged military confrontations, and with Japan feeling a need to take sides once too often, we may not be that far from that moment to arise.

Japan may still consider herself as rather detached from the major international domain where most terrorist acts occur but with the increasing tendency of all eco-systems and mechanisms being globally intertwined, it is perhaps a time to consider to rebuild some of the rudimentary instruments and structures upon which the safeguarding of national security principles are based.

References

Defense of Japan (2024), Ministry of Defense, Tokyo, Japan.

DeWitt Smith H. (1970), The Origins of Student Radicalism in Japan, Journal of Contemporary History Vol. 1 No. 5, Generations in Conflict 87-103, Sage Publications Ltd., Thousand Oaks, CA, USA.

Fishlock N. (2019), Policies to Please Political Partners: The Development of Japan's Intelligence Policy in the 21st Century, Focus Asia Perspective & Analysis, Institute for Security & Development Policy, Stockholm, Sweden.

Haley J.O. (2005), Waging War: Japan's Constitutional Constraints, Constitutional Forum, University of Alberta, Edmonton, Canada.

Hazeleger F. (2018), The Making of the Japanese Intelligence Community (An analysis of different factors in the establishment and development of the Japanese intelligence community: a case study of the Cabinet Intelligence Research Office and the Public Security Intelligence Agency, a Master's Thesis), Utrecht University, Utrecht, Netherlands.

Herf J. (2016), Palestinian Terrorism in 1972: Lod Airport, the Munich Olympics, and Responses, Cambridge University Press, Cambridge, United Kingdom.

Japan's Intelligence Capabilities with Professor Richard Samuels, Professor Kotani Ken and Hosaka Sanshiro

(2024), Transcript of the Podcast Episode.

Jo G. (2015), The Revival of Japanese Right-Wing Thought and the Coincidental Collaboration of the Left and Right, Seoul Journal of Japanese Studies Vol.1, No.1: 29-56, Institute for Japanese Studies, Seoul National University, Seoul, Republic of Korea.

Kapur N. (2022), The Japanese Student Movement in the Cold War Crucible (1945-1972), The Asia-Pacific Journal Japan Focus (Volume 20, Issue 14, Number 1, Article ID 5724), Cambridge University Press, Cambridge, United Kingdom.

Katzenstein P.J. (2002), September 11 in Comparative Perspective: The Antiterrorism Campaigns of Germany and Japan, International Organization Foundation and the Massachusetts Institute of Technology, Boston, MA, USA.

Kobayashi Y. (2023), Re-assessing the Organizational Characteristics of Japan's Intelligence Community and Its Social and Political Backgrounds, The Graduate School of Governance Studies, Meiji University, Tokyo, Japan.

Kotani K. (2006), Current State of Intelligence and Intelligence Issues in Japan, The National Institute for Defense Studies News, No. 100, Tokyo, Japan.

Lombardi M. (2024), Defining Terrorism Today: Focusing on the Act and its Effects, Media Version at https://360info.org/, Milan, Italy.

Midford P. (2006), Japanese Public Opinion and the War on Terrorism: Implications for Japan's Security Strategy, Policy Studies 27, East-West Center Washington, Washington DC, USA.

Muttaqien M. (2007), Japan in the Global "War on Terrorism", Global & Strategis, Surabaya, Indonesia.

Protecting the People with the Power of Intelligence (2023), Public Security Intelligence Agency, Tokyo Japan.

Radcliffe W.L. (2023),Review Essay: Perspectives on Japan's Intelligence and National Security Challenges, Studies in Intelligence Vol. 67, No. 1, CIA's Directorate of Digital Innovation, Langley, VA, USA.

Randall J. (2023), Global Revolution Starts with Palestine: The Japanese Red Army's Alliance with the Popular Front for the Liberation of Palestine, Comparative Studies of South Asia, Africa and the Middle East 43 (3): 358-369, Duke University Press, Durham, NC, USA.

Review and Prospects of Internal and External Situations (2023), Public Security Intelligence Agency, Tokyo Japan.

Ushiyama, R. (2022), Aum Shinrikyo and Religious Terrorism in Japanese Collective Memory, British Academy Monographs, Oxford University Press, Oxford, United Kingdom.

Van Winkle A.B. (2012), Separation of Religion and State in Japan: A Pragmatic Interpretation of Articles 20 and 89 of the Japanese Constitution, Washington International Law Journal Vol. 21, No. 2, University of Washington, Seattle, WA, USA.

Oltre l'emergenza. Il terrorismo jihadista in Francia tra analisi dei problemi contemporanei e delle origini coloniali

Uliano Conti

Uliano Conti[1] è Professore Associato di Sociologia Generale presso il Dipartimento di Filosofia, Scienze Sociali, Umane e della Formazione dell'Università degli Studi di Perugia. È stato visiting researcher all'Arizona State University. Si occupa di metodologia della ricerca sociale e di sociologia visuale. È vicedirettore del Centro di Ricerca in Sicurezza Umana (CRISU) dell'Ateneo perugino e autore di numerose pubblicazioni, tra le più recenti: "Il legame sociale e il reato di terrorismo. Considerazioni sociologiche a partire da alcune radicalizzate jihadiste italiane, 2023, Sociologia del Diritto, 1, pp. 146-162"; "The Day After. Considerations and Future Prospects for Studying the Phenomenon of Othering after Jihadist Terrorist Attacks, 2018, Italian Sociological Review, 8, 2, pp. 201-215"

Abstract

Article examines hatred against France, as a humus for terrorism. Article focuses on most serious recent episode, namely the terrorist attack of 13 and 14 November 2015 in Paris. In this perspective, paper presents state of the art relating to jihadist terrorism. Article presents the perspective of post-colonial studies: in the Algerian war not only roots of hatred against France can be sought, but also operational analogies, such as violent actions that hit bars. This approach proposes a strong connection between colonial history and terrorism. A second approach proposes a soft connection: adhesion to terrorist groups involves contemporary social and subcultural factors. In this sense, the first perspective can be enriched by the interpretative lens of Bourdieu, who analyzed the transformations of Algeria under French domination. Confinement of the peasant population, consequences of war, socio-economic drift, social and political crisis and emergence of terrorist groups in the African country have not only had local effects, but also repercussions in France.

L'articolo esamina l'odio contro la Francia, come humus per il terrorismo e si concentra sul più grave episodio recente, ovvero l'attacco terroristico del 13 e 14 novembre 2015 a Parigi. In questa prospettiva, presenta lo stato dell'arte relativo al terrorismo jihadista. L'articolo presenta la prospettiva degli studi postcoloniali: nella guerra d'Algeria si possono cercare non solo le radici dell'odio contro la Francia, ma anche analogie operative, come le azioni violente che colpiscono i bar. Questo approccio propone una forte connessione tra storia coloniale e terrorismo
Un secondo approccio propone una connessione morbida: l'adesione ai gruppi terroristici coinvolge fattori sociali e subculturali contemporanei. In questo senso, la prima prospettiva può esse-

[1] Dipartimento di Filosofia, Scienze Sociali, Umane e della Formazione. Università degli Studi di Perugia. Email: uliano.conti@unipg.it. Tel.: 3485464622.

re arricchita dalla lente interpretativa di Bourdieu, che ha analizzato le trasformazioni dell'Algeria sotto la dominazione francese. Il confinamento della popolazione contadina, le conseguenze della guerra, la deriva socio-economica, la crisi sociale e politica e l'emergere di gruppi terroristici nel Paese africano non hanno avuto solo effetti locali, ma anche ripercussioni in Francia.

Keywords

Terrorism, Sociology, Bourdieu, Jihadism, terrorismo, sociologia, Bourdieu, jihadismo

1. Introduzione

A ottobre 2023 l'esplosione del conflitto tra Israele e Palestina e gli attacchi compiuti in Europa (a Bruxelles in Belgio e ad Arras in Francia) hanno riacceso l'attenzione sul tema del terrorismo. Questo termine non è di facile utilizzo, non è accettato in modo unanime all'interno della comunità scientifica delle scienze sociali. Da una parte, convivono molte posizioni politiche, prospettive strategiche, disciplinari e molte definizioni scientifiche di terrorismo. La pluralità è ascrivibile non solo ai diversi approcci disciplinari, ma anche alle differenti circostanze storiche e geografiche.

I fatti di ottobre 2023 riaccendono l'attenzione su questo tema, senza che sia stato compiutamente analizzato quanto accaduto in Francia e in Europa tra 2015 e 2017: la strategia dell'ISIS fatta di attacchi e stragi. In particolare, gli attacchi di Parigi del 13 e 14 novembre 2015 rappresentano il caso più rilevante. In altre parole, sembra utile considerare quanto accaduto a Parigi per comprendere il rancore, l'odio e gli altri elementi che costituiscono l'humus del terrorismo.

Come ha affermato Roy (2023) in merito agli ultimi attacchi[2]:

> I terroristi hanno dichiarato di essere legati a Isis, non ad Hamas. E lo stesso Isis – a differenza di Al-Qaeda – non ha espresso supporto ad Hamas per l'attacco contro Israele perché lo considera un movimento nazionalista che mina le basi del jihadismo globale. I due episodi avvenuti in Francia e a Bruxelles sono in linea di continuità con l'ultima ondata di terrorismo islamico in Europa. (…). Fino ad allora – e a partire dal 1996 – i terroristi appartenevano prevalentemente alla seconda generazione di immigrati arabi in Europa più qualche convertito all'Islam. Erano ben organizzati, coordinati da Al-Qaeda prima e dall'Isis poi. Gli attacchi erano pianificati: avevano armi all'avanguardia, esplosivi. Dal 2016[3] si assiste a un cambiamento radicale: gli attentati si

[2] https://www.open.online/2023/10/19/hamas-israele-olivier-roy-jihad-europa-intervista.

[3] È necessario precisare che nel 2016, però, si sono verificati gli attentati in Belgio alla metropolitana di Bruxelles e all'aeroporto.

> fanno con coltelli, taglierini, armi di fortuna. I terroristi sono persone che agiscono di fatto da sole o con l'aiuto di qualche parente o amico.

Gli attentati terroristici di novembre 2015, quindi, possono essere ulteriormente analizzati. Queste azioni sono ricordate come condotte, in gran parte, da giovani europei (francesi, belgi…) a tutti gli effetti. Al di là della condizione giuridica e dell'origine famigliare, infatti, i giovani che hanno colpito a Parigi nel 2015 sono cresciuti nelle città occidentali, hanno vissuto come migliaia di loro coetanei, fumato hashish, ascoltato musica rap, fatto parte di gang e subculture (Pisoiu, 2015; Roy, 2017; Kepel, 2017). Il loro odio verso la Francia e loro scelta di aderire a gruppi terroristici non sono imputabili a un'origine *altra*, alla nazionalità dei loro genitori o dei loro nonni, e tantomeno alla loro religione. I *foreign fighters* e i terroristi non venivano da famiglie particolarmente devote. Infatti, si sono convertiti poco prima di aderire a ISIS. Si tratta di una patinatura falsamente religiosa di attitudini violente (Roy, 2005; 2008; 2016; Tirozzi, 2019).

Per capire come si crei il contesto, il brodo di coltura dell'odio si possono cercare elementi di carattere storico-sociale (la guerra d'Algeria, ad esempio), ma le analisi dell'origine storica e coloniale colgono un tassello di un quadro interpretativo complesso (Saïd 2000, Spivak, 1999; Mohammed, 2022). Infatti, hanno aderito a ISIS come *foreign fighters* anche giovani autoctoni inglesi, italiani o svedesi. Inoltre, elementi di carattere psicopatologico, strategico, subculturale, socio-economico, ambientale si combinano. Gli studi post-coloniali che sostengono una connessione forte tra passato coloniale e terrorismo possono essere discussi considerando i fattori contemporanei di adesione dei giovani europei a gruppi terroristici che si presentano come una Ummah globale (Khosrokhavar, 2013; 2018; Pisoiu, 2015; Antonelli, 2020), autonoma rispetto alla storia e alle società dei Paesi colonizzati. Allo stesso tempo, gli studi che si concentrano sui contesti sociali europei contemporanei, possono essere integrati da contributi sociologici come quello di Bourdieu (Bourdieu, Sayad, 1964), affinché non sia tralasciata la storia dei Paesi colonizzati.

2. Lo stato dell'arte. Per una definizione di terrorismo

È necessario definire il terrorismo. Le definizioni sono centinaia, come sono anche molte le prospettive disciplinari che analizzano questo fenomeno (Victoroff, 2005). Ad esempio, mentre alcune ricerche condotte coinvolgendo detenuti appartenenti all'IRA e all'ETA, come anche alcune ricerche sulle Brigate Rosse non hanno rilevato psicopatologie significative tra gli appartenenti a questi gruppi (Della Porta, 1990), altri studi, più recenti, sui *foreign*

fighters e sugli appartenenti all'ISIS mettono, invece, in evidenza l'esistenza di psicopatologie individuali significative (Tirozzi, 2019). La teoria della scelta razionale, d'altro canto, considera l'azione terroristica come un mezzo consapevolmente usato per il raggiungimento di alcuni obiettivi, altrimenti non ottenibili. In tale prospettiva rientrerebbero gli attacchi condotti da forze e gruppi (come i movimenti di liberazione nazionale, i movimenti indipendentisti, i movimenti anti-colonialisti) che, in modo strategico, scelgono di agire attraverso azioni violente per raggiungere obiettivi politici, non solo contro. Un nodo concettuale, poi, riguarda il nesso tra povertà e terrorismo: alcuni studiosi analizzano il nesso tra questi due elementi, prendendo come esempio il caso Israelo-palestinese, mentre altri studiosi sostengono che non ci sia un nesso tra svantaggio socio-economico e terrorismo (Cottee, 2015).

Alcuni studiosi (Giglioli, 2018) mettono in discussione il termine stesso di terrorismo, considerandolo come un'etichetta priva di un'autentica utilità euristica: i Paesi occidentali, dal secondo dopoguerra in poi, hanno etichettato come terrorismo lo spazio dove relegare tutte le forme di conflittualità che non hanno compreso all'interno del proprio perimetro linguistico, politico e simbolico. In altre parole, per Giglioli (2018) la definizione dipende fortemente da chi applica l'etichetta. Una democrazia definisce come terrorismo il conflitto violento condotto secondo regole estranee. Una dittatura, come il nazismo, definisce come terroristiche le azioni dei partigiani. Tale posizione, però, finisce per sfociare in un relativismo che non distingue l'azione di un gruppo che fa strage di civili inermi con l'azione delle forze di polizia che in uno Stato si occupano del controllo del territorio. Altri studiosi, come Roversi (2006), in una prospettiva critica, ma diversa dalla precedente, utilizzano non il termine terrorista ma 'combattente', perché privo di connotazione stigmatizzante. Non rinunciano, però, alla possibilità di studio del fenomeno in questione.

In merito alle definizioni, guardando a istituzioni e organismi internazionali di diversa natura – si pensi all'Organizzazione delle Nazioni Unite, alla Unione Europea o all'FBI – cinque sembrano essere gli elementi che fanno da minimo comune denominatore di tutte le definizioni: utilizzo della violenza; obiettivo politico; target civile e non militare; ricerca dell'eco comunicativa; esistenza di un gruppo. Da questi cinque elementi, ciascuno dei quali è necessario, ma non sufficiente, perché si possa parlare di terrorismo, derivano una miriade di variazioni e possibilità.

In merito all'esistenza del gruppo, possono verificarsi azioni organizzate e condotte da un singolo attore, il cosiddetto lupo solitario. Studi sul tema, però, mostrano che il lupo solitario non è mai così solitario come appare. In altre parole, emerge assai spesso l'esistenza di contatti, legami, più o meno forti e di reti, anche se fondate sull'utilizzo della comunicazione mediata dal

computer e che collegano attori distanti migliaia e migliaia di chilometri. La dimensione gruppale, quindi, emerge come molto rilevante (Victoroff, 2005; Tirozzi, 2019).

Per quanto riguarda l'utilizzo della violenza, un gruppo terroristico può compiere azioni criminali (rapine, traffico di sostanze stupefacenti, ad esempio) non immediatamente dirette contro le persone, ma, comunque, utili al finanziamento e all'assicurazione di risorse economiche.

In merito al target, possono esserci attacchi terroristici contro forze militari come gli eserciti, ossia azioni di guerra condotte attraverso una modalità terroristica (Ganser, Calzavarini, 2005). Il caso di ottobre 2023, a riguardo, è degno di nota. Hamas, nel corso della prima intifada (1987-1993), emise *fatwa* per giustificare l'uccisione di civili nei primi attentati per mezzo di *suicide bombers* sugli autobus e nei bar israeliani. Lo *shahid* era un martire, chi moriva con lui nel corso del suo attacco lo sarebbe stato altrettanto (Kepel, 2004; Tirozzi, 2019). Quanto accaduto al festival musicale, l'azione casa per casa condotta con tecniche militari accurate ha previsto l'impiego di uomini armati che hanno rastrellato e ucciso bersagli inermi, non martiri. Nessuna traccia della militarità che aveva contraddistinto Hamas, come Hezbollah, dalla nascita ad oggi.

Di qui la necessità di riprendere il filo delle analisi scientifiche proprio dalla stagione francese degli attacchi orchestrati da ISIS, che ereditava da Al-Qaeda le pratiche di un ventennio di azioni terroristiche.

La letteratura sociologica su ISIS ha considerato diversi aspetti: sono emersi elementi strategici e organizzativi, economici, ideologici, biografici. Sono state analizzate le biografie dei terroristi coinvolti a Parigi ed è stato studiato il loro percorso di radicalizzazione (Roy, 2016). Esistono molti studi anche sulle biografie dei *foreign fighters*, almeno di quelli di cui è nota l'identità (Stenersen, 2009).

L'ideologia di ISIS è stata studiata in modo approfondito, grazie a ricerche sulla propaganda, sui mezzi utilizzati per coinvolgere giovani occidentali come *foreign fighters*. In tal senso, soprattutto la Rete, piattaforme come Youtube o app come Telegram diffondono video e immagini dal forte impatto visuale (Vergani, Zuev, 2015).

ISIS e gruppi che a esso si sono ispirati sono analizzati dal punto di vista economico, considerando i modi in cui hanno accumulato risorse finanziarie, ad esempio attraverso il traffico di esseri umani e antichità (Pauwels, 2016).

Dal punto di vista organizzativo sono state studiate la struttura di questo gruppo e le modalità di connessione strategica tra Medio-Oriente ed Europa (Gupta, Özyer, Rokne, & Alhajj, 2019). Gli studi strategici (Tirozzi, 2019) considerano l'evoluzione espressa da ISIS, ossia la concomitanza di generi

di attacco che Al-Qaeda aveva espresso in due momenti distinti della propria storia, prima e dopo l'11 settembre 2001. La trasformazione di Al-Qaeda da organizzazione terroristica di tipo strutturato e verticistico, capace di organizzare il più devastante attacco terroristico della storia, in un *brand* del terrore capace di ispirare azioni in chi non aveva alcun collegamento diretto con essa, era stata dettata dalla contingenza, ossia l'eliminazione dei suoi vertici da parte degli Stati Uniti. Si apriva la stagione del terrorismo *homegrown*. Con ISIS le azioni tornavano a essere complesse e condotte con elevata capacità operativa, come nei casi di Ahmedì Coulibalì, il parigino di origine maliana attivato nella strage di Charlie Hebdo dall'ISIS); del commando di Verviers (eliminato dal DSU belga il 15 gennaio 2015 e da cui fuggiva Abdelhamid Abaoud); della successiva azione al Bataclan (capeggiata dal medesimo Abdelhamid); dell'aeroporto di Zaventem e della metropolitana di Bruxelles nel 2016.

A queste azioni l'ISIS abbinava una propaganda mediatica spinta fino alla formazione on line che permetteva attacchi spontanei, ma ben organizzati, sdoganando la modalità dei vettori lanciati sulla folla. In questo modo, abbinando azioni complesse e contraddistinte da capacità militare ad azioni sul modello *homegrown*, ISIS ottimizzava il percorso fatto da Al-Qaeda in oltre 20 anni di operazioni del terrore.

Nella letteratura sugli attacchi di ISIS in Francia attenzione è stata posta su alcuni aspetti di carattere storico-sociale. Infatti, molti studi sul tema della connessione tra colonialismo francese e avversione e odio verso la Francia sono successivi al 2001 (anno che ha segnato l'inizio di una nuova attenzione scientifica al terrorismo) e precedenti rispetto al 2015, anno in cui gli attacchi terroristici danno la possibilità di ulteriori analisi (Marrouchi, 2003; Carroll, 2007; Aben, 2018). Pratiche e strategie terroristiche dirette contro la Francia emergono infatti anche in passato, nel periodo della colonizzazione del Nord-Africa e del Sahel e nelle guerre necessarie per porre fine al dominio coloniale (Marrouchi, 2003; Carroll, 2007; Aben, 2018; Mohammed, 2022). In tale prospettiva, guerra e terrorismo sono un binomio di non facile lettura: in una guerra, infatti, ciascuna delle parti in conflitto tende a definire come terroristiche le azioni dell'avversario. Agli studi che sostengono una forte connessione tra passato coloniale e terrorismo, sono da accostare studi (Khosrokhavar, 2013; 2018) che – sottolineando il senso di appartenenza a una Ummah globale dei giovani radicalizzati europei, la loro adesione a gruppi terroristici nella forma subculturale (Pisoiu, 2015) tipicamente occidentale – discutono la nozione di connessione forte e ne propongono un superamento alla luce di fattori presenti nei Paesi europei contemporanei. Però, anche grazie al contributo di Bourdieu (1964) occorre non dimenticare e tenere presente il contesto coloniale e le conseguenze sulla Francia di oggi.

2.1 Il terrorismo che attacca bar, cafè e locali notturni. Una cronologia

Gli attacchi a Parigi del 2015 hanno avuto come bersaglio: Le Carillon e Le Petit Cambodge, tra Rue Alibert e Rue Bichat; Café Bonne Bière e Casa Nostra, presso Rue de la Fontaine au Roi; il Teatro Bataclan in Boulevard Voltaire; La Belle Équipe in Rue de Charonne; Comptoir Voltaire in Boulevard Voltaire e lo Stade de France. I morti sono stati 130.

Il 13 novembre 2015, poco dopo le 21:00, davanti all'ingresso D dello Stade de France avviene un'esplosione. Nella zona dello stadio agiscono tre persone. Ukashah Al-Iraqi, alias Ahmed al-Mohammed, o Ammar Ramadan Mansour Mohamad al Sabaawi, iracheno, arrivato in Europa passando dalla Grecia, reclutato da ISIS, che ricompensa la sua famiglia in Iraq[4]. Ali al-Iraqi, alias Abbdulakbak B., o M. al-Mahmod, iracheno, si fa esplodere nei pressi del *fast food* Quick vicino allo stadio. Bilal Hadfi si fa esplodere al Mc Donald vicino allo stadio; è un giovane ventenne di origine marocchina, di nazionalità francese. Viveva in Belgio, a Neder-over-Heembeek. Era incensurato, si convertì e andò in Siria come *foreign fighter*. Al ritorno in Belgio entrò in clandestinità[5].

Del gruppo che attacca i bar, i ristoranti e i cafè fanno parte Salah Abdeslam, di origine marocchina; il fratello Brahim Abdeslam, di origine marocchina, come anche Abdelhamid Abaaoud e Chakib Akrouh, anche lui di origine marocchina.

La strage al Teatro Bataclan è compiuta da Ismaël Omar Mostefaï, Samy Amimour e Foued Mohamed-Aggad. Ismaël Mostefai, di 27 anni, è nato e cresciuto a 80 chilometri da Parigi, è di origine algerina come la moglie Khadidja (lui stesso si recò in Algeria per cercare una sposa); è coinvolto in episodi di spaccio e rissa, poi frequenta le moschee di Beaulieu e Lucé. Foued Mohamed Aggad, 21 anni, di Wissenbourg, di origine algerina, aveva un'esistenza comune, si era diplomato a pieni voti e rimase deluso per aver fallito il concorso per entrare in Polizia. Infine, c'è Samy Amimour, del 1987, anche lui di origine algerina.

Nel 2021, inoltre, è individuato a Bari Athmane Touami, alias Tomi Mahraz, già detenuto per altri reati, giovane di origine algerina, che ha avuto un ruolo di supporto fornendo documenti falsi ai terroristi del Bataclan[6].

[4] https://www.repubblica.it/esteri/2017/01/18/news/parigi_identificato_kamikaze_dello_stade_de_france_isis_pago_alla_famiglia_5mila_euro_e_un_gregge-156278937.

[5] https://www.ibtimes.co.uk/paris-attacks-islamic-states-dabiq-magazine-identifies-two-stade-de-france-suicide-bombers-1538995.

[6] https://www.ilfattoquotidiano.it/2021/03/09/bataclan-il-fermo-dellalgerino-a-bari-conferma-il-ruolo-dellitalia-nel-fornire-documenti-falsi/6126517.

Tra questi nomi appena citati ci sono legami e incontri che precedono gli attacchi. Ad esempio, Ablehamid Abaaoud, a 24 anni, nel 2010, viene detenuto a Molenbeek in camera di sicurezza e, in base a quanto raccontò alla sorella, torturato dalla polizia belga. Nel 2010 è arrestato per un tentativo di rapina compiuto insieme a Salah Abdeslam, poi nel 2011 per aggressione. Salah e Ibrahim Abdeslam sono due fratelli francesi di nazionalità, e belgi per residenza; a Molenbeek sono dediti a furti, rapine e allo spaccio di hashish nel bar che gestiscono. Il bar è frequentato anche, appunto, da Abdelhamid Abaaoud, da Mohammad Abrini (belga di origine marocchina, arrestato nel 2016) e Bilal Hadfi.

Nel 2013 Abdelhamid Abaaoud è in Siria. Dove poi arriveranno anche tre francesi, i già citati Mostefai, Aggad e Amimour, che, pare, si siano conosciuti nel Paese medio-orientale[7]. Dalla Siria i giovani torneranno in Europa, organizzando e conducendo gli attacchi a Parigi. L'anno successivo, nel 2016, gli autori dell'attacco alla chiesa di Saint-Étienne-du-Rouvray sono Adel Kermiche, di origini marocchina; e Abdel Malik Petitjean, di origine algerina. Abdesalem Lassoued, tunisino, a ottobre 2023 colpisce a Bruxelles. Chérif Chekatt, autore dell'attacco a Strasburgo nel 2018, è di origine marocchina.

Come emerge dai percorsi biografici, il gruppo che attacca i bar e i cafè è di origine marocchina; il gruppo che attacca il Bataclan è di origine algerina. Considerare l'origine nazionale non serve a stigmatizzare una provenienza geografica, ma a mettere in evidenza che i piccoli gruppi che colpiscono sono legati da legami amicali e fiduciari che risalgono alla giovinezza. In questo caso, l'origine di entrambi i gruppi rimanda al nord-Africa e a due Paesi che hanno subito la dominazione coloniale francese. Il Marocco, dopo una serie di rivolte, diventa indipendente nel 1956. L'Algeria, dopo la guerra, nel 1962. L'insurrezione algerina del 20 agosto 1955 inizia in una data che rimanda al secondo anniversario della deposizione da parte della Francia del sultano del Marocco Mohammed V. Mentre l'indipendenza del Marocco fu esito di un processo sì conflittuale, ma negoziale e relativamente meno cruento, l'indipendenza dell'Algeria avvenne dopo una guerra, che arrivò anche su suolo francese.

A riguardo, i luoghi colpiti, ossia i cafè e i locali, sono simbolo di vitalità urbana, gioia di vivere e divertimento. I luoghi degli attacchi del 2015 sono stati individuati evidentemente perché consentivano di colpire un numero elevato di civili e per dare risalto all'azione omicida, dal momento che il terrorismo si caratterizza per la ricerca dell'eco comunicativa. La scelta dei

[7] https://www.carabinieri.it/Internet/ImageStore/Magazines/Rassegna/Rassegna%203-2016/mobile/index.html#p=145.

luoghi, però, sembra avere anche un'altra caratteristica, legata ad azioni terroristiche che in passato colpirono la Francia.

Il più rilevante precedente storico degli attacchi terroristici a Parigi del 2015 è la cosiddetta *caffè war*, inteso come scontro tra *Front de libération nationale* e *Mouvement National Algérien* (entrambi schiaranti dalla parte algerina, ma contrapposti tra loro), accompagnato dall'azione eversiva dell'*Organisation de l'armée secrète*: un insieme degli attacchi che insanguinarono la Francia tra anni Cinquanta e Sessanta, come conseguenza della guerra d'Algeria[8]. In particolare, i primi due gruppi si sono combattuti attraverso omicidi e attentati nei cafè parigini. Tra anni Cinquanta e Sessanta, quindi, la Francia è stata teatro di una serie di attacchi terroristici compiuti da gruppi differenti, legati alla guerra d'indipendenza che tra 1954 e il 1962 ha insanguinato l'Algeria. In Francia hanno colpito FLN, MNA e OAS. Circa cinquant'anni dopo i locali parigini sono di nuovo il contesto che viene colpito da azioni, questa volta organizzate e condotte da un gruppo terroristico in senso stretto, cioè da ISIS e dai suoi seguaci in Europa.

3. Il superamento della connessione forte. La collocazione interpretativa delle dinamiche coloniali

L'accostamento tra i fatti sopra citati non è sufficiente a stabilire un legame tra gli attentati del 13 novembre 2015 a Parigi con gli effetti prodotti in Francia dalla condizione post-coloniale dei cittadini di origine algerina o marocchina. Questo tema è stato esplorato dalla letteratura: il legame tra processi di radicalizzazione, soprattutto in Francia, e dinamiche post-coloniali è discusso a livello internazionale. Per esempio, Khosrokhavar (2009; 2013; 2018), lo richiama nei suoi lavori: in tal senso, appare superata l'idea di una connessione forte tra il passato coloniale della Francia e le azioni radicali dei terroristi che hanno preso parte agli attentati del 13 novembre. Infatti, è un dato consolidato – sostenuto dai lavori già citati di Roy (2005) e di Kepel (2004) – che questa dimensione entri come dato di sfondo e fattore ridefinito dall'affermazione di un senso di rabbia e di orgoglio ferito espresso dai radicalizzati francesi di matrice jihadista, in rapporto all'Ummah universale, anziché ad una singola e specifica origine nazionale (Khosrokhavar, 2018). L'adesione jihadista è considerata come ampiamente – anche se non totalmente – riassorbita nella dimensione del senso di frustrazione e nel revanscismo identitario che anima alcuni cittadini di seconda e terza generazione in

[8] FLN e MNA erano gruppi politici, non originariamente terroristici, che però adottavano talvolta strategie operative terroristiche. OAS era un'organizzazione eversiva segreta, che nei suoi caratteri originari era terroristica.

riferimento all'Ummah, più che ad una singola identità nazionale. In più, l'adesione a gruppi estremistici passa attraverso processi di socializzazione e soggettivazione nel gruppo di pari, in luoghi di incontro come le palestre, i centri culturali o le carceri (Khosrokhavar, 2013; 2018; Antonelli, 2020) e tramite la Rete. Se, quindi, da una parte è assai difficile sostenere un legame forte tra il passato coloniale della Francia e gli attori radicali dei terroristi, allo stesso tempo non si può non considerare l'esistenza del tema del colonialismo, seppur inquadrandolo in un *frame* interpretativo dove un ruolo più rilevante è ricoperto dall'adesione contemporanea a subculture jihadiste caratterizzate da forme pop e post-ideologica (Pisoiu, 2015). Per sostenere l'esistenza e la rilevanza di una, seppur debole, connessione, utile è il riferimento al lavoro di Bourdieu *Le déracinement: La crise de l'agriculture traditionnelle en Algérie*, il cui focus, seppur non immediatamente riferito al terrorismo, riguarda le trasformazioni radicali dei mondi di vita delle ex-colonie francesi e i loro effetti.

4. Per una connessione debole. La lente interpretativa di Pierre Bourdieu

Da una parte, per la comprensione delle cause del rancore e dell'odio come humus in cui affondano le radici le azioni dei giovani citati, intesi non meramente nella loro dimensione individuale ma come attori sociali, la lente interpretativa utilizzata può essere il lavoro di Pierre Bourdieu *Le déracinement: La crise de l'agriculture traditionnelle en Algérie* (1964). Lo studioso francese analizza la connessione tra le dinamiche abitative, la disuguaglianza e la stratificazione sociale e la guerra (1954 – 1962) che coinvolgono la popolazione algerina (Bourdieu, Sayad, 1964). Dall'altra, come già sottolineato, la nazionalità non va intesa come un elemento stigmatizzante.

Nel 1954 Ahmed Ben Bella fonda il *Front de libération nationale* (FLN), unendo diversi gruppi contrari al colonialismo francese in Algeria. La sua ala militare è l'*Armée de Libération Nationale* (ALN). Nel 1954 il FLN dà vita a un'insurrezione armata, grazie all'azione dei propri militanti contro forze di polizia e militari in Algeria; la reazione della Francia prevede l'impegno delle truppe presenti in loco e l'invio di nuove forze militari dalla Francia. Il 20 agosto 1955 nel nord-est dell'Algeria si verifica un intensificarsi dell'insurrezione armata diretta contro obiettivi militari, ma nella quale rimangono uccisi anche 71 civili europei. Il 30 gennaio 1956 inizia la cosiddetta Battaglia di Algeri, con l'esplosione di tre bombe in luoghi della città frequentati dai francesi. Il *Front de libération nationale* (FLN) dall'agosto del 1958 attacca anche la Francia nel suo territorio attraverso azioni terroristiche, tra le quali gli attacchi a depositi di carburante e sabotaggi. Nel 1961, tra i mesi di agosto

e ottobre, il FLN colpisce in Francia anche la Forza di polizia ausiliaria (FPA, composta da algerini)[9].

Si fronteggiavano, inoltre, due differenti fazioni entrambe ostili alla Francia, ma politicamente distanti: FLN e MNA, schieramento di sinistra fondato da Messali Hadj. Si tratta di una sanguinosa contrapposizione che in Francia fa circa 5.000 morti tra i due gruppi rivali, in una serie di omicidi e attentati terroristici nei cafè (la cosiddetta *caffè war*). A questo quadro di guerra, accompagnata atti terroristici, si aggiunge l'azione eversiva dell'OAS (*Organisation de l'armée secrète* o *Organisation armée secrète*) composta da militari francesi contrari all'indipendenza dell'Algeria che dal 1961 è protagonista di azioni terroristiche, soprattutto contro algerini. Il 18 giugno 1961 l'OAS compie un attentato in Francia con una bomba sotto il binario del treno Strasburgo – Parigi (a Vitry-Le-François) e uccide 28 persone.

Soprattutto dall'inizio della guerra d'Algeria la presenza coloniale e militare francese costringe milioni di contadini ad abbandonare le fertili terre di origine per spostarsi nei cosiddetti *regroupement* (campi di raggruppamento) o nelle grandi città come Algeri, mettendo in crisi il sistema di vita agricolo tradizionale algerino. Così, i contadini perdevano le proprie terre, i propri averi, insieme alle norme socioculturali tradizionali alle quali erano legati, per vivere una condizione anomica nelle grandi città, dove, inoltre, faticando a trovare lavoro, restavano coinvolti nel fenomeno della clochardizzazione (Tillion, 1966; 1973; 2007).

Perdita delle terre, abbandono dell'economia contadina, disintegrazione delle norme di vita tradizionali sono le componenti della deruralizzazione dell'Algeria: il fenomeno sociale che, per Bourdieu, accompagna la guerra. Inoltre, durante la guerra l'esercito francese è molto violento non solo nei confronti del *Front de libération nationale*, ma anche verso la popolazione civile, ad esempio attraverso la distruzione dei villaggi delle aree contadine e rurali. Inoltre, nell'ottobre del 1961 a Parigi la repressione violenta della polizia francese di una manifestazione di miglia di algerini residenti in Francia causa più di 100 morti tra manifestanti inermi.

I contadini, quindi, abbondano le proprie terre, vivono confinati nella miseria dei campi, delle *bidonvilles*, degli accampamenti, delle tendopoli urbane. Lo sradicamento dalle campagne e il confinamento nei campi e lo spostamento nelle città sono mutamenti radicali e violenti: trasformano l'*habitus*, inteso come principio, fatto di interazioni e relazioni con lo spazio del vivere e dell'abitare, generatore di pratiche, di percezioni e di disposizioni degli attori sociali locali (Bourdieu, Sayad, 1964).

[9] Tra i poliziotti della Fpa si contano 11 morti e 17 feriti.

Nella guerra tra Francia e movimenti per l'indipendenza, la strategia terroristica emerge su entrambi i fronti. In particolare, sono teatro delle azioni in Francia bar, locali e cafè, luoghi di socialità e di vitalità urbana.

Alla fine della guerra, dagli anni Sessanta, continua la tradizionale migrazione dall'Algeria verso la Francia, ma il flusso è costituito da gruppi più poveri e diseredati che in passato; gli immigrati algerini finivano nelle grandi periferie metropolitane o nelle *bidonville* francesi. Emerge, quindi, di un doppio confinamento. Il primo in Algeria dove i contadini erano confinati nei campi di raggruppamento; il secondo in Francia dove i migranti erano confinati nelle *bidonville* e nelle periferie (Boukhobza, 1991).

Lungo il corso degli anni Sessanta, la deruralizzazione algerina modifica l'assetto e gli spazi famigliari. Trasforma l'economia agricola rurale sostituita dalla miseria delle *bidonville* e delle periferie; fa scomparire i riferimenti formativi e interrompe la trasmissione delle norme socio-culturali. Le famiglie non vivono più unite in contesti tradizionali Questa trasformazione, violenta e repentina, contribuisce all'acuirsi dell'odio e del fanatismo religiosi in Algeria e in Francia.

Nuovi riferimenti normativi, che propongono una peculiare versione radicale della religione islamica, sostituiscono i riferimenti normativi tradizionali cancellati con la deruralizzazione. Si tratta (Roy, 2005; 2008) di un insieme di nuove caratteristiche che iniziano ad emergere verso gli anni Ottanta, quando attori come il Fronte Islamico di Salvezza (FIS) conquistano la scena politica: visione binaria del mondo; disumanizzazione degli avversari; enfasi sulla purezza; legittimità della violenza; odio per l'Occidente sono elementi che progressivamente si solidificano nell'interpretazione della religione.

Questo cambiamento avviene nel corso del tempo: negli anni Sessanta, l'Algeria indipendente di Ben Bella si orienta al socialismo. Il successore, pur essendo salito al potere con un colpo di Stato, Houari Boumedienne prosegue la politica socialista, accompagnata da una significativa espansione industriale e dalla crescita della popolazione. Alla morte di Boumedienne sale al potere Chadli Bendjedid, che prosegue il mandato presidenziale anche nel 1984 e nel 1988. Tra anni Sessanta e Settanta, il socialismo laico dell'Algeria rappresenta un elemento in grando di mantenere la coesione nazionale, sentimento che arriva fino alle periferie francesi che erano state il luogo di destinazioni dei flussi di migranti dal Nord-Africa. Dagli anni Ottanta, con la fine delle ideologie politiche, ulteriori riferimenti normativi vengono meno (Boudjedra, 1992) e, soprattutto, una grande crisi economica, dovuta al calo internazionale del prezzo del petrolio sconvolge l'Algeria. Nel 1988 le proteste giovanili sono represse nel sangue dall'esercito con centinaia di morti. Nel 1990 le elezioni amministrative sono vinte dal Fronte Islamico di Salvezza, ma, prima che il FIS possa conquistare il governo della nazione, l'esercito

prende il potere con un colpo di Stato. Nel 1992 il FIS viene sciolto e i suoi leader incarcerati. La reazione consistette nella nascita del Movimento Islamico Armato (MIA, che poi insieme ad altri gruppi si definì *Armée islamique du salut*, AIS a richiamare il FIS) e, nel 1991, del più violento e terroristico Gruppo Islamico Armato (GIA), da cui poi si separò negli anni Novanta il Gruppo Salafita per la Predicazione e il Combattimento (GSPC). Quest'ultimo citato interpreta in senso salafita la religione musulmana: l'interpretazione radicale della religione, l'esaltazione della violenza, la concezione confessionale dello Stato e del potere, l'odio per l'Occidente si affermano in Algeria e tra coloro che, anche fuori dalla nazione, non hanno e non trovano altri riferimenti politici e religiosi.

Esiste una linea rossa tra la guerra d'Algeria e l'odio contemporaneo verso la Francia, rancore che è il terreno fertile del terrorismo: nel tempo permangono l'odio e la costante attività dei gruppi succitati. Tra gli episodi degli anni Sessanta e il 2015, la Francia, e Parigi in particolare, sono colpite da numerosi attacchi terroristici. Il Gruppo Islamico Armato nel 1996 attacca la metropolitana di Parigi, ci sono 4 morti (Gregory, 2003)[10]. Inoltre, nel 2012 Mohammed Merah, francese di origine algerina, afferente al movimento estremista francese Forsane Alizza, uccide sette persone. Nel 2014 Mehdi Nemmouche, francese di origine algerina, colpisce il museo ebraico e la Sinagoga a Bruxelles, uccidendo quattro persone. Aveva combattuto per circa un anno con ISIS in Siria.

Le caratteristiche degli attacchi di novembre 2015 li inseriscono in una linea rossa, si pensi ad esempio alla scelta dei bersagli (i cafè e i locali), con la storia patria e coloniale francese. Per interpretare l'odio, il risentimento, il rancore che alcuni attori sociali nutrono verso la Francia, organizzando azioni dirette contro locali, bar e cafè, è utile considerare le conseguenze della guerra d'Algeria e della strategia terroristica che comportò, arrivando sino all'affermazione di gruppi come il GIA e il GSPC.

5. Conclusioni

L'odio e il rancore verso una nazione, tali da creare il terreno fertile per il terrorismo di alcuni gruppi che la colpiscono sul suo suolo, hanno radici profonde. Nel caso della Francia, secondo una lettura forte degli effetti del passato coloniale l'odio sembra avere origine dalla guerra d'Algeria. Tra questo conflitto e gli attacchi parigini del 2015 sembra emergere un filo rosso.

[10] Negli anni Novanta dal GIA si distacca il "Gruppo salafita per la predicazione e il combattimento" (GSPC); intorno al 2007 questo gruppo aderisce ad Al-Qaida, cambiando il nome in "al-Qāʿida nel Maghreb islamico" (AQMI).

Secondo tale posizione, è utile analizzare le radici dell'odio e del rancore verso la Francia e la storia coloniale francese, non per stigmatizzare alcune nazionalità, né quella francese, né altre, ma per focalizzare il rapporto tra il colonialismo e l'humus di odio, il terreno fertile del rancore del terrorismo che colpisce in Europa.

In base, però, alle analisi condotte sul terrorismo jihadista emerge il ruolo di fattori presenti nella Francia contemporanea, legati ai contesti di vita periferici, alla mancanza di opportunità, allo svantaggio socioeconomico, alla *strain* identitaria.

Nel tempo, infatti, si assiste a un cambiamento: emergono elementi nuovi, come le azioni di francesi di origine cecena. Questi (come il ceceno che a ottobre 2023 ha colpito ad Arras) non hanno legami generazionali con ex-colonie francesi. Erano di origini cecene Abdoullakh Abouyedovich Anzorov, che nel 2020 uccise il professore Samuel Paty[11], e Khamzat Azimov, un giovane che a maggio del 2018 ha ucciso un passante a Parigi. Sembra interrompersi il legame con i contesti storici e coloniali africani, ma comunque permangono e rimangono vivi l'odio e il rancore verso la Francia, indipendentemente ormai dall'origine storica. La Francia, così, sembra essere diventata un capro espiatorio nel senso girardiano del termine, un attore, cioè che, pur in assenza di elementi causali specifici contingenti, catalizza verso di sé l'odio e la violenza.

Tali evidenze suggeriscono la necessità di temperare la lettura di un legame forte con una interpretazione secondo cui tale connessione sì esiste, ma in un senso più debole; in modo da non dimenticare gli effetti del passato coloniale, conciliandoli con elementi contemporanei. In altri contesi colonizzati emergono sentimenti di odio che fanno da terreno fertile per l'azione terroristica. Si pensi alla guerra mahdista a fine Ottocento in Sudan, conflitto che si aggiungeva alla contrapposizione tra sunniti (egiziani) e sciiti (mahdisti); ai pogrom anticristiani del 2008 in India nello Stato di Orissa, da parte di estremisti induisti. Insieme alle contrapposizioni locali, emergevano l'odio e il rancore verso alcuni attori. Ciò che caratterizza il caso francese è il trasferimento del terrore sul suolo europeo.

L'odio verso la Francia sembra essere collegato alle dinamiche della guerra d'Algeria e al peculiare stravolgimento che coinvolse la popolazione rurale (deruralizzazione) e al "doppio confinamento", ossia nei campi di raggruppamento algerini e nelle periferie e *bidonvilles* francesi, che separarono nettamente e in modo definitivo la popolazione francese da quella di origine nord-africana. Lì si realizzano le condizioni studiate in sociologia da molti approcci: dalla teoria della disorganizzazione sociale; dalla teoria del conflitto

[11] https://ednh.news/it/cronologia-degli-attacchi-terroristici-in-europa-dal-2004-al-2017.

culturale e dalla teoria del rapporto tra condizioni socio-economiche e opportunità. Si tratta di contesti socialmente disorganizzati, in cui spesso emergono conflitti tra le norme socioculturali degli autoctoni e quelle dei gruppi di provenienza *altra* e dove le condizioni strutturali di tali gruppi e la disponibilità di mezzi come l'istruzione e il lavoro li allontanano dal raggiungimento degli obiettivi socio-economici dominanti.

Riferimenti bibliografici

Aben, S.M. (2018), *The ISIS eradication of christians and yazidis: human trafficking, genocide, and the missing international efforts to stop it*, «Revista de Direito Internacional, Brasília», v. 15, n. 1, pp. 238-253.

Antonelli, F., 2020, *Il posto dell'attore sociale nei radicalization and terrorism studies*, «Rivista Trimestrale di Scienze dell'Amministrazione», 1, pp. 1-19

Crenshaw M., 1981, *The causes of terrorism*. Comparative Politics, 13, 4: 379. Testo disponibile all'indirizzo web: https://courses.kvasaheim.com/hist319a/docs/Crenshaw %201981.PDF (25/03/2020).

Bourdieu P., Sayad, A. (1964), *Le déracinement: La crise de l'agriculture traditionnelle en Algérie*, Les Éditions de Minuit, Paris.

Bourdieu, P. (2005), *Il senso pratico*, Armando, Roma.

Boudjedra, R. (1992), *FIS de la haine*, Editions Denoël, Paris.

Boukhobza, M. (1991), *Octobre 88: Evolution ou rupture?*, Bouchène, Alger.

Carroll, D. (2007), *Albert Camus the Algerian: Colonialism, Terrorism, Justice*, Columbia University Press, New York.

Cottee, S. (2015), *The Challenge of Jihadi Cool*, The Atlantic. The Atlantic Monthly Group, pp. 1-2. Link: http://www.theatlantic.com/international/archive/2015/12/isis-jihadi-cool/421776/.

Crenshaw, M. (1981), *The causes of terrorism*, «Comparative politics», XIII, pp. 379-399.

Della Porta, D. (1990) *Il terrorismo di sinistra*, il Mulino, Bologna.

Id. (a cura di) (1992) *Social movement and violence: participation in underground organizations*, Greenwich, Conn., pp. 259-290.

Ganser, D., Calzavarini, S. (2005) *Gli eserciti segreti della NATO. Operazione Gladio e terrorismo in Europa occidentale*, Fazi, Roma.

Giglioli D. (2018), All'ordine *del giorno è il terrore, I cattivi pensieri della democrazia*, il Saggiatore, Milano.

Grégoire V. (2016), *Clochardisation, déracinement, dépersonnalisation. La fin de l'Algérie coloniale*, Dans Sens-Dessous, 1, 17, pp. 91-102.

Gregory, S. (2003), *France and the War on Terrorism*, «Terrorism and Political Violence», 15 (1), pp. 124-147.

Gupta, A., Özyer, T., Rokne, J., & Alhajj, R. (2019), *Social network analysis to combat terrorism: 2015 Paris Attacks*, «Social Networks and Surveillance for Society», pp. 165-179.

Di Marco, A.G. (1991), *La storia universale come storia comparata in Max Weber*, «Archivio di teoria della cultura», IV, pp. 165-187.
Houellebecq, M. (2015), *Sottomissione*, Bompiani, Milano.
Krais, B., Gebauer, G. (2009), *Habitus*, Armando, Roma.
Khosrokhavar, F. (2009), *Inside Jihadism: Understanding Jihadist Movements Worldwide*, Paradigm, Boulder and London.
Id. (2017), *Radicalisation*, Éditions de la Maison des sciences de l'homme, Paris.
Id. (2018), *Le nouveau jihad en Occident*, Robert Laffont, Paris.
Id. (2013), *Radicalization in Prison: The French Case*,
«Politics, Religion & Ideology», Vol. 14, No. 2, 284-306, http://dx.doi.org/10.1080/21567689.2013.792654
Kepel, G. (2004), *Jihad. Ascesa e declino. Storia del fondamentalismo islamico*, Carocci, Roma.
Kepel G. (2017), *Terror in France: The Rise of Jihad in the West*, Princeton University Press, Princeton.
Marrouchi, M. (2003), *Introduction: Colonialism, Islamism, Terrorism*, «College Literature», 30 (1), pp. 6-55.
Mohammed, I. (2022), *Decolonialisation and the Terrorism Industry*, «Critical Studies on Terrorism», 15:2, 417-440, DOI: 10.1080/17539153.2022.2047440
Pauwels, A. (2016), *ISIS and illicit trafficking in cultural property: Funding terrorism through art*, «Freedom from Fear», 11 (7), pp. 64-71
Pisoiu, D. (2015), *Subcultural theory, jihadi and right-wing radicalization in Germany*, «Terrorism and Political Violence», 27 (1), pp. 9-28.
Roy, O. (2005) *La Laïcité face à l'Islam*, Stock, Paris.
Id. (2008) *La sainte ignorance. Le temps de la religion sans culture*, Seuil, Paris.
Id. (2016), *Peut-on comprendre les motivations des djihadistes?*. Pouvoirs, 158, pp. 15-24. https://doi.org/10.3917/pouv.158.0015
Id. (2017), *Generazione ISIS. Chi sono i giovani che scelgono il Califfato e perché combattono l'Occidente*, Feltrinelli, Milano.
Saïd, E. (2000), *Nationalism, Human Rights, and Interpretation*, Reflections on Exile, and Other Essays, Harvard University Press, Cambridge.
Spivak, G.C. (1999), A Critique of Postcolonial Reason: Toward a *History of the Vanishing Present*, Harvard University Press, Cambridge.
Stenersen, A. (2011) *Al Qaeda's Foot Soldiers: A Study of the Biographies of Foreign Fighters Killed in Afghanistan and Pakistan Between 2002 and 2006*, «Studies in Conflict & Terrorism», 34, 3, pp. 171-198.
Tillion, G. (1966), *Le harem et les cousins*, Seuil, Paris.
Tillion, G. (1973), *Ravensbrück*, Seuil, Paris.
Tillion G. (2007), *Combats de guerre et de paix*, Seuil, Paris.
Tirozzi, G. (2019), *D'incanto il terrore. Storia di combattimenti e pazzi furiosi*, Acar edizioni, Milano.
Victoroff, J. (2005), *The Mind of the Terrorist. A Review And Critique Of Psychological Approaches*, in «Journal of Conflict Resolution», 49, 1, pp. 3-42. DOI: 10.1177/0022002704272040

Zuev, D., Vergani, M. (2015), *Neojihadist Visual Politics: comparing YouTube videos of the North Caucasus and Uighur militants*, «Asian Studies Review», 39 (1), pp. 1-22.

Weber, M. (1922), *Gesammelte Aufsätze zur Wissenschaftslehre*, Mohr, Tübingen.

Wieviorka, M. (2009), *Violence: A New Approach*, Sage, London DOI: 10.4135/ 18

Fading jihadism? Understanding Hayat Tahrir al-Sham's online propaganda campaign

Miron Lakomy

Miron Lakomy is a Professor at the Institute of Political Sciences, the University of Silesia, Poland, and a non-resident fellow at the ITSTIME research centre in Italy. His research primarily focuses on various aspects of political violence and terrorism on the Internet, as well as military conflicts. He has published five monographs and more than 70 scientific papers in the United States, United Kingdom, Israel, Spain, Italy, Netherlands, Ukraine, Czech Republic, and Poland. He held multiple visiting research positions during his career, including those at the University of Oxford, the University of Cambridge (Corbridge Trust scholarships), and the European University Institute in Florence.

Abstract

This article, founded primarily on the combination of open-source intelligence (OSINT) and social network analysis (SNA), discusses the most important features of Hayat Tahrir al-Sham's (HTS) propaganda campaign on the Internet between mid-2023 and February 2024. It proves that during this period, HTS maintained a relatively small but well-designed information ecosystem founded on two distinct pillars. The first was composed of three standalone websites, run by Amjad Foundation and Alaskary Media, which served as hotspots for pro-HTS strategic communication on the surface web. The second pillar was founded on several Telegram channels, which makes it similar to information ecosystems maintained by other Salafi-jihadist violent extremist organizations. This paper also demonstrates that in 2023 and 2024, HTS and its media offices visibly drifted away from most types of narratives and topics that could be associated with Salafi-jihadist terrorism, which seems to be a long-lasting priority in its strategic communication. However, its focus on militarism and the promotion of suicide attacks confirms that HTS still constitutes a violent extremist organization that carries out a broad range of controversial activities and maintains links with more radical entities based in Idlib. Last, this study shows that Alaskary Media had much greater propaganda production capabilities than the Amjad Foundation. The latter, however, frequently produced technically better, alluring videos portraying the dynamically growing HTS's military capabilities.

Questo articolo, basato principalmente sulla combinazione di open-source intelligence (OSINT) e social network analysis (SNA), discute le caratteristiche più importanti della campagna di propaganda di Hayat Tahrir al-Sham (HTS) su Internet tra la metà del 2023 e il febbraio 2024. Il documento dimostra che in questo periodo HTS ha mantenuto un ecosistema informativo relativamente piccolo ma ben progettato, fondato su due pilastri distinti. Il primo composto da tre siti web autonomi, gestiti dalla Fondazione Amjad e da Alaskary Media, che fungevano da hotspot per la comunicazione strategica pro-HTS sul web di superficie. Il secondo fondato su diversi canali Telegram, rendendolo simile agli ecosistemi informativi gestiti da

altre organizzazioni estremiste violente salafite-jihadiste. Questo articolo dimostra anche che nel 2023 e nel 2024, HTS e le sue articolazioni mediatiche si sono visibilmente allontanate dalla maggior parte dei tipi di narrazioni e tematiche generalmente associati al terrorismo salafita-jihadista. Questa appare essere una priorità duratura nella sua comunicazione strategica dell'organizzazione. Tuttavia, la sua attenzione al militarismo e alla promozione di attacchi suicidi conferma che HTS costituisce ancora un'organizzazione estremista violenta che svolge un'ampia gamma di attività controverse e mantiene legami con entità più radicali con sede a Idlib. Infine, questo studio dimostra che Alaskary Media ha capacità di produzione di propaganda molto più elevate rispetto alla Fondazione Amjad. Quest'ultima, tuttavia, ha spesso prodotto video tecnicamente migliori e maggiormente capaci di attrarre, che ritraggono le capacità militari HTS in dinamica crescita.

Keywords

Terrorism, violent extremism, propaganda, Hayat Tahrir al-Sham, Alaskary, Amjad

Acknowledgment

This study was supported by the Polish National Agency for Academic Exchange (NAWA – Narodowa Agencja Wymiany Akademickiej) under the Bekker programme (grant no.: BPN/BEK/2022/1/00002/U/00001).

1. Introduction

Hayat Tahrir al-Sham (HTS) has been the subject of a heated academic debate in recent years. Due to its control over the Northwestern part of Syria – the Idlib Governorate – scholars have intensively studied its role in the Syrian civil war, including its complex relations with Turkey or the competition with other rebel and terrorist groups (Schwab, 2023; Martinez & Eng, 2018; Zelin, 2023; Bakkour, 2023). Aside from its role in the military conflict in the Levant, Hayat Tahrir al-Sham attracted the interest of terrorism and political violence researchers. This is because it represented the Salafi-jihadist ideology, at least partially inherited from the al-Qaeda-aligned Jabhat al-Nusra. It also hosted other violent extremist organizations (VEOs) on its territory and had a long track record of violating human rights in the area (Heller, 2017; Hamming, 2019). These are the primary reasons why certain states, such as the United States, have designated HTS as a terrorist organization (Amendments to the Terrorist Designations, 2018). However, in recent years, the group has undergone a process of at least partial "mainstreamization," manifesting in attaching, at least officially, lesser importance to traditional elements of Salafi-jihadist *credo* despite still carrying out a broad range of controversial activities in Syria. While there is no consensus among scholars on

how to perceive this shift, it is still widely considered the most powerful and one of the most controversial violent extremist organizations in the Levant (Zelin, 2022; Drevon & Haenni, 2021).

Surprisingly, in this heated scientific debate, relatively little attention has been devoted to better understanding its propaganda activities. Only a handful of studies have focused on identifying the most essential features of HTS's strategic communication (Haid, 2019; Barnard, Winter, 2023). This is despite the fact that HTS has been known to carry out complex and well-developed media activities on the Internet since its creation. Throughout the years, the group's capabilities in this regard were supported by a number of official and unofficial media outlets, such as the Amjad Foundation for Media Production, Ebaa News Agency (ENA), Alaskary Media, and al-Bunyan Radio,[1] which employed differentiated approaches to influence online audiences. They included, among others, methods and narratives that are usually associated with digital *jihad* (Lakomy, 2023a; Online jihadist propaganda, 2023, p. 21). In this context, while there are studies that cover selected aspects of HTS's propaganda campaign (Barnard, Winter, 2023), we still do not have enough understanding of how its propaganda machine evolves and how it adapts to the aforementioned political and ideological changes introduced by its leadership in recent years.

This study aims to fill this gap in research. It has four scientific objectives. First, to understand the most important features of Hayat Tahrir al-Sham's propaganda campaign on the Internet between mid-2023 and March 2024. Second, to map the structure and evolution of the information ecosystem utilized by this group and its followers on the surface web during this period. Third, to measure the propaganda output generated by the group's official (the Amjad Foundation for Media Production) and unofficial (the Alaskary Media) media offices. Fourth, to understand what themes have been primarily exploited in the HTS-aligned propaganda. In order to reach these objectives, this study exploited a combination of open-source intelligence (OSINT), online observation, content, comparative analysis, and social network analysis (SNA).

This paper has been divided into three sections. The first briefly covers the methodology of this project. The second explores the evolution and structure of the pro-HTS information ecosystem discoverable on and from the surface web from July 2023 to February 2024. The third section discusses the scope of pro-HTS propaganda production during this period. It also identifies the most critical tendencies regarding the topics its media offices covered at the time.

[1] ENA and al-Bunyan Radio went inactive in recent years.

2. Methodology

This study is predominantly founded on open-source intelligence, which Rita Gill (2023) defines as "intelligence produced by collecting, evaluating, and analyzing publicly available information with the purpose of answering a specific intelligence question." It employed a broad range of different OSINT tools and techniques to reach research objectives. First, it exploited so-called "Google hacking," which manifests in using advanced options and operators in the Google search engine (Mider et al., 2019). Other available and capable search engines, including Bing and Yandex, were utilized in a similar manner. Advanced operators and options were combined with Arabic and English keywords associated with Hayat Tahrir al-Sham, including names of its media offices, titles of prominent propaganda productions, or associated terminology. This allowed the identification of primary surface web locations, which were subject to subsequent verification regarding being associated with Hayat Tahrir al-Sham, including supporting its agenda even unofficially. Aside from search engines, this step also included the use of popular reverse image search tools, such as *TinEye* (Bitirim, 2022). Several popular visuals associated with HTS, such as its logotypes, were subject to reverse image search, allowing to find locations where they were posted.

In the second phase of the study, all discovered and available surface web locations aligned with HTS were subject to data scraping (Niu et al., 2022), which was founded on a broad range of tools, including primarily the *Spiderfoot* web reconnaissance software. Its goal was to detect information on other interconnected communication channels constituting part of the HTS-associated information ecosystem. This includes predominantly external links, although other significant data, such as webpages co-hosted on the same server, were also considered. It should be stressed that in this phase, the study collected links to surface, deep, and dark web locations, as well as information about channels and profiles on messaging apps. Subsequently, each link was verified regarding its association with HTS or its followers. Internet addresses, which could be accessed with an ordinary web browser without additional registration, were subject to similar data scraping in the third phase. Effectively, this approach allowed the registration of all discovered URLs associated with HTS and their interconnectedness in the database.

It must be emphasized that this study has focused on communication channels available on the surface web or discoverable from it (Mead & Agarwal, 2020). For the purpose of this project, the surface web is perceived as the part of the Internet that is available to the general public, does not require an additional signing-up procedure, and can be detected by search engines. There are three particular reasons why this approach was adopted. First, ter-

rorist-operated websites (TOWs) have remained an essential means of distributing propaganda by a broad range of non-state actors, including violent extremist organizations, in recent years (Lakomy, 2023b). This is mainly because the surface web is the easiest for all interested users to access. Second, the use of this layer of Internet communication by VEOs has remained under-researched for years as scholars were more inclined to analyze messaging apps and social media platforms (Conway & Looney, 2021). Thirdly, there are certain legal constraints on the territory of some of the European Union's member-states – where this study was carried out – in researching violent extremist communication channels located on restricted communication channels, such as messaging apps (Lakomy, 2024). Effectively, the adopted approach allowed for the detection of HTS-aligned communication channels available on and from the surface web. This includes not only standalone websites and blogs but also Telegram channels and profiles on social media.

Each detected and positively verified URL was subject to coding into several categories in databases. First, its location was registered under Web 1.0 (standalone websites, blogs, message boards), Web 2.0 (file-sharing services, social networks), dark web (.onion domains), and messaging apps (including, for instance, Telegram, WhatsApp, or Rocket Chat). Its availability in a given month was also verified at the beginning and the end of each period. The website was coded as "positive," even if it was available only for one day in a month. Thirdly, for the purpose of mapping the whole of the information ecosystem, all outlinks leading to other HTS-aligned URLs were registered. In this context, it should be stressed that file-sharing platforms were subject to slightly different coding due to their function as storage for individual propaganda files (Macdonald et al., 2022). To be more precise, links leading from one website to multiple propaganda pieces stored on a single file-sharing platform were still treated as one link in the database. Multiple links were included only if they led to file-sharing services constituting separate propaganda dissemination channels, such as the Internet Archive. On top of this, the study registered specific functions of each URL and the approximate dates of their creation and takedown. New URLs identified in a given month were counted separately. Overall, this approach allowed the creation of eight monthly databases covering the period between July 2023 and February 2024.[2] Each database was cumulative, i.e., it contained all newly collected data on top of all the information gathered in previous periods.

[2] All monthly databases were cumulative, meaning they were built upon the data gathered in a previous period and included new discoveries and changes on the monitored communication channels. Databases included both available and unavailable Internet addresses.

All collected data was subject to subsequent social network analysis that focused on identifying the most critical parts of the information ecosystem maintained by Hayat Tahrir al-Sham, as well as understanding its evolution over eight months. In order to do so, all individual Internet addresses in this study were assigned unique IDs used in SNA. Due to counterterrorism reasons, IDs were only loosely associated with URL titles acquired through OSINT. Subsequently, collected data allowed the creation of two databases exploited in social network analysis. The first – node list – consisted of IDs of all URLs included in eight monthly databases, as well as their selected attributes, including availability in a given month and the number of mirrors detected. The second database – edge list – included all connections between nodes in the form of external links leading from one ID to another. Both databases combined were subject to the SNA, which focused predominantly on the network's degree level, modularity, and page rank (Hua et al., 2019). This approach allowed identifying the most crucial elements of the propaganda dissemination network of HTS.

Aside from OSINT and SNA, this study also adopted a combination of online observation and content analysis, which were used in two distinct ways (Słupińska, 2020). First, the content of the Amjad Foundation's webpage, being an official propaganda arm of HTS, was subject to monitoring at regular intervals. All individual propaganda productions published on this website between July 2023 and February 2024 were subject to limited analysis and coding in four general categories (visuals, audiovisuals, audio content, text content) and 24 subcategories. The topic of each propaganda production was also individually assessed. This approach allowed measuring the propaganda output generated by the group's official propaganda arm throughout the eight-month period. Second, content released on the two other unofficial websites linked to HTS, run by Alaskary Media, was also assessed. However, both domains were subject to more general screening, aiming to measure the quantity of propaganda items available under all sections of its domains.

Finally, the study employed a limited comparative analysis. Both quantitative and qualitative approaches were adopted. The quantitative comparative analysis focused on identifying monthly changes in the number and types of URLs exploited in the HTS's information ecosystem, as well as the changes in the Amjad Foundation's propaganda production. On the other hand, the qualitative approach focused on changes in the essential features of the information ecosystem over time, as well as in the topics covered in propaganda productions.

This study has four caveats. First, for the reasons discussed above, it focused on exploring HTS's propaganda dissemination networks detectable on and through the surface web. Effectively, there is a risk that not all communi-

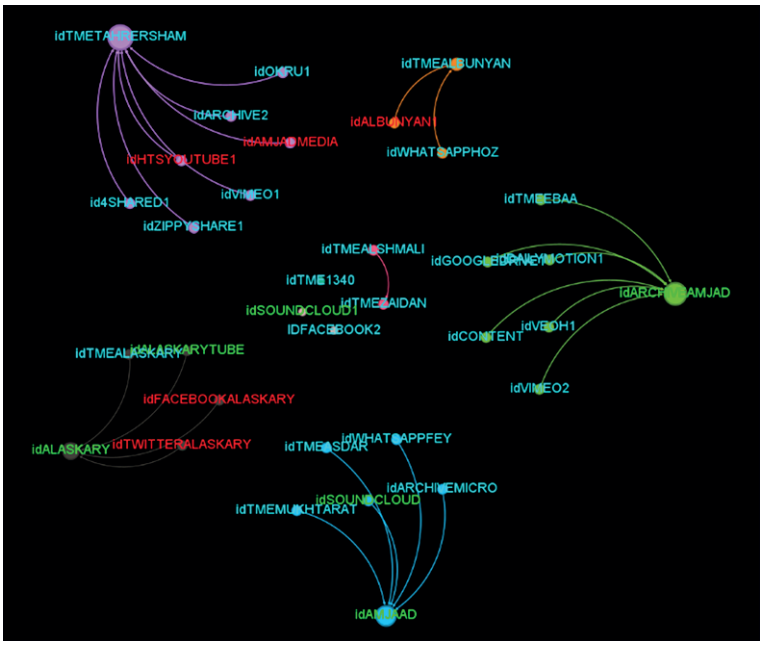
cation channels exploited by this VEO have been uncovered. Still, this study allowed the discovery of the core, most crucial, and available propaganda dissemination channels used by this violent extremist organization. Second, for security and ethical reasons, this paper does not provide the exact Internet addresses used by Hayat Tahrir al-Sham. Instead, it refers to IDs used in social network analysis. Third, the study disregarded all data that could potentially lead to identifying individuals engaged in propaganda dissemination. It did not consist of activities understood as profiling natural persons with online identifiers (Lakomy, 2024). Fourth, the study focused on mapping communication channels directly associated with pro-HTS propaganda. Therefore, it did not consider websites maintained by the Syrian Salvation Government.

3. Mapping Hayat Tahrir al-Sham's information ecosystem

Hayat Tahrir al-Sham's propaganda dissemination network uncovered in July 2023 consisted of 35 individual Internet addresses, including five domains on the surface web, 19 Web 2.0 locations, and 11 channels on encrypted messaging apps. No .onion domain was discovered. Three of five surface web locations were available at the time (Figure 1). The first was the official website of the Amjad Foundation for Media Production (*idAMJAAD*), which constituted a critical means of influencing HTS's followers on the surface web. This domain maintained a relatively small network of interconnected communication channels, including two Telegram channels, a WhatsApp group, an Internet Archive profile, and a Soundcloud profile, which focused on disseminating *nasheeds*. A second crucial standalone domain was run by Alaskary Media (*idALASKARY*). In contrast to the Amjad Foundation, it avoided being labeled as an official media outlet for HSM. Still, the vast majority of its activities focused on discussing the situation in Idlib and Syria, as well as highlighting Hayat Tahrir al-Sham's activities in the area. Due to these features, it seemed to replace the Ebaa News Agency, which went inactive in 2021, as a media outlet that supports HTS while pretending to be an instance of non-partisan journalism in the Levant. The Alaskary's webpage redirected users to four interconnected propaganda dissemination channels, namely Facebook and Twitter profiles, both unavailable as of July 2023, a Telegram channel, and another standalone website. The latter called the Alaskary Tube (*idALASKARYTUBE*), has proved to be a video-sharing platform. It constitutes a solution similar to the one adopted by the Ebaa News Agency, which ran a separate "tube" website in 2020 (Lakomy, 2023a). These features may hint at a possible organizational or functional connection between Alaskary Media and Ebaa News Agency. The other two detected standalone websites, including an old domain used by al-Bunyan Radio, proved to be inaccessible

as of July 2023. In this context, it should be stressed that other HTS websites that were active in 2020 and 2021, including the aforementioned domains run by ENA (Lakomy, 2023a), were unavailable in mid-2023.

Figure 1 – *Hayat Tahrir al-Sham-associated information ecosystem as of July 2023*[3]



Source: OSINT

As for the relevant Web 2.0 communication channels, the study detected an old Facebook profile of al-Bunyan Radio with 282 followers. It was still available in July 2023, but it has not been updated since 2020. Two Internet Archive (IA) profiles were also discovered, which were associated with the Amjad Foundation for Media Production. The first one (*idARCHIVEAMJAD*) contained 13 videos released by this office in 2017 and 2018 and viewed by a limited number (100-1000+) of users. It redirected all the visitors to a former Ebaa News Agency's Telegram channel and a number of file-sharing platforms, including Vimeo, Google Drive, and veoh.com. A second repository on IA (*idARCHIVEAMJADMEDIA1*) consisted of only three items from 2019, which were viewed more than 2600 times. This channel lacked any

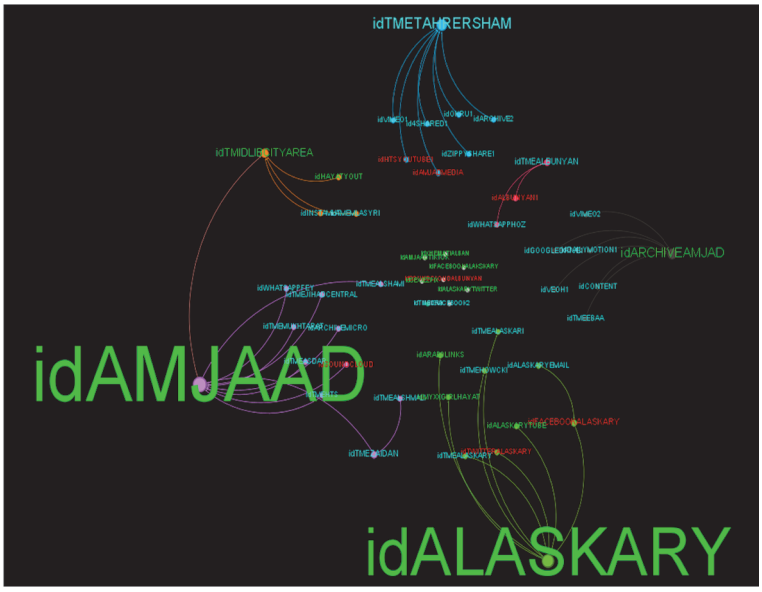
[3] The size of the nodes indicates their degree level and the number of mirrors detected. The green color indicates accessible nodes, red inaccessible, and blue communication channels, which were not subject to monthly monitoring due to the reasons mentioned above. It should be stressed, however, that upon their detection, most of the Web 2.0 communication channels identified were available.

connectivity with other parts of the HTS-aligned ecosystem. On top of this, an old al-Bunyan Radio profile on Soundcloud was detected. It consisted of 14 tracks and had 115 followers as of July 2023. However, it was last updated in 2021. Effectively, these Internet addresses were mostly remnants of the propaganda distribution activities carried out several years earlier.

The last part of the uncovered propaganda dissemination network associated with HTS consisted of several channels in encrypted messaging apps. The first one was run by Zidane Media on Telegram and had more than 10,000 subscribers. It frequently shared Amjad's content and redirected users to its official webpage. Another Telegram channel, discovered through one of the search engines, had more than 22,000 subscribers but seemed inactive in July 2023. It comprised links leading to six file-sharing or streaming platforms, including Vimeo, Internet Archive, and YouTube, although none of these locations were accessible as of July 2023.

In this context, during a period of another eight months, this study discovered 18 unique new Internet addresses used by Hayat Tahrir al-Sham and its followers for propaganda dissemination. Effectively, as of February 2024, its network (Figure 2) consisted of ten domains on the surface web (additional five), 25 Web 2.0 URLs (additional six), and 18 channels on encrypted communication apps (an additional seven).

Figure 2 – *HTS's-associated information ecosystem as of February 2024*



Source: OSINT

Additional surface web domains detected included primarily another mirror of the Amjad Foundation home page, as the former one was blocked in December 2023. Interestingly, the new address used the exact Top-Level Domain (TLD) as the old one – .video. A second new domain proved to be a mirror of the Alaskary Media website,[4] which was also banned in September 2023. Similarly to Amjad Foundation's URL, it exploited the same TLD as its predecessor – .media. It is also worth mentioning that while the main page of Alaskary got blocked, the "tube" platform remained accessible, which demonstrates the lack of consistency on the part of authorities involved in this removal. Another standalone website detected proved to be an official webpage for Xhemati Alban, an Albanian jihadist group associated with HTS and active in Idlib in recent years (Shtuni, 2019). The webpage featured mainly photo reports and videos from combat training and *ribat* service (Lecoquierre, 2023) by the members of this organization. The last two domains proved to be quite unusual, as both constituted niche platforms predominantly used for uploading pornography. Both were, however, used to distribute HTS-related content.

The most important new Web 2.0 location detected proved to be a TikTok profile run by the Amjad Foundation for Media Production. Despite the fact that it had only 59 followers as of December 2023, it proved that HTS-affiliated media offices made some attempts to establish their presence on mainstream social networks. This trend was also demonstrated by other new profiles supporting HTS, which were discovered on Twitter and Facebook. None of them had significant reach, indicating the lack of success in the exploitation of social media.

As for the changes in the use of encrypted messaging apps, a new Telegram channel for the Idlib city area seemed particularly important. It is because it developed its own propaganda distribution network, which was composed of an Instagram profile, another Telegram channel, and a YouTube profile. The whole network was directly associated with the Amjad Foundation, as all channels redirected visitors to its home page.

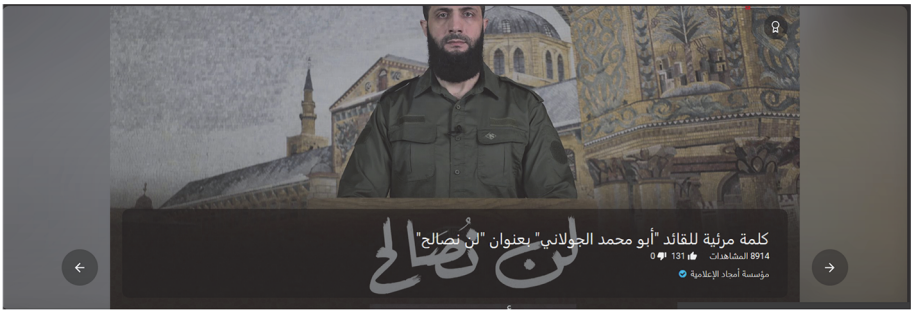
4. Exploring the thematic landscape of the Hayat Tahrir al-Sham's propaganda campaign

The social network analysis of Hayat Tahrir al-Sham's information ecosystem shows that there were two core propaganda communication channels responsible for conveying its message to the surface web audience. The first

[4] It should be stressed that multiple mirrors of one webpage of HTS were treated as a single node in social network analysis.

official was the Amjad Foundation for Media Production's website (Figure 3). Its content, exclusively in Arabic, was divided into eight sections: Everyone, Documentary, Video clips, Short Films, Dangerous Moments series, and Vocal Anthems, which is a relatively classic structure for many Salafi-jihadist websites in the Middle East. Most of the content released by this domain was either audiovisual or visual. While other types of propaganda were present, they usually originated from a period predating summer 2023. Amjad's general attitude was to release relatively infrequent but usually high-quality audiovisuals highlighting Hayat Tahrir al-Sham's military capabilities and achievements. In eight months, this domain published 39 combat videos. They can be generally divided into two distinct groups. On the one hand, they included a variety of short clips depicting artillery shelling and sniping attacks against the Syrian Arab Army (SAA). For instance, on December 23rd, 2023, it released a recording of the HTS sniper shooting at Syrian soldiers on the *ribat*, all in first-person perspective reminiscent of the FPS video games. A similar propaganda item was also released on November 18th, 2023. As for the artillery attacks, they were frequently published in October 2023 and depicted both rocket and classic artillery barrages against al-Assad forces in a third-person perspective. Such videos were usually relatively short and lacked advanced editing or special effects.

Figure 3 – *Amjad Foundation for Media Production's main page as of July 2023*



Source: OSINT

On the other hand, Amjad released less numerous but much more advanced audiovisual productions that featured combat training carried out by HTS's militants. These videos consisted of advanced directing, editing, and professional special effects combined with an alluring soundtrack. These propaganda items were designed to highlight the professionalism and dedication of the group's members, as well as showcase their special forces-like equipment (Figure 4). In a certain way, these videos exploited the same aesthetics that special forces worldwide frequently utilize in their promotional

materials. An audiovisual, which was released at the end of July 2023, may serve as a good example. It depicted a "graduation training," which focused on testing militants' skills in seizing a multi-story building. A similar video portraying HTS members carrying advanced training on the shooting range somewhere in the Syrian mountains was released at the beginning of November 2023.

Figure 4 – *Screenshot from a combat training video released by Amjad Foundation for Media Production*

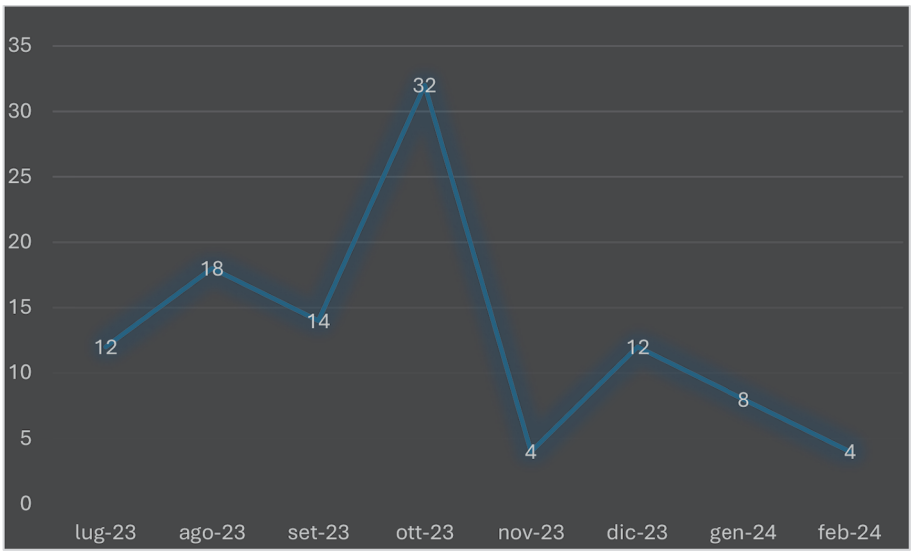
Source: OSINT

Aside from these productions, during the eight-month period, Amjad also released three short news videos, one music video, two advertisements, and seven productions coded as "miscellaneous." The two news videos focused on the HTS *shura* council meeting in Idlib and night operations north of Latakia. Two advertisements, produced in January 2024, publicized HTS's military potential and leaders. One concentrated on praising Abu Muhammad al-Jawlani's role in the organization, while the second compared HTS militants to *mujahidin* fighting against Crusaders. Miscellaneous videos were largely politics-related and usually consisted of statements from military commanders on a variety of issues.

Overall, in eight months, the Amjad Foundation's website published only 104 individual propaganda items, including 52 audiovisuals and 52 assorted images. From a monthly perspective, the greatest output was generated in October 2023 (32 items), followed by August (18) and September (14). Start-

ing from November 2023, Amjad's propaganda production dropped significantly (Figure 5).

Figure 5 – *Amjad Foundation for Media Production propaganda releases on the surface web between July 2023 and February 2024*



Source: OSINT

The second website, run by Alaskary Media, proved much more abundant in propaganda items, although it pretended not to be formally associated with Hayat Tahrir al-Sham in a similar manner to Amjad. Aside from HTS, it also reported on other groups active in Idlib, such as Ansar al-Tawhid. Its content was organized into six sections: Main Page, News, Visuals, Field Coverage, Military Graphics, and Who We Are. The most important News section comprised seven subsections:

- Special Statements, having a similar visual form to Islamic State's Amaq News Agency communiqués;
- Detailed News, which usually focuses on frontline events in Syria;
- Written Reports, being, in fact, standalone articles on a variety of subjects;
- News with Picture, combining information with photo reports;
- News Infographics, which summarized activities of Syrian rebel factions or the SAA;
- Interviews, frequently with field commanders;
- Military Analyses, which were op-eds prepared by Syrian, rebel-aligned pundits.

The Visuals comprised three subsections: Short Films, Knowledge is Power, and Visual Reports. Knowledge is Power proved to be the most interesting one, as it consisted of manuals on various aspects of military tactics. Among others, these materials highlighted the importance of camouflage on the battlefield. Other types of Visuals also had an alluring form. For instance, they consisted of video reportages made by Alaskary's media officers on the frontlines of Syria.

Other sections seemed slightly less important in the website's structure of content. Field Coverage consisted of photo reports and videos portraying military-related activities of the Syrian opposition, including primarily HTS, as well as attacks against forces loyal to Bashar al-Assad's regime. Similarly to Visual Reports, this section featured Alaskary's media operatives visiting the frontlines and conducting interviews with *mujahidin*. The Military Graphic featured visual and audiovisual propaganda in the form of, among others, infographics and posters. They covered a variety of topics, ranging from combat training of the Syrian rebels to the Ramadan wishes (Figure 6). Finally, the Who We Are section merely briefly described the objectives of this media office in the form of a single infographic.

Figure 6 – *Alaskary Media's webpage, as of September 11, 2023*

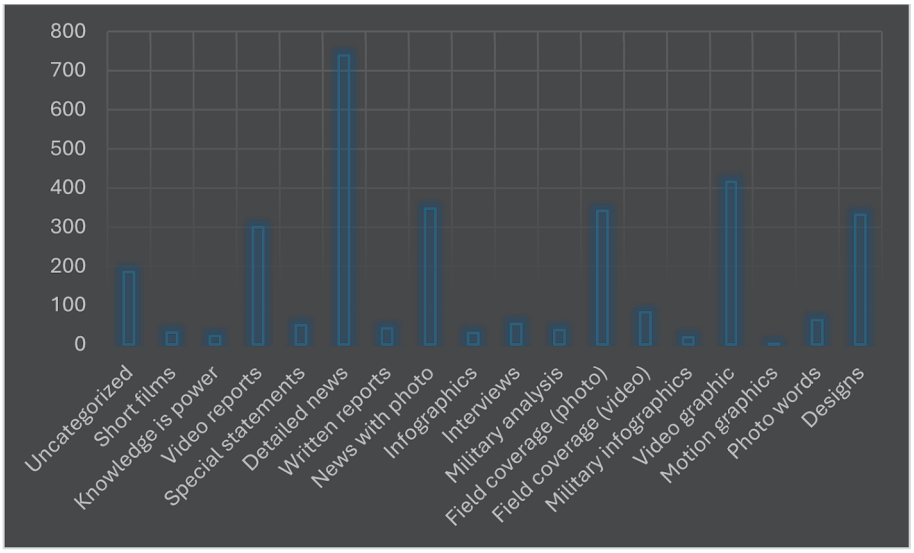
Source: OSINT

In this context, it must be stressed that the structure of the content of Alaskary Media's website reminded, in many aspects, the domain run by the Ebaa News Agency in 2020, before this propaganda bureau went inactive. This is hinted by the identical names of many subsections on their websites, including "News with Picture," "Graphic Videos," and "News Reports," which indicates a similar approach in designing webpages. Moreover, ENA and Alaskary released similar types of content, such as *quasi*-journalist reports

from the frontlines and interviews with *mujahidin* (Lakomy, 2023a, pp. 11-12).

Furthermore, it should be noted that the Alaskary Media's propaganda production capabilities proved to be significantly greater than those of the Amjad. While the latter focused on a relatively narrow set of topics and produced primarily audiovisuals, the Alaskary released a broad spectrum of propaganda materials with much greater intensity. As of March 13th, 2024, the Alaskary Tube webpage alone comprised 1068 individual video productions uploaded since its creation.[5] The Alaskary's main page was much more abundant in content, as it consisted of 3078 individual propaganda entries at the time, all released since November 2021 (Figure 7). This means that this media office was capable of releasing approximately 106 propaganda items per month on average (November 2021-March 2024). The categories that consisted of the greatest amount of content were Detailed News (738), Video Graphics (415), and News with Photos (347).[6]

Figure 7 – *Structure of the Alaskary Media propaganda uploads on its main website as of March 13th, 2024*



Source: OSINT

[5] According to the data collected from the Internet Archive's Wayback Machine, Alaskary Tube's domain was accessible since November 2021.

[6] It should be noted that Alaskary's predecessor – Ebaa News Agency – released even more than 400 propaganda items monthly (Lakomy, 2023a, pp. 14-15).

In this context, the pro-HTS media machine proved dedicated to shifting away from the traditional narratives used in Salafi-jihadist propaganda (Zelin, 2022). The content released by Amjad and Alaskary paid particular attention to promoting the political, social, economic, and military achievements of Hayat Tahrir al-Sham in Syria, as well as negatively framing all enemies of this group. While doing so, both media offices visibly tried to avoid the exploitation of themes, narratives, and propaganda devices usually present in content released by Salafi-jihadist terrorist organizations, such as Islamic State or al-Qaeda (Winter, 2017). This was consistent with its strategy, which was designed to improve the international image of HTS. However, not all traces of extremist narratives in its strategic communication were completely erased. This is because both Alaskary and Amjad, from time to time, conveyed content containing controversial messages, which did not match well with its new, "moderate" image. Aside from evident militarism, predominantly represented by the Amjad Foundation, for instance, HTS-aligned media also promoted *inghimasiyyin*, i.e., units of highly dedicated combatants wearing suicide vests (Barfi, 2016).

5. Conclusions

This study allows several conclusions to be made. It shows that Hayat Tahrir al-Sham, the most prominent violent extremist organization in Syria, carried out a well-thought-out online propaganda campaign in 2023 and the beginning of 2024. It developed and exploited a relatively small but well-designed information ecosystem founded on two distinct pillars. The first was composed of three websites, run by the Amjad Foundation and Alaskary Media, which served as hotspots for pro-HTS strategic communication on the surface web and were supported by a number of secondary communication channels. The second pillar was founded on several Telegram channels. The latter makes the HTS-aligned network similar to information ecosystems maintained by other Salafi-jihadist violent extremist organizations in existence.

Throughout eight months (mid-2023-February 2024), this information ecosystem grew by 66%, although the introduction of most new channels had little impact on its overall functionality. The most important changes were related to establishing mirrors of the blocked domains used by both propaganda offices aligned with HTS, which ensured stable access for all supporters of the group on the surface web. Other changes, including the rising use of social media, had little impact on the overall connectivity of this network.

Pro-HTS media offices proved to have differentiated capabilities in propaganda production. The Amjad Foundation produced relatively few pieces

of content during this period. However, their overall quality was very high, sometimes comparable to the best audiovisuals released by Islamic State at the apogee of its online campaign in 2014 and 2015 (Dauber et al., 2019). Alaskary Media regularly provided large amounts of media items through its standalone website and most of them demonstrated professionalism of their media operatives. It is worth mentioning that Alaskary's releases were usually met with much greater interest from the online audience than the Amjad Foundation. Aside from this, available communication channels consisted of large amounts of pro-HTS propaganda produced in earlier periods.

In this context, a comparison of the information ecosystem of HTS detected in 2023 and 2024 with its network mapped in 2020 (Lakomy, 2023a) shows that the overall approach of HTS towards propaganda distribution on the surface web has not changed significantly, although some innovations can also be spotted. The group still primarily relied on standalone websites and Telegram channels, but the number of essential domains decreased. Compared to 2020, the HTS-aligned network lacked, for instance, the al-Bunyan Radio. HTS has also probably resigned from utilizing the dark web, which was tested during the COVID-19 pandemic. Furthermore, as of 2023 and 2024, Hayat Tahrir al-Sham made some attempts to exploit mainstream social media, although these experiments proved rather unsuccessful, considering the popularity and accessibility of its profiles. In contrast to 2017-2020, the group also released visibly fewer propaganda items, although their quality remained extraordinary when compared to productions of other Salafi-jihadist violent extremist organizations. On top of this, as discussed above, HTS-aligned media offices paid visibly more attention to avoiding controversial topics and narratives.

Lastly, this study identified multiple similarities between media operations carried out by the Ebaa News Agency in 2020 and Alaskary Media in 2023 and 2024. Both offices used similar propaganda dissemination methods, produced similar types of content and the overall layout of their pages was alike in many aspects. They also played identical roles by promoting the HTS agenda in Syria disguised as instances of non-partisan journalism. On top of this, an interesting chronological coincidence may be spotted, as ENA went inactive in the second half of 2021, i.e., roughly at the same time when the Alaskary Media was established, at least according to the Wayback Machine data.[7] These similarities may hint that either Alaskary Media is a direct successor of ENA or it constitutes the same bureau after a rebranding process. However, no definitive evidence could be found to confirm any of these explanations.

[7] More data on the accessibility of the ENA webpage can be found at: https://web.archive.org/web/20240000000000*/ebaa.news.

References

"Amendments to the Terrorist Designations of al-Nusrah Front," (2018), U.S. Department of State. Retrieved from: https://2017-2021.state.gov/amendments-to-the-terrorist-designations-of-al-nusrah-front/.

Bakkour, Samer (2023). "The Last Jihadist Battle in Syria: Externalisation and the Regional and International Responses to Hayat Tahrir al-Sham in Idlib," *Religions*, vol. 14, no. 9.

Barfi, Barak (2016). "The Military Doctrine of the Islamic State and the Limits of Ba'athist Influence," *CTC Sentinel*, vol. 9, no. 2.

Barnard, Ines K., Winter, C. (2023). "Reframing Jihadism. Deciphering the Identity, Politics, and Agenda of Hay'at Tahrir al-Sham in Northwest Syria," in *The Handbook of Media and Culture in the Middle East*, eds. Joe F. Khalil, Gholam Khiabany, Tourya Guaaybess, Bilge Yesil. New Jersey: John Wiley & Sons.

Bitirim, Yiltan (2022). "Retrieval Effectiveness of Google on Reverse Image Search," *Journal of Imaging Science and Technology*, vol. 66, no. 1.

Conway, Maura, Looney, Sean (2021). *Back to the Future? Twenty First Century Extremist and Terrorist Websites*, Luxembourg: Publications Office of the European Union.

Dauber, Cori, Robinson, Mark D., Baslious, Jovan J., Blair, Austin G. (2019). "Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos," *Perspectives on Terrorism*, vol. 13, no. 3.

Drevon, Jerome, Haenni, Patrick (2021). "How Global Jihad Relocalises and Where it Leads. The case of HTS, the Former AQ Franchise in Syria," *EUI Working Papers*, no. 8.

Gill, Rita (2023). "What is Open-Source Intelligence?," SANS. Retrieved from: https://www.sans.org/blog/what-is-open-source-intelligence/.

Haid, Haid (2019). *HTS's Offline Propaganda: Infrastructure, Engagement, and Monopoly*, London: International Centre for the Study of Radicalisation.

Heller, Sam (2017). "The Strategic Logic of Hayat Tahrir al-Sham," *Perspectives on Terrorism*, vol. 11, no. 6.

Hua, Jie et al. (2019). "Applying Graph Centrality Metrics in Visual Analytics of Scientific Standard Datasets," *Symmetry*, vol. 11, no. 1.

Lakomy, Miron (2023a). "Crouching *shahid*, hidden *jihad*: Mapping the online propaganda campaign of the Hayat Tahrir al-Sham-affiliated Ebaa News Agency," *Behavioral Sciences of Terrorism and Political Aggression*, vol. 15, no. 3.

Lakomy, Miron (2023b). "The virtual 'Caliphate' strikes back? Mapping the Islamic State's information ecosystem on the surface web," *Security Journal*, vol. 36.

Lakomy, Miron (2024). "Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas," *Media, War & Conflict*, vol. 17, no. 1.

Lecoquierre, Marion (2023). "*Ribat* in Palestine: life on the frontier," *Contemporary Levant*, vol. 8, no. 2.

Macdonald, Stuart, Rees, Connor, Joost S. (2022). *Remove, Impede, Disrupt, Redirect: Understanding & Combating Pro-Islamic State Use of File-Sharing Platforms*, Washington D.C.: RESOLVE Network.

Martinez, Jose C., Eng, Brent (2018). "Stifling stateness: The Assad regime's campaign against rebel governance," *Security Dialogue*, vol. 49, no. 4.

Mead, Esther, Agarwal, Nitin (2020). "Surface Web vs Deep Web vs Dark Web," in *Encyclopedia of Big Data*, eds. Schintler, L.A., McNeely, C.L., Cham: Springer.

Mider, Daniel, Garlicki, Jan, Mincewicz, Wojciech (2019). „The Internet Data Collection with the Google Hacking Tool – White, Grey or Black Open-Source Intelligence?," *Internal Security Review*, vol. 20.

Niu, Qingli et al. (2022). "Web Scraping Tool for Newspapers And Images Data Using Jsonify," *Journal of Applied Science and Engineering*, vol. 26, no. 4.

Online jihadist propaganda. 2022 in review (2023), Luxembourg: Publications Office of the European Union.

Schwab, Regine (2023). "Same but Different? Ideological Differentiation and Intra-jihadist Competition in the Syrian Civil War," *Journal of Global Security Studies*, vol. 8, no. 1.

Shtuni, Adrian (2019). "Western Balkans Foreign Fighters and Homegrown Jihadis: Trends and Implications," *CTC Sentinel*, vol. 12, no. 7.

Słupińska, Kamila (2020). "Secondary Observation as a Method of Social Media Research: Theoretical Considerations and Implementation," *European Research Studies Journal*, vol. XXIII, no. 2.

Tore Refslund Hamming (2019). "Global Jihadism after the Syria War," *Perspectives on Terrorism*, vol. 13, no. 3.

Winter, Charlie (2017). *Media Jihad: The Islamic State's Doctrine for Information Warf*are, London: The International Centre for the Study of Radicalisation and Political Violence.

Zelin, Aaron Y. (2022). *The Age of Political Jihadism. A Study of Hayat Tahrir al-Sham*, Washington D.C.: The Washington Institute for Near East Policy.

Zelin, Aaron Y. (2023). "Jihadi 'Counterterrorism:' Hayat Tahrir al-Sham Versus the Islamic State," *CTC Sentinel*, vol. 16, no. 2.

Nuove minacce, genere e sicurezza: prospettive sociologiche e comunicative

Barbara Lucini

Barbara Lucini (phd in Sociology and Methodology of Social Research), is Researcher at the Faculty of Arts and Philosophy, Catholic University of Sacred Heart, Milan.
She is a Senior Researcher at the Italian Team for Security Terroristic issues and Managing Emergencies – ITSTIME. She coordinated the research activities of the EU Project – H2020 – CounteR – Countering Radicalization for a Safer World Privacy-first situational awareness platform for violent crimes, terrorism and crime prediction, counter radicalisation, and citizen protection.
She is professor of Theories and Techniques of Media Communication Faculty of Arts and Philosophy,
Catholic University of Sacred Heart, Milan.
She has been involved in the scientific coordination of several research projects (European and others) focused on crisis management, risk communication, risk perception, security, resilience, radicalisation and extremisms. Her research interests are oriented to sociology of disaster, disaster resilience, disaster management, extremisms and radicalisation. Further, the issue of the relationship between terrorism and resilience as well as political extremism have been studied. She is the author of several publications and the Disaster Resilience from a Sociological Perspective Exploring Three Italian Earthquakes as Models for Disaster Resilience Planning, Springer International Publishing, 2014; The Other Side of Resilience to Terrorism A Portrait of a Resilient-Healthy City, Springer International Publishing, 2017

Abstract

The social changes present in current societies and digitalization as a new dimension of life represent the relational and communicative context within which the gender issue has developed.
This paper offers a reflection from a sociological perspective on the social construction of gender with reference to the processes of radicalization and extremism phenomena, going beyond the initial approaches based in particular on the role of women as victims of radicalization processes.
After a brief sociological study on the social construction of gender, gender issues will then be addressed from a threefold perspective: gender and forms of extremism; gender themes and narratives; and gender representations.
These orientations support the idea that gender, understood not only in the traditional sense of male and female, has become an agent of socialization capable of catalyzing different forms of extremism and therefore able to attract multiple extremist narratives transversal to contemporary geopolitical scenarios.

The interpretative models that can be developed in consideration of this approach, in addition to providing a sociological in-depth analysis of the issue of gender, also have methodological and operational implications in the practice of security agencies responsible for assessing risk, new threats and systematizing intelligence and communication practices that can prevent and counter increasingly labile and heterogeneous forms of extremism.
This paper therefore presents some preliminary results of the studies and analyses conducted within the D1 research line. "Radicalization and emerging threats: sociological and gender perspectives" funded by the Department of Sociology, Catholic University of the Sacred Heart, Milan.

I cambiamenti sociali presenti nelle attuali società e la digitalizzazione come nuova dimensione di vita rappresentano il contesto relazionale e comunicativo all'interno del quale la questione del genere si è sviluppata.
Il presente contributo offre una riflessione da una prospettiva sociologia sulla costruzione sociale del genere in riferimento ai processi di radicalizzazione e ai fenomeni di estremismo superando gli approcci iniziali fondati in particolare sul ruolo della donna come vittima dei processi di radicalizzazione.
Dopo un breve approfondimento sociologico sulla costruzione sociale del genere, si affronteranno quindi le questioni di genere secondo una triplice prospettiva: il genere e forme di estremismo; temi e narrative di genere; rappresentazioni di genere.
Questi orientamenti supportano l'idea che il genere, inteso non unicamente nell'accezione tradizionale di maschile e femminile, sia diventato un agente di socializzazione capace di catalizzare forme differenti di estremismo e per questo in grado di attrarre narrative estremiste molteplici e trasversali agli scenari geopolitici contemporanei.
I modelli interpretativi che possono essere sviluppati in considerazione di questo approccio, oltre a fornire un approfondimento sociologico al tema del genere, hanno anche risvolti metodologici e operativi nell'ambito della pratica delle agenzie di sicurezza deputate alla valutazione del rischio, delle nuove minacce e alla sistematizzazione di pratiche di intelligence e comunicative che possano prevenire e contrastare forme di estremismi sempre più labili ed eterogenee.
Questo paper presenta quindi alcuni risultati preliminari degli studi e analisi condotte nell'ambito della linea di ricerca D1. *"Radicalizzazione e minacce emergenti: prospettive sociologiche e di genere"* finanziata dal Dipartimento di Sociologia, Università Cattolica del Sacro Cuore, Milano.

Keywords

Gender; extremism; radicalisation; MUU ideologies, Genere; estremismo; radicalizzazione; ideologie MUU

1. Introduction: Which gender for which threats?

The current era is increasingly characterized by the digitization of communication and socialization processes, as well as a growing climate of pervasive hatred and conflict that, even in latent way, feed the perception of insecurity and precariousness of contemporary life.

The expression of these conflictual and violent feelings and attitudes takes place within a system of relationships that is structured both in the off-line and in the on-line dimension through digital processes of hybridization of personal and social identities.

The social changes taking place are therefore many and affect all spheres of social life, from the most personal to that concerning nation-states and their geopolitical positioning.

These dynamics intersect with two fundamental factors such as the construction of digital social identity and the level of conflict and extremism reached in a large part of the world's population. The latter is a very relevant phenomenon because it is based on elements of cognitive perception that orient attitudes towards others and social behaviors in the digital world.

In this context defined by digital socialization processes and dominated by factors of uncertainty, insecurity, and conflict, it is essential to be able to better understand the role of gender and the differentiation of gender-related roles in socialization processes that result in radicalization and extremism phenomena, transcending traditional ideological boundaries based on radically different political and religious positions.

Such a reflection in the sociological field has not yet been fully systematized, as in the last two decades, gender in the context of radicalization processes has been predominantly identified as a factor of vulnerability with particular reference to the role of women and programs to prevent and counter forms of extremism and radicalization of which women may be victims.

Contemporary history highlights how the role of women, in certain extremist and terrorist social contexts, has been central and very active for the constitution of the group, for the vetting processes or selection of future members and for the maintenance of the group itself over time. An example of this is the phenomenon of some Western women who, as foreign fighters, have left for Syria and Iraq to fight in the ranks of the ISIS group (Saltman & Smith, 2015).

In light of this, retracing the models of socialization to gender from a social perspective is important for understanding how this socio-cultural factor acts in contemporary digital contexts and contributes to the narrative of the phenomena of radicalization and extremism, both political and religious.

Finally, despite the sociological approach, it is considered essential to consider the role of geopolitical scenarios and how they influence socialization dynamics and cultural and communicative processes in the digital dimension of current life. In this regard, Crespi (2008), citing authors such as Friedman (1994), Bauman (2002), and Bartholini (2003), highlighted how the phenomenon of globalization had influenced the processes of construction

of individual and social identities, thus recognizing its role and specific effects produced by a phenomenon of the global context.

2. Sociology and gender: perspectives and models

For more than twenty years there has been increasing attention on the part of sociology to the theme of gender and its declination in the sociological field.

Sociology has questioned the role that gender plays in the construction of personal and social identity and in the system of relationships within which a person is inserted.

The sociologist Crespi (2008) has systematized the models of gender-related socialization processes, considering the classical authors and the history of sociology.

In particular, the analysis conducted by Crespi (2008) shows four models related to the development of gender identities:

- *Integrationist model* that is characterized by the functional role attributed to the relationship between men and women;
- *Conflictualist model* through which the character and level of conflict between genders is highlighted;
- *Communicative model* through which the focus on gender is linked to its level and its modes of discursiveness;
- *Relational model* which emphasizes the reciprocity of recognition and relationship that exists between genders

These four theoretical models developed in different historical eras in which social relations, the construction of social identities, and belonging to a gender identity were determined by socialization agencies such as the family and school, elements that today appear increasingly weakened and empty of their socialization purpose.

Moreover, all these approaches, except the last relational one, are placed in pre-digital social context, in which the development of social relationships and communication processes took place for the most part in the off-line dimension.

The advent of new technologies and specifically of social platforms and instant messaging has made it possible to continue the erosion of the roles of mediators of society of socialization agencies typical in modern and post-modern times, to reach a sort of digital socialization characterized by a process of learning social norms, moral and cultural values, of being together that takes place for the most part in self-referential way and mediated by communication technologies.

Most of today's societies are characterized by a plurality of senses and meanings attributed to the construction of gender identity, sometimes discordant with each other, which seek increasingly pervasive and social representative modes with regard to the request for external confirmation.

This point has been well underlined by Crespi (2008):

> This is how relational (gender) identity takes shape, in which there is a continuous verification of the "fixed points" that constitute it and an incessant confrontation with the multiple stimuli that come from global society (Rossi, 2001).[1]

Alongside this perspective, the communicative orientation typical of the processes of construction of social identity is taken up again as central in the current era of digital societies:

> Identity becomes a communicative (and partly linguistic) process built-in interactions (situational aspect) and is continuously in question (processual aspect). It is therefore open, flexible, dynamic and subject to continuous reworking.[2] (Crespi, 2008)

The re-elaboration of identity of which Crespi (2008) argues is a typical element of the processes of socialization and of the dynamics of construction of contemporary gender identities and actualizing this perspective in particular, it is considered that the processes of construction of social identity are characterized by a lack of traditional socialization agencies, thus making it possible to speak of digital social identities strongly characterized by the characteristics themselves of the dimension of digital life as the pervasiveness and spatial and temporal continuity.

The theme of gender and gender identity is a traditional theoretical line of sociological thought that can however be declined originally and innovatively, taking into consideration how gender dynamics and the construction of social gender identity develop in relation to radicalization processes and participation in digital extremist groups.

This is theoretically and sociologically relevant because gender identities, their representations and narratives have a significant impact on digital relationships of conflict, hatred and violence as well as on organizational and power dynamics between members of different genders.

1 In italiano nel testo originale: *"Prende forma così l'identità relazionale (di genere), in cui c'è una verifica continua del "punti fermi" che la costituiscono e un incessante confronto con gli stimoli molteplici che provengono dalla società globale (Rossi, 2001)."*

2 In italiano nel testo originale: *"L'identità diventa un processo comunicativo (e in parte linguistico) costruito nelle interazioni (aspetto situazionale) ed è continuamente in discussione (aspetto processuale). È quindi aperta, flessibile, dinamica e soggetta ad una continua rielaborazione."*

It is in this context that the need to understand how gender has become an agent of socialization between different forms of extremism and its narratives, cognitive warfare strategies and disinformation is substantiated.

3. Extremisms and gender: social and security perspectives

The perspective that we want to propose here as a line of theoretical and methodological research concerns the role of gender in the dynamics of socialization and construction of social identity in extremist digital communication ecosystems.

For some years now, the context of digital extremism has been characterized by a strong hybridization between different ideologies and by a difficulty, even objective and therefore relevant for security agencies, in the certain systematization of the various extremist ideologies and orientations in their own and defined cultural spaces.

In this regard, for example, conspiracy theories, siege culture, accelerationism, incel sub-culture and eco-extremism can coexist and feed conflicting social representations and extremist interpretations of global events, influencing a public opinion – prosumer – which has now become both a user and a producer of the same content.

In the theoretical field, this phenomenon has been described by Criezis (2020), as intersections of extremism precisely in view of the impossibility of identifying specific forms of extremism and characterized by any cultural, ideological and technological distinctive trait.

For these reasons, Brace et al. (2023) have recently coined the acronym MUU which identifies forms of contemporary extremism as mixed, unclear and unstable.

These three elements highlight the essential features of current extremist phenomena that present mixed ideological and cultural orientations, unclear in their definitions and theoretical orientations and decidedly unstable in the methods of selecting new members, for which forms of permeability and openness between different extremist groups are increasingly present, in the communicative and narrative choices, in the maintenance of the original group and the continuation of propaganda activities and support for extremist visions.

Furthermore, it has been noted in recent years, precisely in consideration of the fact that the processes of radicalization and extremism are phenomena of secondary digital socialization, a limit to the recognition of this variegated extremist landscape according to the current legal systems and criteria of national security agencies.

In essence, the socio-anthropological forms of the global and current extremist phenomenon take on indistinct characteristics that are reflected in the need to update the monitoring and analysis systems of emerging threats.

This is also in consideration of how extremist phenomena and their digital representations are profoundly influenced by the possibilities made available by new technologies both in terms of specific functionality and in terms of the way in which communication and social relationship processes can be shaped by new digital technologies (Lucini, 2022a).

The recognition of new technologies as active social actors in the definition of an extremist digital communication ecosystem is fundamental for analyses that want to be effective and in line with the changes in the more general phenomenon.

This theoretical and methodological premise is declined in the study of the relationship between the new forms of extremism and the question of gender, wanting to answer in particular the question which gender for which extremism?

In particular, the role of gender in the context of current forms of hybrid and digital extremism can be deepened by considering three framework orientations such as:

- gender and some forms of extremism;
- gender themes and narratives;
- gender representations

In this context, gender from a social, cultural and anthropological instance (Kaufam et al., 2024) takes on the role of actor in the conflictual and extremist dynamics expressed by some forms of extremists such as the three that are now being considered.

4. Incel

The Incel – Involuntary celibates – subculture (ICSR, 2024), represents a form of extremism that has its roots a decade ago and the first case that can be identified as Incel is that of Elliot Rodger in 2014:

> The incel subculture, often referred to as the 'incelosphere' due to its inherently online nature, entered the public consciousness after the 2014 killing spree in Isla Visa, California by the 22-year-old Elliot Rodger, who, after killing six people died at the hands of his own gun.3 Rodger left behind a sprawling manifesto entitled "My Twisted World", in which he described his lifelong

> misery over his inability to lose his virginity or get a girlfriend, and his intention to murder as many women as possible in an act of revenge.[3] (ICSR, 2024)

This represents the first case of extremism and killing attack perpetrated by a member of the Incel subculture, which provides for an exclusively male membership of its members, who perceive themselves as victims of a social system and often report feeling rejected and excluded by the existing social system.

The interesting issue to note is that the first online Forum that began to collect the lives and experiences of these people was founded by a woman, Alana, in 1997 (ICSR, 2024) who then moved away from the community she had created.

The Incel phenomenon shows that technological evolution has made it possible to create digital hubs, sort of social attractors and catalysts of individual frustrations, feelings of hatred towards other social categories considered as causes of one's evil of living.

On a narrative level, the line chosen by Incel members is that of misogyny and the narratives that underlie hatred towards women, but it must be pointed out that over the last few years even the Incel orientations have witnessed a hybridization of their original extremist theories and new ideological orientations have arisen such as transphobia and transmisogyny which, as shown by Craanen et al. (2024), are the new representations of hatred and extremism in digital environments.

Finally, another characteristic element of the Incel community is that precisely in view of the broadening of the ideological base and the inclusion of ideologies contrary to the recognition of genders outside the traditional binary perspective, it becomes difficult to attribute specific actions and attacks as Incel as argued in the ICSR report (2024): *"Yet proving that a specific act is motivated by inceldom remains difficult."*

This supports the idea that even in the context of risk assessments and explosive threats, new interpretive and threat definition categories must be considered.

5. Tradwife

The Tradwife phenomenon – Traditional Wife was born in the United States a few years ago and then expanded mainly in Germany, France and the United Kingdom.

3Elliot Rodger, 'My Twisted World: The Story of Elliot Rodger,' 2014. http: https://schoolshooters.info/sites/ default/files/rodger_my_twisted_world.pdf.

It is an interesting phenomenon because the promoters are mainly influencers and use Tik Tok as the main platform for sharing their content and narratives that focus on the theme of the lives of women considered in the traditional roles of mothers and wives.

From a sociological perspective, the phenomenon is interesting for several reasons: the first concerns the cultural datum of the vision of women rooted in a traditional society of the 50s and 60s and which is expressed in a visual representation of environments, clothes and accessories that confirms the years to which they refer.

The second reason is that it is a phenomenon born on Tik Tok and that exploits the topicality of the platform, especially among an audience of young people, thus intercepting segments of the population potentially sensitive to the issue of lifestyle and personal choices.

In addition, video sharing is in line with the communication and narrative choices of these influencers, for whom showing a traditional family life is essential and the purpose of their communication strategy.

A strategy that is not new, however, and that is indeed based on the narratives of the nascent Islamic State, when at the beginning of its development, interested in attracting new members and showing the possibility of a serene and happy family life, they showed videos developed for these specific purposes.

The third reason is that the phenomenon of Tradwives, despite being undersized in terms of aspects related to forms of violent extremism, has often been associated with the American far right and with white supremacism (Sitler-Elbel, 2021).

This is an interesting element that highlights the question of the ideological areas within which to understand phenomena that could represent security threats in the future.

In fact, in addition to the association of the Tradwife phenomenon with white supremacism, some support (Sykes and Hopner, 2023) that these women are commodifying the ideology of the right, especially American, influencing the people who meet them not only from a cultural but also from a political perspective.

The case of the Tradwives is also relevant to argue that, although this phenomenon cannot be counted among the ranks of officially declared extremist groups, in reality, both some narrative modes and the sharing of an ideological and political substrate should lead to greater attention to the digital social and communicative dynamics active on the main platforms used (Tik Tok but also Reddit), in order to be able to identify any more evident signs of systematization and radicalization.

6. Eco extremism and gender

A very interesting position is also held by the relationship between phenomena and movements of eco-extresmism and the gender issue.

Gender is an element that in recent times has been the subject of reflections, even critical, on the relationship between gender and conceptions of nature.

In particular, the theories and movements belonging to queer culture and the vision of a post-gender society bring the issue back to some fundamental assumptions such as the fact that the subdivision and recognition of genders according to the binary perspective is something normed for men and taken for granted for women, seeing in the relationship between men nature the reproduction of powers on a patriarchal scale of society itself (Ourkiya, 2023).

This is directly related to a heteronormative ecological vision that is associated with a far-right vision to be overcome in its binary logic to reach a queer and postgender ecological vision:

> This gendering, however, has been focused on the feminine, the female, the woman, as if gender is exclusive to women while men are the norm. Nevertheless, recent years have seen the emergence of ecomasculinities, which as a field has finally begun to stand on its own. The main reason behind the need for a specific focus on masculinities is to remind the world that the masculine is gender, has feelings, can be oppressed and has the ability to care and nurture just like its contrasting feminine. Thus, in order to move forward a post-gender nonbinary approach, an ironically binary work needs to be completed by giving equal attention to masculinities in the study of ecology and the nonhuman world. (Ourkiya, 2023)

The overcoming of the opposition between the two binary genders therefore leads to a new theorization of the relationship between people and nature, placing a different consideration on how this relationship influences the dynamics of socialization and the construction of gender identity:

> This completion lies in the way ecological masculinities address oppressive masculine hegemonies that people have long used to dominate the Earth, women, Indigenous peoples, people of color, LGBTQI+ communities and other marginalised groups. Yet the reality is not black and white, as not all oppressed groups fall under the umbrella of woman/close to nature and not all oppressing individuals or institutions fall under the umbrella of man/close to culture. Gender identities are diverse and so should be the theories to address these identities within any ecological framework.

The demands of a non-gender-oriented ecology but inclusive of the various orientations could become the object of exploitation for propaganda, disinformation and extremism, especially considering the current conflictual

global geopolitical scenario, in which issues related to ecology and environmentalism are increasingly the subject of the various political agendas.

In this regard, the intersections with various extremist ideologies from the anarchist to the far right are an element of attention, considering how these extremist orientations can appropriate some narratives, such as that of power between genders, to exploit their potential to catalyze extremist attitudes, narratives and actions.

An example of this perspective is the case analysis of Cyprus' far-right National Popular Front's (ELAM) and its visual communication of the environment (Christou, 2023).

In particular, the results that emerged from the analysis conducted highlighted that the concepts of purity and control disseminated through the images chosen by National Popular Front's (ELAM) overlap with the typical ideologies of nationalism and male hegemony (Christou, 2023).

The function of appropriation and the catalyzing purpose of gender instances with reference to the ecological and environmental framework by extremist elements must make us reflect both for its theoretical and socializing scope and for the practical and operational implications that affect the security agencies responsible for monitoring and identifying a potential security threat.

7. Conclusion: Risk assessment and gender perspectives in the extremisms digital domains

The preliminary results that emerged from this first study on the relationship between gender and processes of extremism, in which gender is understood as an agent of socialization and a factor capable of catalyzing very different forms of extremism, can be declined according to three theoretical and methodological perspectives.

The first concerns the consideration of the way in which gender is theorized according to sociological theory and declined in the context of digital and on-life life (Floridi, 2014).

In the contemporary world, the processes of socialization as well as those of radicalization and adherence to extremist visions take place in the digital dimension that represents a mixture of the dimensions and characteristics of off-line and on-line life.

The digital dimension is in fact central to the construction and development of personal and social gender identity, so attention must be paid to the digital socialization processes of identities in the contexts of digital communication ecosystems.

The digital communication dynamics underlying the processes of socialization spread and socialize gender culture and therefore also the practices of the relationship between genders, belonging to and recognition of an idea of gender and cultural and representative practices of gender.

This theoretical perspective actually underlies methodological and operational determinants for the identification and understanding of possible new threats constituted around the concept of gender and its narratives. This represents a first factor of strategic importance, for the development and consideration of methods and techniques for monitoring and analyzing digital communication ecosystems that consider this multidimensionality and its equally multiple modes of expression and socio-cultural representation.

In fact, the second perspective opens up to the vision of gender which can, in the light of the cases considered, be defined in its varieties as an agent of socialization even between different forms of extremism, a catalyst of narratives and instances that intersect between elements of gender, culture, politics, economics, geopolitics and international security.

In addition, digital communication strategies and narratives that are produced with reference to gender issues can be part of cognitive warfare, strategic communication and disinformation such as the case of Algerian boxers Imane Khelif and Taiwanese Lin Yu Ting at the recent Paris 2024 Olympics (Lucini, 2024).

These events are not new in the digital landscape and refer to other cases that occurred in 2020 and on which the attention of a report by ISD - Institute for Strategic Dialogue, which in 2022 supported the central role of social platform companies in the spread of hate content towards athletes of other kinds:

> At the very least, however, social media companies must ensure that prominent media outlets and public figures are not able to generate support or gain traction with such content. One such way of achieving this could be through actively monitoring accounts that have shown to be repeat offenders on this issue, such as those highlighted in this research. (ISD, 2022)

It is in this context that the gender issue, originally anchored in socio-anthropological dimensions, manifests its geopolitical and international significance.

In this regard, the need emerges for security agencies to monitor the appropriation and use of gender in extremist digital contexts, as this issue, as already noted in the cases explained above, can become a risk factor for security, fueling hatred and social violence, although this phenomenon cannot always be counted in the context of more structured extremist and terrorist phenomena.

This leads to the third perspective, namely the consideration that the current state of potential extremist threats that have as their ideological substrate the variously explicit gender issues requires a different vision about the assessment of risk and the extremist threat, refining the methods, techniques and tools of Digital Humint from a gender perspective to be able to better answer the question: Which gender for which extremism?

In particular, the declination of this question refers to two further declinations of the same.

On the one hand, there is the need to be aware that current extremism and terrorism risk assessment tools (Lucini, 2022 b), the TRA-Is-Terrorism Risk Assessment Instruments consider gender in its binary meaning. Similarly, little attention is paid to the gender of the personnel who use these tools. In this regard, the theories relating to Cultural Studies dating back to the middle of the last century already highlighted how gender of belonging influenced the vision and interpretation of social practices.

On the other hand, but connected to the previous point, the need to include a reflection on gender theories, in particular feminist theories that can define the cybersecurity domain and guide the identification of digital extremism (Bengtsson Meuller, E. (2023) is considered.

In Bengtsson Meuller's (2023) study, it is argued that there are cultural and social biases in the field of cybersecurity and the way in which forms of online extremism and abuse are defined and identified.

In addition, the author focuses on the role that gender vision has in practices of preventing and countering extremism:

> Current P/CVE and cybersecurity areas' (including national policies) disengagement with gendered and racially oppressive structures means that strategies and activities that strive to counter extremisms are effectively built on male supremacist logic and consequently lack impactful intervention measures.

This underlines the need to consider, both from a theoretical-methodological point of view and from a training point of view for the personnel involved, gender perspectives and their repercussions in the definition of extremist digital communication ecosystems and the risk of extremism.

In general, therefore, the issue of gender, as emerged from this preliminary analysis, assumes strategic importance, especially as gender contrasts can become an activator and catalyst of other digital extremist dynamics and be exploited by international actors present in the broader geopolitical scenario of current cognitive wars and disinformation practices.

Finally, in agreement with Baele et al. (2024) and their research question "Is AI-Generated Extremism Credible?", it argues for the need to deepen the

issue of gender in relation to the possible new socio-cultural constructs and related communicative products developed by AI technologies and how these can potentially be exploited by extremist phenomena of other origins, but which intercept the destabilizing potential of gender issues debated in the broader framework of cognitive warfare.

Bibliography

Baele, S.J., Naserian, E., & Katz, G. (2024). Is AI-Generated Extremism Credible? Experimental Evidence from an Expert Survey. Terrorism and Political Violence, 1-17.

Bartholini, (2003), Uno e nessuno. L'identità negata nella società globale, Franco Angeli, Milano

Bauman, Z. (2002), Il disagio della postmodernità, Paravia Bruno Mondadori, Milano

Bengtsson Meuller, E. (2023), A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism, GNET Report, Retrieved online: https://gnet-research.org/wp-content/uploads/2023/05/GNET-36-feminist-cybersecurity_web.pdf

Brace, L., Baele, S.J.E Ging, D. (2023), Where do "mixed, unclear, and unstable" ideologies come from? A data – driven answer centred on the incelosphere, Journal of Policing, Intelligence and Counter Terrorism, Routledge, Taylor & Francis Group

Craanen, A., Gleeson, C., Meier, A.A., (2024), Transmisogyny, Colonialism and Online Anti-Trans Activism Following Violent Extremist Attacks in the US and EU, GNET Report, Retrieved online: https://gnet-research.org/wp-content/uploads/2024/05/GNET-43-Transmisogyny-Colonialism-Anti-Trans-Activism_web.pdf

Crespi, I. (2008), *Processi di socializzazione e identità di genere Teorie e modelli a confronto*, Franco Angeli, Milano

Criezis, M. (2020), Intersections of extremisms: White nationalist/salafi-jihadi propaganda overlaps and essentialist narratives about Muslims. Journal of Education in Muslim Societies, 2(1), https://muse.jhu.edu/article/811620/pdf

Christou, M. (2023), *Purity and control Gender and visual environmental communication by the extreme right in Cyprus*, in Visualising far-right environments, Bernhard Forchtner (ed.), Manchester University Press, UK

Floridi, L. (2014), The Onlife manifesto—being human in a hyperconnected era. Dordrecht: Springer

Friedman, J, (1994), *Cultural identity and global process*, Sage, London

Ingram, K. (2024), *Why Gender Matters in Violent Extremist Propaganda Strategy*, ICCT Policy Brief, Retrieved online: https://www.icct.nl/publication/why-gender-matters-violent-extremist-propaganda-strategy

International Centre for the Study of Radicalisation (ICSR), (2024), The Incel Subculture, King's College London, United Kingdom, Retrieved online: https://gnet-research.org/wp-content/uploads/2024/07/GNET-44e-Incel-Subculture_web.pdf

ISD - Institute for Strategic Dialogue, (2022), A Snapshot of Anti-Trans Hatred in Debates around Transgender Athletes, Digital dispatches, Retrieved online: https://www.isdglobal.org/digital_dispatches/anti-trans-hatred-against-athletes-highlights-policy-failures-facebook-twitter/

Kaufam, G., Stambolis-Ruhstorfer, M., Roberts, S., Ralph, B., (eds), (2024), *Research Handbook on the Sociology of Gender*, Edward Elgar Publishing, UK

Lucini, B. (2022a), Vetting e processi di radicalizzazione come pratiche di comunità digitali: dai TRA-I al metaverso, in *Sicurezza Terrorismo Società - Security Terrorism Society*, *International Journal Italian Team for Security*, *Terroristic Issues & Managing Emergencies*, Educatt, Università Cattolica del Sacro Cuore, Milano. Vol. 16, Issue 2

Lucini, B. (2022b), *I TRA-I e i processi di radicalizzazione: considerazioni attuali e prospettive future*, #React2022 – Rapporto dell'Osservatorio sul Radicalismo e il Contrasto al Terrorismo, https://www.startinsight.eu/tag/react/

Lucini, B. (2024), *Genere e Radicalizzazione: prospettive sociali e di sicurezza*, Retrieved online:https://www.itstime.it/w/genere-e-radicalizzazione-prospettive-sociali-e-di-sicurezza-by-barbara-lucini-english-version-at-the-bottom/

Ourkiya, A. (2023), *Queer Ecofeminism: From Binary Environmental Endeavours to Postgender Pursuits*, Rowman & Littlefield, USA

Rossi, G. (a cura di), (2001), *Lezioni di sociologia della famiglia*, Carocci, Roma

Saltman, E.M. and Smith, M., (2015), *"Till Martyrdom Do Us Part' Gender and the ISIS Phenomenon*, Retrieved online: https://www.isdglobal.org/isd-publications/till-martyrdom-do-us-part-gender-and-the-isis-phenomenon/

Sykes, S. and Hopner, V. (2023), Tradwives: The Housewives Commodifying Right-Wing Ideology, Retrieved online: https://gnet-research.org/2023/07/07/tradwives-the-housewives-commodifying-right-wing-ideology/

Diversity in media discourse. Plotting a way to break the usual frames and regain the trust of the audience and the safety of journalists

Giacomo Buoncompagni

Giacomo Buoncompagni, Università di Macerata, È docente di Sociologia del Giornalismo presso l'Università di Verona e di Antropologia giuridica e dei processi culturali presso l'Università di Macerata. E' research fellow in sociologia all'Università LUMSA di Roma. Ha pubblicato diversi articoli e saggi sul tema dell'immigrazione, della sicurezza e dei media digitali.

Abstract

In today's media ecology, it is not so much a question of entering the debate on whether or not to cover news related to the phenomenon of discrimination, but rather how the mediatisation of minorities and cultural diversity often does not go beyond certain narrative frames. Within the field of journalism, there are frames that (re)produce and reinforce negative stereotypes of groups and communities over time, often due to confused and overloaded information or journalists' lack of training in specific historical and cultural realities. The aim of this paper is to reflect on the relationship between the media, the profession of journalism and discrimination, and to offer useful perspectives and tools for exploring the ways in which journalism deals with the current pervasive challenges of multiculturalism.

Nell'odierna ecologia mediatica, non si tratta tanto di entrare nel dibattito sull'opportunità o meno di coprire le notizie relative al fenomeno della discriminazione, quanto piuttosto di capire come la mediatizzazione delle minoranze e della diversità culturale spesso non vada oltre certe cornici narrative. Nel campo del giornalismo, esistono cornici che (ri)producono e rafforzano nel tempo stereotipi negativi su gruppi e comunità, spesso a causa di informazioni confuse e sovraccariche o della mancanza di formazione dei giornalisti su specifiche realtà storiche e culturali. L'obiettivo di questo articolo è riflettere sul rapporto tra i media, la professione giornalistica e la discriminazione e offrire prospettive e strumenti utili per esplorare i modi in cui il giornalismo affronta le attuali sfide pervasive del multiculturalismo.

Keywords

Media; diversity; journalism; discrimination; ethnic media

1. Introduction

In the last months of the year 2023, one of the institutions most active in analysing changes in the news business, the Reuters Institute for the Study of Journalism, circulated questions to many newsrooms for an annual survey on two main topics: how greater flexibility in face-to-face work is changing newsrooms and how newsrooms are positioning themselves with regard to creating more 'diversity' within them. In this case, the term diversity was used to refer to diversity, a word that is at the forefront of an almost all-American debate on the under-representation of 'minorities' of various natures in journalism where ethnicity, disability and gender are mentioned.

The Reuters Institute's questions pose issues that are for the most part far removed from the agenda and thoughts present in the newsrooms of our country, with the exception perhaps of the one concerning the role of women. Even if we are talking about communities that are currently much smaller than those present in the American or English, French or even German reality, those minorities exist and grow in Italy too, but it is our entire cultural system that does not seem to contemplate them except in their transitory and coarse form of 'migrants'.

Reflections should be made on this, which could even precede the issue of 'diversity' in editorial offices, or be stimulated precisely by starting from this recent fact that fully touches the world of information from within, its actors and its practices, such as the reporting methods used by journalists on ethnic or religious issues, or the cultural level of the latter on issues that cross national borders.

Some examples can still be commonly read in newspapers today: from disrespecting the dignity of a migrant to unacknowledged gender identity, from pointing the finger at a suspect as guilty to the publication of photos of minors involved in news cases.

While in some cases discrimination does not reflect the intent of the writer and publisher, it is just as frequent that discriminatory language is purposely used in both print and digital environments.

Studying the causes and processes of representation of discrimination, reported by traditional and digital media, means first of all recognising their existence, being able to identify them within the multiple narratives that are increasingly hybrid today, and shedding light on the connections that exist between the communication systems of modern Western countries and a social structure that is often unequal and unjust. The media frame the world around us in a way that favours certain interpretations and inevitably play a major role in our societies (Newman, 2023).

The phenomena that contribute to discrimination are widespread, are rarely the expression of a clearly identifiable intentionality and act in an inconspicuous manner. The detrimental effects of this sort of insidious, multifactorial mechanism weigh ever more heavily in our public and private lives.

Critically analysing journalism in relation to the phenomena of discrimination allows us to take a critical stance towards intolerant and violent behaviour, to consider the links between information systems and the broader prevailing social structures that may eventually be challenged in the public space (Gottfried et al 2022).

Thus, it is not a question of calling a journalist a racist or a xenophobe, or accusing that specific media outlet or platform, blocking a protester's account or filling public profiles with vulgar comments, but of understanding how a specific system, in our case that of constant news production, can fuel or reduce discrimination.

In the following paragraphs we will highlight the increasingly fluid boundaries and critical issues of the contemporary publishing world that could jeopardise the main social functions of journalism (finding, disseminating and commenting on news; building a culture of dialogue; accompanying critical thinking) by reducing the process of news construction, as well as the profession of journalist, to mere containers/actors polluted by prejudice and disseminating information without any ethics, passion and credibility.

2. Beyond the "usual frames"

Journalistic narratives reflect heterogeneous editorial lines. Nevertheless, certain articles, news reports or interviews, convey negative stereotypes, reproducing prejudices and contributing to the creation of hostile and stereotypical narratives (Bhatia et al. 2018). Generally, the treatment of religious, linguistic, historical or ethnic elements, peculiar to minorities within a specific community, tends to focus on deviant cultural behaviours or practices.

In the article proposed here, it was not so much a matter of entering into the debate on whether or not such news needs to be dealt with, but of noting how the mediatisation of minorities and diversity often does not go beyond these narrative frames. Such frames (re)produce and reinforce negative stereotypes, ingredients underlying not only prejudice, but also the stigmatisation that groups and communities suffer on a daily basis, as well as often indications of a lack of knowledge of the subject on the part of information workers.

These aspects have been the subject of countless media and entertainment studies. Regardless of editorial line or political connotation, most journalists vehemently contest the idea that the information produced may contribute, even unintentionally, to discrimination.

In fact, it is difficult to admit that the pursuit of truth in the service of the public interest can foster intercultural conflicts within social groups.

The most 'problematic' media content or content with obvious discriminatory aims is in fact signed by journalists who are often ill-intentioned, provocative or racist, particularly close to a political party that is intolerant on certain ethnic issues, or who have a low level of knowledge of the phenomena or characteristics of the communities that are the subject of their narratives. Profiles of professionals who nevertheless remain a minority and tend to be ostracised by their peers, while exposing themselves to penal sanctions of a criminal nature (Bhatia et a. 2018; Gottfried et al. 2022).

Beyond the exceptions, or the more complex cases, an important question remains open.

Very often, journalism contributes to the creation and reproduction of stereotypes, prejudices and discriminations that weigh heavily on social coexistence by fuelling phenomena of hatred, polarisation and incivility, falling victim to the logics that characterise the profession itself (Bentivegna, Rega 2022).

Prejudices do not explain everything, they advocate an approach that questions the factors intrinsic to public information production systems. The media's emphasis on deviance and immigrant criminality, for example, also stems from the routines and constraints intrinsic to news production.

Nevertheless, journalists often find themselves in situations that they find impossible to cover satisfactorily. This is the case of the numerous nationalities and religions that have a low percentage of presence within a specific community, of peoples with ancient, tormented and complex histories, of countries where personal rights and freedoms struggle to assert themselves and local information can hardly be defined as 'free and impartial', and therefore credible, since it is under the control of political power (Caliendo et al. 2011).

Elements that, while favouring the abuse of generalisations by some commentators or public figures, are not always able to go into the details of the story, but are nevertheless indispensable for the understanding of a criminal case, or to distinguish a hate crime from a hate incident, incitement to violence and freedom of opinion from public opinion.

Various characteristics of the journalistic profession and of the media system more generally, among them competition, organisation, genre, format and technological nature, largely contribute to the emergence of potentially discriminatory content.

The main effect of strong competition, for example, is the urge to process and publish a news item as quickly as possible through the fastest possible medium (Kovach, Rosenstiel 2001).

It is in this way that contextual elements that could minimise the risk of abusive generalisations are omitted or, conversely, stigmatising terms and formulations are included. It is precisely competition that is at the origin of the media's sometimes deliberate choice to distance themselves from other publications.

As is to be expected, these logics move mainly through narrative formulas and content with a strong discriminatory potential, such as when a media outlet decides to mention the nationality of a suspect in its article when its competitor-colleague journalist has made no mention of it in his piece (Belluati, 2018).

Narrative choices and the constraints of form and format can also reinforce the discriminatory potential of a journalistic production. Storytelling, as opposed to classical reporting, may involve wording that alludes to negative stereotypes. At the same time, even any newspaper, by reserving a very limited space for a news story, can induce journalists to sacrifice fundamental contextual elements in order to avoid any 'problematic' associations (Marini, 2021).

In this sense, an in-depth examination of information today, taking the issues of discrimination and fundamental rights together, means rethinking the function of the media and journalism at the same time, and it is possible to extend this consideration within, and beyond, the contemporary communication environment.

Paraphrasing the words of Richard Sennett (2012), ours is a world populated by strangers who are different from us, but where, paradoxically, what we have in common with the Other is difference. For centuries we may have been able to conceal and remove this plurality, but the current processes of global information impose the discovery and narration of otherness.

The attempt of the reflection proposed here is to understand how to study the role and transformation of the new media, as well as the journalistic profession, in relation to the treatment of different discriminatory phenomena and its hybrid forms in the public sphere. Specifically, the aim is to redefine the most common interpretative frameworks used to address the complex issue of discrimination, especially discrimination of ethnic origin, within the field of journalism and the media space more generally, while offering useful perspectives and tools to investigate the relationship between otherness and hypermedia.

3. Haunting realities

In the field of journalism, where duty of truth and accountability have historically been considered deontological principles, an undeniable but intricate relationship emerges that is intertwined with the lingering spectre of

discrimination (Stephens 1988; Kovach, Rosenstiel 2001). Journalism, as a provider of information and forerunner of social change, has always grappled with the profound implications of discrimination and its far-reaching effects on the stories it tells and the communities it informs.

Discrimination, in its myriad manifestations, remains a 'haunting reality' to be explored, even for the media, a phenomenon that hinders human progress and the path to equality (Sacks, 2002). Within information processes, discrimination weaves its fine threads, shaping distorted narratives, influencing representation and, at times, reinforcing societal prejudices.

The media, as a reflection of the world they tell, should face that uncomfortable truth that through their practices, both intentional and unintentional, they can perpetuate stereotypes, amplify prejudice, silence marginalised voices, and remove the dignity of Difference (Farrell et al. 2020).

Yet, amidst the shadows cast by social (and digital) discrimination and the rigid logics that guide organisational media behaviour, journalism could still be a potential catalyst for social change, for exposing injustice and inequality.

In 1995, Barrett and colleagues, in their well-known work entitled The central role of discourse in large-scale change: a social construction perspective, believed that real change could only take place when a 'certain way of talking would be able to replace another way of telling social facts'.

The authors believed that effective change required the members of an organisation intent on communicating (in our case, a newsroom) to alter their cognitive schemata in order to understand and respond to the events that are the subject of the narrative under construction, since it is language that frames and determines how and what we think about things. When a new language begins to generate new actions, in turn, different possibilities for social action are triggered, and basic assumptions and beliefs will thus be altered (Gottschall, 2022).

The power to inform and educate offers journalists the opportunity to shed light on untold stories, unveil the reality of systemic biases, work towards the construction of appropriate public policies and practical solutions in collaboration with institutions and non-profit organisations for the respect of diversity and human rights (Balabanova 2014; Zindritsch 2016).

4. The importance and role of media trust/safety

In a hybrid, de-facto, multimedia and multicultural, news-overloaded world, there is a need to properly recognise the ambiguities and contradictions of global culture and cultures. We need to know what needs to be done to preserve diversity and enhance the interests of minorities who find them-

selves having to negotiate their specificity in different contexts in and through the media.

The media offer resources for these operations on both sides: the information that minorities often produce and that they receive, local news or news more related to their culture of origin and news from the host culture, even if not always accessible due to language.

In any case, whether it is social justice or a war crime, the news-event is now global and shared from the moment it enters public space. The story penetrates into the deepest layers of national, regional, ethnic and religious cultures, and while on the one hand it becomes a resource for expressing local and particular identities and interests, on the other its meaning and importance are shattered.

Indeed, it cannot be assumed that there is a single interpretation, nor can it be assumed that the extraordinariness of the story-news and its global presence can generate an unambiguous response.

Newspapers, radio, television and digital platforms still offer ample space for a plural traffic of voices, images, ideas, beliefs that can be shared cross-media.

However, the tension towards pure truth and the taste for information-entertainment often overlap and make the relationship between reality and fiction even more complicated.

In this sense, when we talk about the importance of regaining trust in the media, this does not simply mean trusting the ability of the individual newspaper, or television programme, to tell the truth through a post, but it is about trusting that 'the media are what they are supposed to be and do what they are asked to do' (Kovach; Rosenstiel 2001).

Too often, the playful dimension of the media allows them to evade criticism and share banal views and cultural prejudices through the most varied forms of entertainment, feeding a vulgar culture, interested in frivolous things presented as important (Postman, 2021).

In the new ecology of information, both audiences and journalists can make errors of judgement, sometimes cunningly and competently. Media communication processes are increasingly shared activities involving reciprocity and mutual assistance, as well as responsibility, despite the fact that they take place within an infrastructure whose guidelines are most often dictated by politics and ideology.

Trust in the media is something extremely topical and problematic, as it is difficult for users and institutions to manage and because it forces a confrontation not only about ends, but also about means.

Following Roger Silverstone's suggestion (2009, 203-204), we should trust the media 'despite their weakness if we want social life and relations with the

Other to continue. A trust that obviously cannot, however, be blind, we must be sceptical, we must ask questions (..) we must demand that the media take responsibility, we must demand respect and hospitality'.

This last word, in particular, is the necessary requirement for the existence of a multimedia and multicultural society. Hospitality is the mark that seals our relationship with the stranger and our openness to diversity; within the mediated representation of the world, it is the precondition of media justice.

As Rawls (1999) has already suggested, injustice can be fought in the periphery with social policies adapted to the context, but also by offering minorities spaces of communication that do not allow distortions, distortions, discrimination and by allowing, for example, access to the net, the birth of local radio and TV stations representing that community in that same periphery.

If we accept this principle of media justice, then we need to imagine and guarantee the presence of a subject that Silverstone calls a 'universal audience'. Universal, and not global, since this is more a philosophical than an empirical concept and because it is based on the assumption that being a member of an audience is a right.

Indeed:

> 'no one should think that he or she can be excluded, although of course in practice it is impossible for a condition of total inclusion to occur (...) Medial justice needs an institutional system of global scope that through its intervention can enhance and maximise basic rights, without which the mediapolis would continue to be plagued by injustice, unfairness, discrimination (...) What the system needs (...) is accountability' (Silverstone, 2009, 237-238).

A concept that cannot, however, be dissociated from that of citizenship.

To be responsible, the individual who produces or consumes media content must be in a position to see and act beyond that often limiting and limited representation of the world.

The ecological transformation of the media has not only changed the relationship between physical and social place, but has broken down the distinctions between the here and the there, the direct and the mediated, the personal and the public (Colombo, 2020). The new social movements, the disruptions, the speaking out in the squares of minorities in neighbourhoods all over the world, are just some of the adaptations of behaviour, attitudes and laws to adapt to the new socio-media scenarios.

It is perhaps the result of a now evident and lasting merger of previously separate environments and a backstage now revealed no longer, or not only, by newspapers:

> '(the media) have helped to move from the deferential 'nigger' to the proud black, they have united ladies and young ladies under one appellation, they

> have transformed the child into a human being with natural rights (...) They have fostered the emergence of hundreds of minorities, individuals who, having perceived the existence of a larger world, have begun to consider themselves unjustly isolated' (Meyrowitz 1993, 510).

5. Between indifference, spectacle and complexity

This Differences between individuals are better noticed by sharing the same environment than by being apart. But in spite of the many media injustices still present and the 'indifference' of the in-between space, the media-dense public sphere has shed more light on the forms of discrimination present in the information space, has offered almost every individual a new perspective from which to see Others and gain a reflexive perception of Self.

However, when the media alter the boundaries of situations, they often also affect value systems, and our evaluation of actions follows the boundaries and definitions of the new situations as they appear in the communication space.

Therefore, any judgement on new social phenomena, on what is or is not right or wrong, discriminating or inclusive, moral or immoral, must be made today with great caution. We can condemn and appreciate particular aspects, but considering today's information environment to be made up only of therapeutic sick parts can lead to a further misunderstanding of the general dynamics involved in social change.

Both pleasant and unpleasant aspects are often part of the same process.

Today we witness different 'spectacles' in the media, instead of a greater or lesser amount of spectacle, we have a different reality and not a different amount of reality (Boorstin, 1962).

As Sennett (1982) states, we have perhaps lost the sense of distance that once characterised social life, and today the belief that closeness between people is in any case a moral good dominates.

Being aware of the limitations of information systems means being aware that one is resorting to assumptions about unknown or empirically not always verifiable aspects (such as anthropological ones), or, again, that one is selectively emphasising one part of reality at the expense of others (Barisione, 2021).

The issue of diversity and its public narrative is a rather complex operation that has to do with the everyday lives of subjects, relationships, norms, rights, and cultural-institutional contexts. It is about understanding the needs, emotions, conditions and useful tools of important parts of the world's population and elaborating common political strategies to avoid forms of abuse and surveillance. Also in the media.

The problem is that while journalists show us the Difference outside and inside the screens, they are more often than not unable to offer us the appropriate tools to understand it. Certain media and political narratives/views have, over time, produced hostility and indifference, reactions or, rather, drinking strategies of removal (Sacks, 2002).

Perhaps the time has come to build a moral public space, also made up of good information, but not only.

The condition of pluralism of postmodern societies is also characterized by this ability of the individual to fully express his or her subjectivity, to satisfy his or her communication and information needs. The need to be adequately informed, outside and inside one's own borders, as well as maintaining a link with one's origins, translate for minorities into useful strategies to try to emerge from invisibility, take the floor, participate in collective life and communicate with institutions, supported by local media, even if often with unsatisfactory results (Giaccardi, Magatti 2022).

Resuming the thought of Edgar Morin (2015), people are able to feel human sympathy and understanding especially when suffering and injustice suddenly appear to us through an image or on any other technological support. Even through social and media representation, understanding of the Other and altruism can be generated.

This happens because a process of identification and sympathy is implemented that allows us to see the complexity of the aspects of a person. The important thing, however, is not to forget the entire context, limiting oneself to the sole search for a forgotten place or to the care of a single wounded community, only because it is illuminated by the powerful beacon of empathy and the media narrative (Bloom, 2016).

6. Conclusion

Technological infrastructure moves and evolves faster than journalism and it couldn't be otherwise. Information follows different times, dictated by the care that each reality puts into producing its own content and maintaining solid editorial standards.

Just think of artificial intelligence (AI), a topic that is still a protagonist in global public debate, already a tool available to the most important newsrooms, used both for gathering information and for its processing and distribution. Journalism that is born from artificial intelligence is guided by highly sophisticated algorithms, but this does not mean that it is never subject to errors (Jarvis, 2023).

These are complex calculation procedures that are difficult to verify and, therefore, it will become complicated to attribute any amount of responsibility to them.

This is because AI is a tool created by humans and can make mistakes, just like them. Errors that often arise from the prejudices of our world and that we insert into our technical systems.

The result of an algorithm will only have value if the human inputs are correct.

The pervasive diffusion of AI could therefore create the ideal condition of cultural conflict for those who intend to fuel and reinforce stereotypes and prejudices starting from journalistic stories.

The debate around the issue of AI non-neutrality is leading, albeit with a certain delay, national and international organizations to equip themselves with tools to increase the awareness of developers and users and to promote the design of ethical and reliable solutions (Jarvis, 2023).

Complex and still open questions, therefore, that cannot be addressed by absolutizing the relevance of techno-communicative processes in an uncritical way, thus adhering to a mythologized vision of communication (Sorrentino, 2021). Rather, by knowing the cultural contexts specifically and contributing to the construction of a less stereotyped media narrative, and more attentive to social injustices, as well as to the defense of a universal culture of human rights in society, with a vision of the promotion and protection of fundamental freedoms.

Displacements and censorship, manipulations and disinformation have always characterized journalism that has always suffered or committed them. The current problem of the journalistic field concerns the communicative abundance of powerful and contradictory stories, the divergence of opinions on the one hand, and the reduction of discursive space, on the other.

However, precisely because it is increasingly less possible to think of an all-encompassing citizen and universally accepted opinions, there is a need for what journalism can still do: to be a negotiating field in which various actors, different opinions, stories - news move. A guide, therefore, that helps to connect and interpret the many points of view characterizing every fact, every social phenomenon, every form of discrimination (fig.1)

Journalism also retains, therefore, an absolutely central function in the fight against discrimination, which goes well beyond the reporting of facts: building meaning, that is, those forms of social bonds that are created through interaction with the Other and that allow us to understand the world around us (Buoncompagni, 2021).

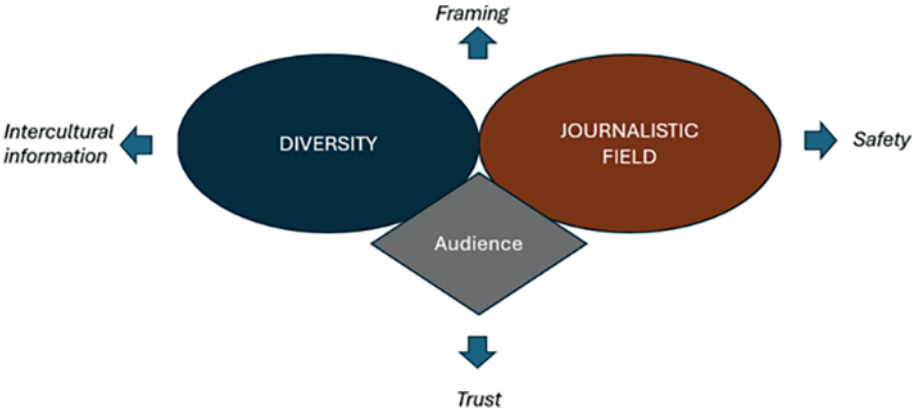
Even the most hybrid forms of contemporary racism.

However, information professionals should refer to a different journalistic epistemology, which cannot still be based on the old rhetoric of "mirroring reality".

It remains essential today to take into account the dynamism of facts and contexts, which are never immobile and always evolve, recognizing the limits of a journalism too often focused on opposition and slogans that only hopes for the pursuit of spectacular and business logic.

Informing, limiting discrimination, means making journalism that is able to contextualize the facts, to provide them with a perspective that allows users to interpret them with greater knowledge of the facts. No longer hiding behind the hypocritical expression of "limiting oneself to the facts", but going further by trying to give shape and meaning to the innumerable information that increasingly occupy the media ecosystem through a critical reading of the data at our disposal.

Figure 1 – *Connections between news media, audience, diversity*



References

Barisione, M. (2020), Contro il comunicazionismo. Per una critica del riduzionismo comunicativo, Comunicazione politica. *Quadrimestrale dell'Associazione Italiana di Comunicazione Politica*, 3, pp. 347-370.

Barrett, F.J., Thomas, G.F., & Hocevar, S.P. (1995). The Central Role of Discourse in Large-Scale Change: A Social Construction Perspective. *The Journal of Applied Behavioral* Science, 31(3), 352-372.

Bloom, P. (2016), *Against Empathy: The Case for Rational Compassion*, Ecco: New York.

Blumler., J. (2016), *The fourth age of political communication*, *Politiques de la communication*, 16, pp. 19-30.

Buoncompagni, G (2021).,Techno-altruism. From cultural conflict to constructive and supportive use of online environments, *Geopolitical Social Security and Freedom Journal*, 4, 2021, pp. 16-32.

Buoncompagni, G. (2023), The Perception of Anti-Semitic Hatred in the Italian Media and Justice System, *Fieldwork in Religion*, 18, 2023, pp. 84-199.

Gottfried, J.. Mitchell, A., Jurkowitz, M.. Liedke, J., (2022) "Journalists give industry mixed reviews on newsroom diversity. lowest marks in racial and ethnic diversity": https://www.pewresearch.org/journalism/2022/06/14/journalists-give-industry-mixed-reviews-on-newsroom-diversity-lowest-marks-in-racial-and-ethnic-diversity/.

Gottschall, J. (2022), *Il lato oscuro delle storie*, Bollati Boringhieri: Torino.

Jarvis, J. (2023), *The Gutenberg Parenthesis*, Bloomsbury Publishing: London.

Kovach. Rosenstiel (2021), *The elements of journalism*, Three Rivers Press.

Meyrowitz, J. (1993), *Oltre il senso del luogo*, Baskerville: Bologna.

Morin, E. (2015), *Etica e identità umana*, Egea: Milano.

Newman M., *Media. Una cassetta degli attrezzi*, Einaudi: Torino.

Pihlajarinne, T., Alén-Savikko, A. (2022), *Artificial Intelligence and the Media: Reconsidering Rights and Responsibilities*, Edward Elgar Publishing: Cheltenham.

Postman, N. (1985), *Divertirsi da morire*, Longanesi: Milano.

Robinson, S., Lewis, S.C., Carlson, M.(2019), Locating the "Digital" in Digital Journalism Studies: Transformations in Research, *Digital Journalism*, 7, pp. 368-377.

Rodríguez,-Wangüemert C., Martínez-Torvisco, J. (2017), Human rights through the paradigm changes of the social communication theories, *International Review of Sociology*, 27, pp. 230-240.

Sacks, J. (2002), *The Dignity of Difference: How to Avoid the Clash of Civilizations*, Continuum: London.

Schudson, M. (2013), Would journalism please hold still in Peters C. Broersma M.J. eds.. *Rethinking Journalism. Trust and participation in a transformed news Landscape*, Routledge London, pp. 191-199

Silverstone, R. (2009), *Mediapolis*, il Mulino: Bologna.

Sorrentino, C. (2008), *La società densa*, Le Lettere: Firenze-

Splendore, S. (2017), *Giornalismo ibrido*, Carocci: Roma.

The Potential Use of Artificial Intelligence in Crisis Management

Krzysztof Kaczmarek, Mirosław Karpiuk, Urszula Soler

Krzysztof Kaczmarek[1] Ph.D. in Social Sciences in the discipline of political science and administration. Currently, he works at the Koszalin University of Technology, Faculty of Humanities, Department of Regional and European Studies. He specialises in issues related to hybrid threats, including cybersecurity, disinformation, and critical infrastructure protection.

Mirosław Karpiuk[2] professor of social sciences in the discipline of legal sciences. Currently employed at the University of Warmia and Mazury in Olsztyn, at the Faculty of Law and Administration, Department of Administrative Law and Security Sciences. He specialises in issues related to security and defence, including the administration of security and public order or cybersecurity.

Urszula Soler[3] is graduated in polish literature, social philosophy and sociology. She is Assistant Professor at the John Paul II Catholic University of Lublin. She is specialized in disposition groups of the military social system. Her research interests are focused on security, paramilitary organizations, food security, technology assessment, sustainable development and innovations. She is founding member of the PANTA (Polish Academic Network of Technology Assessment) and founder of Polish Academic Legion; cooperates also for many years with Catholic University of Sacred Heart (Milan).

Abstract

This article focuses on the application of artificial intelligence (AI) in crisis management, taking into account both the legal and practical aspects. In the circumstances of growing challenges related to crisis management, AI is emerging as a key tool enabling high-speed big data analysis and decision-making processes. The author discusses how AI might contribute to better prediction, monitoring and response in emergencies, including natural and man-made disasters. Emphasis is also placed on the ethical and legal aspects of AI, including the need to develop a regulatory framework and to take into account accountability and transparency

[1] PhD, Koszalin University of Technology, Faculty of Humanities, Eugeniusza Kwiatkowskiego 6e, 75-343 Koszalin, Poland, ORCID: https://orcid.org/0000-0001-8519-1667 Corresponding author e-mail: puola@tlen.pl.
[2] Prof., PhD, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Dybowskiego 13, 10-723 Olsztyn, Poland ORCID: https://orcid.org/0000-0001-7012-8999 Corresponding author e-mail: miroslaw.karpiuk@uwm.edu.pl.
[3] Assoc. Prof., PhD, The John Paul II Catholic University of Lublin, Institute of Political Science and Public Administration, Al. Racławickie 14, 20-950 Lublin, Poland ORCID: 0000-0001-7868-8261 Corresponding author e-mail: urszula.soler@kul.pl.

principles. The paper sheds light on the limitations of AI, indicating the need for continued supervision and algorithm updates, and points to the potential risks resulting from errors in algorithms and unconscious bias. In the context of crisis management, the role of AI in counteracting disinformation that might trigger or escalate emergencies has also been discussed. The author of the paper stresses that, despite the enormous potential of AI, its effective application in crisis management requires a responsible approach, taking into account the ethical, legal, and social aspects.

Questo articolo si concentra sull'applicazione dell'intelligenza artificiale (IA) nella gestione delle crisi, prendendo in considerazione sia gli aspetti legali che quelli pratici. In un contesto di sfide crescenti legate alla gestione delle crisi, l'IA sta emergendo come uno strumento chiave che consente di analizzare ad elevata velocità i big data e i processi decisionali. L'autore discute come l'IA possa contribuire a migliorare la previsione, il monitoraggio e la risposta alle emergenze, compresi i disastri naturali e quelli causati dall'uomo. Viene posto l'accento anche sugli aspetti etici e legali dell'IA, compresa la necessità di sviluppare un quadro normativo e di tenere conto dei principi di responsabilità e trasparenza. Il contributo fa luce sui limiti dell'IA, indicando la necessità di una supervisione continua e di aggiornamento degli algoritmi, e sottolinea i potenziali rischi derivanti da errori negli algoritmi e da pregiudizi inconsci. Nel contesto della gestione delle crisi, è stato discusso anche il ruolo dell'IA nel contrastare la disinformazione che potrebbe scatenare o aggravare le emergenze. L'autore dell'articolo sottolinea che, nonostante l'enorme potenziale dell'IA, la sua applicazione efficace nella gestione delle crisi richiede un approccio responsabile, che tenga conto degli aspetti etici, legali e sociali.

Keywords

Artificial intelligence, big data, crisis management, data analysis, decision-making algorithms

1. Introduction

Technological progress, the growing computing power of digital tools, and the emergence of new ones contribute to transforming how individuals, societies and states function. A substantial part of such operations has been moved to the Internet, and algorithms control an increasing share of human activity. This refers to both the private and professional life and social interactions. Artificial intelligence is the most advanced among all the currently available digital tools. However, we should remember that AI is evolving, expanding the range of its potential applications.

The algorithms that form part of AI can make autonomous decisions based on big data analysis, self-correct errors and make decisions based on previous experience. Given that, it can be used where it is necessary to rapidly analyse information and identify patterns and interdependencies. This allows AI to find optimum solutions to a given problem in an incomparably shorter time than it would be needed for a human to complete. Therefore, AI might find specified applications in crisis management.

The literature on the subject does not provide a single, widely applied and accepted definition of an emergency and crisis (Walas-Trębacz, Ziarko 2011, p. 19). However, for the purpose of this paper, it has been assumed that an emergency is a set of circumstances that disrupt the normal functioning of a system in a sudden way (Walas-Trębacz, Ziarko 2011, p. 23). As per Article 3 (1) of the Polish Crisis Management Act of 26 April 2007 (consolidated text, Journal of Laws of 2023, Item 122), an emergency situation is understood as circumstances which have a negative impact on the level of security of the population, property of significant size, or the natural environment and result in substantial limitations of the activities performed by public administration authorities due to insufficient forces and resources.

The use of the opportunities that AI provides allows us to predict the occurrence of an emergency and provides the possibility to prepare appropriate forces and resources for adverse circumstances. It is also important to note that the analysis of large quantities of information and data allows the identification of patterns that a human is most often unable to notice, given especially that the rapidly changing surroundings result in the occurrence of new factors or in the increased probability that the factors which have previously been highly unlikely will occur. In crisis management, it is worth remembering that unlikely events are not impossible (Kaczmarek, 2023, p. 78). It is particularly crucial at the prediction and preparation stages. Unlike humans, AI can predict such situations.

However, the opportunities that AI creates in crisis management will not guarantee that they will be used effectively. In this context, it is critical to ensure that persons using digital tools have the appropriate skills to do so. It should also be noted that current AI technology is not the peak achievement in this sphere and is still evolving. Moreover, it is a man-made algorithm that might contain errors that have not been identified. Given that, the decisions it makes may also be faulty. However, such deficiencies are most often the outcome of the user's error, not the system. They might result from the user's incorrectly interpreting or ignoring analysis results.

Artificial intelligence has the potential to bring multiple benefits to people, both in the social and economic spheres. It is becoming an increasingly important tool in the operations of public and private entities. On the one hand, artificial intelligence tools are aimed at accelerating and streamlining decision-making processes or allowing the personalisation of products and services to tailor them to individual needs. On the other hand, the data being collected at a large scale, which is necessary for the proper operation of artificial intelligence, and automated decision-making processes, always pose a risk of infringing specified human rights and liberties, both at the algorithm design stage and at the AI functioning stage (Kostrubiec 2021, p. 37).

2. Limitations of AI

In the context of crisis management, it is imperative to understand the limitations of AI, and the need for continued supervision and algorithm updates. The monitoring of, and response to, the rapidly changing conditions of natural disasters may be a good example here. AI may provide data on changes in the environment. However, the final decision on evacuation or other preventive measures should be made by experienced experts who can assess the social or political context. Integrating data from various sources and systems is one of the key challenges related to using AI in crisis management. The multitude of data formats, communication protocols and security levels might hinder the effective coordination of actions. Therefore, it is essential to develop standards and protocols allowing seamless information exchange between entities and systems.

Furthermore, emphasis should be placed on the ethical and legal aspects of using AI in crisis management. Decisions made by AI could have far-reaching consequences for individuals, societies and states. For that reason, it is essential to take into account the principles of accountability, transparency and respect for human rights in designing and implementing AI algorithms. In the legal context, it is necessary to create a regulatory framework that will specify the entities accountable for decisions made by AI. This includes issues related to the responsibility for algorithm errors, personal data protection and compliance with local and international laws. Special attention should also be paid to cybersecurity, defined as the capacity of information networks and systems to maintain proper operation capabilities (Kostrubiec 2022, p. 28).

In a digital state, information and communication (ICT) systems are particularly vital. They serve fast communication purposes and may also be used to provide services or perform certain tasks. They have a wide range of applications, from entertainment, through communication, education, and employment, to the assurance of digital security. From the perspective of the normal functioning of the state, it would be crucial to not only perform tasks with the use of cyberspace but also to ensure cybersecurity. Cyberspace must be protected continuously as the state uninterruptedly performs its tasks in times of crisis or conflicts (Bencsik, Karpiuk 2023, p. 83).

Cyberthreats can result in various negative phenomena. This might lead to a crisis, particularly if cyberattacks are targeted against ICT systems used by the state to fulfil its strategic objectives, including those related to the assurance of the uninterrupted operation of critical infrastructure. Threats in cyberspace might often give rise to an emergency, particularly if public institutions and private entities are, to a large extent, computerised, and the ICT systems they use are not always duly protected (Karpiuk 2022, p. 114). In the

event of states that rely on ICT systems in their operations, the interference in such systems might take the form of cyberattacks. Given the functioning of the state, and the public structures and private entities operating within its framework, it is crucial to ensure the efficient protection of critical infrastructure covering strategic sectors. The protection of such infrastructure consists of safeguarding ICT systems against cyberthreats (Czuryk 2023, p. 50). In addition, critical infrastructure can be duly protected by using artificial intelligence. With AI, it is not only possible to predict the risk of threats affecting the proper functioning of the infrastructure but also to eliminate them.

3. The application of artificial intelligence in counteracting the impact of natural disasters

Artificial intelligence plays a key part in combating the effects of natural disasters, offering a wide range of advanced options to choose from. Some of the main AI applications include early warning and prediction of disasters. AI systems may analyse big data sets from various sources, such as satellite data, weather data, or social media. Regarding social media, AI can analyse user content with information about any anomalies and their locations (Kejriwal 2019). These may include, for example, information about unusual weather phenomena or any non-standard animal behaviours.

Social media is additionally an important communication channel during various stages of emergencies or crises, allowing fast and effective communication. For the tool to be used effectively, however, it is necessary to counteract disinformation. It is particularly important in times when information is spreading fast and is not always reliable (Brando 2020). In such an event, AI may be applied in the analysis and management of data streams. This gives rise to another dilemma related to how a given algorithm is to make a distinction between accurate information and disinformation.

Once a natural disaster occurs, AI helps analyse and evaluate damage. It may quickly analyse satellite images and data from UAVs. This, in turn, facilitates the planning of rescue operations and the dispatching of aid to places where it is most needed. Regarding coordinating rescue actions, AI can optimise logistics and the distribution of aid (Khalil et al., 2008). It analyses the needs of the victims and available resources, which allows a more effective division of humanitarian aid. Moreover, in search and rescue operations, AI-controlled robots and drones can search areas affected by a natural disaster, detect victims and deliver required aid. The technology might greatly contribute to increasing the effectiveness and speed of responding to natural disasters. This can save lives and minimise the impact of such events. At the same time, it should be asserted that public administration authorities are

responsible for the planning and preparation of AI resources used in emergencies (Karpiuk 2021, p. 46).

4. The role of artificial intelligence in combating disinformation in the context of crisis management

Universal access to information results in the fact that contemporary societies are struggling with information overload. This makes it difficult to distinguish between reliable and true information and false and manipulated information (Lombardi 2020, p. 13-14). In the face of growing information overload, characterised by the excess and diversity of contents, disinformation has become an effective method for exerting influence.

Disinformation means false information deliberately and often covertly spread to influence public opinion or obscure the truth (Merriam-Webster 2019). In broader terms, it refers to information that is not wholly true or accurate (Learners Dictionary 2019). Disinformation that was historically developing in Russian politics is classified as an action aimed at supporting foreign policy and, as such, it should be separated from intelligence and counter-intelligence, and from traditional diplomacy and informational measures (Active Measures 1986). It should be noted here that the essence of disinformation is the intentional creation and distribution of false or manipulated content to evoke specified social behaviour (Chałubińska-Jentkiewicz, Soler, Makuch 2021). Thus, it might have a destructive impact on the functioning of the state (Chałubińska-Jentkiewicz 2021, p. 14). Disinformation campaigns can indicate that a traditional military operation, or even war, is being prepared. They can also form part of irregular measures combining conventional armed operations with operations carried out by civilians. They are usually long-term campaigns aimed at evoking and amplifying social divides and undermining trust in state institutions (Pietras 2021, p. 25). Disinformation may not only create emergencies but may also be used to escalate social unrest during existing crises (Kaczmarek, 2023, p. 20). Given that, it appears that combating disinformation should be one of the priorities of actions undertaken by entities responsible for crisis management. In the meantime, even democratic states that are strong in economic and military terms do not have effective tools to combat disinformation, and their preventive measures only consist of informational and educational campaigns (Wasilewski 2021, p. 9), which are considered to be critical in counteracting disinformation (Soler, Busiło 2019).

The most straightforward example of evoking or aggravating a crisis because of disinformation measures is a situation where a given population needs to be evacuated. For such evacuation to take place, it is necessary to in-

form the residents of the area concerned. In the meantime, statements negating the need for evacuation or suggesting that the evacuation notice is disinformation might appear in the information space, particularly in social media and online news platforms. Unfortunately, as already mentioned, tools that can effectively counteract such measures are either unavailable or unused. In exceptional circumstances, there should be a possibility for AI to filter information available in a given area according to pre-defined criteria. At the same time, based on the results of analyses, AI algorithms could adjust methods for communicating about existing threats to specified recipients. This might give rise to certain doubts about the ethical aspect of such measures, as citizens are deprived of access to information. However, we should bear in mind that human health and lives should be the highest priority, as evacuation can be ordered as a result of such factors as chemical or radioactive contamination, flood threat or information on a possible terrorist attack. For that reason, if attempts to destabilise social order through disinformation campaigns are detected in cyberspace during an emergency, it is advisable to announce one of the states of exception (Czuryk 2021, p. 86).

Another example where AI could block access to unverified sources of information is a situation where a terrorist attack is being planned to kill as many people as possible. Such an attack could be preceded by a mass disinformation campaign about other events that require the engagement of services. Such actions may be detected and neutralised by AI at the outset. Such planned terrorist attacks might also be preceded by the perpetrators' using the Internet to disseminate information that, on a transport route near the planned attack, there has been a road accident as a result of which cash or other valuable items have been scattered around a vehicle. The publication of such a message could result in jamming all access roads and significantly hindering the work of services that should reach the attack site. Social tensions and emergencies can also be triggered by false information about financial markets or attacks targeting bank infrastructure (Pelc 2020, p. 96). To counteract such situations, AI should also be able to block contents that might evoke adverse social behaviours. In the event of false reports on accidents, catastrophes, etc., AI can analyse information from the Internet of Things (IoT) in real time (Pietryka 2021, p. 25).

5. The prospects of applying the development of artificial intelligence in predicting, managing and preventing emergencies: from distributed systems to image analysis

Predictions concerning the future directions of AI development suggest that we will witness the growth of distributed AI systems, acting independent-

ly in various spheres, and integrated systems that will synchronise data with learning between individual modules. Such an approach will make it possible to create more holistic and effective solutions. AI systems will probably utilise autonomous action in combination with cooperation capabilities, exchange information and learn from other systems. This is likely to contribute to the development of more advanced applications. The analysis of data generated by IoT will play a key role here, allowing real-time monitoring, prediction and response to emergencies. AI will also find its application in the prediction of natural disasters thanks to the possibility to process data from satellites, on-ground sensors and climate models, which will facilitate better forecasting of, for instance, extreme weather conditions whose number has been increasing significantly in recent years (Perdikou et al., 2014, p. 569). The development of AI is also likely to improve the modelling of potential natural disasters by analysing patterns, trends and interdependencies based on historical and current data. Moreover, AI can play a vital part in preventing emergencies, providing a possibility to prepare for such events beforehand based on the results of analyses conducted by such systems. The possibility of early detection of, and fast response to, threats thanks to AI might significantly reduce the risk and effects of crises, including natural and artificial disasters.

In the future, advanced mathematical models used by AI may be crucial for predicting human behaviour that might result in emergencies. The use of AI to analyse CCTV camera images, coupled with deep learning and statistical modelling, is likely to allow the identification of behaviour and action patterns that often precede the occurrence of an emergency. They include aggression, unusual gatherings or non-typical traffic in critical locations.

The AI analysis of camera images might provide information about crowd movement and congestion, behaviours indicating potential violence, or even identify suspicious packages or vehicles. These systems can be programmed to detect specific gestures, facial expressions or other subtle hints that the human eye could miss. Thanks to analysing various data sources, AI can also combine information from cameras with data from other sources, such as social media, telecommunications or meteorological data, to provide the full picture of potential threats.

6. Conclusions

To conclude, the role of AI in crisis management is, without doubt, significant. Thanks to its ability to quickly process and analyse large data sets, AI might contribute to better prediction, monitoring and response to emergencies. This is crucial in preventing natural disasters, handling the consequences of emergencies and combating disinformation that might result in escalating

conflicts or misunderstandings. Nonetheless, emphasis should be placed on the importance of human supervision over AI activities. As has been shown, artificial intelligence algorithms are not free of errors. They could be limited in their actions due to unconscious bias on the part of programmers or limitations of data on which the systems are being trained. Incorrect operation of AI algorithms may also result from learning on outdated and/or erroneous data sets (Surma 2023, p. 40-41). Therefore, it is necessary to continuously monitor and update AI systems to ensure their effectiveness and avoid unintentional consequences.

Furthermore, attention should be paid to the ethical and legal aspects of using AI in crisis management. It is vital to develop a clear legal framework governing the use of AI to protect human rights and ensure accountability for decisions made by algorithms. It is particularly important because such decisions will likely have serious consequences for individuals, societies and states. At the same time, AI-based systems and the information flow between them should be protected against unauthorised access by persons who may use advanced malware for the purpose (Radoniewicz 2021, p. 55).

In the context of future AI development, we can expect enhanced integration and technological advancement in this sphere. AI should be able to analyse a greater number of data sources. This is likely to contribute to better prediction capabilities and faster response to crises. The development of IoT technology, coupled with advanced AI algorithms, might enable far more effective real-time monitoring and crisis management.

The growing significance of analysing images and data from various sensors, which can potentially provide valuable information on the development and scale of crises, is also worth noting. The integration of data with AI systems will facilitate faster identification of threats and better response planning.

Despite the huge potential and benefits that AI might bring in crisis management, we must not forget about maintaining a balance between technological progress and the protection of privacy and human rights. AI should be introduced to crisis management with ethical and social aspects in mind to ensure that this technology serves common interests and does not infringe on fundamental rights and liberties.

Artificial intelligence has immense potential in the sphere of crisis management. Its ability to process large quantities of data and to provide a fast response might significantly contribute to mitigating the impact of crises. However, the intentional and responsible implementation of the technologies is equally important, and all the ethical, legal and social aspects should be regarded. Only then can we guarantee that the benefits that AI might bring will serve everyone, not just selected groups or interests. The future

of AI-supported crisis management seems to be promising, but it requires caution and continuous reflection on the direction of its development and implementation.

AI currently constitutes one of the most advanced technological tools, offering unmatched capabilities related to data analysis, machine learning and automation. However, despite its advanced nature, AI is still a tool, which means that its effectiveness, ethics and use directions depend directly on users' intent and actions. The final impact and results that AI may provide in various sectors – from medicine, through finance, to crisis management – are, to a large extent, shaped by our decisions concerning its programming, implementation, and monitoring. This reminds us of the fundamental principle that technology, irrespective of its advancement level, reflects the values and goals of those who apply it.

References

Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns, p. 1, July 1986, Washington.

Bencsik A., Karpiuk M. (2023). Cybersecurity in Hungary and Poland. Military aspects, *Cybersecurity and Law*, 1, pp. 82-94.

Brando M. (2020). Covid-19 - Comunicazione in emergenza: si insegna nelle università, però nessuno la mette in pratica, https://www.academia.edu/attachments/62873002/download_file?st=MTcwNjU1NTczNiw4My4yMy4xNDYuMTgsMTAwMzQ4MjI%3D&s=profile

Chałubińska-Jentkiewicz K., Soler U., Makuch A. (2023). Disinformation in Polish society in 2021 – trends, channels, sources, *Polish Political Science Yearbook*, 1, pp. 93-107.

Chałubińska-Jentkiewicz, K. (2021) Disinformation – and what else?, *Cybersecurity and Law*, 2, pp. 9-14.

Czuryk M. (2023). Cybersecurity and Protection of Critical Infrastructure, *Studia Iuridica Lublinensia*, 5, pp. 43-52.

Czuryk, M. (2021). Cybersecurity as a premise to introduce a state of exception, *Cybersecurity and Law*, 2, pp. 83-90.

Kaczmarek, K. (2023) Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych, *Roczniki Nauk Społecznych*, 2, pp. 19-30.

Kaczmarek, K. (2023) Zatopione w Morzu Bałtyckim bojowe środki trujące – analiza możliwości wykorzystania ich przez Federację Rosyjską w działaniach terrorystycznych, *Acta Politica Polonica*, 2, pp. 75-82.

Karpiuk M. (2022). Crisis management vs. cyber threats, *Sicurezza, Terrorismo e Societa*, 2, pp. 113-123.

Karpiuk, M. (2021). Cybersecurity as an element in the planning activities of public administration, *Cybersecurity and Law*, 1, pp. 45-52.

Kejriwal M. (2019). Crisis management: Using Artificial Intelligence to help save lives. *Research Outreach*. https://researchoutreach.org/articles/crisis-management-artificial-intelligence-save-lives/

Khalil, K.M., Abdel-Aziz, M., Nazmy, T.T., Salem, A.B.M. (2008). The Role of Artificial Intelligence Technologies in Crisis Response. https://doi.org/10.48550/arXiv.0806.1280

Kostrubiec J. (2021). *Sztuczna inteligencja a prawa i wolności człowieka*, Warsaw.

Kostrubiec, J. (2022). The position of the Computer Security Incidents Response Teams in the national cybersecurity system, *Cybersecurity and Law*, 2, pp. 27-35.

Learnersdictionary (2019). Misinformation, http://www.learnersdictionary.com

Lombardi M. (2020). Communication Crisis: COVID-19. Nothing since Chernobyl. *Sicurezza, Terrorismo e Società*, 12, pp. 7-30.

Merriam-Webster (2019). Disinformation, https://www.merriam-webster.com/

Pelc, P. (2020). The COVID-19 pandemic and the functioning of financial institutions in Poland. Cybersecurity issues, *Cybersecurity and Law*, 1, pp. 93-101.

Perdikou, S., Horak, J., Palliyaguru, R., Halounová, L., Lees, A., Ranguelov, B., & Lombardi, M. (2014). The current landscape of disaster resilience education in Europe. *Procedia Economics and Finance*, 18, pp. 568-575.

Pietras, M. (2021) Wojna informacyjna jako współczesne narzędzie działań nieregularnych, *Cybersecurity and Law*, 2, pp. 21-41.

Pietryka, K. (2021). *Nowe technologie informacyjno-komunikacyjne w zarządzaniu kryzysowym*. In: Danielewska., A., Maciąg, K. (eds.), Wybrane aspekty kryminologii, kryminalistyki i bezpieczeństwa w wymiarze narodowym i międzynarodowym, Lublin, pp. 19-31.

Radoniewicz, F. (2021). Network eavesdropping, *Cybersecurity and Law*, 1, pp. 53-63.

Soler U., Busiło M. (2019). Education of society as a tool to counteract disinformation in implementing new technologies. On the example of 5G mobile telecommunications network and Warsaw sewage system, *Applications of Electromagnetics in Modern Engineering and Medicine (PTZE)* 2019, pp. 210-214.

Surma, J. (2023). *Wprowadzenie do ataków na systemy uczenia maszynowego*. In: Cyberbezpieczeństwo w AI. AI w cyberbezpieczeństwie, Warsaw, pp. 34-44.

Walas-Trębacz, J., Ziarko, J. (2011) *Podstawy zarządzania kryzysowego. Część 2. Zarządzanie kryzysowe w przedsiębiorstwie*, Kraków.

Wasilewski, K. (2021) Fake News and the Europeanization of Cyberspace, *Polish Political Science Yearbook*, 4, issue 50, pp. 61-80.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 979-12-5535-352-2